ASSOCIATION SUPPORTING COMPUTER USERS IN EDUCATION

Proceedings of the 2013 ASCUE Summer Conference

46th Annual Conference
June 9 - 13, 2013

North Myrtle Beach, South Carolina

Edited by Peter Smith, Saint Mary's College, Notre Dame, IN

Association Supporting Computer Users in Education
"Our Second Quarter Century of Resource Sharing"

Proceedings of the 2013 ASCUE Summer Conference
46th Annual Conference
June 9 – 13, 2013
Myrtle Beach, South Carolina
Web: http://www.ascue.org

ABOUT ASCUE

ASCUE, the Association Supporting Computer Users in Education, is a group of people interested in small college computing issues. It is a blend of people from all over the country who use computers in their teaching, academic support, and administrative support functions. Begun in 1968 as CUETUG, the College and University Eleven-Thirty Users' Group, with an initial membership requirement of sharing at least one piece of software each year with other members, ASCUE has a strong tradition of bringing its members together to pool their resources to help each other. It no longer requires its members to share homegrown software, nor does it have ties to a particular hardware platform. However, ASCUE continues the tradition of sharing through its national conference held every year in June, its conference proceedings, and its newsletter. ASCUE proudly affirms this tradition in its motto: "Our Second Quarter Century of Resource Sharing"

ASCUE's LISTSERVE

Subscribe by visiting the site http://groups.google.com/a/ascue.org/group/members and follow the directions. To send an e-mail message to the Listserve, contact: members@ascue.org Please note that you must be a subscriber/member in order to send messages to the listserve.

NEED MORE INFORMATION

Direct questions about the contents of the 2012 Conference to George Pyo, Program Chair, ASCUE 13, Saint Francis University, Loretto, PA 15940, 817-472-3090, gpyo@francis.edu Web: http://www.ascue.org

Association of Small Computer Users in Education
ASCUE 2011-2012 Board Members
(years remaining in office including current year)

Table of Contents

Keynote Speaker

This year we are replacing the keynote speaker with a "Five Minutes of Fame" program. Each school that volunteers will have the opportunity to provide a five minute update on something innovative happening on their campus. The audience will vote for the best two or three presenters who will receive prizes.

Pre-conference Workshops

These have been replaced by late afternoon 90 minute sessions during the conference.

Workshop 1
The Ability to Innovate Can Be Taught and Anyone Can Learn It
Date: Monday, June 10
Time: 3:00pm - 4:30pm
Instructor: Dr. Ron Fulbright, Assoc. Professor and Chair, University of South Carolina Upstate

Working as a patent clerk in 1946, Russian scholar, engineer and inventor, Geinrich Altshuller, began wondering what made inventors different than everyone else. Thus began an effort, still in progress, to study and understand how technological systems evolve –in short, how humans invent. For over 45 years, this effort was hidden behind the Iron Curtain in the Soviet Union. However, over the last 20 years, TRIZ and modern Western extensions such as I-TRIZ have proliferated around the world, is used by some of the largest companies, but is still unknown in education. Through the work of the workshop presenter, Dr. Fulbright, the I-TRIZ line of development has led to instruction that fits nicely within a semester-long college/university-level course. Dr. Fulbright has developed and refined the course so that we can now teach students how to innovate just like we can teach them to write a sentence or solve a mathematical equation. The workshop will present the general concepts of I-TRIZ, demonstrate some of the learning objectives, and give attendees an opportunity to innovate on demand. Experience has shown this course to be a wonderful lateral/creative/out-of-the-box thinking technique stimulating STEM-like systems analysis in students. The hope is that you will take back to your respective schools the idea of incorporating instruction in innovation in your curricula.

Workshop 2
Let's Go Google!
Date: Monday, June 10
Time: 3:00pm - 4:30pm
Instructor: Janet Hurn, Miami University

Are you a Google Apps for Education school? Or are you considering it? Come learn some great tips and tricks for utilizing Google apps in the face to face and virtual classroom. Bring a device and use your Google Apps account or your personal Google account to participate. We will explore labs and chrome extensions and demonstrate actual applications for the classroom.

Workshop 3
Hands-on Security Labs – Teaching Hacking Principles to Help Illustrate the Need for Information Assurance
Date: Tuesday, June 11
Time: 3:00pm - 4:30pm
Instructor: Michael R. Lehrfeld, Assistant Professor, East Tennessee State University

This workshop will present the attendees with two different Information Security Labs that can be used to demonstrate wireless security and network security techniques. At East Tennessee State University it has become apparent that most students that take an information security class have never seen an exploit of a system that they are charged with protecting. This can lead to a more theoretical approach to security than an applied one. In recent years, the Computer and Information Sciences department has made the decision to make Information Security more 'hands-on' to provide the students with a concrete learning curriculum. What has been implemented is a series of labs that reinforce the importance of various security techniques using hacking labs. Two of these labs will be presented in this workshop.

Workshop 4
More iPad Apps for Use In and Out of the Classroom!
Date: Tuesday, June 11
Time: 3:00pm - 4:30pm
Instructor: Tom Marcais, Sweet Briar College & Steve Anderson, Sr., University of South Carolina Sumter

iPad usage continues to gain momentum in education. Finding the right Apps can make a huge difference in your life, but there's so many Apps it's not always easy to know where to begin. Come join us to see how an iPad can make your time more productive. We will demo some of the popular and not so well known apps. Some of them cost a little bit of money and some are free. We will also show you how the iPad makes our lives more productive and can make teaching better. Bring your iPad or just come and see if an iPad is something you should invest in. Throughout the workshop, we'll be using video mirroring with AirPlay and AirServer. We've worked hard to ensure that the content in this workshop is not a duplicate from last year. Whether you're a beginner or a Pro, you'll pick up some valuable tricks and tips for the iPad!

Workshop 5
Screencasting Workshop
Date: Wednesday, June 12
Time: 3:00pm - 4:30pm
Instructor: Steve Anderson, Sr., University of South Carolina Sumter

This combination show & tell & "tutorial" session will explore some of these uses of Screencasting inside and outside of the traditional, online, or hybrid classroom. We will actually create some short productions to demonstrate the shortened learning curves that continue to become more manageable, even for the novice user. We hope you will return to your campus motivated to expand your screencasting capabilities and opportunities. You bring a flash drive, and a headset if you have one (I'll bring some)

Activities will include (as time permits):
PC-based screencasting:

- Narrating PowerPoint slideshows
- Downloading, editing and narrating YouTube (and other) videos
- Utilizing screen/camera captures, both still and video footage, to create videos
- Whiteboard ink-based captures

iPad-based screencasting:

- Video capture on iPad
- Whiteboard capturing on the iPad
- Projecting iPad output through a projector

Time permitting, we will identify software and apps that range from free or inexpensive… all the way to full featured and powerful. We will also share our own best and worst practices.

Organization for the Proceedings

ASCUE initiated a refereed track for paper submissions to the conference in 2008. In fact, at the 2008 business meeting, the membership approved three different presentation tracks: refereed with 3 blind reviews for each paper, session with paper where the author submits a paper but it is not reviewed, and session without paper where no paper is submitted and only the abstract is included in the proceedings. To reflect this division, we will divide the proceedings into three sections. The first section, up to page 58, will contain the refereed papers, the second section, from 59 to 104, will hold the papers from the sessions with paper, and the last section will list the abstracts for the other sessions.

ASCUE BOARD OF DIRECTORS FROM 1967 to 2012

At this conference we celebrate the 46th anniversary of the founding of ASCUE at a meeting in July, 1968, at Tarkio College in Missouri of representatives from schools which had received IBM 1130 computers to help them automate their business functions and teach students how to use computers. They decided to form a continuing organization and name it CUETUG, which stood for College and University Eleven-Thirty Users Group. By 1975, many of the member schools were no longer using the IBM 1130, and were requesting to be dropped from the membership lists. At the same time, other small schools were looking for an organization that could allow them to share knowledge and expertise with others in similar situations. The name was changed from CUETUG to ASCUE at the 1975 business meeting and we opened membership to all institutions that agreed with our statement of purpose.

Our historian, Jack Cundiff, has collected the names and schools of the officers for ASCUE and its predecessor CUETUG for the last forty-five years and we have printed these names on the following pages.

ASCUE BOARD OF DIRCTORS FROM 1967 to 1972

	1967-68	1969-70	1970-71	1971-72
President	Ken Zawodny St. Joseph's College	Howard Buer Principia College	Jack Cundiff Muskingum College	Wally Roth Taylor University.
Program Chair	Wally Roth Taylor University	Jack Cundiff Muskingum College	Wally Roth Taylor University	James McDonald Morningside College
Past President	Al Malveaux Xavier, New Orleans	Ken Zawodny St. Joseph's College	Howard Buer Principia College	Jack Cundiff Muskingum College
Treasurer	Howard Buer Principia College	Al Malveaux Xavier University	Al Malveaux Xavier University	Al Malveaux Xavier University
Secretary	John Robinson	Dorothy Brown South Carolina State	Dorothy Brown South Carolina State	Dick Wood Gettysburg College
Board Members	James Folt Dennison University	James Folt Dennison University	James Foit Dennison University	John Orahood U. of Arkansas, LR
At Large	Don Glaser Christian Brothers C.	Don Glaser Christian Brothers	Don Glaser Christian Brothers	N. Vosburg Principia College
Public Relations				Dan Kinnard Arizona Western
Librarian				Jack Cundiff Muskingum College
Equip. Coordinator				
Web Coordinator				
Location:	Tarkio College	Principia College	Muskingum College	Christian Brothers

ASCUE BOARD OF DIRCTORS FROM 1972 to 1976

	1972-73	1973-74	1974-75	1975-76
President				
	James McDonald Morningside College	Dan Kinnard Arizona Western	T. Ray Nanney Furman University	Larry Henson Berea College
Program Chair				
	Dan Kinnard Arizona Western	T. Ray Nanney Furman University	Larry Henson Berea College	Jack McElroy Oklahoma Christian
Past President				
	Wally Roth Taylor University	James McDonald Morningside College	Dan Kinnard Arizona Western	T. Ray Nanney Furman University
Treasurer				
	J. Westmoreland U. Tenn Martin	J. Westmoreland U. Tenn Martin	Jim Brandl Central College	Jim Brandl Central College
Secretary				
	Ron Anton Swathmore College	Ron Anton Swathmore College	Harry Humphries Albright College	Harry Humphries Albright College
Board Members				
	John Orahood U. of Arkansas, LR	Al Malveaux Xavier, New Orleans	Sister Keller Clarke College	Sister Keller Clarke College
At Large				
	N. Vosburg Principia College	Wally Roth Taylor University	Wally Roth Taylor University	Mike O'Heeron
Public Relations				
	Dan Kinnard Arizona Western	Dan Kinnard Arizona Western	Dan Kinnard Arizona Western	Dan Kinnard Arizona Western
Librarian				
	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College
Equip. Coordinator				
Web Coordinator				
Location:	Georgia Tech	Morningside	Furman	Berea

ASCUE BOARD OF DIRCTORS FROM 1976 to 1980

	1976-77	1977-78	1978-79	1979-80
President				
	Jack McElroy Oklahoma Christian	Harry Humphries Albright College	Fred Wenn Caspar College	Doug Hughes Dennison University
Program Chair				
	Harry Humphries Albright College	Fred Wenn Caspar College	Doug Hughes Dennison University	J. Westmoreland U. Tenn Martin
Past President				
	Larry Henson Berea College	Jack McElroy Oklahoma Christian	Harry Humphries Albright College	Fred Wenn Caspar College
Treasurer				
	William Roeske Houghton College	William Roeske Houghton College	James Foit Central Ohio Tech	James Foit Central Ohio Tech
Secretary				
	Doug Hughes Dennison University	Doug Hughes Dennison University	Dave Dayton Grove City College	John Jackobs Coe College
Board Members				
	Dave Dayton Grove City College	Dave Dayton Grove City College	Jan C. King Chatham College	Wally Roth Taylor University
At Large				
	Fred Wenn Casper College	John Jackobs Coe College	John Jackobs Coe College	Jan C. King Chatham College
Public Relations				
	Dan Kinnard Arizona Western	Sister Keller Clarke College	Sister Keller Clarke College	Sister Keller Clarke College
Librarian				
	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College
Equip. Coordinator				
Web Coordinator				
Location:	OK Christian	Albright College	Casper College	Dennison University

ASCUE BOARD OF DIRCTORS FROM 1980 to 1984

	1980-81	1981-82	1982-83	1983-84
President	J. Westmoreland U. Tenn Martin	John Jackobs Coe College	Jan Carver Chatham College	Wally Roth Taylor University
Program Chair	John Jackobs Coe College	Jan Carver Chatham College	Wally Roth Taylor University	Dudley Bryant Western Kentucky
Past President	Doug Hughes Dennison University	J. Westmoreland U. Tenn Martin	John Jackobs Coe College	Jan Carver Chatham College
Treasurer	Ron Klausewitz W. Virginia Weslyan	Ron Klausewitz W. Virginia Weslyan	Harry Lykens Mary Institute, St L.	Harry Lykens Mary Institute, St. L.
Secretary	Jan Carver Chatham College	Ken Mendenhall Hutchinson CC, KS	Ken Mendenhall Hutchinson CC, KS	John Jackobs Coe College
Board Members	Dudley Bryant Western Kentucky	Dudley Bryant Western Kentucky	William Roeske Houghton University	William Roeske Houghton University
At Large	Wally Roth Taylor University	Chuck Mcintyre Berea College	Chuck Mcintyre Berea College	Bob Renners Kenyon College
Public Relations	Sister Keller Clarke College	Sister Keller Clarke College	Sister Keller Clarke College	Sister Keller Clarke College
Librarian	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College	Jack Cundiff Muskingum College
Equip. Coordinator				
Web Coordinator				
Location:	U. Tenn Martin	Coe College	Chatham College	Taylor University

ASCUE BOARD OF DIRCTORS FROM 1984 to 1988

	1984-85	1985-86	1986-87	1987-88
President				
	Dudley Bryant	Paul Pascoe	Jack Cundiff	Keith Pothoven
	Western Kentucky	Vincennes University	Horry-Georgetown	Central College
Program Chair				
	Paul Pascoe	Jack Cundiff	Keith Pothoven	David Cossey
	Vincennes University	Horry-Georgetown	Central College	Union College
Past President				
	Wally Roth	Dudley Bryant	Paul Pascoe	Jack Cundiff
	Taylor University	Western Kentucky	Vincennes University	Horry-Georgetown
Treasurer				
	Harry Lykens	Harry Lykens	Maureen Eddins	Maureen Eddins
	Mary Institute, St. L	Mary Institute, St. L	Hadley School Blind	Hadley School Blind
Secretary				
	John Jackobs	John Jackobs	John Jackobs	Dudley Bryant
	Coe College	Coe College	Coe College	Western Kentucky
Board Members				
	Keith Pothoven	Keith Pothoven	Robert Hodge	Robert Hodge
	Central College	Central College	Taylor University	Taylor University
At Large				
	Bob Renners	Carol Paris	Carol Paris	Ann Roskow
	Kenyon College	Goshen College	Goshen College	Ister CC
Public Relations				
	Dough Hughes	Wally Roth	Wally Roth	Wally Roth
	Dennison University	Taylor University	Taylor University	Taylor University
Librarian				
	Jack Cundiff	Jack Cundiff	Jack Cundiff	Jack Cundiff
	Muskingum College	Muskingum College	Horry-Georgetown	Horry-Georgetown
Equip. Coordinator				
Web Coordinator				
Location:	W. Kentucky	Vincennet	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 1988 to 1992

	1988-89	1989-90	1990-91	1991-92
President				
	David Cossey Union College	Tom Warger Bryn Mawr College	David Redlawsk Rudgers University	Bill Wilson Gettysburg College
Program Chair				
	Tom Warger Bryn Mawr College	David Redlawsk Rudgers University	Bill Wilson Gettysburg College	Carl Singer DePauw University
Past President				
	Keith Pothoven Central College	David Cossey Union College	Tom Warger Bryn Mawr College	David Redlawsk Rudgers University
Treasurer				
	Maureen Eddins Hadley School Blind	Maureen Eddins Hadley School Blind	Tom Pollack Duquesne University	Tom Pollack Duquesne University
Secretary				
	Dudley Bryant Western Kentucky	Kathy Decker Clarke College	Kathy Decker Clarke College	Dagrun Bennett Franklin College
Board Members				
	Kathy Decker Clarke College	Dagrun Bennett Franklin College	Dagrun Bennett Franklin College	Mary Connolly Saint Mary's College
At Large				
	Ann Roskow Ister CC	Rick Huston South Caolina/Aiken	Rick Huston South Caolina/Aiken	Rick Huston South Caolina/Aiken
Public Relations				
	Wally Roth Taylor University	Wally Roth Taylor University	Wally Roth Taylor University	Wally Roth Taylor University
Librarian				
	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown
Equip. Coordinator				
Web Coordinator				
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 1992 to 1996

	1992-93	1993-94	1994-95	1995-96
President	Carl Singer DePauw University	Rick Huston South Carolina/Aiken	Mary Connolly Saint Mary's College	Paul Tabor Clarke College
Program Chair	Rick Huston South Carolina/Aiken	Mary Connolly Saint Mary's College	Paul Tabor Clarke College	Carl Singer DePauw University
Past President	Bill Wilson Gettysburg College	Carl Singer DePauw University	Rick Huston South Carolina/Aiken	Mary Connolly Saint Mary's College
Treasurer	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University
Secretary	Dagrun Bennett Franklin College	Dagrun Bennett Franklin College	Dagrun Bennett Franklin College	Dagrun Bennett Franklin College
Board Members	Mary Connolly Saint Mary's College	Gerald Ball Mars Hill College	Gerald Ball Mars Hill College	Rick Huston South Carolina/Aiken
At Large	Tom Gusler Clarion University	Tom Gusler Clarion University	Tom Gusler Clarion University	Tom Gusler Clarion University
Public Relations	Don Armel Eastern Illinois U.	Don Armel Eastern Illinois U.	Don Armel Eastern Illinois U.	Peter Smith Saint Mary's College
Librarian	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown
Equip. Coordinator				
Web Coordinator				
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 1996 to 2000

	1996-97	1997-98	1998-99	1999-2000
President	Carl Singer DePauw University	Carl Singer(acting) DePauw University	Bill Wilson Gettysburg College	Dagrun Bennett Franklin College
Program Chair	Chris Schwartz Ursuline College	Bill Wilson Gettysburg College	Dagrun Bennett Franklin College	Carol Smith DePauw University
Past President	Mary Connolly Saint Mary's College	Mary Connolly Saint Mary's College	Carl Singer DePauw University	Bill Wilson Gettysburg College
Treasurer	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University
Secretary	Dagrun Bennett Franklin College	Dagrun Bennett Franklin college	Tom Gusler Clarion University	Nancy Thibeault Sinclair CC
Board Members	Richard Stewart Lutheran Theological	Richard Stewart Lutheran Theological	Nancy Thibeault Sinclair CC	Fred Jenny Grove City College
At Large	Rick Huston South Carolina/Aiken	Rick Rodger Horry-Georgetown	Rick Rodger Horry-Georgetown	George Pyo Saint Francis College
Public Relations	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College
Librarian	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown
Equip. Coordinator				Rick Huston South Carolina/Aiken
Web Coordinator				
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 2000 to 2004

	2000-01	2001-02	2002-03	2003-04
President				
	Carol Smith	Fred Jenny	Nancy Thibeault	Barry Smith
	DePauw University	Grove City College	Sinclair CC	Baptist Bible College
Program Chair				
	Fred Jenny	Nancy Thibeault	Barry Smith	George Pyo
	Grove City College	Sinclair CC	Baptist Bible College	Saint Francis College
Past President				
	Dagrun Bennett	Carol Smith	Fred Jenny	Nancy Thibeault
	Franklin College	DePauw University	Grove City College	Sinclair CC
Treasurer				
	Tom Pollack	Tom Pollack	Tom Pollack	Tom Pollack
	Duquesne University	Duquesne University	Duquesne University	Duquesne University
Secretary				
	Nancy Thibeault	Kim Breighner	Kim Breighner	Kim Breighner
	Sinclair CC	Gettysburg College	Gettysburg College	Gettysburg College
Board Members				
	Barry Smith	Barry Smith	David Frace	David Frace
	Baptist Bible College	Baptist Bible College	CC Baltimore County	CC Baltimore County
At Large				
	George Pyo	George Pyo	George Pyo	Jim Workman
	Saint Francis College	Saint Francis College	Saint Francis College	Pikeville College
Public Relations				
	Peter Smith	Peter Smith	Peter Smith	Peter Smith
	Saint Mary's College	Saint Mary's College	Saint Mary's College	Saint Mary's College
Librarian				
	Jack Cundiff	Jack Cundiff	Jack Cundiff	Jack Cundiff
	Horry-Georgetown	Horry-Georgetown	Horry-Georgetown	Horry-Georgetown
Equip. Coordinator				
	Rick Huston	Hollis Townsend	Hollis Townsend	Hollis Townsend
	South Carolina/Aiken	Young Harris College	Young Harris College	Young Harris College
Web Coordinator				
			Carol Smith	Carol Smith
			DePauw University	DePauw University
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 2004 to 2008

	2004-05	2005-06	2006-07	2007-08
President	George Pyo Saint Francis College	Jim Workman Pikeville College	Lisa Fears Franklin College	George Pyo Saint Francis College
Program Chair	Jim Workman Pikeville College	Lisa Fears Franklin College	George Pyo Saint Francis College	Fred Jenny Grove City College
Past President	Barry Smith Baptist Bible College	George Pyo Saint Francis College	Jim Workman Pikeville College	Lisa Fears Franklin College
Treasurer	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University	Tom Pollack Duquesne University
Secretary	Kim Breighner Gettysburg College	Kim Breighner Gettysburg College	Kim Breighner Gettysburg College	Kim Breighner Gettysburg College
Board Members	Lisa Fears Franklin College	Blair Benjamin Philadelphia Bible	Blair Benjamin Philadelphia Bible	Janet Hurn Miami U. Middleton
At Large	David Frace CC Baltimore County	David Frace CC Baltimore County	David Fusco Juniata College	David Fusco Juniata College
Public Relations	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College	Peter Smith Saint Mary's College
Librarian	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown	Jack Cundiff Horry-Georgetown
Equip. Coordinator	Hollis Townsend Young Harris	Hollis Townsend Young Harris	Hollis Townsend Young Harris	Hollis Townsend Young Harris
Web Coordinator	Carol Smith DePauw University	David Diedreich DePauw University	David Diedriech DePauw University	Blair Benjamin Philadelphia Bible
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

ASCUE BOARD OF DIRCTORS FROM 2008 to 2012

	2008-09	2009-10	2010-2011	2011-2012
President				
	Fred Jenny	Janet Hurn	Janet Hurn	Andrea Han
	Grove City College	Miami U Middleton	Miami U Middleton	U of British Columbia
Program Chair				
	Janet Hurn	Dave Fusco	Andrea Han	Tom Marcais
	Miami U Middleton	Juniata College	U of British Columbia	Sweet Briar College
Past President				
	George Pyo	Fred Jenny	Fred Jenny	Janet Hurn
	Saint Francis College	Grove City College	Grove City College	Miami U Middleton
Treasurer				
	Tom Pollack	Tom Pollack	Dave Fusco	Dave Fusco
	Duquesne University	Duquesne University	Juniata College	Juniata College
Secretary				
	Kim Breighner	Kim Breighner	Kim Breighner	Kim Breighner
	Gettysburg College	Gettysburg College	Gettysburg College	Gettysburg College
Board Members				
	Dave Fusco	Thomas Marcais	Thomas Marcais	Jeffery LeBlanc
	Juniata College	Lee University	Lee University	U of NW Ohio
At Large				
	Andrea Han	Andrea Han	Mark Poore	Mark Poore
	Miami U Middleton	Miami U Middleton	Roanoke College	Roanoke College
Public Relations				
	Peter Smith	Peter Smith	Peter Smith	Peter Smith
	Saint Mary's College	Saint Mary's College	Saint Mary's College	Saint Mary's College
Librarian				
	Jack Cundiff	Jack Cundiff	Jack Cundiff	Jack Cundiff
	Horry-Georgetown	Horry-Georgetown	Horry-Georgetown	Horry-Georgetown
Equip. Coordinator				
	Hollis Townsend	Hollis Townsend	Hollis Townsend	Hollis Townsend
	Young Harris	Young Harris	Young Harris	Young Harris
Web Coordinator				
	Steve Weir	Steve Weir	Steve Weir	Steve Weir
Location:	Myrtle Beach	Myrtle Beach	Myrtle Beach	Myrtle Beach

Using Facebook to Engage Stakeholders: Developing a Content Strategy to Meet Dynamic Social Media Challenges

Amanda Foster
Information Literacy Librarian
afoster@coastal.edu

Scott Bacon
Web Services and Emerging Technologies Librarian
sbacon@coastal.edu

Kimbel Library
Coastal Carolina University
Conway, SC 29528
843-349-2400

Abstract

Facebook is often used by higher education institutions to increase engagement with the campus population and larger community. Facebook page administrators must successfully navigate Facebook's News Feed algorithm to have content reach the largest possible audience. This algorithm uses different measures of audience interaction when determining how "engaging" a post is, rewarding the more engaging posts by increasing the likelihood that they will show up in a fan's News Feed. This paper will explore the process taken by Coastal Carolina University's Kimbel Library to re-develop our content strategy in order to increase engagement on our Facebook page. The authors recommend developing a content strategy that addresses the goals and outcomes of having a Facebook presence, the needs and characteristics of the target population, various themes to be used when creating Facebook posts, and logistics for content creators and scheduling.

Introduction

Coastal Carolina University is a mid-sized academic institution in Conway, South Carolina that currently enrolls over 8,000 undergraduates. Kimbel Library, the university's central information hub, has as its mission to serve as a vibrant, student-centered gathering place for the academic community, offering portals to information and ideas that enhance learning and research for a successful, engaging and diverse community of learners. To extend that gathering place to our online, social community, Kimbel Library created a Facebook fan page in late 2007. The page generated approximately 300 likes in its first few years, showing a steady rise within that time. By early 2012 Kimbel Library had added several more social media platforms, but consistency in content strategy, scheduling and marketing was less than optimal for these tools.

In order to address these problems, the Web Services and Emerging Technologies Librarian and Information Literacy Librarian created a four member Social Media Working Group. The group was tasked with developing a strategic plan for the library's social media presence, choosing appropriate social media platforms that support the strategic plan and creating content for use on library social media sites.

To serve library patrons most effectively, the Social Media Working Group first gathered account information for each of the library's social media platforms and examined whether the platforms were being regularly updated, if two or more platforms were performing the same function, and whether the platforms reflected the library's direction for social media. The working group used this information to consolidate the library's social media platforms down to the most needed tools. Facebook was considered one of the library's essential social networking tools, and the working group chose to test and assess its use as a primary social access point with library patrons. To measure our success, we would use Facebook analytics to gather and analyze data. Once successful practices with Facebook could be identified, these practices could in theory be extended and built upon with other possible social media platforms in the future.

Before developing a strategy for content creation, the working group drafted a social media policy to help library staff in creating and maintaining all social media tools, and to define goals and outcomes for Kimbel Library social media. The policy outlined the library's initial broad goals regarding social media by stating the need to engage and educate the Coastal Carolina University community. In our social media policy our objectives for engagement were to "provide interactive content that starts a conversation with our target audiences, promote involvement with the library or university, and develop engaging content that promotes the academic mission of the university and library" (Foster & Bacon, 2012).

In order to meet these objectives, the working group developed the following outcomes for our Facebook content:

- Outcome 1: Post to Facebook at least three times per week
- Outcome 2: Increase Reach per post to 25% of our fans
- Outcome 3: Increase People Talking About This by creating engaging, dynamic content

Outcomes and success could be measured through the project by using extant metrics provided in the Facebook administrative interface, called Facebook Insights. Analytics and metrics culled from Facebook developer pages would be analyzed by the Social Media Working Group to work toward a better content strategy based on engaging users. Analytics would be compared before and after content strategy implementation in order to measure the effect of our policy changes and strategies across time.

Engagement

To assess whether or not the library's Facebook page was meeting its outcomes for engagement, it was first important to understand how Facebook measures engagement and reports this information to administrators. Facebook provides developers and administrators with an interface called Facebook Insights that supplies and tabulates metrics about their content. Facebook Insights allows administrators

to measure factors like Reach and Virality in order to develop a better content strategy. These analytics factors will now be described in more detail to illustrate how page administrators can create more engaging content.

Facebook Insights allows page administrators to find out "which content resonates with" the community (*How can I use Page Insights to improve my Page?*, Facebook Help Center). This resonance is assessed through several factors:

> ***Reach***: Reach is measured by the number of people who have seen a post. A post is seen when it appears in someone's News Feed.
>
> ***People Talking About This***: People Talking About This is defined by Facebook Insights as "the number of people who have created a story from your Page post" (*How is People Talking About This defined for each of my Page posts?*, Facebook Help Center). Stories are created when someone likes, comments on or shares a post, among other interactions.
>
> ***Virality***: As *Figure 1* illustrates, Virality is defined as "the number of people who have created a story from your post as a percentage of the number of people who have seen it" (*How is Virality defined for each of my Page posts?*, Facebook Help Center). There are no limits to how "viral" a post can become.

$$\text{Virality} = \frac{\text{People Talking About This}}{\text{Reach}}$$

Figure 1: Virality equation

Figure 2 shows Facebook posts from a month-long period sorted by Reach from highest to lowest. Reach is highest for the library post about Spring Break. This means that more people saw this item in their News Feed than any other post that month. However, as is noted in the Engaged Users column, that post only has the fifth-highest number of people, which means that only a small percentage of those who saw the post clicked on it. The post has the second-highest number of People Talking About This, or people who liked, commented on or shared it. This inconsistent set of numbers causes the Spring Break post to have only a 4.64% Virality number. This ranks behind the Virality numbers of two other posts which were more engaging: a trivia post which asked users to guess the most popular DVD checked out of the library, and a post showing an image of librarians wearing school colors on Teal Tuesday. The DVD post received more comments, which pushed the Engaged Users component very high. The Teal Tuesday post had a high Engaged Users number and also received a relatively high amount of comments, likes or shares. The latter two posts were therefore rewarded with high Virality numbers (7.52% and 6.07%, respectively).

Date	Post	Reach	Engaged Users	Talking About This	Virality
3/14/13	We hope you are enjoying Spring Break! ...	496	42	23	4.64%
4/2/13	Kimbel Library is feeling the teal on Teal T...	412	74	25	6.07%
4/5/13	Friday Trivia Time! How many puppets do...	407	49	18	4.42%
3/25/13	Collect them all!	300	56	2	0.67%
3/22/13	Friday Trivia Time! What is the most popul...	266	56	20	7.52%
4/4/13	The Edible Book Festival is coming! Join us...	217	28	7	3.23%
3/19/13	Our Muslim Journey's books have arrived!...	213	28	8	3.76%
3/28/13	This holiday weekend, the Kimbel Library ...	136	26	4	2.94%

Figure 2: Facebook Insights table showing Reach, People Talking About This and Virality

After monitoring the library's Facebook Insights numbers for several weeks, it became clear to the page administrators that the overall Reach of our Facebook posts unexpectedly began to drop in the fall of 2012. After numerous reports from Facebook page administrators citing similar issues with Reach, Facebook released a statement acknowledging the matter: "In the fall we made a quality adjustment to the News Feed algorithm to reduce negative feedback on stories from people. This meant that some Pages saw a drop in Reach on their less engaging posts" (*News Feed Algorithm*, Facebook Newsroom).

At that point, our page administrators realized Facebook changed their News Feed algorithm so that only the most "engaging" content showed up on fans' News Feeds. Less engaging content was less likely to be seen by the Kimbel Library community.

Content Strategy

Taking Facebook's changes to the News Feed algorithm into consideration, the Social Media Working Group determined that in order to achieve the engagement outcomes for the library's Facebook page, a content strategy would have to be researched and developed. This new strategy would tailor Facebook posts to a particular audience of users. It would call for posts to be fun, relevant and engaging while also remaining smart, classy and informative. After monitoring our Insights data for several weeks, we would be able to analyze which strategies were most effective.

To tailor the content strategy to the campus community most effectively, the library needed to know who were its current (and potential) Facebook users. These segments of the audience could then have content most relevant to them appear in their News Feeds. After examining demographics through Facebook Insights (*Figure 3*), it became clear that a major number of our page fans (45%) were aged 18-

24 and living the area surrounding Coastal Carolina University. This data suggests that our largest and most important audience is Coastal Carolina University students. Other audiences indentified included Coastal Carolina University faculty, staff, and administration, alumni, and prospective students and their families.

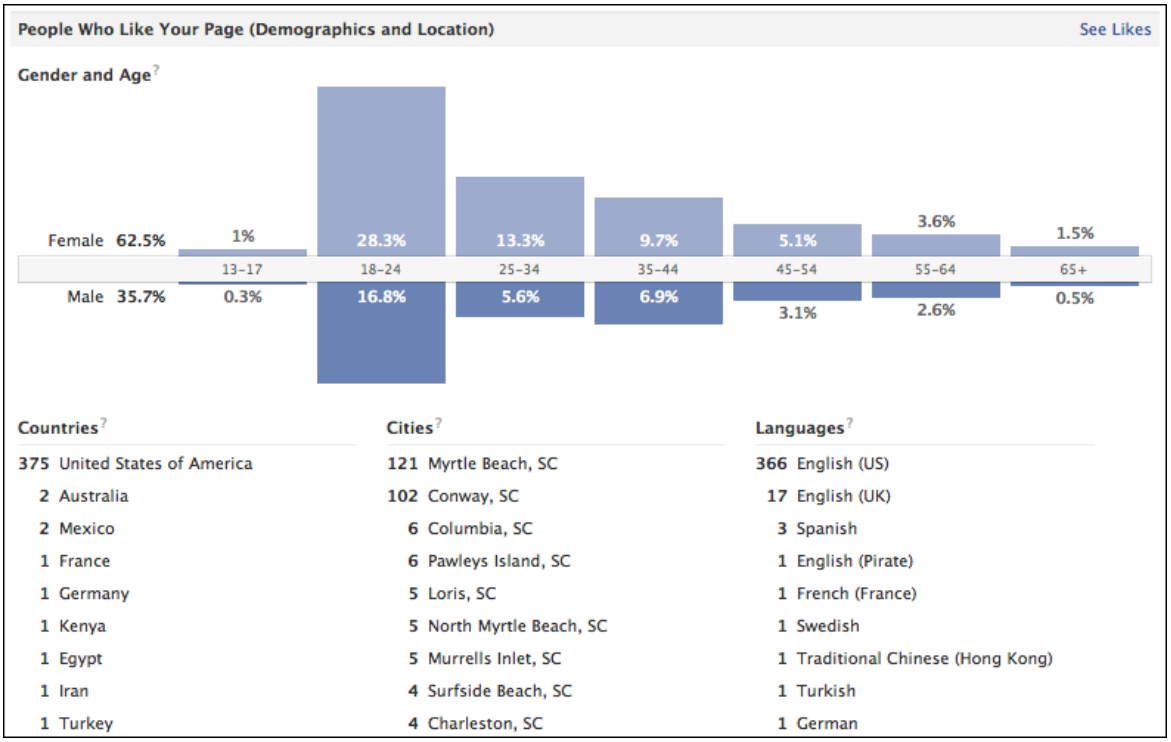


Figure 3: Facebook Insights Demographics

After determining our page's various audiences, page administrators set out to research how to maximize engagement with our Facebook fan page. Several social media administrators have written about how to create engaging content on Facebook. Featuring photos, videos, links, and questions and targeting a freshman audience has been suggested as an effective way to engage users (Gagliardi & Mathews, 2011). In addition to photos with questions and fill in the blanks with photo captions, tips and quotes were explored in an article featured on the technology and social media blog, *Mashable* (Lee 2012). According to the Facebook Help Center, the News Feed algorithm determines the engagement of a post by calculating several factors, "including the number of comments, who posted the story, and what type of post it is (ex: photo, video, status update, etc.)" (*How does my News Feed determine which content is most interesting?*, Facebook Help Center). Taking this research into consideration, the Social Media Working Group developed the following successful strategies for Facebook content creation:

> **Show, Don't Tell.** As a Facebook user scrolls down their News Feed, posts with photos, graphics and videos are more likely to catch their eye. When Facebook's News Feed algorithm calculates engagement, it measures how many users click on a photo or graphic to make it larger or how many users play a video. It is not able to measure how many people read a text status update. For example, rather than tell our users we were busy during exam week, we opted to

show them with a bar chart (*Figure 4*). That post garnered 21 likes, 9 comments, and 66 people clicked on the photo from their News Feed.

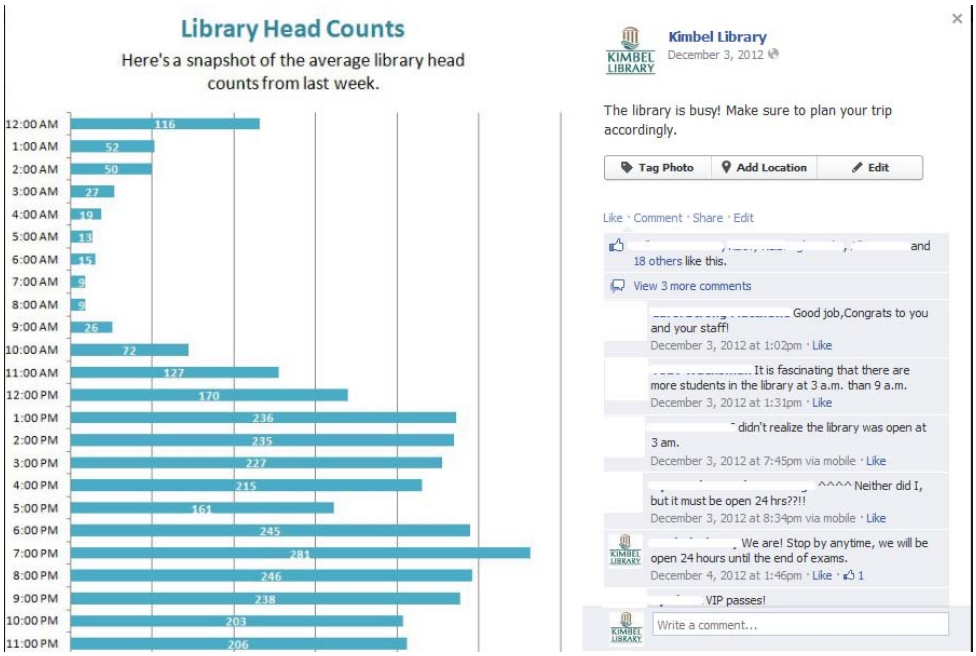


Figure 4: Show, Don't Tell

Start a conversation. Start a conversation with your users by asking for community feedback or posting trivia questions. Every Friday that school is in session, Kimbel Library's Facebook page posts a trivia question about our collection, university history or a current event. Avoiding questions that are easy to look up online helps in getting the most guesses in the form of Facebook comments. Kimbel Library has whiteboards stationed at every entrance to the library and we periodically use it to ask students fun questions relating to the library or a current event (*Figure 5*). If a question is particularly successful in getting feedback, we post the question to Facebook and ask our online community to weigh in. A post asking students which literary character they would vote for to be president garnered 13 likes, 10 comments and one share.

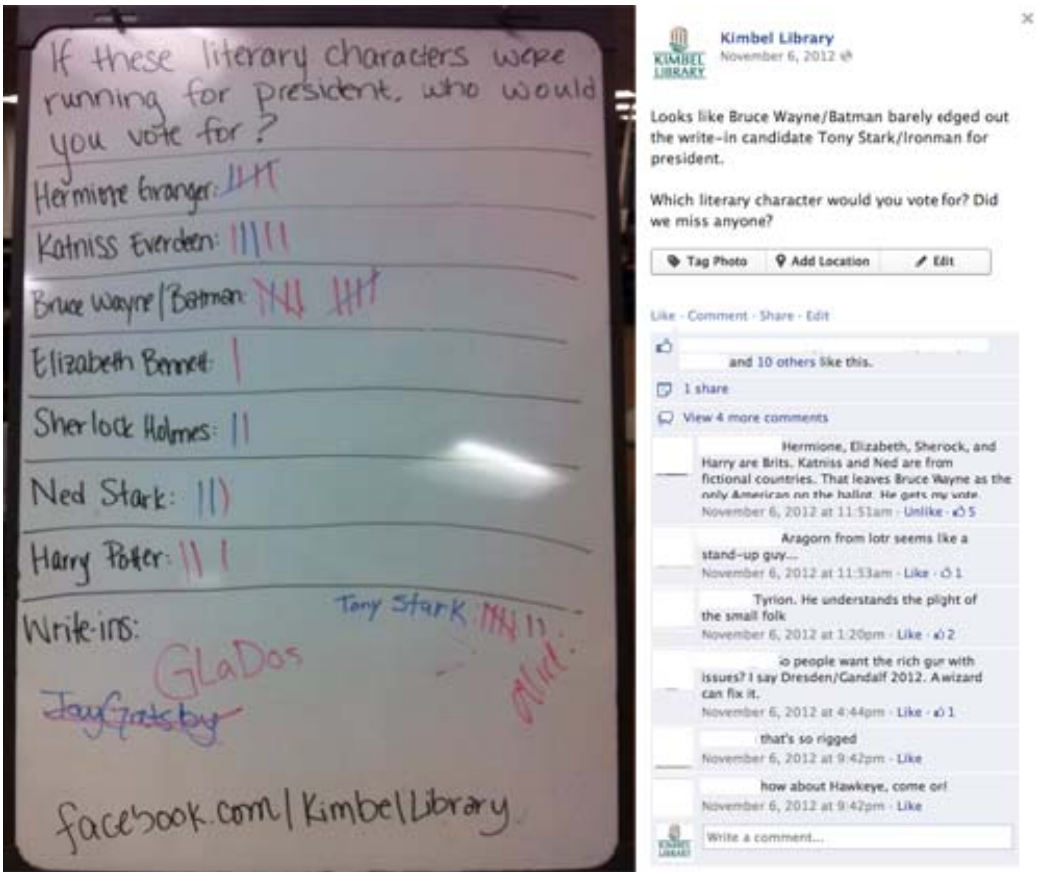


Figure 5: Start a Conversation

Make connections to your physical space. Another content strategy is to take photos of new additions to your physical space or showcase an interesting architectural feature of your building or surrounding area. For example, the library recently posted a photo of the exterior of our building featuring new spring blossoms and lots of sunshine. We encouraged students to enjoy the day to the tune of 9 likes and one share.

Take pictures of your community. This has two benefits. First, people are likely to look for photos taken of them on Facebook. They may comment on the photo or tag themselves, which results in more people seeing the post and interacting with a page. Secondly, other fans of the page may look through photos to find friends or acquaintances, which increases engagement with the post. For example, Kimbel Library hosted a De-Stress Fest Photo Booth during finals week. We took photos of over 60 students posing for pictures with a variety of silly props. Photos in the album generated dozens of likes and the library saw an increase in likes in the days after the album was published on Facebook. Kimbel Library ensures that every person consents to having their picture posted on Facebook by having them sign a social media consent form.

Get connected. Make contact with other campus departments and campus units who are using Facebook by liking their pages and arranging in-person meetings with Facebook administrators.

- The community manager set up a meeting with the university-wide Marketing and Outreach coordinator to learn about using Facebook more effectively and to network with other campus units using Facebook.
- Like other departments' and campus units' Facebook pages, and like, comment on, and share their posts. They are likely to return the favor, which will expose your page to a new potential audience.

Get to know your community. There are several factors to consider here:

- Use Facebook Insights data to learn the demographics of your Facebook audience and make adjustments accordingly. For example, since our primary audience is college students who typically hold later hours than some other communities, we tend to post in the late morning or afternoon. Make sure to post during the hours your community will be checking their News Feed.
- Tie posts to relevant, real-life experiences in your community. A funny post about Spring Break lets the community know that the library recognizes that midterm exams are over and it is time to relax. Posts of this sort reflect on the library as part of the campus community.
- What works for some communities might not work for others. For example, after seeing other university libraries experience success with fill in the blank posts, we tried a post asking, "What are you working on in the library tonight?" No one responded. Now, the library sticks with trivia questions or posting photos of whiteboard questions and asking for feedback.

Determine a good posting schedule. The audience expects to see a post a few times a week. Posting too little causes a page to be lost in the mix; posting too much may cause fans to react in an adverse manner.

Find good employees to help out. Few Facebook pages are completely maintained, administered and written by one person. A good team can provide broader points of view and break up posts so they stay fresh and relevant. Roles that emerged from our working group included:

- *Social Media Administrator*. This person is responsible for the development, maintenance and administration of social media tools.
- *Social Media Community Manager*. This person is responsible for creating and scheduling of content, content quality and moderating and responding to comments on social media platforms.
- *Social Media Working Group Members*. These members are responsible for creating content and contributing ideas about the direction of social media at Kimbel Library. These group members rotate weekly posting duties with the Social Media Community Manager.

Assessment

In order to assess the success or failure of the Social Media Working Group's initial outcomes, daily data from the spring 2013 semester was analyzed and charted. Grouping data this way seemed like the obvious choice due to the fact that the page administrators tried to map the library's content strategy to the university's academic calendar. Numbers appearing to drop on a specific week could be explained

as a result of Fall Break or Spring Break, for instance. Data was gathered by using the Export Data function in Facebook Insights. Data was exported into Excel spreadsheets and analyzed to measure the success or failure of our earlier stated outcomes.

Outcome 1: Post to Facebook at least three times per week

The Kimbel Library Facebook page gained traction among our audience in part due to the development of a regular posting schedule. As page fans expected to see new content on a regular basis, they may have become more receptive to the content. After selecting ideal days of the week and times of the day to post, the working group could then optimize posts with more engaging content in order to increase Reach and People Talking About This numbers.

Outcome 2: Increase Reach per post to 25% of our fans on average

Facebook has acknowledged that, on average, a Page only reaches about 16% of Page fans (*Sponsor your Page posts*, Facebook Notes). The Social Media Working Group stated as an outcome that it wanted to increase page Reach to 25% per post. *Figure 6* shows a steady increase in our Facebook page Reach from the beginning weeks of the spring 2013 semester until mid-March, where Reach leveled out a bit. During the spring 2013 semester, Daily Total Reach came in at an average of over 84%, or 68% more than the Facebook average. We saw this as a major success, which can be directly attributed to the revised content strategy changes detailed above.

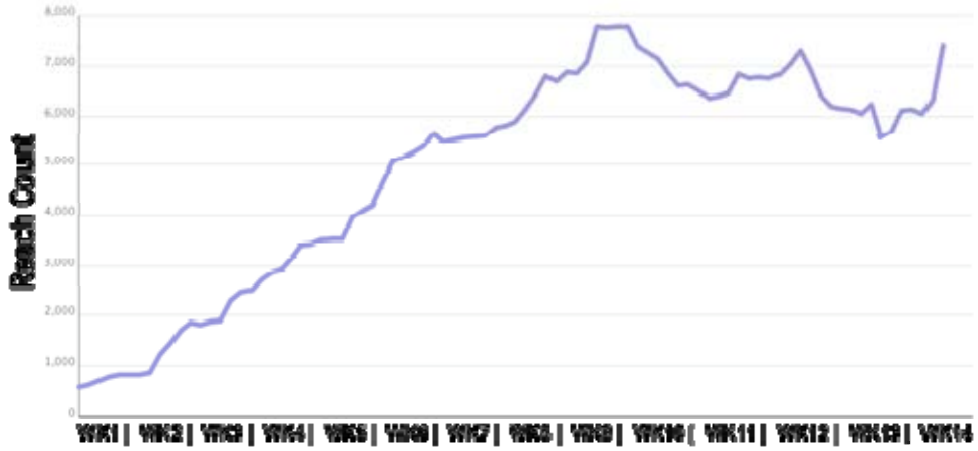


Figure 6: Reach, Spring 2013

Outcome 3: Increase People Talking About This by creating engaging, dynamic content

The working group had as another stated outcome to increase our People Talking About This numbers, in order to bring our Virality numbers up. This outcome was achieved due to the revised content strategy, which increased both Reach and People Talking About This, the two quantities of the Virality equation. The larger the ratio of People Talking About This is in relation to the number of page fans and other Facebook users, the larger the Virality percentage. *Figure 7* shows a rise in data that basically mirrors the rise in Reach data for the first few months of the spring 2013 semester. Since our Reach data leveled out at a higher plateau than the People Talking About This data, the Virality percentages leveled out slightly lower than in the first few months of the semester, to between 1.5% and 2.5%. However, there was an overall increase in Virality of 1.33% during the spring 2013 semester when compared with Virality data from the fall 2012 semester.

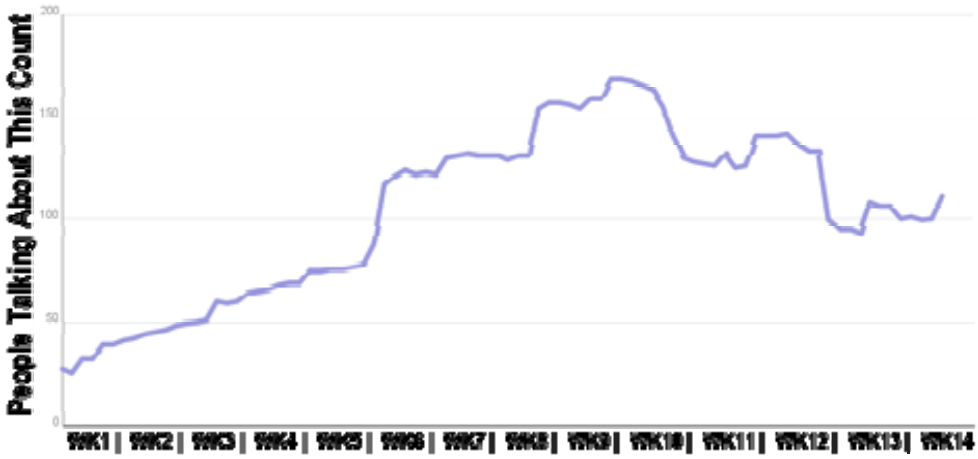


Figure7: People Talking About This, Spring 2013

Limitations

Although the Social Media Working Group project was an overall success, some limitations to the project should be noted in order to place the numbers in perspective. The demographics of our audience, while comprised of a diverse body of users from several backgrounds and locations, is still constrained by many factors. We are a library in a mid-sized university in the state of South Carolina, and our audience is a specific community of users unlike any other. Others can certainly glean trends from this project, but those trends should be put into context by recognizing our unique situation.

Another limitation surfaces when digging through data on posts. When we don't post on a specific day, the data looks very low. Since we only post three times a week, analyzing daily data can be an issue. And since our primary audience is collegiate, we post more often when classes are in session. Data for times when classes are out of session are much lower. The authors decided to only use data from the beginning to the end of the semester in order to avoid many of these skewed numbers.

The authors of this study used Facebook Insights as the sole data source for analysis because it offers highly-detailed data about many factors that contribute to user engagement. But page administrators wishing to obtain further analytics information about their Facebook page will find no shortage of third-party tools available. A detailed analysis of third-party analytics tools is beyond the scope of this paper, yet these are readily available on the Web.

Looking to the Future

Another of the initial goals of the Working Group was to increase Kimbel Library Facebook page likes three-fold from the totals in late 2012 (approximately 300 likes) by the summer of 2014. Increasing likes to 1000 or more is no small task, however, as many communities have an upper ceiling which a page cannot reasonably be expected to reach above organically. The relatively slow rise of likes on the

page in its first several years of existence may necessitate finding new ways to engage and interact with potential fans. The authors chose not to focus on likes in this publication, though those numbers rose approximately 8% throughout each of the past two semesters. The revised content strategy will likely continue to contribute to increased likes, but there are other options should this slow and steady rise not yield as many likes as expected. Page administrators can increase the possibility of getting more likes by buying ads targeted to specific users and by paying to promote sponsored stories. The authors recommend that page administrators take care to have a balanced approach to seeking likes organically, however, as it is often better to build slowly than appear too intrusive or even aggressive in trying to grow your community.

One of the first tasks of the Social Media Working Group was to choose the most appropriate social media platforms for the library and focus on using those to the best of our ability. As our content strategy has been successful thus far, we are ready to apply it to our other social media platforms, such as Twitter, Flickr, Blogger and YouTube. The library decided to disable its Twitter account in late 2012 in order to focus on making Kimbel Library Facebook successful. As the library now moves toward an even more coherent content strategy, Twitter will soon be re-launched with a more streamlined mission. Other future considerations that the Working Group will address include targeting mobile social media users, experimenting with Facebook ads, working closely with other similar library committees and working groups such as the marketing and outreach groups.

The authors would like to note that there are several challenges to maintaining a successful Facebook fan page. Facebook's News Feed algorithm has not been released to the public, so those trying to optimize their content to reach the most users are left wanting more information. The algorithm is dynamic, and can change at a moment's notice. The Facebook Statement of Rights and Responsibilities is similar in its fluid nature. In order to keep up with these myriad changes, page administrators would do well to keep a close eye on Facebook news. Browse social media and technology publications, be proactive by creating search engine alerts for specific terms and periodically review Facebook rules and regulations. It also behooves administrators to revise their policy and content strategy as needed. These documents should not be inflexible, but rather should reflect the ever-changing nature of the social media landscape.

References

Facebook Notes. (2012). Sponsor your Page posts. Retrieved April 12, 2013, https://www.facebook.com/notes/facebook-marketing/sponsor-your-page-posts/10150675727637217

Facebook Help Center. (2013). How can I use Page Insights to improve my Page? Retrieved April 8, 2013, https://www.facebook.com/help/200504156688306/

Facebook Help Center. (2013). How is People Talking About This defined for each of my Page posts? Retrieved April 10, 2013, https://www.facebook.com/help/293874353972579

Facebook Help Center. (2013). How is Virality defined for each of my Page posts? Retrieved April 10, 2013, https://www.facebook.com/help/279981958693502/

Facebook Newsroom. (2013). News Feed Algorithm. Retrieved April 3, 2013, http://newsroom.fb.com/Fact-Check/537/News-Feed-Algorithm

Foster, A., & Bacon, S. (2012). Kimbel Library Social Media Policies and Procedures. Unpublished internal document.

Gagliardi, K., & Mathews, B. (2011). How to Use Social Media to Engage Students. Retrieved from https://docs.google.com/document/d/1dvxlOmQUm9j20r8tuf1oRMlfq-1P5-DszvJC0u9Agug/edithl=en

Gerolimos, M. (2011). Academic Libraries on Facebook: An Analysis of Users' Comments. *D-Lib Magazine, 17*(11/12). Retrieved from http://www.dlib.org/dlib/november11/gerolimos/11gerolimos.html

Lee, A. (2012, Jul. 5). 6 Posts That Build Engagement on Facebook. *Mashable*. Retrieved from http://mashable.com/2012/07/05/facebook-build-engagement/

Using Portable Technology to Teach Web Programming and Database Classes

Sam Hijazi
Texas Lutheran University
1000 W Court St Seguin, TX 78155
830-372-8000
drhijazisam@gmail.com

Abstract

Teaching a web programming class requires multiple software programs, a secured server, and sustained IT support. If a student can access all these technologies directly from a jump drive, it will alleviate many of these issues, especially the security matter. In the last two years, there was a major upgrade to XAMPP, a free and downloadable software. XAMPP contains all the technologies needed in this course, including Apache Server, MySQL engine, PHP interpreter, and phpMyAdmin.
This paper will explore the benefit of teaching a web programming or a relational database class directly from portable media, such as a jump drive, without putting university IT security at risk. A student will be able to utilize all the required software including tools, directories, and files directly from a flash memory card. In the last two web programming classes taught using this technique, I have noticed an increase in productivity, creativity, and output. Students felt free to work on their own directly from their laptops regardless of space and time. Students were productive, creative, and unbounded by a physical place.

This research will also discuss portability issues in the information system fields. The research will include some feedback from the students concerning their satisfaction when using XAMPP. Also, the research will explore other applications that use portable technology to teach additional subjects, such ecommerce applications, and relational database.

Introduction

This paper is in support of using portable technologies such as XAMPP to teach data driven web development from a jump drive. This paper shows that depending on IT departments might not result in enough support to these web development classes. The reasons are due to inadequate resources and security issues. The reviewed literature shows that it is more practical to teach web development from portable media due to the ease of installation and direct access from a jump drive. This paper surveys a small sample of students who have taken class using XAMPP. The results show that most of the students have enjoyed the freedom to work directly from their jump drive without any concern with security problems. Finally, this paper shows how to install XAMPP, how connect to an Apache server, how to connect to a database by utilizing phpMyAdmin, and how to retrieve data from MySQL to be used in a website.

The Problem and its Components

Teaching data driven web development classes can be a daunting issue to many instructors. People know from previous experience that it is not easy to install an Apache web server, especially when there is a need to add a MySQL server, a PHP interpreter, Perl, and phpMyAdmin (apachefriends.org). Ironically many information systems professors consider teaching web programming classes rather an exciting and a fulfilling subject. According to the web article *Study Web Design and Development (2013)*, the author stated that studying web design and development creates a perfect combination of fun along with a high prospect for a productive job. The problem lies in configuring the various technologies and in receiving adequate support from one's IT department. Most IT departments are busy responding to many requests. Many IT directors are also concerned with security more than anything else, especially non-authorized persons hacking into the university intranet.

From a personal experience, I found it difficult to depend on my IT department to install multiple technologies in order to teach one web development class. The problem stemmed from the lack of freedom and the need to access the server directly within the university. Even though, we get the needed support, the security issues remain a big factor. Thus, finding a package such as XAMPP that contains all the required tools to teach a class directly from a jump drive has been nothing short of a technological blessing.

In addition to the variety of applications that come with XAMPP, its installation is a breeze. From the article *developerWorks* (2004) by IBM, the writer stated "Open source stacks such as XAMPP from Apache Friends are simplifying open source development by making it easier to write and distribute applications in a stable and standardized environment." Further the article added that XAMPP is a full-featured AMPP (Apache, MySQL, PHP, and Perl) package. These applications are tightly integrated.

Advantages of XAMPP

As stated earlier, this paper attempts to examine the use of XAMPP to teach web programming and database classes from portable media such as a jump drive. Another focus is to show how easy it to install and use varieties of technologies directly from portable media. These technologies include but are not limited to Apache server, MySQL, PHP interpreter, Perl, and an administrative tool to facilitate the access of all these technologies, that is, phpMyAdmin.

According to *sourceforg.net* (2013), XAMPP includes an easy installation to Apache Distribution. It is available for Linux, Solaris, Windows, and MAC. The web page also stated that the package comes with the Apache web server, MySQL, PHP interpreter, Perl, a FTP and phpMyAdmin. The author of the article *XAMPP – A web server and database package* stated that the problem is always in finding a web server to run the web programming requirement. Typically, developers have to pay for a service to access this requirement before they can test their data driven web pages. XAMPP is a convenient package that will provide developers with all their needs to design, implement, and test their final products without the constraints or the cost associated with a commercial server. The author also mentioned that you can set up your server for free on any computer or laptop. Furthermore, the article added that "you can use this package with Joomla and similar [Content Management System] CMS web sites."

Dvorski (2007) states that XAMPP is a small Apache distribution. The author added that XAMPP contains all web development technologies in a single package. Its portability and its small size make it an excellent tool for "student development and testing applications in PHP and MySQL." Furthermore, it is free and available to download in two flavors: lite and full. Memory requirements have changed since the writing of Dvorki's article; however the benefits of using XAMPP in teaching a web programming and database classes are still the same.

The other obvious benefits of using XAMPP as a web development tool are the increased confidence of the students. Learners do not have to worry about their codes being seen by others (Dvorski, 2007). Students can create databases, enter data, write PHP scripts, test the scripts, rewrite the scripts and run a variety of software on their machines. If the website, including all its components, is ready to be posted live for the general public, then the only thing the students need to worry about is finding a secure server to host their website. XAMPP's main advantage is to prevent unwanted access to the code during development.

Feedback from the Students

The author of this article observed the reaction of his students to using the XAMPP package. Most of the students provided him with positive feedback. In order to confirm some of his beliefs, a small survey was sent to 16 students who took a web programming class. Nine of the students answered the survey. The results confirmed the instructor's assumption. The survey used these six criteria:

0. Extremely inaccurate
1. Moderately inaccurate
2. Slightly inaccurate
3. Slightly accurate
4. Moderately accurate
5. Extremely accurate

The first statement in the survey was: "The software package provided me with the freedom to work from anywhere and at any time." Table 1 shows the results:

Table 1

Extremely inaccurate	Moderately inaccurate	Slightly inaccurate	Slightly accurate	Moderately accurate	Extremely accurate	Total	Average Rating
11.11% 1	**11.11%** 1	**0%** 0	**0%** 0	**55.56%** 5	**22.22%** 2	9	4.44

The second statement in the survey was: "The software package provided me with more opportunity to learn about issues that could not be easily learned through a traditional setting, such as the university server." Table 2 shows the results:

Table 2

Extremely inaccurate	Moderately inaccurate	Slightly inaccurate	Slightly accurate	Moderately accurate	Extremely accurate	To-tal	Average Rating
11.11% 1	**11.11%** 1	**0%** 0	**11.11%** 1	**22.22%** 2	**44.44%** 4	9	4.56

The third statement in the survey was: "XAMPP has allowed me to test my web site before uploading it to a live server." Table 3 shows the results:

Table 3

Extremely inaccurate	Moderately inaccurate	Slightly in-accurate	Slightly accurate	Moderately accurate	Extremely accurate	To-tal	Average Rating
11.11% 1	**11.11%** 1	**0%** 0	**0%** 0	**22.22%** 2	**55.56%** 5	9	4.78

The fourth statement in the survey was: "I recommend XAMPP as a convenient learning package to other students." Table 4 shows the results:

Table 4

Extremely inaccurate	Moderately inaccurate	Slightly in-accurate	Slightly accurate	Moderately accurate	Extremely accurate	To-tal	Average Rating
11.11% 1	**11.11%** 1	**0%** 0	**0%** 0	**11.11%** 1	**66.67%** 6	9	4.89

Installation of the Package

This section will discuss briefly how to download, install, activate, and start using the package to create a very easy database. A PHP script will retrieve the data from the database and display it in a website. The idea here is to avoid complexity in database design. The illustration will provide the learner with a simple example to assure complete understanding. The final step is to communicate the data to a web-site. In order to assure a better understanding of the process, this section will cover each step individu-ally with a figure. The whole idea is to show the simplicity of installing XAMPP as a portable and pro-ductive web development tool. See Appendix A for details.

Purpose of the Study

This paper attempted to show the benefit and ease of using portable technologies such XAMPP directly from a jump drive. In addition, it should be noted that there is a major emphasis on the freedom to de-velop data driven websites without concern initially with any security issues. This paper shows step by step how to install XAMPP as a multi-technology package, including Apache server, MySQL, PHP, Perl, and phpMyAdmin.

Universities and colleges have limited resources, especially the time to support multiple classes with all the needed technologies. Research shows that IT departments have an overwhelming number of duties to accomplish on a daily basis. Feeling secured, students should be able to develop, test, and retest their

databases and PHP codes directly from their jump drives. The desired outcome is the learners' ability to handle all the intricacies of a website development securely before they attempt to upload it to a live server.

Limitation/Delimitation of the Study

This is a local study pertaining to students enrolled in a web programming class at Texas Lutheran University. The number of surveyed students is part of the limitation of the study. The author contacted his students to complete a survey and not all the students completed the survey. Another limitation is the fact that some of the positive feedback provided by the students were based on observations by the instructor. The instructor observed and communicated directly with students during a web programming class to reflect on their satisfaction and independence.
The delimitation of this paper is that the study covers students who are pursuing a degree either in computer science or information systems. Another delimitation is that students are computer literate and a have taken computer programming classes.

Recommendation

Technology changes rapidly resulting in a constant need to reexamine such packages. In a future study of the same package, XAMPP, there is a need to examine the other components such as Perl, ProFTPD, an FTP server and OpenSSL, for secure sockets layer support. Future follow-up can include additional students from different institutions who are using the same package.

Conclusion

This section is to remind us of the four sections of this paper. First section is related to the nature of problems associated with the dependency and the difficulty of installing multiple technologies before you can teach a web development and/or a database class. The second section is concerned with literature review. Research showed clearly those portable packages such as XAMPP is not only time and cost saving, but also a convenient and productive approach to teach a web development class. The third section is to test students' satisfaction with XAMPP as an alternative to traditional servers. The last section is to show step by step how to install XAMPP, connect to the Apache server, connect to MySQL, Query the database using PHP commands, and display the results to a website.

References

Apache Friends (March 02, 2013). XAMPP for Window. Retrieved April 20, 2013 from . http://www.apachefriends.org/en/xampp-windows.html

DeveloperWork (2004). Install XAMPP for easy, integrated development. Retrieved April 20, 2013, from http://www.ibm.com/developerworks/linux/library/l-xampp/

Dvorski, D. D. (2007). Installing, Configuring, and Developing with XAMPP. Retrieved April 21, 2013, from http://dalibor.dvorski.net/downloads/docs/InstallingConfiguringDevelopingWithXAMPP.pdf

International Computer User Fellowship of Rotarians. (2013). XAMPP- A Web server and database package. Retrieved April 22, 2013, from http://www.icufr.org/index.php/other-resources/1865-xampp-a-web-server-and-database-package

International student. (2013, March 6).Study Web Design and Development. Retrieved April 22, 2013, from http://www.internationalstudent.com/study-web-design-and-web-development/

PHPID. (2013). How to install Xampp- step by step Tutorial. Retrieved April 21, 2013, from http://www.phpide.com/php-tutorials/how-to-install-xampp-step-by-step-tutorial/

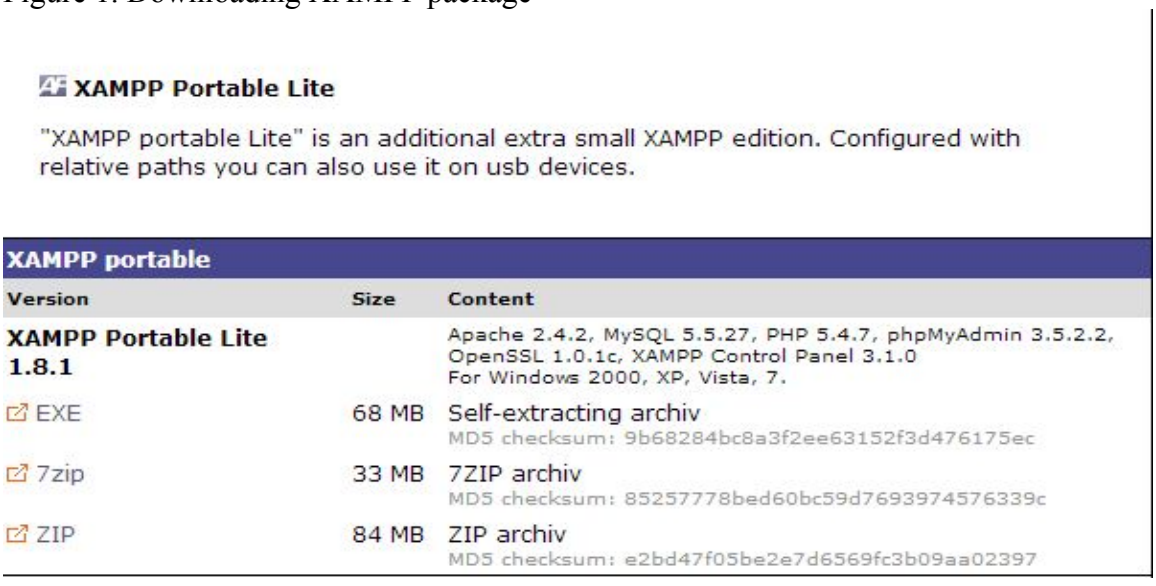
Sourceforge. (2013). XAMPP. Retrieved April 23, 2013, from http://sourceforge.net/projects/xampp

Appendix A – Implementing XAMPP

Downloading the software

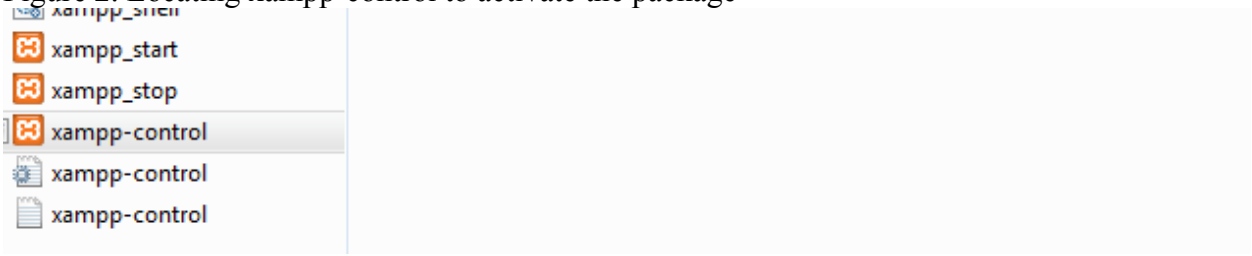
The first step is to go to the main site to download the package. We will download XAMPP for Windows. After typing the URL in your favorite browser: http://www.apachefriends.org/en/xampp-windows.html, scroll down to find the option found in figure 1. The figure shows our choice to download XAMPP as a portable version. At the time of writing this article, it is version 1.8.1. The best choice is to click on the "self-extracting archive." After the completion of downloading the package, the process of installing the software will ask us where to save the package. At this stage, we it direct it to a jump drive. The recommended amount of memory is 8 GB. Once the package is saved on our jump drive, we can access the software from the newly created folder. The name of the new folder is XAMPP 1.8.1.

Figure 1. Downloading XAMPP package



Activating the package. Examining the XAMPP folder, we will see multiple subfolders and other files. Our focus is to locate the file "xampp-control" as seen in figure 2. Once we locate the file, we need to click on it.

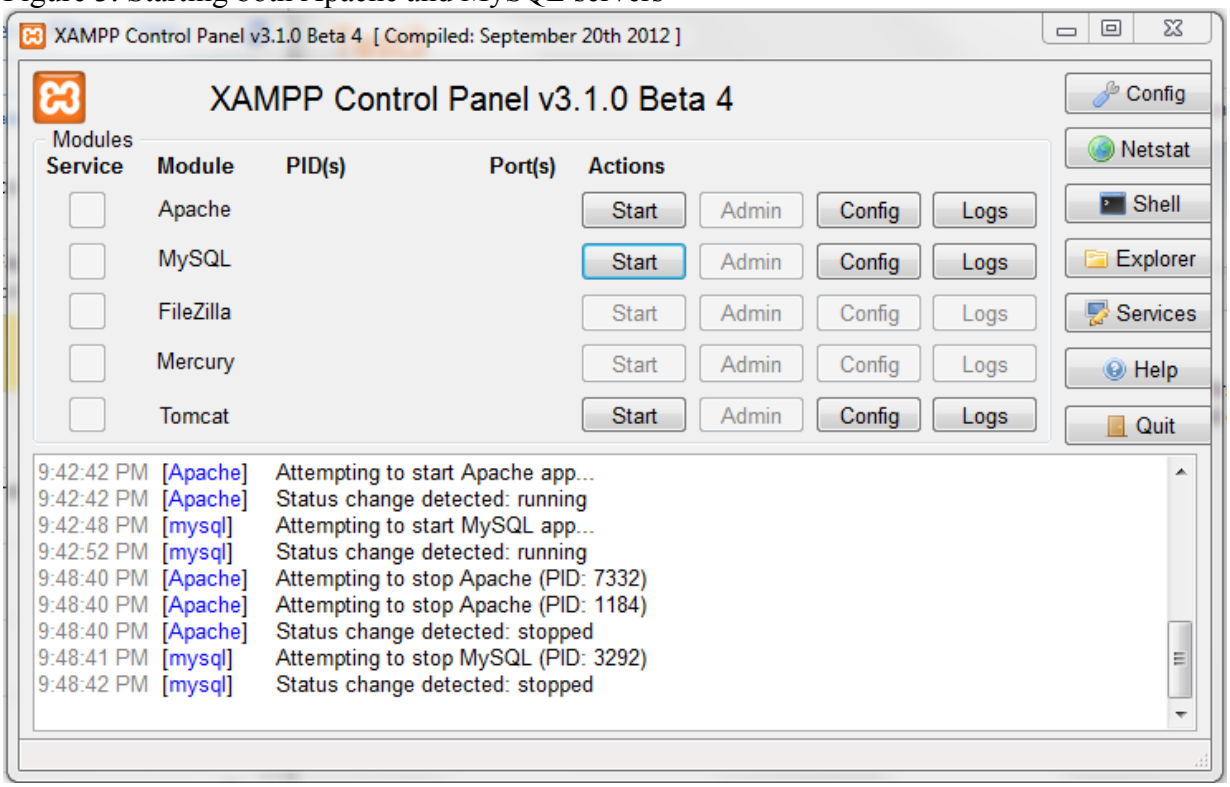
Figure 2. Locating xampp-control to activate the package



Starting Apache and MySQL servers

By activating xampp-control, XAMPP Control Panel v3.1.0 Beta 4 will be displayed. As we see from figure 3, we need to "start" both actions for the Apache and MySQL.

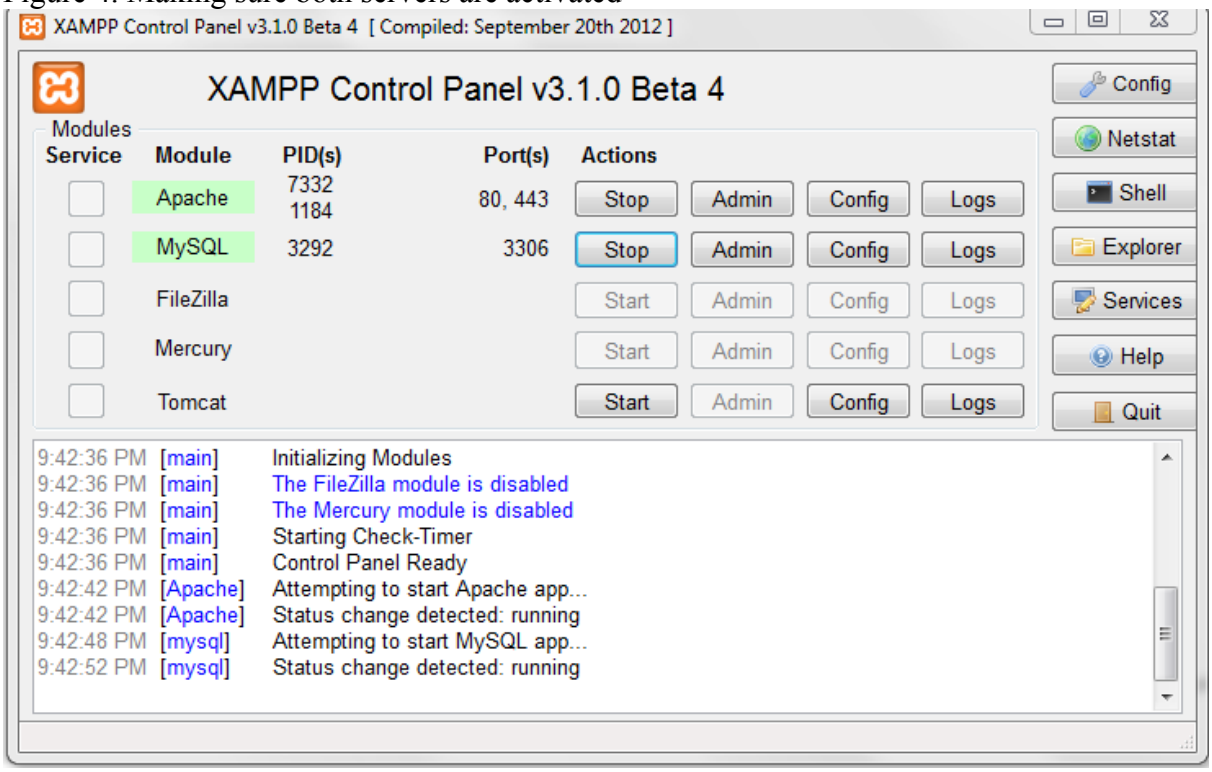
Figure 3. Starting both Apache and MySQL servers



Making Sure both severs are activated

The only way to make sure that both Apache and MySQL servers are ready is to see that both actions in the figure 3 changed from "start" to "stop." Figure 4 shows additional options that a learner can tweak to their liking including the configuring of both servers. For the purpose of this paper, we will try to keep it simple. Having said that, there is a common problem that happens frequently with port numbers. Make sure to use port 80 or 443 for the Apache server. Some users might have to free these ports in order to launch the Apache server. As we see from the below figure, we activated both the Apache server and MySQL database. At this stage, we are ready to use the package.

Figure 4. Making sure both servers are activated



Getting ready to use localhost

At this stage, we can go to our favorite browser and type: localhost/xampp/ and hit enter to assure ourselves that the Apache server is ready and running. After typing localhost, Figure 5 should show. By choosing English as our language, we are ready to launch phpMyAdmin.

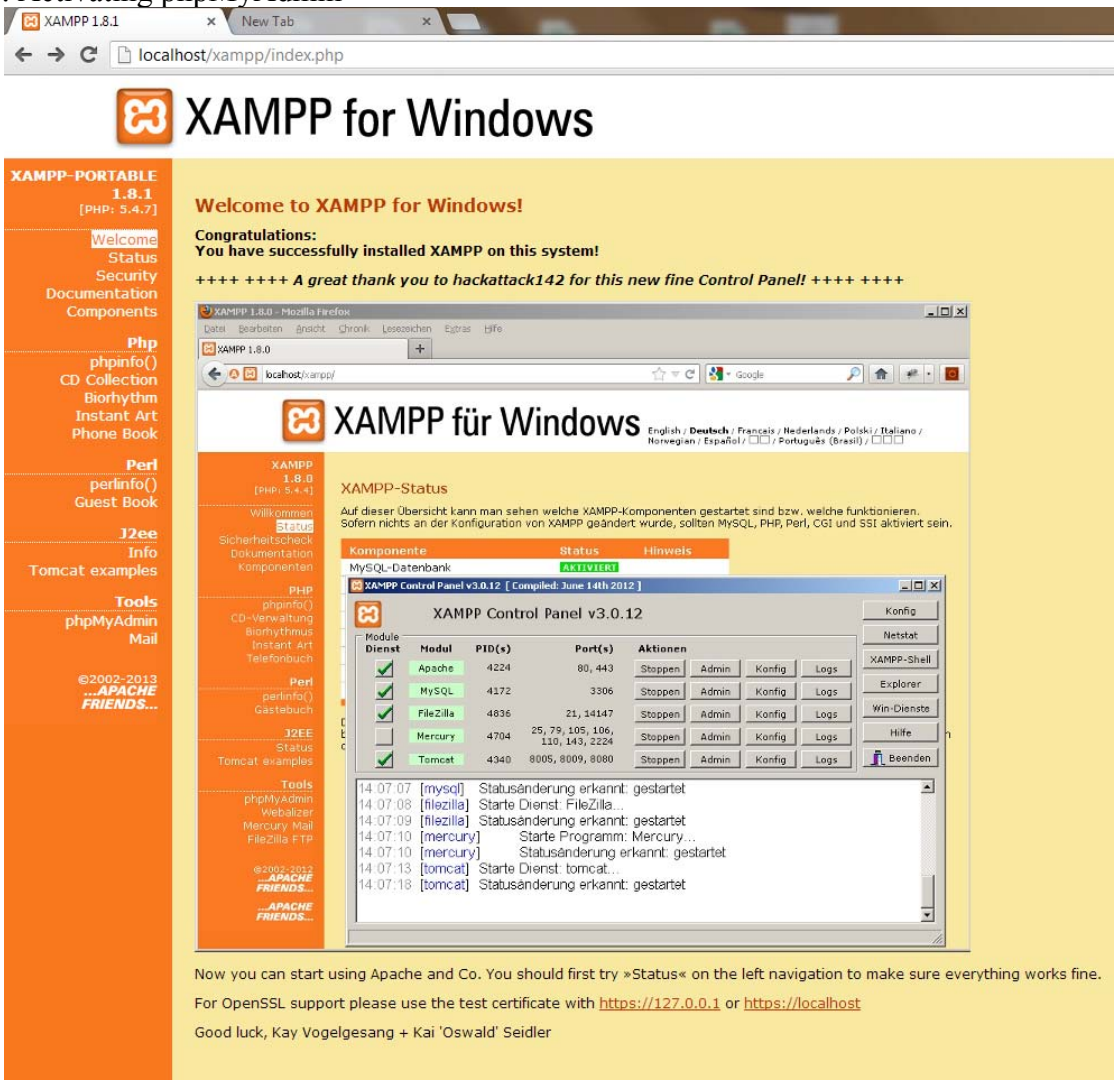
Figure 5. Activating the Apache Server by using localhost

Activating phpMyAdmin

Figure 6 below shows that we can click on the option "phpMyAdmin." This will lead us to access MySQL server. There are multiple options that we can experiment with using phpMyAdmin. Again, to

keep this paper as simple as possible, we will focus only on using MySQL server to build a small database with a single table. The whole idea is to prove that we can access the database later through a PHP script without any problem. We should be able to do this regardless of the complexity of the database, its size, or the number of its relations.

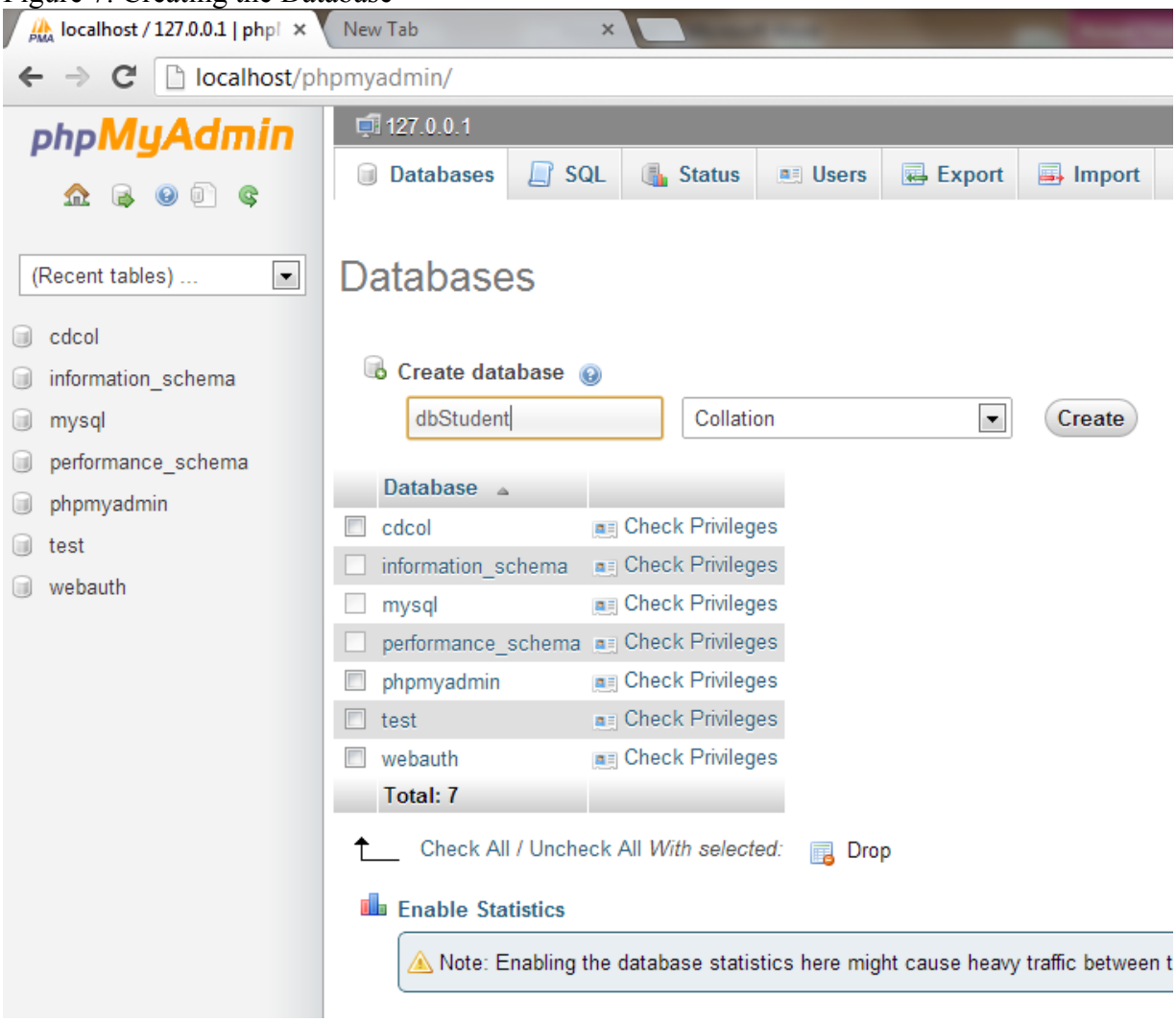
Figure 6. Activating phpMyAdmin



Creating the database

Once we activate phpMyAdmin, it will display MySQL database as shown in figure 7. The first step is to create the database by giving it an appropriate name. In this illustration, a database by the name dbStudent will be created. Of course, there are multiple options to select if a user wants to be more specific. These include access methods such ISAM and InnoDB .

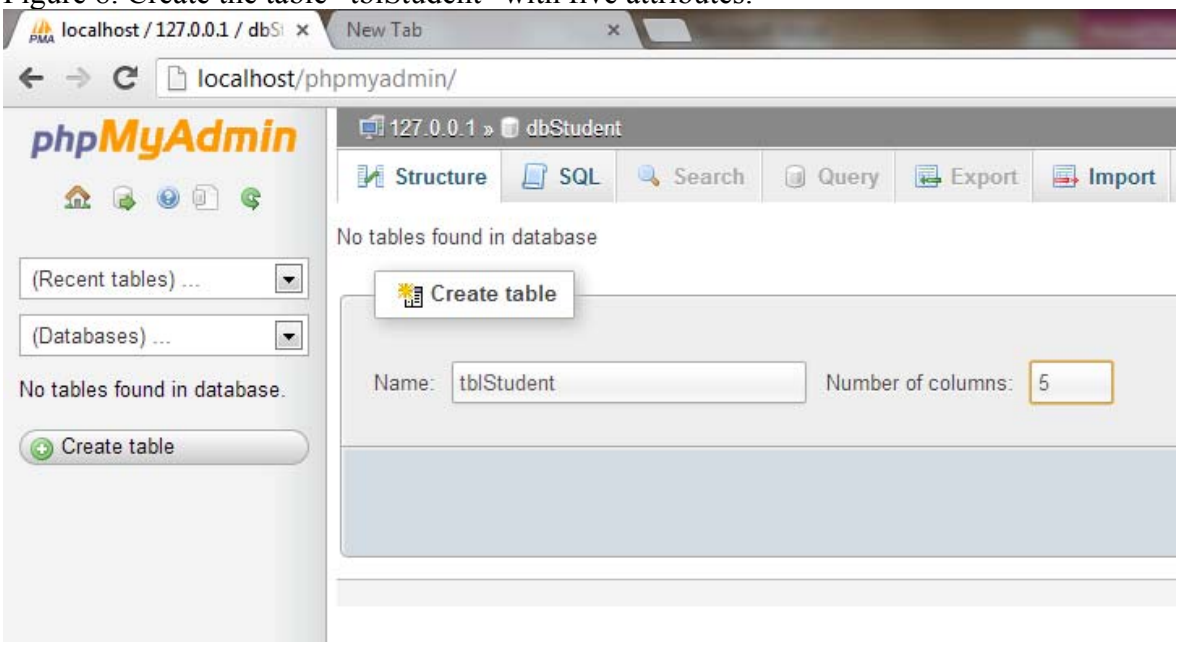
Figure 7. Creating the Database



Creating the table

Although we can create multiple tables with their relations, we will be using a single table to simplify the process. The name of the table is tblStudent. It will illustrate the use of database as seen in figure 8. The main idea is to create the table, enter the data, and later to retrieve the data from the database through a PHP script. Naturally, we need to specify the number of attributes. In this example, there will be five.

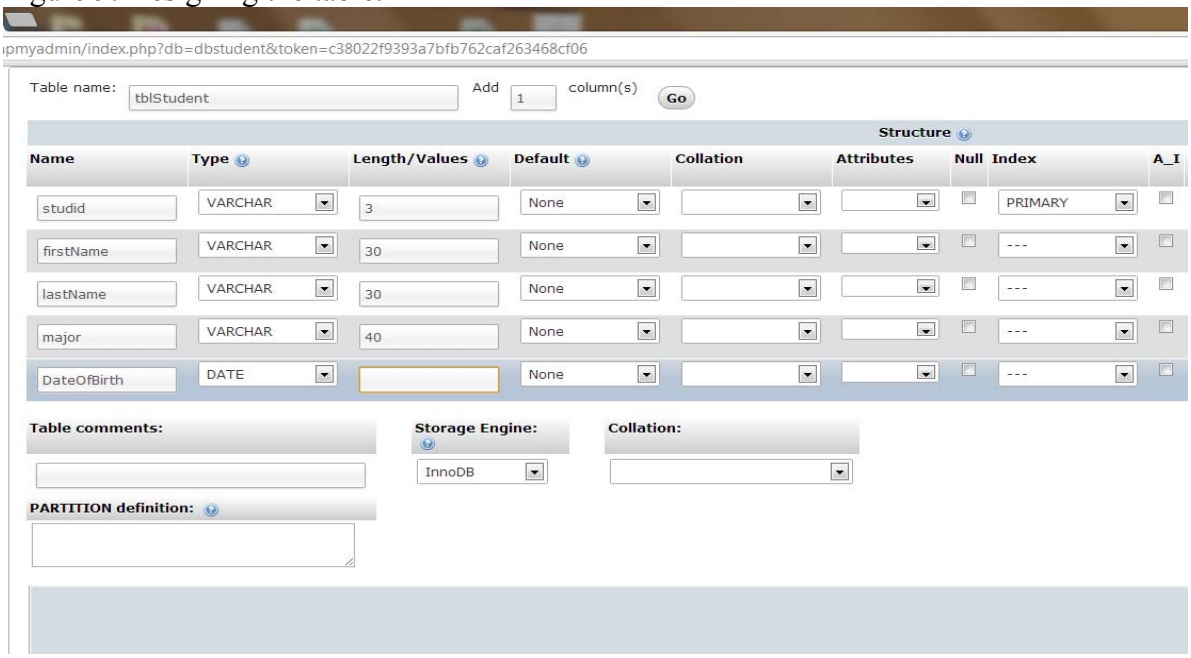
Figure 8. Create the table "tblStudent" with five attributes.



Choosing the data types

As we see from figure 9, the first attribute was named studid and was declared as varchar (3). Studid is the PRIMARY KEY. The other attributes are firstName as varchar(30), lastName varchar(30), major as varchar(40) and dateOfBirth as date, respectively. We need to press the "Go" button to confirm our design.

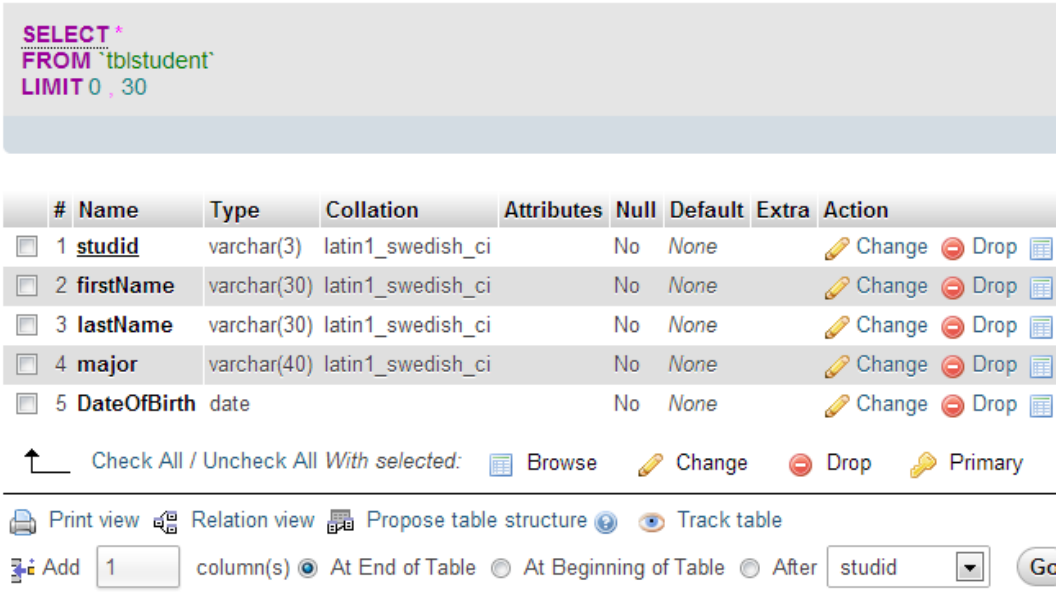
Figure 9. Designing the table.



Examining the structure of the table

As we see from figure 10 below, the structure shows each attribute along with the data type. At this stage, we still have the chance to change the data type, drop any attribute, change the primary key or drop the table as a whole.

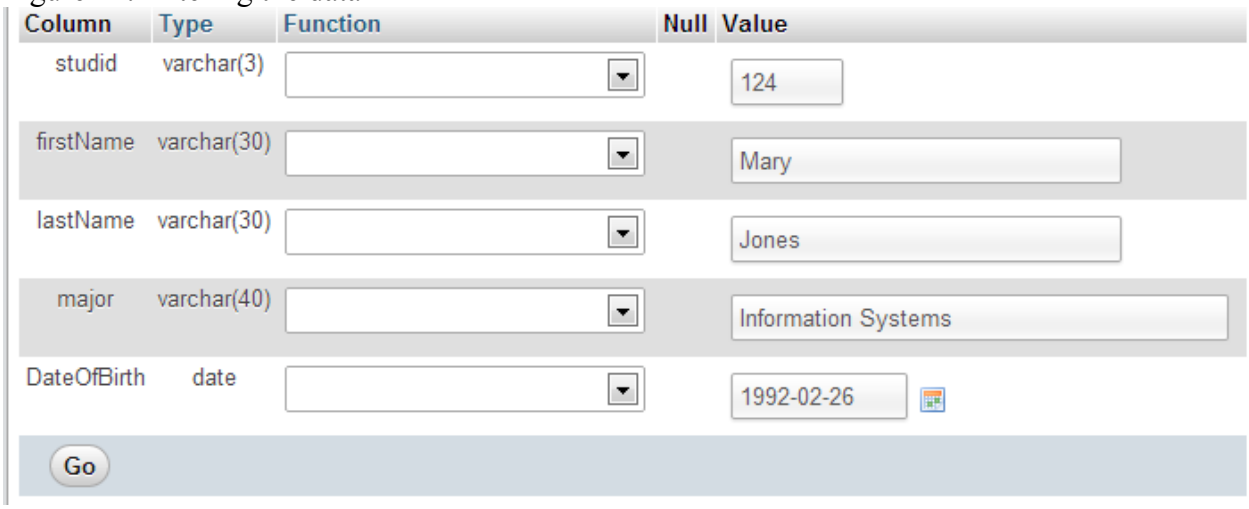
Figure 10. Viewing the structure of the table



Enter the actual data.

At this stage, we are ready to enter the real data. It is very easy to move from one field to another as seen in figure 11. We can choose the number of records ahead of time or add new ones as we go. Of course, we need to press the "Go" button to confirm the data entry in the table.

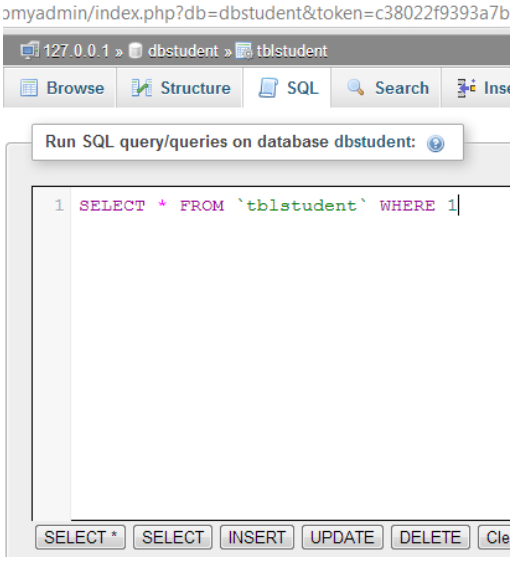
Figure 11. Entering the data



Using SQL

At this stage we can use any SQL command to query our data as seen in figure 11.

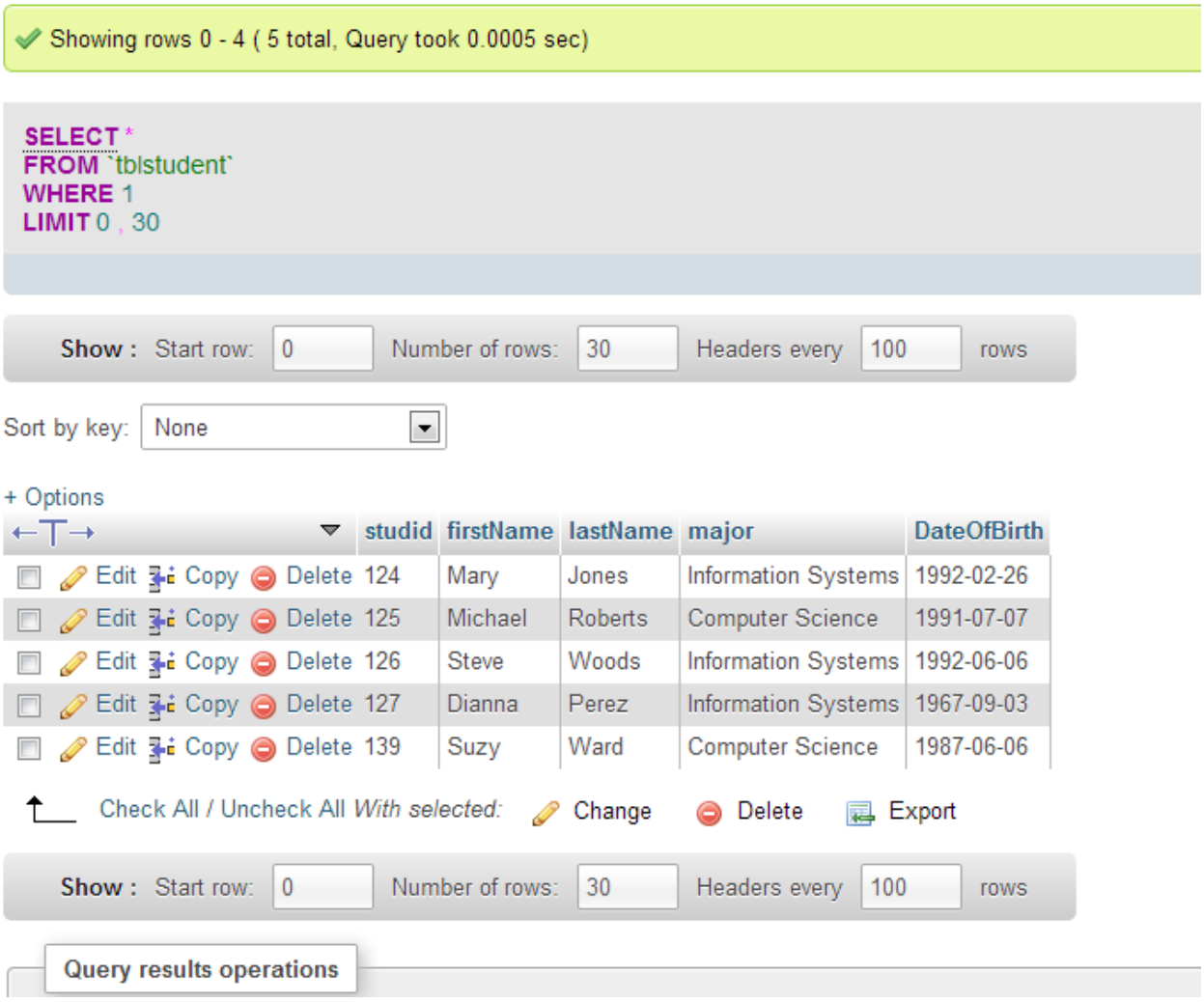
Figure 11. Using SQL commands to query the database



Viewing the results from the queries

AS seen from figure 12, we can view the results with the ability of changing, deleting, or exporting our data.

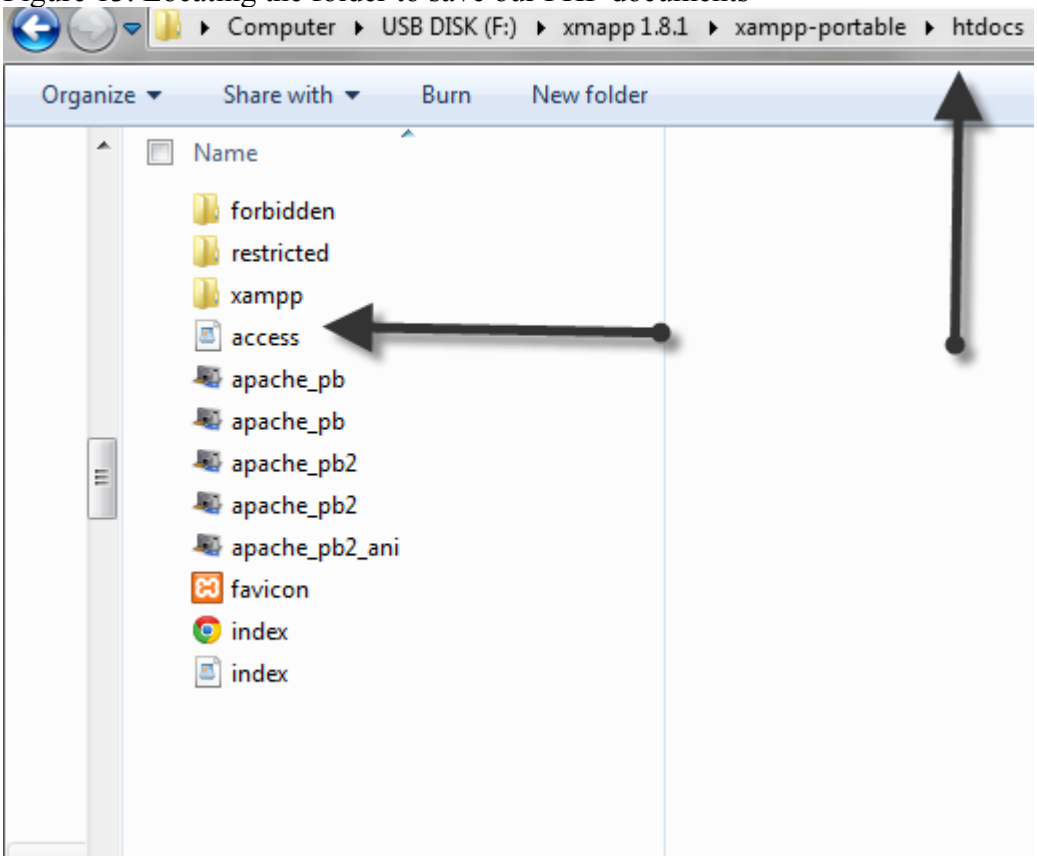
Figure 12. Displaying the results from a query



Writing a PHP file to access the data

At this stage, we need to go back to the folder we created when we downloaded XAMPP package. All our PHP scripts must be saved to a specific folder by the name "htdocs." The path to the folder is jump_drive:xampp 1.8.1/xampp-portable/htdocs as seen in figure 13. We can create other folders within "htdocs" to organize our files to access different databases. We access these files relatively or absolutely in our websites.

Figure 13. Locating the folder to save our PHP documents



The following code is a typical PHP file to access the data from the database. The statement in Line six connects to the database. We should remind the user that the connection is not secured. As we see from line six, there is no password associated with the connection. Once we connect to the database, we select the database by name as seen in line seven. If the connection is successful, we will be notified as stated in line eight. The remaining PHP statements will allow us to query the table in the database. The result of the query will be stored in $result. Later, we will use while loop to fetch the records one row at a time from $result. The code will display the data in a tabular format.

```
1  <html>
2  <body>
3  <?php
4
5
6  mysql_connect("localhost","root","") or die(mysql_error());
7  mysql_select_db("dbStudent") or die(mysql_error());
8  echo "Connected to Database";
9
10  $query =  "SELECT * from tblStudent"  ;
11
12
13  $result = mysql_query($query);
14
15
16  echo "<table border='5'>";
17  echo "<tr><th width = 120>Student id</th><th width 120>First Name</th>";
18  echo "<th width = 120>Last Name</th>;
19  echo "<th width = 200>Major</th><th width = 200>Date of Birth</th></tr>";
20
21  while( $record = mysql_fetch_assoc($result)){
22
23     echo "<tr>";
24     echo "<td >".$record['studid']."</td>";
25     echo "<td>".$record['firstName']."</td>";
26     echo "<td>".$record['lastName']."</td>";
27     echo "<td>".$record['major']."</td>";
28     echo "<td align='right'>".$record['DateOfBirth']."</td>";
29
30     echo "</tr>";
31          }
32
33     echo "<br/><br/>";
34  echo  "</table>";
35
36  ?>
37  </body>
38  </html>
```

Showing the result

Figure 14 show the result from the PHP code. It shows that the PHP scripted successfully retrieved and formatted the data according to the imbedded HTML tags.

Figure 14. Result from the database to be displayed in a page in a website

Connected to Database

Student id	First Name	Last Name	Major	Date of Birth
124	Mary	Jones	Information Systems	1992-02-26
125	Michael	Roberts	Computer Science	1991-07-07
126	Steve	Woods	Information Systems	1992-06-06
127	Dianna	Perez	Information Systems	1967-09-03
139	Suzy	Ward	Computer Science	1987-06-06

Development of a Security Awareness Program to Reduce Security Breaches and Virus Outbreaks

Michael R. Lehrfeld
Jack Ramsey, Jessica Burnside, Nathan Bordelon, Mackenzie Hazelwood, Kenneth Loveday
Department of Computing
East Tennessee State University
Johnson City, TN 37614
423-539-6952
Lehrfeld@etsu.edu

Abstract

This paper will investigate the development of white papers and short 3-5 minute security awareness training videos that are targeted at the local community to determine their effectiveness in decreasing security breaches at work. East Tennessee State University, like many organizations, is looking for security controls to decrease the number and severity of computer virus outbreaks across campus. Traditional virus software has not eliminated viruses, or even caught all of the infestations. Many of the viruses brought onto campus originate from poor or misinformed decisions made by users on machines at home as well as at work.

To combat this issue, ETSU is launching a security awareness training initiative that targets the local community in addition to ETSU faculty and staff. The hypothesis of this project is that, by training our target audience about safe computing practices, this process will provide benefits at home and at work. This would result in a decrease in virus outbreaks and ultimately lead to a safer, more secure, community computing environment.

During the spring semester, a pilot program was started, charged with creating short security awareness videos and accompanying white papers that focused on common computing tasks. The videos are generally 3-5 minutes long and directly relate to a single security idea and how it benefits a user to practice the concept discussed. The white papers provide more detail and provide additional links for more information. The metric that will be used to gauge the program's success will be helpdesk call volume, specifically those calls that can be traced back to a virus or Internet surfing activity.

Introduction

East Tennessee State University is a regional state university which enrolls over 15,000 students per term. The university started keeping accurate university-wide statistics on helpdesk tickets in 2003. Of particular interest to this study was the helpdesk categorization *spyware*. Within the confines of ETSU, the spyware categorization is used when a technician is dispatched on a trouble ticket because of a user issue with either a poor performing computing resource or an actual overt virus or malware activity present on a machine, and the root cause can be tracked back to some type of malware. Using an average hourly rate of $26.25 as a basis of cost for IT resources, it was discovered that the university was spending over $15,000/year on virus and spyware removal. This number does not take into account

productivity loss or security breaches of sensitive information, which, in general, doubles the average to $30,000/year.

Since 2003, the university has employed active virus scanning technologies at a considerable expense and there are still incidences of spyware and lost productivity. This study was initiated to evaluate complementary measures that would aid in mitigating the spyware problem. Even minor improvements in spyware detection/avoidance would potentially yield large financial savings and the ability to reallocate IT resources to more productive activities.

The current helpdesk process currently used at ETSU does not accurately document the root cause of spyware/virus related tickets. To get a better picture of potentially how the spyware gets on the victims' machines, an informal conversation was conducted with helpdesk technicians. A strong consensus emerged during the conversation, blaming most infestations on a general lack of victims' understanding and adherence to proper safe computing hygiene. The discussion subsequently focused on development of an effective vehicle to deliver essential training in a meaningful way that would be well received at all levels of technical expertise.

Many security awareness programs exist within the government, academia, and private industry. The SANS Institute's Security the Human [1] initiative is a comprehensive program that can be purchased and has excellent content. Many local large companies have security awareness programs that focus on their particular view of security and how it applies to their environment. All of these initiatives meet needs that are specific to a particular security setting. As an academic institution, we wanted to investigate a version of security awareness training that could be consumed by the community as a public service and track its effectiveness back to a specific environment. The seed of this delivery model is in direct relation to the lack of participant buy-in associated with the framework of other in-service training efforts that are generally regarded as tedious and self-evident: mainly sexual harassment, safety, and other yearly models.

Providing security awareness training for the community would have to take the shape of 1) something non-technical, 2) immediately applicable in the users computing experience, and 3) provide for timely information. To achieve these goals, the traditional yearly model had to be abandoned. As a pilot program, five computing topics were selected and white papers and training videos were created for these five topics. The selected topics were *Staying Safe on Facebook, Twitter Security, Staying Safe on Google Docs and Drive, Using Online Banking Safely, and LinkedIn Safety*.

The remainder of this paper will discuss how a computer security awareness program was developed along with a discussion of the materials developed and the delivery process that was used to start the long journey of educating the local community on safe computing hygiene.

White Paper Topics

The development of white papers outlining safe use practices centered on the idea that these documents and training should be understandable, usable, practical, and timely for non-technical users. The five areas that were selected were chosen by perceived frequency of use by the general public as well as familiarity with the topics [2]. Future technologies, such as Pinterest and Flickr, may be developed at a future date.

Safety on Facebook

Facebook.com is a very popular social networking site that launched in 2004. At the time of this writing, it boasts more than 1 billion users, whom ½ are mobile. Facebook enables users to connect with friends, acquaintances, and businesses and share ideas and pictures. Additionally, Facebook accounts can be used for authentication for other non-Facebook sites. Because of its widespread adoption and use, the following section will discuss some of the highlights for staying safe on Facebook.

Facebook Account Creation

The signup process at Facebook is fairly straight forward; but there are some areas of concern where users can expose more information than intended. During the signup process, Facebook asks for your email user ID and password. Facebook will then log into your email account, copy all of your contact information, and email your contacts about you joining Facebook (Figure 1).

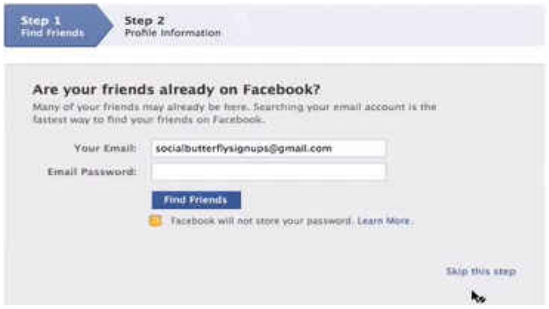


Figure . Facebook asking a user for their email account credentials.

Facebook Privacy Settings

Facebook has recently implemented a fine grained approach for security and privacy settings on user accounts. The white paper for Facebook focused on how to limit the accidental sharing of private information. Examples of this are private email addresses, birthday, gender, and location services.

Coupled with privacy settings is the capability of blocking what information a user sees within their Facebook wall; i.e. the Facebook mechanism for displaying a user's information intermingled with information from friends. Users have control over blocking a particular user, blocking invites, as well as blocking applications (games) that some users automatically post. These settings are discussed in greater detail in the Facebook white paper.

Facebook also includes functionality that enables it to be utilized as a single-sign-on repository with third party applications. For example, a user can log into Hulu.com using their Facebook credentials. Though branded as a convenience, this is not a recommended practice. A couple of issues are presented with this model. Use of this option grants the third party application privileges to post information about the user publicly without his or her consent. The third party site may also lack robust security, which would jeopardize the user's Facebook account in the event of a data breach.

Overall, Facebook has a high degree of flexibility concerning security and privacy settings, though it has been demonstrated repeatedly that subscribers must be diligent in ensuring that their desired security levels are maintained.

Twitter Security

Twitter.com is a social networking site that facilitates the transmission of micro blogs to a user's followers. Twitter takes a different approach to security and privacy. Initially, the model was intended to allow anyone to read a user's tweets (a short transmission of up to 140 characters). Privacy settings have subsequently been introduced, however. As Twitter is not designed as a Facebook competitor, users do not have large collections of data stored on the site or use single-sign-on capabilities like Facebook. Users publish *tweets* about something they are currently experiencing; and by design they are less than 140 characters.

Location Services

The majority of tweets that are sent use mobile device platforms as their access method – either smartphones or tablets. As many of these devices come equipped with GPS capabilities, the location of the tweet can be captured by Twitter. Fortunately, Twitter's default configuration is to have this feature turned off. However, this policy could change and users would then be responsible for managing it.

Twitter makes it very easy to click through the location information in a tweet and locate it on a Google Map (Figure 2). Users should be conscious of the potential dangers associated with publicly disclosing their location and movements. The criminal element could potentially make use of this information to facilitate crimes including burglary, stalking, and harassment in the real world as a result of indiscriminate disclosure of one's movements. Enabling and disabling location services are available through Twitter's settings, which are represented by a 'cog' icon on the Twitter page.

Figure . Tweet with location services enabled.

Staying Safe on Google Docs and Drive

The third white paper topic is Google's Drive cloud storage locker services. Google has merged Google Docs into the Google Drive and now provides 5 gigabytes of free online storage. This tool is particularly popular with college students. The document collaboration tools enable students to quickly share and create documents and presentations when working on team projects or preparing for exams. The white paper focuses on proper procedures for sharing information that is stored with the service. At issue is the accidental sharing of information with unintended groups.

Google Drive sharing implements a three-option interface – *Public on the web*, *Anyone with the link*, and *Private*. Users can easily misinterpret the meanings these settings. Both "Public on the web" and "Anyone with the link" are accessible to anyone on the internet. The difference between the two lies in whether Google indexes the document or not. The *Public* setting allows Google to index the document whereas *Anyone with a link* does not. The latter is available to anyone who has the link to the document. Sharing of the link has no restrictions tied to it that the user can control. *Private* allows the user to invite other people to see or edit the document.

When a user is given access to a document, three additional settings are available – *Can edit*, *Can comment*, and *Can view*. These settings are straightforward. The document owner can allow others to modify a document, leave comments only, or view the document only, respectively.

The ambiguous nature of Google's sharing options may lead a document owner to unintentionally share information. The most important take-away is that both *Public on the web* and *Anyone with the link* allow uncontrolled access to the document. In a group project setting or an academic experience, a misconfiguration may lead to potential issues with information being made available to unintended groups.

LinkedIn

LinkedIn is another popular social networking site that is similar to Facebook but is intended for a more professional setting. LinkedIn users can post business related personal information, current and past job information, and host online resumes that are searchable by recruiters or employers. It is important to note that there is little personal picture posting, musing, or games as is common with Facebook.

As with other social networking sites, the most prominent security issue is oversharing of information. LinkedIn is billed as a professional social networking site, so it is even more important that users ensure their posts do not contain too much personal information. Topics such as vacations and relationship status should not be posted.

Over-connecting can also pose security problems. For example, if a user posts that they are looking for a job while they are currently employed and the employer sees this information the user may face sanctions at work. To compound this issue, LinkedIn's privacy settings are not straightforward. As a result, users may not know exactly what is being shared and with whom it is being shared. Concepts such as 'second-tier connections' can lead to confusion or simple misunderstanding with regard to what information is available to whom.

Oversharing information can lead to targeted cyber-attacks such as spear phishing, sending fake emails designed to trick victims into revealing personal information and/or inadvertently downloading malware to their computers. Another issue is password reuse. In 2012, LinkedIn suffered a major security breach in which over 6 million password hashes were stolen. If these passwords were compromised an attacker could use them to exploit users who reused the same password at their place of business or other venues [3].

Online Banking

The final white paper produced for this project was the examination of safe computing practices for online banking. The approach for this particular paper discussed six best practices that users can employ when banking online. The major points addressed were:

- Ensure that the operating system and all applications are running the latest versions,
- Be wary of any email, particularly those asking for personal information (spear phishing),
- Use strong passwords, and limit password reuse,
- Don't bank on public networks or computers,
- Always check for a secure connect – https, and
- Use of mobile devices should be avoided.

The white paper provides further details about these six techniques and discusses current statistics about cybercrime. For example, for the 2011 calendar year, there were over 300,000 complaints to the IC3 complaint center [4] totaling a projected half a billion dollars in loss. Although not a highly technical whitepaper, the simple safe computing techniques can help to prevent users from becoming victims of banking cyber theft.

Video Creation

To accompany the whitepapers, short videos were created that highlighted safe computing practices. The video creation process had the following attributes:

- 3-5 minutes in length,
- Focused on a single idea,
- At a technical level that a beginner can understand,
- Provide value for the user at home.

Two tools were used to create the videos. Camtasia [5] was utilized for four of the videos. An online paid subscription service, powtoon.com [6] was used to create the online banking safety video. This site enabled the creation of a video with graphics and a more professional look and feel. For future videos, funding will be evaluated for more use of powtoon.com and an overall improvement of the video quality.

Currently, there are no mechanisms in place to track if users take advantage of the videos or whitepapers. They are temporally hosted on a wordpress.com site and youtube.com. The goal of this project is to eventually incorporate this information into the University's training portal. This migration would add the benefit of having an official appearance; possibly add user tracking, and the inclusion of closed captioning for videos.

Tool Evaluation and Conclusion

At the time of writing, the white papers and videos have been or will be demonstrated with two different populations; a group of computer science undergraduates and a monthly InfraGard [7] meeting, at-

tended by security professionals and students alike. The content is hosted on a WordPress site at *etsucybersafety.wordpress.com*.

Currently, there are no formal measurements for the success or failure for the security awareness training material. By the time this material is presented, more informal and formal metrics will be developed to help guide the future of the program. The primary goal thus far has been the development of the initial content as a litmus test to determine feasibility and potential effectiveness within certain economic and time constraints.

Lessons Learned

Moving this project forward will require an investment into a quality video creation tool. Two different tools are being considered; Camtasia for the desktop capture software and Powtoon.com for a more animation feel. Additionally, the creation of a system that is accessible, easy to use, and will allow for user tracking, needs to be considered. The current WordPress.com site does not allow for tight integration into the overall ETSU web design nor the adaptive accessibility that needs to be developed to reach the target audience.

The University staff and faculty are somewhat hesitant to add additional required training to an already burdensome required training regimen. The key to this security awareness training program is to add value in the user's personal lives with the hopes that those practices carry over to the work place. In this scenario, the goal is to develop modules that are short, to the point, and add immediate value, thus side-stepping the required training issue. The information is intended to be presented in a ubiquitous manner, so that it is viewed and internalized without the resistance that typically accompanies more formal, required training. Such training is necessary and has value, but it is believed that the approach utilized by this program will be more effective in this context. Readers who recall past campaigns such as "Schoolhouse Rock," or the Ad Council's Crash Test Dummy campaigns will appreciate the spirit on which this project is attempting to leverage.

Future Work

This work serves to document the initial starting point for the development of security awareness training that targets home users. Help desk ticket analysis at ETSU indicate that over $30,000/year is spent directly on spyware removal. This number does not take into consideration data lost or potentially exfiltrated from the University. An effort has been launched to break down the help desk tickets by user role and department so a targeted training effort can be implemented for those people who would most benefit from it. Additionally, data mining analysis will help target the day of the week of ticket generation and pay grade of the user.

References

[1] "SANS: IT Information Security Awareness Training." SANS: IT Information Security Awareness Training. 12 Apr. 2013 <http://www.securingthehuman.org/>.

[2] Sakamuro, Sachiko, and Karl Stolley. "Welcome to the Purdue OWL." Purdue OWL: White Papers. 12 Apr. 2013 <http://owl.english.purdue.edu/owl/resource/546/01/>.

[3] Anders, George. "LinkedIn's Password Breach Draws FBI's Attention." Forbes. 07 June 2012. Forbes Magazine. 12 Apr. 2013 http://www.forbes.com/sites/georgeanders/2012/06/07/linkedins-password-breach-draws-fbis-attention

[4] "Internet Crime Complaint Center (IC3) | Home." Internet Crime Complaint Center (IC3) | Home. 12 Apr. 2013 <http://www.ic3.gov/>.

[5] "Screen Recording & Video Editing Software." TechSmith. 12 Apr. 2013 <http://www.techsmith.com/camtasia.html>.

[6] "Make animated explainer videos and presentations!" PowToon. 12 Apr. 2013 <http://www.powtoon.com/>.

[7] InfraGard. <https://www.infragard.org/>.

Implementing an Online Employee Scheduling and Management Software

Jennifer Hughes
Kimbel Library Head of Access Services
Coastal Carolina University
Conway, SC 29528
jhughes@coastal.edu
843-349-2400

Abstract

Kimbel Library developed an online scheduling software system to manage the schedules of 100+ student assistants working in a 24 hour environment. The supervising staff contributed to the transformational design to create a fully functional employee management system complete with employee profiles, schedules, supervisor notes, and training modules.

Introduction

Coastal Carolina University administration made a decision to significantly increase the number of student assistant positions on campus in January 2009, and the library increased from 39 student workers to 119. Although most student employees worked in the Access Services Department, there were a few positions in other areas of the library. The new initiative led to the creation of new positions in all departments throughout the library. Then, in October 2009 Kimbel Library began operating on a 24/5 schedule. Student assistants were employed for varying length shifts 7:00am-2:00am and those working overnight were required to work a five hour shift from 2:00am - 7:00am.

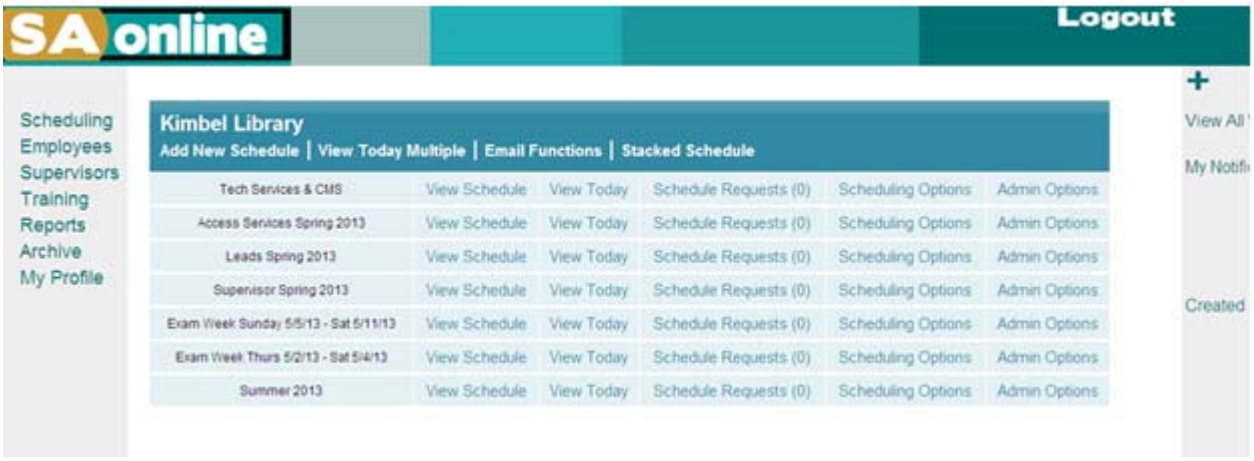
In the term "student employee", being a "student" is the priority. Therefore, student employees are allowed to request a work schedule for the duration of the semester that works around their class and extra-curricular obligations. Student shifts can be as short as 30 minutes in between classes or as long as an 8 hour day based on the students' preference. Scheduling this number of student assistants to work varying length shifts 24 hours per day in multiple departments was a tremendous amount of work for supervisors. Displaying the schedule in a readable format on a large white board also proved to be extremely challenging. It became part of the library's strategic plan to implement electronic scheduling software. There are many free and cost-based electronic scheduling software packages out there, but none quite met the library's need.

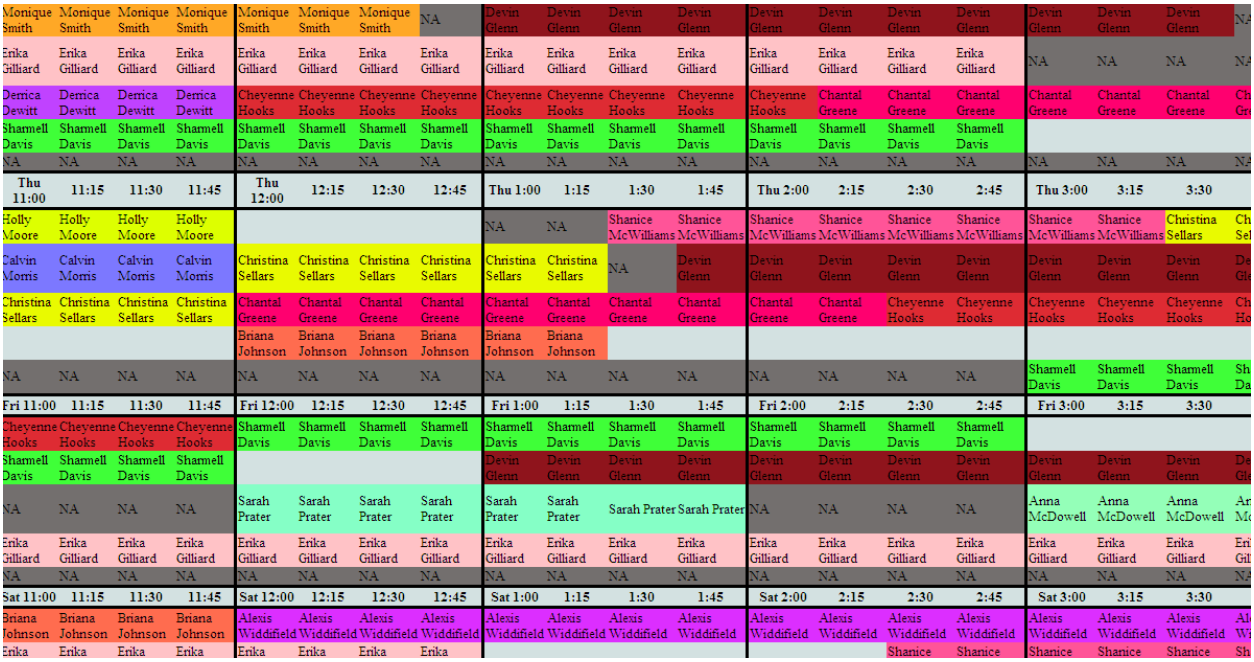
In the Access Services Department of Kimbel Library, 21 supervisors oversee the work performance of 100+ student employees 24 hours per day, 7 days per week. Supervisors are scheduled to work 1st, 2nd, or 3rd shift while student employees are scheduled to work up to 20 hours per week to cover all hours every day. These means multiple supervisors are responsible for supervising each individual student employee. There is a need for constant communication amongst supervisors to ensure consistency in training, performance monitoring, and coaching.

Coincidentally, a library specialist was hired in fall 2010 who had experience using Excel to create schedules. He also reviewed the electronic scheduling options available and found a couple shareware software packages that were close to meeting the needs of the library. Although one person was responsible for performing all the coding, all employees in the department were responsible for beta testing the software and making recommendations. The program called SA Online, and has morphed from a simple student assistant scheduling software to a complete employee management system.

SA Online Student Management Software

SA Online is designed to allow managers to make blank schedules, students request preferred hours, and managers to approve the schedule requests. At the beginning of the semester, student employees set a schedule for the normal hours to be worked each week. Using SA Online, supervisors create a blank schedule for all hours of operation and make the appropriate number of employee slots per 15 minute period. Student employees submit requests for preferred hours and supervisors approve the requests. Multiple supervisors can approve requests simultaneously, and all supervisors have access to real time data reflecting the number of hours each student employee has scheduled to prevent over/under assigning hours to an individual employee.

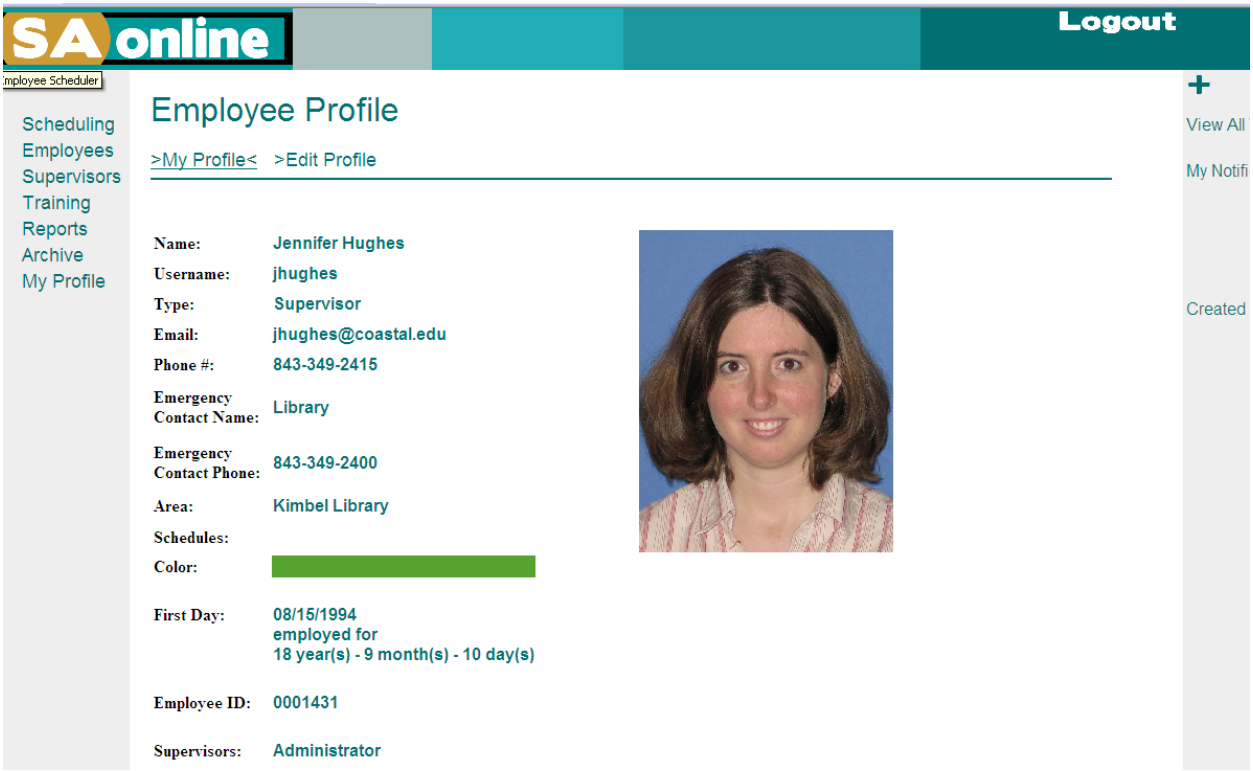




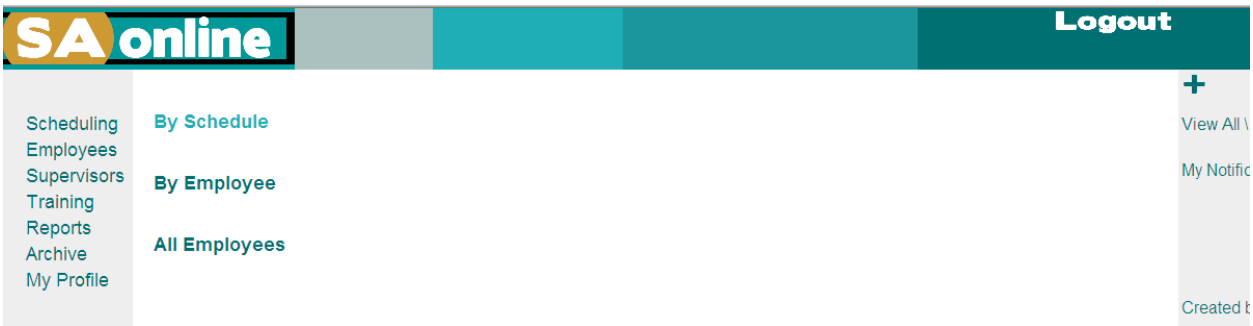
Monique Smith	Monique Smith	Monique Smith	Monique Smith	Monique Smith	Monique Smith	Monique Smith	NA	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	NA
Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	NA	NA	NA	NA
Derrica Dewitt	Derrica Dewitt	Derrica Dewitt	Derrica Dewitt	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Ch Gr
Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Chantal Greene	Chantal Greene				
NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Thu 11:00	11:15	11:30	11:45	Thu 12:00	12:15	12:30	12:45	Thu 1:00	1:15	1:30	1:45	Thu 2:00	2:15	2:30	2:45	Thu 3:00	3:15	3:30	
Holly Moore	Holly Moore	Holly Moore	Holly Moore					NA	NA	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Shanice McWilliams	Christina Sellars	Ch Se
Calvin Morris	Calvin Morris	Calvin Morris	Calvin Morris	Christina Sellars	Christina Sellars	Christina Sellars	Christina Sellars	Christina Sellars	Christina Sellars	NA	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	De Gl
Christina Sellars	Christina Sellars	Christina Sellars	Christina Sellars	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Chantal Greene	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Ch Ho
				Briana Johnson	Briana Johnson	Briana Johnson	Briana Johnson	Briana Johnson	Briana Johnson										
NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sh Da
Fri 11:00	11:15	11:30	11:45	Fri 12:00	12:15	12:30	12:45	Fri 1:00	1:15	1:30	1:45	Fri 2:00	2:15	2:30	2:45	Fri 3:00	3:15	3:30	
Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Cheyenne Hooks	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis				
Sharnell Davis	Sharnell Davis	Sharnell Davis	Sharnell Davis					Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	Devin Glenn	De Gl
NA	NA	NA	NA	Sarah Prater	Sarah Prater	Sarah Prater	Sarah Prater	Sarah Prater	Sarah Prater	Sarah Prater	Sarah Prater	NA	NA	NA	NA	Anna McDowell	Anna McDowell	Anna McDowell	An Mc
Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Erika Gilliard	Eri Gil
NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Sat 11:00	11:15	11:30	11:45	Sat 12:00	12:15	12:30	12:45	Sat 1:00	1:15	1:30	1:45	Sat 2:00	2:15	2:30	2:45	Sat 3:00	3:15	3:30	
Briana Johnson	Briana Johnson	Briana Johnson	Briana Johnson	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Alexis Widdifield	Al Wi
Erika	Erika	Erika	Erika	Erika	Erika	Erika	Erika							Shanice	Shanice	Shanice	Shanice	Shanice	Sh

What began as a solution for displaying the weekly student assistant schedule, quickly morphed into an employee management package including: employee profiles, supervisors' notes about employees, schedule adjustment forms, and training

Employee Profiles: SA Online has a complete profile for each employee including a photo, start date, university email address, primary and emergency contact information, and the designated color that highlights the student's name on the schedule.



Communication Tool: Supervisors can post a notification for all employees to see when the log in to SA Online. Also, there is email functionality that allows supervisors to send an individual or a mass group email from the system.



Supervisors' notes about employees: Because our student assistants work varying shifts it is important for all supervisors to be aware of performance issues of individual employees. Notes are stored on SA Online in an employee profile only visible to supervisors. Notes are also emailed the supervisors' alias email list, so all supervisors receive a real-time email notifying them about student employee issues. Supervisors' notes are labeled into categories: general note, call outs, praise, and notice.

> *General note*: reflects information all supervisors should know about a specific employee, but is not specifically related to the employee's work performance. General notes are considered to be neutral comments (not negative or positive). Example: The student employee's grandmother is ill in the hospital, John may need to make some last minute scheduling requests.

Call outs – Students can submit schedule changes online for requests with 24 hours notice, and records of these requests are stored in SA Online. However if a student has an unexpected need to be out at the last minute, supervisors can note the tardiness/absence as a call out. Example: The student employee called out sick today.

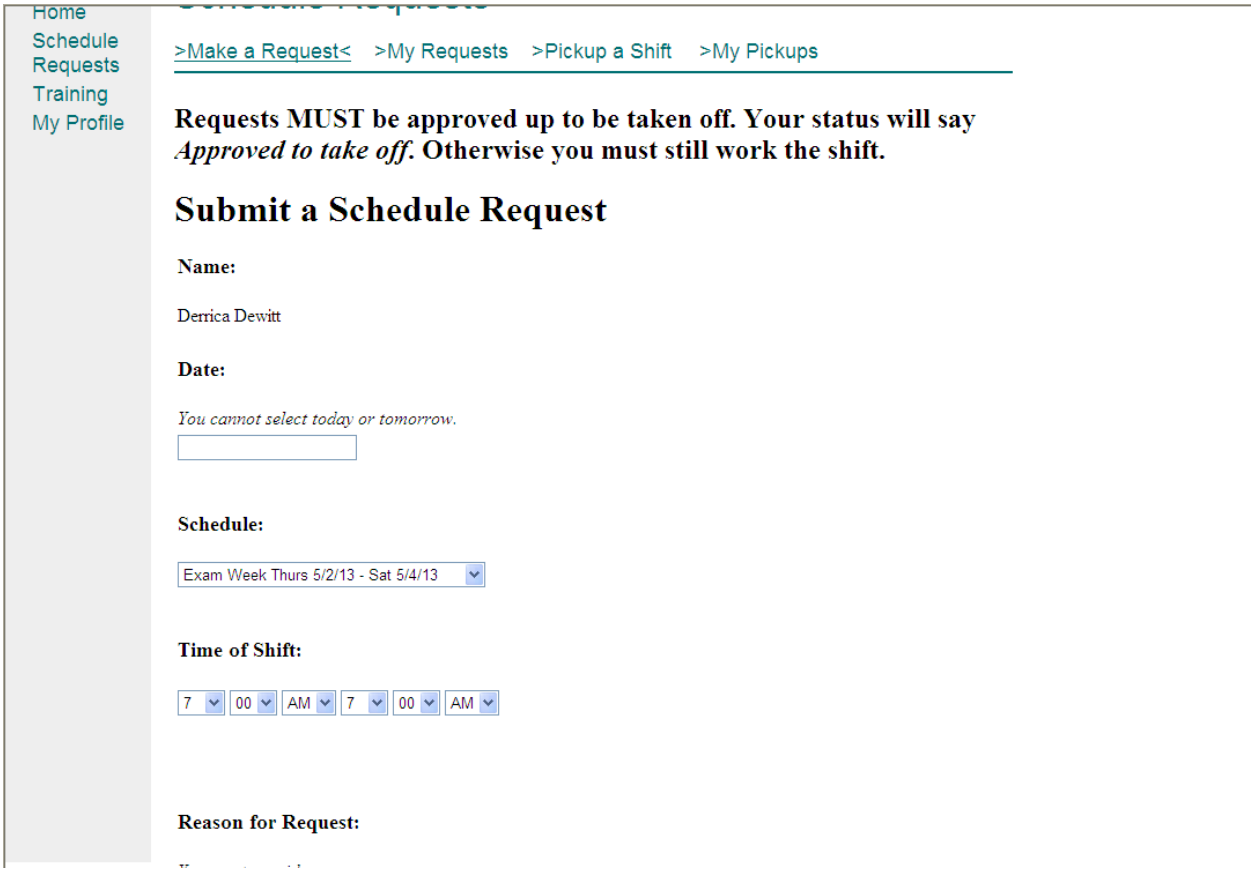
Praise: If a student assistant does something above and beyond the expectations of employment, it can be documented. Example: The student employee provided service excellence to a community user by escorting them to the other side of campus.

Notice: When an employee has multiple supervisors, it is important for all formal and informal coaching moments to be documented. A notice can be as simple as informing a student assistant of a policy or corrective action to improve performance. Examples: The student employee was wearing a baseball cap to work in violation of the university's dress code policy. The student employee was caught napping during his overnight shift.

Tue 02/12/13 4:01 PM	02/12/2013	Call Out	Called out (headache)	Full Description
Thu 01/24/13 10:48 PM	01/24/2013	General Note	Requesting time off for school	Full Description
Sun 12/02/12 4:35 PM	12/02/2012	Notice	Late for Shift	Full Description
Sun 11/25/12 6:04 PM	11/25/2012	Notice	Eating at Service Point	Full Description
Fri 03/29/13 3:20 PM	03/29/2013	General Note	Gabe out April 3 - Weds. Afternoon - Doctor Appt	Full Description
Sat 04/13/13 10:20 AM	04/13/2013	General Note	Praxis test ran over	Full Description
Sat 04/06/13 10:10 AM	04/07/2013	Call Out	Car Broken Down in NJ	Full Description
Thu 04/18/13 5:15 PM	04/18/2013	Call Out	Pink-eye	Full Description
Mon 04/15/13 10:12 AM	04/15/2013	Notice	No Call/No Show	Full Description
Mon 04/01/13 2:32 PM	04/01/2013	Call Out	Sick	Full Description
Tue 03/26/13 8:43 AM	03/26/2013	Notice	Called out for a picked up shift	Full Description
Tue 03/19/13 4:35 AM	03/19/2013	General Note	Catherine will be .25hr over 20hrs this week	Full Description
Mon 02/18/13 1:20 PM	02/18/2013	Call Out	Called Out Sick	Full Description
Sat 02/16/13 10:33 AM	02/16/2013	Praise	Working late on her day off	Full Description

Schedule adjustment requests: Throughout the semester as exceptions to the normal schedule are needed, student employees may submit electronic requests for time off of work. Using a drop down menu, supervisors have the ability to deny a request, approve the request pending pick-up by another

employee, or approve the request without having the shift picked up. All student assistants have the ability to view any shifts available to be picked up; these shifts are requested and then approved by supervisors.



Training: To ensure every student employee is fully trained and that the training is done consistently by every supervisor, training modules were added to SA Online. Student employees and supervisors are able to track the student's progress in completing each lesson. The training lesson provides background information for the supervisor preparing to teach the lesson, a copy of the training lesson in step by step format, and the learning objectives for each lesson. This format enables new and experienced supervisors to train student employees in a consistent manner during all shifts. The modules remain accessible on SA Online throughout the year so student employees can review individual lessons if needed.

Conclusion

SA Online has transformed the management of student employees at Kimbel Library. It has saved significant amounts of time, reduced communication errors, increased supervisors' knowledge of employ-

ee performance, improved consistency in supervisors' methods, and provided structure to what could easily be chaos.

The process of creating a master schedule at the beginning of the semester has been significantly reduced. What used to take a single supervisor days to complete with paper schedule requests and schedule, now allows multiple supervisors the ability to complete in just a couple of hours. The schedule is accessible to all employees and supervisors at all times. This makes it easier for supervisors at different service points to plan for coverage and task assignments, and the more conscientious student employee can ensure adequate coverage before calling in a last minute scheduling request. Allowing student employees to request schedule changes in advance, and having documentation for the employee and supervisor confirming the approval of the request has reduced communication errors and provided a much better structure for this process.

The electronic access to student employees (and supervisors) employment profile has proven to be invaluable, especially the online directory of employees' email addresses and primary (and emergency) phone numbers. In cases of unexpected building closings, for example, it has saved a great amount of time and fret having immediate access to schedules and contact information to notify employees from anywhere.

One of the best unanticipated benefits of this online management system is the documentation of student performance. In small offices where one employee works with one supervisor, it is easy for the supervisor to know what the employee's track record is and what corrective action has been taken. In a chaotic atmosphere of XXX student assistants, 21 supervisors, and 168 weekly hours of operation, it becomes an impossible task without a system like SA Online. Having email notifications sent to all supervisors notifying them of minor and major employee issues, as well as having all issues for an individual employee attached to the profile has made this type of employee management possible. One example is a habitual tardy employee; without this type of system in place, the frequency of the issue could go undetected for months.

The inclusion of training modules in SA Online had great potential for success. It was thought that including the training modules in this system would provide a one-stop-shop for everything an employee would need. Having the training information fully documented and accessible was a great start. However, in actual practice, the way it was configured does not provide the appropriate feedback to supervisors. It is difficult for supervisors to determine where new employees are in the training process, and what level of competency the employee is displaying with specific lessons. Moving forward, we will either be revamping this portion of SA Online, returning to paper documentation, or utilizing a course management system like Blackboard or Moodle.

Overall, the creation and implementation of SA Online has been wildly successful! It quickly grew from being an electronic schedule, to a full functioning employee management system. All supervisors and employees quickly bought into it, tested it, and contributed to its design. After two years of use, it is difficult to remember how the student employee program used to be managed, or imagine having that old system in place today.

Cyber Attacks and Higher Education

Gary S. Rogers
Central Washington University
grogers@cwu.edu
478-919-7960

Tina Ashford
Middle Georgia State College
tina.ashford@maconstate.edu

Robin Snyder
RobinSnyder.com
robin@robinsnyder.com

Abstract

Major Universities have always been instrumental in the research and development of new and innovative technologies and as such it only stands to reason that they would be prime targets for cyber-attacks designed to access that research. Also, a vast amount of personal information of students and faculty are gathered and stored by these institutions and such information is very useful to the criminally minded. Most higher education schools have their own networks and databases so that students and scholars can research almost anything. It is this access that, if the wrong hands get a hold of it, can cause setbacks and also a danger for everyone. And by design, they are obviously connected to the Internet. Therefore, they are highly vulnerable to attack by determined cyberattackers. How often does this occur? It is unclear, however, it is clear these attacks are increasing in both quantity and complexity. Who are these perpetrators? Well, these cyber attacks come from many sources, from individuals intent on disruption of systems for the fun and challenge of it and to increase their own ego factor and reputation among their peers, to criminals attempting to steal personal information for sale and profit, to foreign governments attempting to gain access to sensitive research and development efforts being performed by these research institutions under numerous government contracts.

There are many types of cyber-attacks that institutions of higher education need to be aware of and be able to defend against. The following is a list of the most common threats that IT departments need to protect their information assets against:

- Backdoors & Trapdoors – Often used by software developers to ensure unrestricted access to the systems they create, this method is used to gain access to a computer system, network, or specific applications.

- Bots & Botnets – This is a collection of software robots, or bots, that run automatically and usually invisibly in the background. While these terms are most often associated with malicious software and attacks, it can also refer to a computer network using distributed computing software.

- Buffer overflow – This is a specific type of coding error that enables user input to overflow the allocated storage area and corrupt a running program. Buffer overflows can cause diminished performance and even cause the system to crash.

- Denial-of-service (DoS) attacks – This attack is designed to deprive authorized individuals from accessing a system, its resources and the data it stores or processes. It is also used to disrupt the network to which computer resources are connected.

- Distributed denial-of-service (DDoS) attacks – A special type of DoS attack in which the attacker may use bots or botnets to enlist the unwilling support of other systems to launch a many-against-one attack. This type of attack is used primarily to overload the web servers of target companies or organizations in an act of cyber-activism.

- Drive-by Download attack – An attack on wireless network where content is downloaded without the users' knowledge.

- Header Manipulation – An attack against invalid HTTP header elements which can enable cross-site scripting, page hijacking, cookie manipulation and cache-poisoning.

- Man-in-the-Middle attacks – This is any attack that intercepts a network and acts as an invisible intermediary on the communications channel. Each of the devices at the endpoints thinks it is talking directly to the other, but each is actually talking to the intermediary.

- Pharming – An example of social engineering, this method uses a fake website to trick someone out of their credentials.

- Phishing – Specific to e-mail, this attack is used to trick a user into instantiating a malware-based attack.

- Ping (or ICMP) sweep – This is the use of a series of Internet Control Message Protocol (ICMP) ping messages designed to help map out a network. Usually part of the reconnaissance phase of an attack.

- Port scan – This is the examination of Transmission Control Protocol (TCP) and Universal (or User) Datagram Protocol (UDP) ports to determine which are open and what services are running.

- Replay attack – This is an attack where data is replayed through a network to reproduce a series of bogus transactions. Unless the process is interrupted, the system will be overwhelmed trying to process the stream as valid messages or can result in multiple orders of an item in e-commerce or registration systems.

- Smurf attack – Often used as a component of a Denial of Service (DoS) attack, this is a specialized version of a Ping attack where a server is flooded with spoof ping messages.

- Sniffing – This is similar to a wire-tap, except it's applied to computer networks instead of public switched telephone networks. The most popular of sniffing programs are used for password collection.

- Spear phishing – This is a form of targeted phishing where specific information is included to convince the recipient that the communication is genuine. Often directed as specific personnel in the organization or class of users, such as deans or top management.

- Spoofing – This is making data appear to have originated from another source in an attempt to hide the true origin.

- Spyware – This type of attack "spies" on users and is used to record and report on their network activities.

- SQL Injection Attacks – An attack coming from invalid user input aimed at parsers, either command, Structured Query Language (SQL), or encoding parsers. SQL is commonly used to allow interaction with the users through forms on web pages.

- SYN flood – This is a type of DoS that floods servers with a barrage of synchronize (SYN) requests, requiring the server to acknowledge (ACK) in response.

- Transitive attacks – An attack on the trust chain between machines: A trusts B, which trusts C, so C can attack A. Common examples of this type of attack include penetrating Domain Name Server (DNA) lookup services (it is assumed that a DNS server is a trusted entity) and modifying system files that provide needed resources for applications.

Washington State University

The state of Washington saw a cyber attack in 2010.[1][2][3][4] In November 5, 2010, approximately 12 minutes into the first class of the day in the newly remodeled classrooms of Todd and Sloan halls, the video projection screen automatically descended and students and teachers alike were presented with a figure dressed as V from the movie V for Vendetta who commenced to talk about... squirrels. The video "decried excessive partying at the university and lambasted "squirrels" for wanting to do nothing more than "eat, drink and breed."

The video depicted a scene from the movie "V for Vendetta," showing a masked person sitting against a red backdrop while an electronically altered voice droned on about the university's academic state. The message: "So if you have see nothing, if the crimes committed against us remain unknown to you, then I would suggest that you allow the fifth of November to pass unmarked. But if you see what I see, if you feel as I feel, and if you would seek as I seek then I ask you to stand beside me, and one year

---

1 Storm, D. (2010, November 10). V for Vendetta hacker broadcasts video at Washington State University. Retrieved from http://blogs.computerworld.com/17331/v_for_vendetta_hacker_broadcasts_video_at_washington_state_university

2 Kaya, T. (2010, November 8). Hacker makes the 5th of November one to remember. Retrieved from http://chronicle.com/blogs/wiredcampus/hacker-makes-the-fifth-of-november-one-to-remember/28076

3 Poulsen, K. (2010, November 10). V for Vendetta hacker strikes at Washington State University. Retrieved from http://www.wired.com/threatlevel/2010/11/v-for-vendetta-hacker-strikes-at-washington-state-university/

4 Polo, S. (2010, November 14). Washington State University's projectors hacked to play November 5th message. Retrieved from http://www.geekosystem.com/washington-state-university-hacker-message/

from today on lawns of this fine university we shall give the squirrels a fifth of November that shall never be forgot.""[5]

Campus security assumed that the hacker was a student, or at least somehow affiliated with WSU. What wasn't clear was how it was accomplished. Campus security carefully and thoroughly analyzed all the logs files, etc. of the serve controlling this equipment to no avail (Kaya, 2010; Storm, 2010; Poulsen, 2010; Polo, 2010). IT staff had to unplug computer hard drives to stop the video. The perpetrator was never found.

Mississippi State University

Mississippi State University is another example. In January, 2013, there was an attack against the university a Brazilian hacker. This hacker was attempting to access the information of hundreds of students. According to the Administration, on Wednesday, January 9, 2013, information related to 535 Mississippi State University individuals had been compromised by a hacker. A Brazilian hacker claimed credit for the incident. Fortunately, the Administration indicates that no sensitive data (Social Security numbers, credit card information, health information or grades) was compromised. The University stated after the fact that it separates much of this information to numerous servers, and that they constantly upgrade their security and encryption tools to prevent attacks like this one. Of course, you cannot really prevent an attack of this nature, only mitigate its effects. Total prevention can only be achieved by disconnecting form the internet.

Cambridge University & Oxford University

There were several attacks against the UK Universities of Cambridge and Oxford just this last year.[6] These attacks, however, were more successful. A single hacker was responsible for both of these intrusions, and it is thought that there are political motives behind the attacks. The attack on Cambridge disrupted their network, and the attack on Oxford resulted in access to files and databases. All of the institutions attacked have stated that they will be stepping up their security as a result of the exploited weaknesses. I believe that all of our higher education locations should work on their cyber security, as almost all of them have a network that is not as secure as it should be to handle the transmission of confidential information. As a student of a University, I would hope that all of my information is safe and secure from outside attacks. These attacks do not only have the possibility of stealing tangible items, but also of stealing our peace of mind and trust of those who are responsible for shaping our futures.

---

5 http://blog.seattlepi.com/thebigblog/2010/11/10/hacker-calls-on-wsu-students-to-take-action-against-squirrels/

6 Warrell, H. (2013, April 10). MI5 warns universities on cyber spying. Retrieved from http://www.ft.com/intl/cms/s/0/b687ae0c-a1e0-11e2-8971-00144feabdc0.html

Specifically, in February of 2012 Cambridge and Oxford Universities were both targets of cyber-attack. A hacker named Lewis Martin used denial of service attacks to bring down the websites of both of these universities for several hours. News reports indicate that these were serious attacks with the primary intent being to cause as much disruption and failure as possible. Both Universities reported about two weeks' worth of man hours were spent dealing with these attacks. Mr. Martin was subsequently arrested and charged and recently pleaded guilty to nine counts of computer related offenses.

Later that year (2012), these same two universities came under attack again by a cyberattack group who claimed to be associated with the noted Anonymous international cyberattack group. It was reported that the attack coincided with attacks on several British government websites in an effort to persuade the government to allow WikiLeaks founder Julian Assange leave the country unhampered. Oxford University reported that access was gained to a server owned by its physics dept. and that several potentially-sensitive files had been accessed. A positive from this event is that Oxford University admitted that the attack was a sign that they needed to bolster their network security.

University of Auckland

The University of Auckland in New Zealand was recently attacked. The university e-mailed 4588 past and present students that their personal information had possibly been accessed and stolen by hackers. A major issue, and a disturbing one, is that it was 10 days after the event was discovered before students were notified. A university spokesperson indicated that it was the specific server utilized for storing postgraduate enrollment applications, summer scholarship applications, doctoral research applications, and 2007 Ph.D expressions of interest, which had been successfully attacked by unknown perpetrators.

"Expert forensic analysis has been undertaken in an effort to determine the nature of any data accessed on this server," a university spokesperson said. "Unfortunately, this testing is inconclusive and while there is no evidence that the information was accessed, it cannot be ruled out." A positive is that when university staff realized what had transpired, the affected server was isolated and analyzed. Affected students were advised to "carefully monitor activities based around your identity in the unlikely event that there is an attempt by those who gained access to the server to use this information in a malicious way". The perpetrator has not been found.

University of Michigan

On October 8th, 2012 Iranian hackers took over a University of Michigan computer network during a massive cyber-attack on US financial systems. The attack then used automated malicious software to simulate hundreds of thousands of requests by customers to login to banks networks resulting in an overload of the networks, a typical denial of service strategy. The Bank of America, J P Morgan Chase, Citibank and others were the targets of the attack. Some of the Banks operations were slowed or disrupted by the attack while others were halted entirely. The University of Michigan initially denied that their network had been compromised and used in the attack

An interesting point here is that while major universities have been the target of cyber-attacks, their networks have also been used to target other entities. This is due to several reasons: First, many of

these universities are not fully secured. Second, their access to fast networks is usually present and so provides an efficient highway in which cyber attackers can conduct their attacks.

Massachusetts Institute of Technology

A frequent discussion among hacker circles is that of the notorious Aaron Swartz. Mr. Swartz was an activist for free distribution of information on the internet.[7] His main goals were to give access to everyone, regarding things that should already be accessible. For example, he felt that all public records should be freely available to all, regardless of their economic station in life.

In 2011, Aaron used the MIT campus network to download millions of journal articles from the JSTOR database, allegedly changing his laptop's IP and MAC addresses when necessary to get around blocks put in place by JSTOR and MIT and sneaking into a closet to get a faster connection to the MIT network. **JSTOR, s**hort for Journal Storage is a digital library containing digitized back issues of a wide range of academic journals. It is fairly sophisticated as it provides full-text searches of almost 2,000 journals. And, it is widely used. More than 8,000 institutions in more than 160 countries have access to JSTOR. Mr. Swartz was caught by diligent MIT security researchers and turned over to law enforcement for further action. He was charged with criminal charges with penalties up to thirty-five years in prison, most seriously for "unauthorized access" to computers under the Computer Fraud and Abuse Act. The **Computer Fraud and Abuse Act** of 1984 (CFAA) was intended to reduce cracking of computer systems and to address federal computer-related offenses. [8]The Act was approved by the U.S. Congress, signed by the President and is now codified as 18 U.S.C. § 1030. It covers cases are deemed to be in the realm of federal interest, where U.S. government computers, or those of certain financial institutions are involved, where the crime itself is interstate in nature, or where computers are used in interstate and foreign commerce.

The Act has been amended many times — in 1986, 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act. It is also being currently updated by the Obama Administration and is expected to be completed sometime in late 2013.
It states:[9]

"Subsection (b) of the Act makes it a crime not only to commit (or attempt to commit) an offense under the Act, but also to conspire to do so.

(a) Whoever--
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclo-

---

7 Wikipedia: http://en.wikipedia.org/wiki/Aaron_Swartz

8 http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

9 Legal Information Institute, Cornell University Law School. "18 USC 1030".

sure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)
(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States;
(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;
shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is--
(1)
(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(2)
(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if--
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000;
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(3)
(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
[former paragraph (4) stricken effective Oct. 11, 1996].
(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.'

Federal prosecutors eventually charged him with two counts of wire fraud and 11 violations of the Computer Fraud and Abuse Act,[10] charges carrying a cumulative maximum penalty of $1 million in fines plus 35 years in prison, asset forfeiture, restitution and supervised release.[11]

On January 11, 2013, two years after his initial arrest, Swartz was found dead in his Crown Heights, Brooklyn apartment, where he had hanged himself.[12][13]

---

10 US Attorney's Office District of Massachusetts (July 19, 2011). "Alleged Hacker Charged With Stealing Over Four Million Documents from MIT Network". Press release. Retrieved May, 2013.

11 US Attorney's Office District of Massachusetts (July 19, 2011). "Alleged Hacker Charged With Stealing Over Four Million Documents from MIT Network". Press release. Retrieved May 17, 2013.

12

How did he accomplish this feat? Mr. Swartz was going to Harvard University and had access an academic article database called JSTOR. As an open visitor to MIT, you are allowed to access JSTOR if you have an account.[14]

Dartmouth College

In July of 2004, Dartmouth College was cyber attacked.[15] The perpetrators gained access to at least eight servers, some of which contained sensitive information. It was several days before the college was aware it had been hacked. The attack centered around the installation of file sharing software on these servers. No one is exactly sure what the hacker was after, but some postulate that he was trying to get at software or games, as there is no indication that credit cards or other information seems to have been compromised/accessed. The source of the attack is unknown.

One of the issues that contributed to this attack, and one that many IT professionals have noted, is the somewhat general policy prevalent at many campuses worldwide to allow unrestricted access to the wireless network. This is not a problem by itself, but the fact the every other user on that particular internet network must put trust into others on the network that they are to be trusted. There are many activities, both legitimate and not, a user can do if they have access to an unrestricted wireless network that contains sensitive data or is connected to a network or system that does. In the particular instance of the Dartmouth wireless network, there are applications available for download which give shared access to files between users. The ease of access set up for these networks can make it incredibly easy for anyone to log onto a network, and be able to view files that contain sensitive information. This is what allowed the attacker to send out data to so many computers in such a short period of time.

Another issue related to ease of access is large multifunction printers that are all on the same network. With the sophistication associated with these printers, they often appear as capable as desktop computers in terms of security and data storage. With the continuity in user logon information from users to printer/copier access, they pose themselves as an easy target to access printed information, or simply

---

[1] Thomas, Owen (January 12, 2013). "Family of Aaron Swartz Blames MIT, Prosecutors For His Death". Business Insider. Retrieved May 12, 2013.

13 [1] http://business.time.com/2013/01/13/tech-prodigy-and-internet-activist-aaron-swartz-commits-suicide/ Retrieved May 14, 2013.

14 [1] http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2, Retrieved May 14, 2013.

15 [1] dujs.dartmouth.edu/fall-2009/cyber-attacks-on-the-dartmouth-college-network#.UXrRFLXCaSo

halt use of the printer, which would most likely cause an unwanted disturbance due to the large dependency on printers and copiers on a college campus.

Kirkwood Community College

Another example of a cyber-attack on a college would be what happened to Kirkwood Community College in Iowa.[1617] Hackers originating from an international IP address managed to breach the community college's website and steal archived application data going back almost a decade. This sensitive information consisted of applicant names, birthdates, demographic data, contact information and social security numbers.

Kirkwood Community College listed the following actions as the steps it took once it was discovered there was a breach of their systems:

- "The college immediately took down Kirkwood.edu until the suspicious activity could be isolated. This allowed the college to revoke the unauthorized access quickly.

- The college took action to correct the breach and prevent further unauthorized access to individuals' personal information.

- The college notified local and federal law enforcement. Together we were able to identify the international IP address responsible for the attack.

- The college has engaged a leading firm specializing in data breaches and forensic analysis to assist in the investigation. These steps have helped to fortify the system."

Conclusion

Imagine a leading engineer specializing in stealth metallurgy who has been researching and storing all of his/her research and experiments for past decade in hundreds of documents and associated graphs, etc. files on his computer. Now imagine a rival company from another country hacking into this computer and not only stealing all of the information, but also destroying it when they are done. This could be a rival company in another country or even one in this country or a foreign-owned company in a hostile nation.[18] Now imagine another scenario. All students that apply to a college submit confidential

---

16 http://www.kirkwood.edu/datafaqs

17 http://www.esecurityplanet.com/hackers/kirkwood-community-college-hacked.html

18 Wagner, M. (2012, June 14). Cyber-attacks target US universities, defense contractors. Retrieved from http://www.educationalit.com/author.asp?section_id=2073&doc_id=245736

information to be considered for acceptance. Such items include birth certificates, Social Security numbers, income information, and sometimes credit card and bank account information. All of this information needs to be stored locally in case it needs to be accessed in the future by a school official or registrar. If a hacker managed to locate these files, the safety of many students could be at risk. It is attack such as this that can cause great harm to our country, and this is a primary reason that the higher ed community need to step up their security and privacy of information to prevent these losses. How? Evaluate your vulnerabilities. Identify these security holes and seal them. Apply all legitimate patches. Keep current on the leading cyberattacks and how they might negatively impact you. Never assume you are entirely secure. And, perhaps most important, remain vigilant as they truly ARE out to get you! Or, in another way, sometimes paranoia is GOOD!

Passwords, security, and Google's quest to eliminate the password using the Yubikey (and related technologies)

Robin M Snyder
RobinSnyder.com
robin@robinsnyder.com
http://www.robinsnyder.com

Abstract

The password has been an ubiquitous, but often inconvenient and insecure, cornerstone of security. This paper/session will introduce fundamental principles of security in terms of passwords, two factor authentication, key management, and Google's quest to eliminate the password using the Yubikey - a small USB dongle cryptographic device that emulates a keyboard, is portable to Windows, Linux, and Apple, and is supported by an open source back-end security system. Related to passwords, key management is a process for managing keys for encryption/decryption of sensitive data - important in the PCI (Payment Card Industry) and moving to other areas. The author has been using Yubikey technology for several years - a convenient way to automate secure passwords.

Introduction

The password is an easy way to authenticate, and works well in certain circumstances, but has known issues for which better solutions are needed. This paper/session will introduce fundamental principles of security in terms of passwords, two factor authentication, key management, and Google's quest to eliminate the password using the Yubikey - a small USB dongle cryptographic device that emulates a keyboard, is portable to Windows, Linux, and Apple, and is supported by an open source back-end security system.

Authentication

The central problem of information security is that of determining if the user is who the user claims to be. This is called the authentication problem. There are many ways to authenticate people. These ways include the following.

- What you are (e.g., DNA, fingerprint, eye retina pattern, biometrics, etc.)
- What you have (that is not part of you, e.g. ID card, token, dongle, etc.)
- What you know (e.g. password, cultural authentication, etc.)

Combinations of these methods can be used and some methods can be categorized as belonging to more than one category.

Passwords

A password is a simple what-you-know method that is often used to authenticate that the user is who the user claims to be. If the user knows the password, it is assumed that they are who they claim to be.

This is important when, for example, the server cannot see the client nor the client the server except through information channels.

A password works on the same principle as a combination lock. A combination lock typically provides 40*40*40 = 64,000 combinations. Actually, the order of the numbers in a combination lock does matter so such a lock would be better called a permutation with replacement lock. But the name of combination lock is deeply ingrained in the English language. The 64,000 combinations is a trade-off of time versus safety. Before one has tried all the combinations, one would give up or be caught trying to open the lock. If one really wants to break the lock, side-channels such as a bolt cutter, watching the user enter the combination, social engineering to get an attendant to cut the lock, etc., would be used.

As a cadet at West Point, some cadets would leave the sticker of their combination lock (for their personal item box) on the back of the lock. The order came down that it would be a punishable offense to have a combination sticker on the back of the lock since it made the personal item box not secure. My thought at the time, and since, was and is the following. Buy two combination locks with different combinations. Carefully remove each sticker and replace on the other lock. Now, each lock has a sticker on it with a combination but it is not the combination of that lock. Now, take one lock home (far away) and use the other lock on the personal item box. From the military point of view, one has violated the order and one can be punished for the offense. But the security of the lock has not diminished. Such is the nature of military rules. But in information and physical security hackers will use non-obvious (at least not obvious before-the-fact) behavior to circumvent the current implementation and rules of the system being exploited.

In contrast to combination lock security, password security allows software monitoring of the password attempts so lockout is often used. Side channels include watching the user type the password, social engineering by asking them for their password, MITM (Man in the Middle) attacks, etc. The main help desk request from users is that they lost their password and cannot get into their account. In recent years, Most sites that have online access via user accounts have some way for users to recover their password. In recent years, Apple, Amazon, etc., have had their password recovery systems broken, in various ways, via social engineering, clever exploration of dependencies, etc., so that such secure and reliable password recovery systems are not trivial to implement or operate.

The primary problem with passwords is that easy to remember passwords are easy to guess while hard to guess passwords are not easy to remember. If the password is required to be hard to guess, users will need to write down the password and some users may post the password on their monitor, under the keyboard, etc.

Here are some commonly used passwords. Hackers know have access to these lists so such passwords should not be considered secure.

password
123456
abc123
qwerty
monkey
password1

Some users will re-use the same password among several sites so that if one site is compromised, that password may work at another site.

Many such lists can be found on the Internet. Password managers can help as can devices such as the Yubikey (both to be discussed).

Note that the safety of passwords depends on the way that the password is attacked. If the attacker is first trying common passwords, then a dictionary list, then modified dictionary listsl, then exhaustive search starting with small passwords, then, for this attack, a long non-dictionary password is relatively safe. But this all depends on the method used by the attacker to determine/guess the password. It comes down to probability and keeping the attacker guessing in random mode.

Guessing Passwords

There are two ways in which passwords can be handled by the system requiring the password.

- The password can be stored, encrypted or in plain text, such that the system can recover the password.
- Hash the password using a one-way function such as SHA-1 so that the password cannot be recovered but the password can probabilistically verified (with extremely high probability).

Hashing is the preferred way to store passwords. A site that puts a limit on password size or prohibits certain characters in the password is probably storing the password as recoverable since a hash will always hash to the same size and using the same set of characters regardless of the characters used in the password.

However, sites are increasingly requiring users to maintain a minimum password length, use certain types of characters, etc., all to make it harder to guess the password.

Consider a randomly generated password with 512 bits of entropy.

- The number of seconds in a year, in bits, is about 25 bits.
- Assume that the upper bound on the number of years since the beginning of the Universe is 32,000,000,000 years which is about 35 bits.
- The number of small particles (e.g., protons, neutrons, etc.) in the known universe is estimated to be 10^80 which is about 270 bits.
- Assume we want to guess passwords for each such particle 1,000,000,000 times a second, which is about 30 bits.

To guess a password by brute force means that one must guess passwords for each particle in the known universe 1 billion times a second for the age of the universe which requires

25 + 35 + 270 + 30 bits = 360 bits

So 512 bits of password entropy would allow us to do this more than a million million million million million million times (ignoring the remaining 12 bits which is a factor of 2048) until we are

sure we have guessed the password. So 512 bits in a password makes the password essentially unbreakable. The same type of argument works for the use of RFID tags to uniquely identify any item desired without repetition.

Changing Passwords

How often should passwords be changed? Some organizations require password changes every so many days, weeks, or months. One argument goes as follows.

On the Internet, if a hacker obtains the user name and password of a user, the average time from the time of compromise to the time of exploitation is on the order of 1 minute. So, one can be more safe if one changes their password every 30 seconds.

Of course this is impractical to do manually, but is one principle of the OTP (One Time Password). One time passwords are of one of the two types.

- Time-based password change.
- Event-based password change.

In both cases, the password changes each time it is used and the cryptography of the system should make the acquisition of a sequence of such passwords not usable in determining the next password in the sequence. Time-based password changes have the problem of time zones and time drift so some allowance needs to be made at the boundary of one time to the next. The time period is on the order of 1 minute, more or less. Another trade-off is that where-as event-based one-time passwords need to be coordinated via a central location, time-based one-time passwords require only the time - but does require that one keep the device's time up-to-date in a "timely" fashion.

One time password systems can be

- hardware based or
- software based.

Any software based system is more prone to compromise since the software must be supplied to the user and can therefore be closely inspected to see how it works while hardware based password systems can be made more impervious to inspection of how the system works.

DVDs were very secure as long as the only way to play a DVD was hardware based. As soon as software playing of DVDs was introduced, and despite the security changes introduced in Windows Vista (and thereafter) to preclude pirating, a few days after the software decoding was introduced it was broken. A motivating factor of the DMCA (Digital Millenium Copyright Act) law was to help prosecute intellectual property rights violations since the introduction of software decoding makes it much easier to copy encrypted information.

Certificate-based Authentication

Certificate-based security, based on public key cryptography, is often used for the client to authenticate the server (e.g., in https security) but is not often used for the server to authenticate the client. Client based certificate security can be used but, to date, has now been used often and mostly by larger organizations (e.g., businesses, health care, government, military, etc.). The glaring weakness in certificate-based security is in the chain of certificate authorities that leads up to a collection of certificate authorities rather than to one all-knowing and all-powerful certificate authority.

Multi-factor Authentication

Passwords are one factor in authentication. More secure methods use multi-factor authentication where each factor uses a different channel for authentication. For example, a bank may send a authentication code via a phone channel in addition to an email channel or web channel.

Note that the use of multi-factors in security does not protect against the MITM (Man in the Middle) attack whereby the attacker gets between the sender and receiver (or client and server), passing the information back and forth while eavesdropping and/or actively changing the messages.

Perfect Passwords

The GRC (Gibson Research Corporation) Perfect Passwords page is at https://www.grc.com/passwords.htm. This page uses https security and has several versions of passwords.

- 64 random hexadecimal characters (0-9 and A-F)
- 63 random printable ASCII characters
- 63 random alpha-numeric characters (a-z, A-Z, 0-9)

True randomness is hard to achieve and meta-physical arguments can be made as to whether true randomness even exists. But, for practical purposes, a sequence of symbols that no one could guess could be considered random enough.

The concept of TNO (Trust No One) (i.e., not even grc.com) can be achieved by taking the random password generated at grc.com and modifying it in some way.

Since one cannot easily remember such passwords, these long random passwords are intended for computer processing such as with LastPass, the Yubikey, etc.

Perfect Paper Passwords

GRC also provides PPP (Perfect Paper Passwords) as a manual way to generate sets of passwords. The PPP page is at https://www.grc.com/ppp.htm.

Humans are not good at picking random numbers so an automated method is preferable.

Password Managers

Password managers work on the concept of providing a secure way to manage passwords that rely on the secrecy of only one. master password. Since this password manager has access to all of one's passwords, one wants to be sure that it really is secure and that someone else cannot get access to those passwords.

A popular password manager is LastPass, at https://lastpass.com/. "*LastPass is a password manager that makes web browsing easier and more secure.*". From their web site:

- EASIER: Never forget a password again and log into your sites with a single mouse click.
- EVERYWHERE: Automatically synchronizes your data: access it from anywhere at anytime.
- SAFER: Protect yourself against phishing scams, online fraud, and malware.
- SECURE: All of your data is encrypted locally on your PC - only YOU can unlock it.
- FREE: No catches or gimmicks. It's free to use on all your computers!
- MULTI-PLATFORM: Using a Mac, Windows, or Linux? LastPass works everywhere.

LastPass is free for one computer usage and $1 per month for more than one computer/phone usage. There are tutorial and explanatory videos on the site that make it easier to learn about LastPass, including using LastPass with the Yubikey.

Recently, Yubikey has partnered with LastPass (and some other vendors) to offer Yubikeys bundled with a 1 year subscription to LastPass.

Yubikey

The Yubikey, at http://www.yubikey.com, is a small USB (Universal Serial Bus) device that emulates a keyboard such that, when the finger is pressed on it's contact point, it emits a static or OTP (One Time Password). Not all characters are possible as only keyboard scan codes that are recognized by all major devices (e.g., Apple, Windows, Linux, etc.) are used. Thus, the Yubikey is portable among many different devices.

With a Yubikey, one can use a long hard-to-remember password or simply automate the repetitive entering of the same password. Or one can integrate the Yubikey into a larger security system. The Yubikey is a combination of what-you-know (anyone can determine the password) and a what-you-have (e.g., the Yubikey).

Yubikey provides software that allows individual Yukikeys to be programmed in a variety of modes.

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode

A static password includes typed passwords, randomly generated passwords, etc. A long random static password is a good choice for data drive encryption where one wants a long hard-to-guess random password. As with other modes, only scan codes recognized by all major devices are supported. These scan codes are keyboard layout agnostic, so, for example, if one is using a Dvorak keyboard layout, which is handled at the operating system layer, the Yubikey will only show/support the common scan code characters and not the Dvorak characters. In such cases, where one needs a specific password, one may need to experiment with the scan codes to find the correct way to program the Yubikey.

Here is how the Yubikey OTP works, from their web site.

> *The YubiKey One-Time Password (OTP) is generated from a secret unique to the YubiKey, a number of counters tracking usage and other elements, and a public ID which remains constant and identifies the YubiKey which generated the OTP. Just insert the YubiKey into a USB port and press the button on it to generate an OTP into any selected field.*

This feature works from a unique sequence of characters that is individually unique to each Yubikey combined with a OTP sequence of 44 characters that is then authenticated by the Yubikey authentication servers in conjunction with the intermediate application software. Yubikey publishes an API for how this works as their business model is to make revenue from selling hardware and not software or services.

Note that one could program the Yubikey in OTP mode and then protect the Yubikey with an access code and give the Yubikey to a user to use to access a resource. In such a situation, the user would not know the password and the Yubikey would be a what-you-have way to access a resource since, although one could see any given password at any given time (or in sequence) one would not know the next generated password in the sequence.

12. Google, Yubikey, and NFC

Google has declared war on the password. Despite some secrecy, it appears that Google wants to develop, with Yubikey, a ring-sized authenticator, perhaps with NFC (Near Field Communication) support, that would substitute for the Yubikey keyboard device while providing a more secure way to provide authentication for account access. Support would be built into the Chrome web browser.

In the interim, Google has developed a protocol, OATH TOTP that, with software to provide the time-based information, can interact via challenge-response to a Yubikey, version 2.2 or above, to provide authentication for GMail or Google Apps. This feature uses the challenge-response support available in newer Yubikeys. This mode avoids the requirement of an external validation server.

The Yubikey OATH support allows the Yubikey to work with systems designed with OATH - an open standard introduced by VeriSign.

Here are some features of the Yubikey NEO - a USB Yubikey with an NFC interface, from their web site.

- *Emits One Time Passwords (OTP) through both NFC and USB interfaces*

- *Mobile authentication through NFC contactless technology (NDEF type 4), works with Android, RIM, Windows Phone, Symbian*
- *Featuring Mifare Classic, for legacy physical access control systems*
- *Common Criteria certified bank grade authentication ICs*
- *CCID compliant USB token, including secure element and JavaCard. Current version limited to an OpenPGP applet.*

Here is how the Yubikey NEO works, from their web site.

> *When the YubiKey NEO is introduced to a NFC enabled mobile device, it emits an NFC NDEF tag, which triggers your browser or is handled by supporting applications. The same device can also be used on computers with USB and for physical access control.*

Key Management

Management of encryption and encryption keys is becoming an important part of the PCI (Payment Card Industry) DSS (Data Security Standard). Here is an overview of key management. Similar requirements are emerging in the health care industry and may be moving to an industry near you (e.g., higher education)

Data needs to be encrypted.

- Encryption of data on the move is handled via a certificate system and TLS/SSL (i.e., use an HTTPS connection).
- Encryption of data at rest (storage-based encryption) requires encryption keys.

For a database, there are two primary ways to encrypt data.

- Encrypt the entire database.
- Encrypt columns of tables (sometimes called cell-level encryption).

For a database server such as SQL Server (e.g., SQL Server 2008 R2 or later) with EKM (Extensible Key Management) support and MSCAPI (Microsoft Cryptographic API) can be used to encrypt the entire database in manner transparent to the applications (with less than 5% processing overhead for encryption).

Encryption keys should not be stored on the same server as the database, so encryption key management servers are needed - which can provide other services such as random number generation, database password storage (if desired), etc. Encryption key management servers need to be partitioned in the same manner as databases, meaning at least one for development and at least one for production. Since business continuity depends on having access to the encryption keys, backup/restore, fail over and redundant key servers are advisable. This could mean at least two for development and at least two for production.

Encryption key servers need to have audit logs, alarms, and active monitoring for potential issues.

There should be a separation of duties so that the people monitoring the databases are separate from the people monitoring the encryption keys. Since the databases cannot be accessed without accessing the

encryption key server, a log of database access can thus be maintained. Keys can be expired, changed, etc.

The complexity of fulfilling PCI compliance, in addition to privacy state laws that can vary from state to state, makes it advisable to use encryption key management software from a vendor recognized for PCI compliance expertise. For example, states such as Massachusetts have data encryption requirements that are more stringent than PCI requirements such make total database encryption more advisable.

Summary

This paper/session has introduced fundamental principles of security in terms of passwords, two factor authentication, key management, and Google's quest to eliminate the password using the Yubikey - a small USB dongle cryptographic device that emulates a keyboard, is portable to Windows, Linux, and Apple, and is supported by an open source back-end security system.

RFID tags and NFC (Near Field Communication) technologies, including security and privacy implications

Robin M Snyder
RobinSnyder.com
robin@robinsnyder.com
http://www.robinsnyder.com

Abstract

Whereas bar codes such as a UPC identify one of many similar objects, a RFID (Radio Frequency Identification) tag provides a way to recognize an object as a unique object at a short distance. RFID tags have found use in inventory management and other tracking situations, with associated security and privacy issues. This paper/session will present, discuss, and demonstrate bar codes, such as UPC, using bar code readers, magnetic strip cards using USB magnetic strip card readers, and serial/USB RFID readers and tags, and discuss security and privacy issues related to these technologies. The actual communication of RFID tags at a distance is part of NFC (Near Field Communication) standards, which include cell phone communication and whose workings and security and privacy implications will also be covered.

Introduction

There are many forms of input devices that can be used to identify items. These input devices often become part of a TPS (Transaction Processing System). Such devices include bar code readers, magnetic strip card readers, QR codes, RFID tags, NFC tags, etc. This paper/session will discuss and demonstrate many of these devices with comments on usage, security, etc.

The primary purpose of such devices is to avoid manually typing numbers and/or text into the computer. With the advent of newer technologies such as NFC (Near Field Communication) additional functionality can be obtained.

Check Digits

Errors are always present when entering data manually or when reading data using devices. Modern hard drives, CD's, DVD's, etc., have many sophisticated ways to detect and correct errors when reading data from drives. To help avoid read errors with input devices, such as discussed here, most numbers (and patterns, where applicable) include redundancy in the form of check digits, parity checks, etc., to identify errors.

As part of a TPS, it is always better to identify bad data as soon as possible and not let it into the system. When a credit card swipe beeps, it tells the person that the card did not read properly. This is identified by the card reader since the check digits did not match.

The old idea, used by accountants for centuries, of casting out nines is to pick out digits that sum to **9** and remove them. One can also replace two (or more) digits with the remainder left over when divided by **9**. There is about **1** chance in **9** of detecting an error.

Consider the following example: What is the remainder when both of the following numbers are divided by nine and when both together are divided by nine.

```
5427812
1584721
```

For the individual results, just cross out any two digits that add to nine.

```
5427812 / 9 --> 2
1584721 / 9 --> 1

5427812 / 9 --> 2
1584721 / 9 --> 1
-----------------
7012533 / 9 --> 3
```

One can add all of the digits and divide by nine.

```
5427812 1584721 / 9 --> 3
1584721 5427812 / 9 --> 3
```

Before spreadsheets, the method of casting out nines was used for a long time by accountants to check tables of manual calculations. The check digit (i.e., remainder when divided by nine) should be the same horizontally, vertically, and for the total.

Other check digit techniques work on similar ideas.

The ISBN (International Standard Book Number) standard, actually a collection of standards, uses base 11 in the check digit which is why that last digit may sometimes be an "X". Since the ISBN was originally often typed manually, the ISBN is designed to catch errors where digits are switched.

From a security point of view, a hacker that is guessing potential credit card numbers will use such an algorithm that accounts for check digits such that potentially valid credit card numbers are always generated.

In computer data storage such as hard drives, the PRML (Partial Response Maximum Likelihood) method is used to convert somewhat ambiguous magnetic analog signal on disk into a digital signal.

Magnetic Strips

A magnetic strip card reader reads a magnetic strip on a plastic card. Credit cards, hotel cards, etc., are typically magnetic strip cards. The hotel industry, and the security of rooms, etc., was greatly changed with the move from physical keys, which can be copied, lost, etc., to magnetic

strip cards that can be tracked, changed, etc. Often, sponsors provide advertisements on the keys so that the hotel need not even pay for the actual piece of plastic.

There are various types of magnetic strip technologies and some standardization although there are also proprietary formats and some formats that do not adhere to standards. A visualization of the magnetic areas of the strip would appear somewhat similar to a bar code.

Warning: Sites such as amazon.com will offer many low-cost magnetic strip card readers (and other types of readers). These often appear to be of Chinese origin and may have a few contrived reviews. Unless there are a large number of positive reviews, such readers often simply do not work. Even expensive readers often have no reviews and often appear to look just like the less expensive ones. Buyer beware.

The author did purchase one low cost magnetic strip card reader and it did work for some credit cards but usually not for hotel cards, which appear to use some other way, perhaps proprietary way, of encoding the information.

A few years ago, a hacker published a way (with code) to use low cost parts, including a magnetic head reader that created a recorded audio sound that was then processed with software to reveal the contents of the magnetic strip. There are also ways to encode the magnetic information on a card so one cannot assume that cards cannot be copied, reproduced, etc.

Bar Codes

A bar code reader optically reads a series of bars that represent a sequence of numbers and/or letters. There are many types of bar codes. Most bar codes have some redundancy in the form of check digits, parity checks, etc.,

A UPC code is a bar code that identifies a specific product. It is designed such that it does not matter whether the bar code is scanned in an up or down direction.

Some bar codes, such as the USPS FIM (Facing Indicator Marker) are designed to identify which side of the envelope is "up" which helps the writing recognition software.

A one dimensional bar code is a sequence of bars. Two dimensional bar codes can store more information. States such as Georgia use a two dimensional bar code in tax forms so that more information can be encoded.

A bar code has the advantage of being able to be transferred electronically, printed, and later recognized, whereas magnetic cards, RFID tags, etc., are inherently physical and cannot be downloaded. Train tickets, airline check-in information, etc., use bar codes in this manner.

Years ago, the author used a bar code reader (and manual typing when the bar code was absent) to enter the ISBN (International Standard Book Number) of a book, make an XML query to amazon.com to obtain the book information, parse the XML for title, author, etc., place the infor-

mation in an Access database, and provide references in the format desired for a written work. Such is the power of a bar code when integrated into a complete system.

QR Codes

A QR (Quick Response) (trademarked) bar code is a two dimensional bar code that can represent more information than traditional bar codes. Originally developed for the car industry, QR codes have become very popular in the past few years (after, of course, the original patent has expired and the patent owner decided not to press to exercise any patent rights). Developed in Japan, the QR code supports character sets beyond the traditional ASCII 0 to 127 or ANSI 0 to 255 - in particular the Kanji set used in Japan.

Free scanners are available for smart phones such as Android smart phones. One activates the reader application and points the phone at the QR code. It is a good idea if the reader provides information about the QR code and asks permission before doing anything with it.

Inspect any QR code and one will notice that three of the four corners are similar while one is different. This allows the scanner to determine the orientation. There are also some alignment squares within the rest of the QR code. There is a required "quiet zone" of white space outside the QR code. For the rest of the bar code, there are a variety of ways in which the same information can be expressed. The encoder will look at various ways and attempt to pick the resulting QR code that best distributes the black and white areas to, hopefully, make the QR code easier to read and decipher for the reader application.

QR codes can be a security issue in that the URL (Uniform Resource Locator) address represented by a bar code might take the user to a site that attempts to exploit some vulnerability in a browser, phone, etc., to install malware on the user's computer, phone, etc. In some cases, people have covered legitimate QR codes with codes designed to exploit this consumer behavior.

Like the bar code, the QR code is optical and can be transmitted electronically and printed - ideal for tickets, etc.

RFID

A RFID (Radio Frequency Identification) tag contains a bit pattern that uniquely identifies that tag. While a UPC code identifies a collection of similar products, an RFID tag can uniquely identify each and every instance of a product. RFID tags are useful for inventory control, tracking, etc. Why is this possible. Consider an RFID tag with 512 bits of information.

- The number of seconds in a year, in bits, is about 25 bits.
- Assume that the upper bound on the number of years since the beginning of the Universe is 32,000,000,000 years which is about 35 bits.
- The number of small particles (e.g., protons, neutrons, etc.) in the known universe is estimated to be 10^80 which is about 270 bits.
- Assume we want to change tags for each such particle 1,000,000,000 times a second, which is about 30 bits.

To change tags for each particle in the known universe 1 billion times a second for the age of the universe requires

```
25 + 35 + 270 + 30 bits = 360 bits
```

So 512 bits would allow us to do this more than a million million million million million million million times (ignoring the remaining 12 bits which is a factor of 2048). So 512 bits in an RFID tag is sufficient to represent anything desired without concern about repetition. The same type of argument works for the security of randomly generated passwords (i.e., assuming 512 bits of entropy in the randomly generated password).

In general, a RFID reader emits a frequency which the RFID tag can use to power itself (unless it has a battery in which case the battery would eventually lose power) and send back a lower powered signal with the information encoded on it. While a bar code is optical and line of sight, an RFID tag works via electromagnetic waves over the distance of a few yards.

A passive tag only provides a pre-determined message. Some passive tags can be programmed.

An active tag may allow information to be programmed, changed, etc. Security becomes more of an issue with such tags.

There are many forms of RFID tags. RFID tags can be made small enough to be implanted under the skin. This has been done in animals for many years and in some humans, with permission. The privacy implications are obvious and often debated by privacy advocates.

Consider inventory control. Whereas an ISBN identifies a specific edition of a book, an RFID tag attached to a book uniquely identifies that book. Give a collection of books in a library and the matching database, an inventory of that library could be done by walking through the library with reader and associated software and database. In addition to inventory, such a walk could help identify books that are substantially out of place in the library.

Such monitoring methods using RFID chips, whose cost has consistently dropped over time, can help in areas such as medicine, where each and every instance of a medicine bottle could be monitored. In stores, inventory control may also help with theft management, including theft by employees, since it is estimated that 80% of theft comes from inside the organization and not from outside the organization.

While an RFID tag might uniquely identify a person it is also possible to indirectly identify a person in much the same way that a cookie on a computer can be used to identify a person. The cookie actually identifies the computer/device (or browser on the computer/device). For example, suppose that RFID tags are (and have been) embedded in tires. Suppose that a RFID reader is in a position to record the tags on tires passing by the reader. If the tires can be linked to a vehicle (and tires rarely change vehicles, in a manner similar to cookies) and that vehicle (as in a computer/device) can be linked to the primary driver of the car, then one can identify the location of a person, with high probability, in the same manner that a cookie might identify a person though their computer. There exist low cost camera systems (on the order of $10,000) that,

properly positioned, can identify license plates on cars. As part of a system, RFID then allows such invasion of privacy. The same analogy can be used for RFID tags embedded in clothes, etc. Once the unique code emitted by an RFID tag is matched to that object, that object can be tracked, and, implicitly, any object attached or connected to the object being tracked. Some day, those truckers whose tires blow out and who then leave their tire pieces on the road to later cause an accident, may be held accountable for such incidents. It only takes a few to get caught and prosecuted to motivate other truckers to responsibly pick up the traffic obstructions that they create.

While many RFID readers are quite expensive, there are low cost RFID kits, such as those from Parallax, that provide a RFID Reader USB and Tag Sampler Set. Such kits typically work via free and readily available serial port software and/or USB to serial links, again readily available. The range is limited, but one can experiment with RFID at a low cost.

Many running (and other) races have, for years, used RFID technology to determine when a runner has crossed the start line, crossed the finish line, and, for bigger races, crossed intermediate points (to provide split times, monitor cheating, etc.). Such small lightweight chips are typically attached to the runner's shoe so that it is close to the reader being used to record the crossings. In some races, such identification allows an announcer at the finish line to congratulate, publicly, over the speaker system, runners as they finish the race.

RFID tags can be printed in a thin label form for use in books, etc.

In addition to privacy issues of RFID tags, security issues can arise even in passive tags in the sense that RFID tags could be spoofed since it always yields its numerical code when interrogated using known specs. Thus one can learn what a given RFID tag returns and then attempt to mimic (i.e., spoof) that tag elsewhere.

Active tags can provide more security, but, as in the case of passports, there are special cases that can be obtained to hide the RFID signal when it is not desired to provide that signal.

NFC

NFC (Near Field Communication) that uses the near electromagnetic field, as opposed to the far electromagnetic field (terms coined by Maxwell of Maxwell equation fame from the late 1800's). Such near fields are short range and low power. One can think of the NFC as designed to replace the wires and connections of a smart card in the same manner as Wi-Fi was designed to replace the wires of a wired network, BlueTooth was designed to replace speaker/phone wire, etc. Wires are expensive to create, configure, and maintain, while wireless avoids many of the hassles of physical wiring. But, just as in 1900 when Marconi's wireless communications devices allowed governments to communicate at a distance, it also means that anyone listening can also hear what is being said. In such cases, encryption, security, etc., becomes much more important.

Devices such as the Verizon Droid Razor HD Android smart phone and the Google Nexus 7 Android tablet have NFC built-in. It is not on by default. Like the GPS, one should probably keep it

turned off except when it is needed and then turned off again. This both increases security and saves power on the device.

NFC works at a range of up to 10 centimeters with a typical range of 1 inch so that, with NFC enabled, one can touch phone to phone, tablet to tablet, phone to tag, tablet to tag, etc., in order to initiate the exchange of information between the devices. This transfer may be one way or both ways depending on the software. One does not have to actually touch devices but due to the short range, it is often easier just to touch devices rather than get them sufficiently close.

From a security point of view, despite the range of 10 centimeters it is possible to create highly sensitive receivers that can detect an NFC signal at greater ranges, possible 1 meter for unpowered NFC chips and 10 meters for powered NFC chips. Consider, for example, when it was discovered that a Prlngles Potato Chip can could be fashioned into a highly sensitive Wi-Fi receiver. At any point in time, someone may discover an easy way to create a sensitive receiver that then diminishes the security of a transmission method that relies, in part, on it only being a short-range signal.

The NFC transfer is bi-directional but since NFC tags/chips can act in unpowered mode, NFC tags can be used to achieve the same functionality as RFID tags, albeit with a smaller connection range. Current chips can store up to 4KB, depending on the chip. NFC protocol can detect and handle collisions (not the touch collision, but multiple devices) but due to the short range such electronic collisions are not very likely in practice.

Users can store sensitive payment information in Google Wallet and then, via NFC software on the phone and terminal, use such credentials to transfer payment information.

NFC can make establishing Bluetooth and/or Wi-Fi connections easier and, due to the short range involved, more secure.

The security implications are obvious. How does one know with whom one is sharing information. And, as with QR codes, obtaining information via NFC and then, for example, visiting that site, or downloading information/software, has the same security implications. For some security, as in RFID chips, there are special low-cost envelopes that can keep the NFC signal from penetrating either way.

For smart phone or tablet usage (e.g., Android phones/tablets), NFC tags are readily available. With appropriate software one can touch the phone/tablet to the tag to initiate actions based on that tag. Such actions might be no turn an application on or off. For example, when leaving/returning from one's home, one could place and program NFC tags so that one could take actions such as turning off/on Wi-Fi, turning things on/off in the house, etc.

One interesting and fun application of NFC tags would be to create a scavenger hunt using NFC tags whereby each tag, via software and web server connection, would provide a hint to the next tag, etc.

A security concern for NFC, typical for new technologies, is that some of the neat technology, such as opening web pages, doing transfers, etc., may be enabled by default by the manufacturer of the phone, phone operating system, etc. This is typically a recipe for security exploitation.

Small low-powered devices such as NFC have motivated research into cryptography techniques such as ECC (Elliptic Curve Cryptography). ECC uses simple integer arithmetic while typical RSA cryptography requires more spohisticated and more involved computations, both taking time and, more importantly for NFC, power.

Summary

This paper/session has discussed and/or demonstrated many devices such as bar code readers, magnetic strip card readers, QR codes, RFID tags, NFC tags, etc., with comments on usage, security, etc.

References

Coskun, V. and Ok, K. and Ozdenizci, B. (2013). Professional NFC Application Development for Android. Wiley.

Igoe, T. (2012). Getting Started With RFID. Oreilly & Associates Incorporated.

Patrick J. Sweeney, II and Sweeney, P.J. (2005). RFID For Dummies. Wiley.

Virtualization in the Distance Education Class

Dewey A. Swanson
Associate Professor, C&IT
Purdue University
College of Technology at Columbus
dswanson@purdue.edu
(812) 348-2039

Abstract

Purdue's Statewide Technology program offers the Computer and Information Technology degree at several locations throughout the state of Indiana. With tighter budgets and fewer faculty, it is difficult to deliver a Bachelor of Science degree at each location. Statewide faculty reviewed the curriculum to determine the most appropriate classes to offer through distance education. By offering more of the classes via distance it is easier to share faculty expertise throughout the state. The classes being offered online for the most part do not involve the use of labs. We plan to attempt to offer a few lab based classes via distance and evaluate their viability. In the past I have taught hybrid classes where the lab component was completed at home. Success has been hit and miss depending upon the class. Classes using common products like Microsoft Office tools have worked well, whereas ones using the Oracle DBMS have typically run into glitches. I plan to offer our CNIT 487 Database Administration class using Oracle 11g database via distance and incorporating virtualization software to assist in delivering the lab component. In this paper I will review the use of virtualization in the classroom and expand on what we have learned as we plan to offer the CNIT 487 in the next school year.

Introduction

Purdue University's Computer and Information Technology (CIT) degree is offered at the main campus in West Lafayette, IN and at two other locations, Columbus and Kokomo. CIT classes are also offered at the statewide location in Anderson although the degree is not offered at that site. The curriculum is the same at the regional campuses as on the main campus. There are approximately 400 students and 31 faculty members at the main campus and at the three regional sites there are approximately 150 students and 4 faculty members. In the Computer and Information Technology Plan of Study there are sixteen CIT courses. Faculty at the Statewide locations typically teach 3-4 courses a semester. In Columbus we have gone from four to two full time faculty members. Columbus and the other regional campuses hired adjunct faculty to cover the classes in the curriculum.

Purdue and higher education in general have been under pressure to do something about the rising cost of a college education. With tighter budgets in recent years there has been pressure to hire fewer adjuncts and be more creative in delivering classes in the CIT program. Recently, Purdue froze tuition for two years as a first step to make college more affordable. All faculty and staff are being asked to look at current practices and expenditures and see where they can make changes to eliminate and consolidate efforts wherever possible. Clearly, we will be asked

to do more with fewer resources in many cases to help contain rising college expenses while still maintaining our core missions of teaching, research and engagement.

Online Classes

The question is what can we do at statewide locations to continue delivering a quality education and contain costs? In an effort to be proactive, statewide administration over the past year have asked CIT statewide faculty to review the curriculum to see what courses might be potential classes that lend themselves to distance delivery. Online classes offer potential benefits in an effort to save money and retain quality education. Most CIT classes offered at the statewide locations have excess capacity, especially the junior and senior level. From a quality standpoint, online classes would allow faculty to teach more in their expertise benefitting not only faculty but the students.

Online classes are not a new topic for CIT. The issue has come up before especially with the increased use by some of our sister departments such as Organizational Leadership and Supervision (OLS). They currently have a large offering of online classes. The statewide CIT faculty have not been opposed to online classes. However, in past discussions CIT faculty have resisted totally online classes in two areas. First, the CIT classes that occur early in the curriculum, most freshman and sophomore classes. This has not been just a CIT thought but was also supported by administration and staff. The reasoning, it is beneficial for retention to have the students on campus early in the program and build a relationship with campus life, other students and faculty in the CIT program. Our program in Columbus has been admitting more traditional students (18-22 straight out of high school) in the last few years. This seems to make even more sense. The second area where CIT statewide faculty have resisted online classes are classes that contain a lab component. The thought was that in many classes it is difficult to have an effective lab component via online learning. Besides losing the faculty-student interaction, it is difficult because students have a variety of hardware and software configurations on their own computer to deal with labs that are setup to work in campus labs. These computer labs have been specifically configured to work with the software used in the classes.

Currently, the statewide locations do offer online courses. We offer several online courses at the senior level including CNIT 405, CNIT 489 and CNIT 499. These classes involve lectures, research, discussions and writing but do not include lab components. All of these classes have been offered online for several years and have been well received. Two online classes based out of the Columbus campus are the CNIT 107 and CNIT 136 classes. Both of these are beginning classes that introduce students to Microsoft Office tools such as Word, Excel, PowerPoint and Access. Both classes are service classes provided by CIT for IUPUC's Business Department and Organizational Leadership and Supervision (OLS) students. Both classes used software provided by the textbook publishers like MyITLab, a tool provided by Pearson. These labs provide tools to give students a variety of experience using Microsoft Office tools. Students can use Microsoft Office on their home computer and simulation software for many lab components. These prompt and grade student labs in the simulated Microsoft Office environment. They also provide instructors with many tools to assist with instruction. With MyITLab the software is on the Pearson website and requires only a minimum installation on the home computer. Other than a few minor glitches this has worked pretty well for these introductory classes.

As mentioned, there are issues that need to be addressed when offering lab based classes. First, there is not the capability to be there standing over the student as he/she does the lab, answer questions and provide feedback because one student may be doing a lab at 10 a.m. on Wednesday morning and another at 2:30 a.m. on Saturday morning. This can be addressed several ways; first, by offering the lab classes later in the curriculum to a more mature and hopefully more technically savvy student. Second, by offering the student a variety of avenues for the lab: short lectures and demonstrations which are ideas used by the developers of the material in the CNIT 136 and CNIT 107 courses. Also providing avenues incorporated into some of the online classes used today such as virtual office hours, discussion boards and video conferencing software are an option.

Another issue is the software/hardware problem. One big advantage to having labs on campus is the fact that all of the machines are basically the same. The software image is created and then pushed out to all the lab machines. As an instructor you are pretty sure of what you are going to get. Yes, there may be issues but you have the IT support available to provide assistance. With students taking classes online it is impossible to control the hardware/software configurations that you will encounter and to provide individual support to the students with the current size of the IT staff. When talking to the book publishers there does not appear to be similar availability to the simulation software used in our CNIT 107 and CNIT 136 courses that use Microsoft Office simulation software for topics covered in the higher level CIT classes. These include classes in programming, networking, systems analysis and database using tools such as Visual Studio, Visio, Oracle, SQL Developer, SQL Data Modeler and languages such as SQL, C#, Java and PL/SQL. Surveying some of the more popular free online courses that are available from Khan, Education Portal, MIT, and Stanford for computer related courses did not result in significant help. Most of the computer classes were lower level or were lecture based without a lab or a significant lab component. Searching, I was able to find a few places that were dealing with the issues in a similar way, specifically at the University of Hradec Kralove in the Czech Republic and Kansas State University. Both use virtualization technology successfully.

Virtualization Technology as a Solution

Virtualization seems to be a hot topic in IT. What is a virtual computer? According to Virtualization in Education an IBM White Paper, a virtual computer is a logical representation of a computer in software. According to IBM by decoupling the physical hardware from the operating system, it allows increased utilization of the underlying physical hardware (IBM White Paper, 2007). The basic virtual technology has a host operating system and a virtual operating system that is hosted and called virtual machine and run as user level processes on the host operating system, see Figure 1. The virtual machine has no more privileges than any other user level process does.

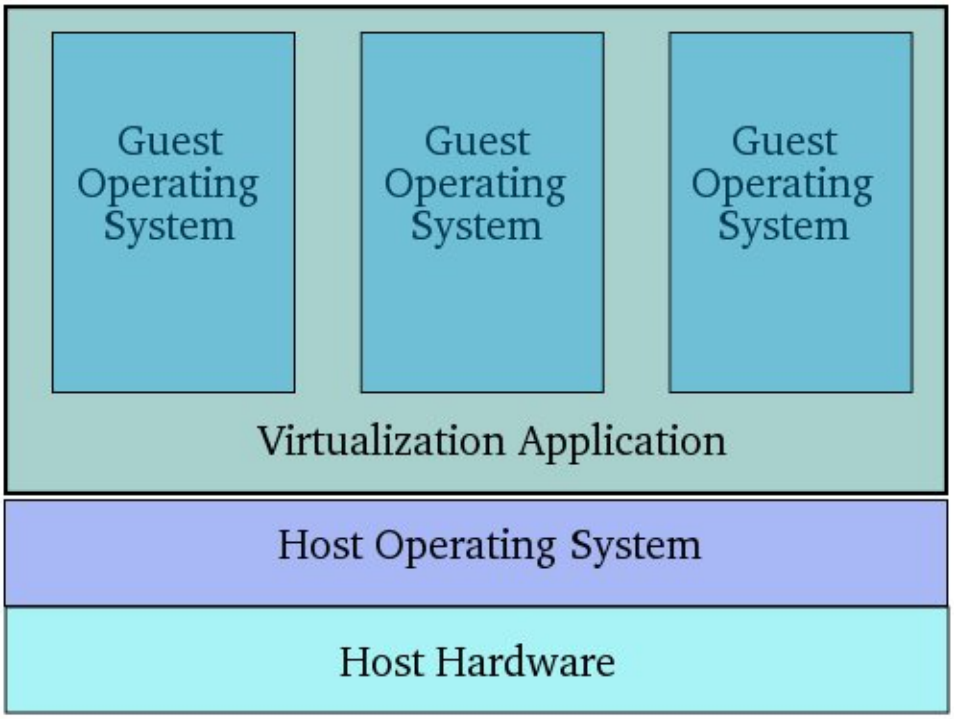


Figure 1

Virtualization is not new and it is not new to education. Many K-12 institutions and colleges are already successfully using virtualization software for purposes such as desktop virtualization or server virtualization. According to the Chronicle of Higher Education some universities are even phasing out computer labs. The idea is that it can lead to significant cost savings by having a virtualized lab instead of a physical lab on campus. With 95% of college students owning at least one computer according to CNN it is definitely possible (Watters, 2010).

The use of virtualization at Kansas State University in Salina seems very promising. They use virtualization technology in several operating systems (OS) classes including a Unix Class and a Unix Administration class (Bower, 2010). My area of expertise is database. Although at the statewide campuses we have to be a generalist because we teach several areas. My work prior to joining Purdue was in the area of application development and administration with database management systems (DBMS). In many respects operating systems are similar to database management system so the use of a virtualized environment for the lab component was promising and appealing considering my background.

CNIT 487 Database Administration

I decided that we would try to develop an online version of our CNIT 487 Database Administration class. This is a senior level class that uses Oracle RDBMS software to teach Database Administration (DBA) skills. We have offered the class at the Columbus site in the past with limited success. Previously, we have used VMware installed on lab machines, had a dedicated lab with Oracle installed on each machine, tried a hybrid approach with students completing labs on their own machines at home all with varying degrees of success. There were several issues with this class content. First, Oracle software can be resource intensive especially depending upon

how memory is configured. The second issue is that DBA activities can require the user to have some administrative privileges on the machine. This has always been an issue with our local lab support. They, with good reason are unwilling to provide students with administrative privileges on university lab machines.

The most successful attempt was using VMware in our labs. However, with the configuration students had to use the same lab for access. The problem we had was that the lab was heavily utilized by CIT classes and left little time for students to work outside the regular class hours. Finally, with VMware running Oracle on the network, response time tended to be very slow.

Based on some of the previous issues I decided to try to develop a course with the students using a virtual machine running Oracle. Virtualization software would allow students running in their own host environment to create and run Oracle in a virtual environment. The advantage this had over the last time we taught the class using a hybrid format was that each student installed the Oracle software on their own machine with different hardware and especially software configurations with the hybrid class. This time we would create the virtual machine with Oracle set up to meet the needs of the class.

Choosing a Virtual Technology

There are many virtualization products on the market today. The criteria for choosing the virtualization tool were pretty simple. First, it should be easy for the student to use. This is especially important since it is going to be an online class with support that would be limited. Second, it should be easy to maintain from an administrative perspective. IT support for virtual machines is limited as far as services they will provide, so it is important that the tool be easy to administer and maintain. Third, it should support Windows and Linux environments. Fourth, it should be capable of hosting the Oracle DBMS and its' tools. Finally, it needs to be free.

There are several products on the market that meet our criteria. Two products are of particular interest. These products are VirtualBox and VMware.

VirtualBox is a virtualization product for enterprise and home use. It has many features and touts high performance and is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number guest of operating systems including Windows, Linux, Solaris, OS/2 and OpenBSD. This product meets all of the criteria that we are looking for. Besides meeting the criteria VirtualBox is owned by the Oracle Corporation. Oracle provides several, what they term, prebuilt appliances. Basically, they have created different prebuilt virtual machines that are Linux based machines that have different Oracle databases and database tools preinstalled. They use this for DBAs and developers to try out the features and test different configurations. We determined this would be a good tool for students to use to perform the labs. Also, Oracle has a large installation base on Linux based machines. With Linux available and also being part of Oracle Academy which allows Purdue to use the software for academic purposes we have no software license issues. Using this technology the plan includes distributing the VirtualBox with the Oracle the appliance Database App Development VM that includes the following features:

- Oracle Linux 5
- Oracle Database 11***g*** Release 2 Enterprise Edition
- Oracle TimesTen In-Memory Database Cache
- Oracle XML DB
- Oracle SQL Developer
- Oracle SQL Developer Data Modeler
- Oracle Application Express 4.1
- Oracle JDeveloper

We would either distribute via Blackboard or we've had approval to purchase flash drives to distribute to students.

We originally thought flash drives would be the path we would take. However, in the past several weeks Purdue IT has offered to provide access to virtualization on their server at the main campus in West Lafayette. Originally, when we discussed this option it didn't look like it would be a consideration. The solution is that our IT department is using VMware Vsphere suite of tools.

Vsphere is a suite of tools or features for utilizing and sharing resources. At the core are server class computers with multiple processors and often 100GB or more of memory. These hosts run the ESXi hypervisor on which a large number of virtual guests are created. The computing, networking, and data storage components are managed in an environment where all of the resources are shared. The VMware vSphere Web Client and the vSphere Client are interfaces to the virtual machines. With the vSphere Web Client and the vSphere Client, the user can connect remotely to a virtual machine.

Each environment offers advantages and disadvantages. The VirtualBox environment works nicely as a standalone environment without depending on the network. The fact that Oracle has prebuilt appliances in a Linux environment would make for easy setup. Oracle has a strong Linux base that would be a good experience for the students. The possible downside would be the student's machine. VirtualBox recommends the following minimum requirements:

- At least 2GB RAM
- At least 15GB of free space (Note: VirtualBox virtualization works best with contiguous space)
- 2GHz Processor (a lesser processor will be acceptable but slower)

Although this is not outrageous it is possible that students will have the minimum requirements and find performance an issue. An upside is that we could handle classes of 15 or more students without a problem.

VMware hosted by the server on the main campus at Purdue should not have a problem with the server performance. The disadvantages to using this would be that Purdue's IT sets up the virtual machines and does so in a Windows environment. This is not a major issue but does limit options to a degree. The major disadvantage is that we would be limited to a maximum of fifteen students. IT is limiting the class size to maintain system performance.

Summary

The choice for a virtualization solution is going to be utilizing both environments. This class is testing the waters for us by adding classes with labs to our distance lineup. This will be a good opportunity in a challenging class to test both environments. That is the plan at this time. This will give students a choice to see which environment they prefer and I can monitor. If one appears to have a clear advantage we will go that route. This will also give students a chance to use Oracle in both a Linux and Windows environment.

References

Virtualization in Education (2007). IBM Global Education White Paper. Retrieved from http://www-07.ibm.com/solutions/in/education/download/Virtualization%20in%20Education.pdf

Watters, A. Virtualizing the university computer lab. (2010, August 19) Retrieved from http://readwrite.com/2010/08/19/virtualizing-the-university-co

Bower, T. (2010). Experiences with virtualization technology in education. *Journal of Computing Sciences in Colleges*, 25(7), 311-318.

Utilization of Social Networks in Teaching and Learning Process

Jamal Al Sharhan
Educational Technology Department
College of Education
P.O. Box 100566 Riyadh, 11645
Kingdom of Saudi Arabia

Abstract:

This paper explores the utilization of social network in teaching and learning process. In recent years, the internet has influence all aspect of social network including the higher education. The implementing of social network is depending on successful delivering contents by academic staff. Discourages will affects the utilization of social network by students. On the other hands, academic staff participants are not enough, and some of them are not responded to use social network in their teaching subject matters. Educators need to take a serious and wary approach to accepting claims of ensured participation social network in teaching and learning in all aspect of education. This paper indicating that the better fit of social network to the skills of an academic staff and more positive its effect on their performance with their students. However, the benefits of social network into teaching and learning process were discussed.

Presenter Bio:

Dr.Jamal Al Sharhan Professor in Educational Technology and Communications Ph.D.in Educational Technology Manchester University, United Kingdom 1990 Educational Technology Department College of Education P.O. Box 100566 Riyadh, 11645 Kingdom of Saudi Arabia Office 014674548

Technology Enhanced Mastery Approach in Quantitative Courses--With Options

Steve Anderson
Math/Computers/Decision Science
University of South Carolina Sumter
200 Miller Road
Sumter, SC 29150
(803) 938-3775
mrspacelysc@uscsumter.edu

Abstract:

Over the last three years, we have pilot studied a student-centric mastery approach in teaching two math courses, as well as developed a mechanism where a student who is ill-prepared may drop within the first 8 weeks and be enrolled in a lower level course (assuming they have not already taken it for credit) in order to "re-mediate". This has worked well on our regional USC campus in gateway non-major math courses, but the main USC campus employs a similar flow chart for their Calculus/Pre-Calculus sequence. I will actually demonstrate the software we utilize to get MORE personal with our students and have WAY MORE VISIBILITY when they become at-risk students. I will present anecdotal data demonstrating how at-risk students get identified early. We can also clearly identify whether it is likely a work ethic issue, or a math preparation deficit. This approach puts the responsibility for closing the "math gap" from high school math preparation to college/university math expectations clearly onto the student. They may enter college with poor math preparation due to: * Social Passing (including credit recovery/lax summer retakes) * "No child left behind" logic (No one is allowed to flunk a student) * lack of study skills/work ethic * Time lapse since last math course * Improper coverage in high school math courses taken * "Bare minimum to pass" performance in key prep courses We become their "learning coach"/motivator, but clearly they MUST attack the deficit head on and properly prepare themselves for the university.

Presenter Bio:

Steve has been presenting at ASCUE since the early 90's. His most recent incarnation has been to go back into the math classroom, where he has made it a mission in life to close the "math gap" in high school math preparation and university math expectations. Bonded with his long-time love affair with screencasting and the EFFECTIVE USE of online learning tools, he seems to have developed an effective and replicable model.

Learning is Not a Spectator Sport--Flip Them on Their Ear

Steve Anderson
Math/Computers/Decision Science
University of South Carolina Sumter
200 Miller Road
Sumter, SC 29150
(803) 938-3775
mrspacelysc@uscsumter.edu

Abstract:

With a professor-centric "lecture approach" where students are asked to "do the odd numbered exercises" at home, we often experience less personal interaction with students, less timely feedback on "problem-children," less student responsibility for their own learning, higher D-F-W rates and lower class GPA's. Come see how we have utilized technology to transform (flip) the learning environment into a student-centric one-room schoolhouse where: 1. Professors can identify EARLY students with inadequate preparation/motivation (allowing early transfers/drops) 2. Students are made responsible to spend as much time as they need (within calendar deadlines) to master material. 3. Mastery (ours at an 80% level) is the norm and most of the learning that (presumably) took place "in lecture" now takes place outside of class. 4. The D-F-W rate is significantly lowered in gateway courses. 5. Professors get to spend LOTS more "quality time" in one-on-one interactions with their students as class time that used to be spent on "lectures" are replaced with authentic learning experiences. Does this sound too good to be true? It has been done effectively in various classrooms over multiple disciplines for over seven years now. Come see how we have implemented this pedagogical shift and hear and discuss the results we have experienced and share your own experiences (best and worst practices) and concerns about its implementation and effectiveness.

Presenter Bio:

Steve has been teaching in a university/college classroom since 1972. He has presented at ASCUE, as well as many other technology conferences, for over 20 years. He regularly is invited to conduct faculty workshops in his areas of expertise. His interests have always centered around pedagogical innovation. His most recent efforts center around the concept of "Flipping the Classroom". His long-time passion for "Screencasting" is well known in the ASCUE circles (and his beef jerky!)

Creating an Academic Library Intranet

Scott Bacon
Web Services and Emerging Technologies Librarian
Coastal Carolina University
Conway, SC 29528
sbacon@coastal.edu
843-349-6631

Abstract:

The Kimbel Library Intranet at Coastal Carolina University is a centralized online tool that allows library faculty and staff to engage in a networked environment. The intranet was initially created to increase staff communication and store documentation. The Drupal content management system was chosen as the intranet platform because of its extensibility, flexibility and community support. The main functions of Phase I of this project were to increase communication across departments and committees, facilitate project management and revise the library's shared drive. Another important function of this phase was to host mission-critical documentation such as strategic goals, policies and procedures. Phase II of this project will focus on porting employee tasks into the centralized intranet environment. This second development phase, which aims to replicate and automate the bulk of staff workflows within a content management system, will be a huge undertaking. This presentation will contain an overview of the intranet project, including the modules that were used, implementation steps and possible directions in future development phases. One possibility for future development includes public-facing pages that could be created and used to enhance teaching and learning in the classroom. Several issues encountered during the project will be noted, including dealing with the university IT department, user buy-in, site navigation, roles, permissions and training.

Presenter Bio:

Scott Bacon is the Web Services and Emerging Technologies Librarian at Coastal Carolina University's Kimbel Library. He is the primary developer and administrator for the Kimbel Library website, web applications, social media and mobile interfaces. He also identifies, assesses and implements emerging technologies that increase and enhance access to library resources and services, such as discovery services, database-driven applications and content management systems.

Student Focus on Distance Learning: Student Perceptions of DL Courses, Library and Course Management Resources

Ariana Baker
Jennifer Shinaberger
Tracy Gaskin
Coastal Carolina University
Conway, SC 29528
abaker@coastal.edu
843-349-5001

Abstract:

Distance learning is an increasingly common type of learning experience, with advances in course management systems and interactive technologies making it easier than ever to communicate in non-traditional settings. Still, not all distance learning classes are as conducive to learning as others. In an effort to understand student expectations and perceptions of their distance learning classes, a distance learning librarian, senior course management administrator and assistant director of distance learning at Coastal Carolina University conducted two student focus groups. Students were asked about their reasons for enrolling in distance learning courses, their use of online library resources, their use and prior understanding of Blackboard, and library and Blackboard resources support services. They also shared their thoughts about improving the overall nature of distance learning courses. In this presentation, we will share the results of these focus groups and discuss improvements that have been made as a result.

Presenters' Bios:

Ariana Baker is the Distance Learning Librarian at Coastal Carolina University. Jennifer Shinaberger is the Assistant Director for Distance Learning & CeTEAL at Coastal Carolina University. Tracy Gaskin is the Senior Course Management System Administrator at Coastal Carolina University

The Circle Approach to QM (Quality Matters)

Jean Bennett
Coastal Carolina University
Conway, SC 29528
jbennett1@coastal.edu
843-349-2481

Abstract:

Coastal Carolina University became a Quality Matters Institution in the fall of 2011. Quality Matters (QM) is a faculty-centered, peer review process that is designed to certify the quality of online and blended courses. In an effort to have faculty engaged in this process the development of a "circle" was implemented in spring 2013. The idea behind "circle" sessions is having individuals commit to attend a set amount of sessions, engaging together for the same purpose. This planned six-week session allows for faculty to see the big picture of QM along with the individual elements within a distance-learning (DL) course. The caveat to participation is that faculty need to have a DL or Hybrid course that has run for a minimum of two semesters. This ASCUE session will look at the process of developing "circles", outcomes of the QM Circle and how this approach works in faculty development.

Presenter Bio:

Jean Bennett has a combined 25 years experience in education as a teacher, director of technology, instructional designer and multimedia instructional technologist. She is a Pennsylvania certified Instructional Technology Specialist and a Quality Matters (QM) Peer Reviewer. In her new position at Coastal Carolina University, she is working with faculty providing consultations for design of instructional strategies in distance learning and developing quality courses. Jean enjoys attending and presenting at ASCUE.

Teaching Writing Online: Building a Community of Practice via Coaching and Peer Review to Initiate and Maintain Active Engagement

Leslie Bowman
Walden University
804-310-0339
leslie.bowman@waldenu.edu

Abstract:

In this session, we will explore innovative methodology for building a community of practice for teaching writing in context, across multi-age grade levels and content areas. Comfortable with text messaging, casual, and informal writing, students often find themselves unprepared for the academic tone and style, as well as the sheer volume, of writing required in online classes. Online learners who are not accustomed to communicating exclusively in writing soon become uncomfortably aware of weaknesses in their academic writing. The community of practice creates a culture of interest, inquiry, risk-taking, and collaboration. The instructor assesses current writing skills, seeds the community with content based on targeted patterns of error, and then coaches students according to individual needs. Using sequential practice, peer review, and reinforcement, students develop academic writing skills that transfer across the curriculum. Instructors and students fulfill roles as coaches, mentors, and reviewers, which form the building blocks for a community of practice that inspires frequent, active engagement. As students realize they have the same challenges and experiences, their comfort level with exposing shortcomings, asking for help, and attempting new writing strategies, increases. Students in a community of practice share common goals and challenges and become actively engaged partners in the learning experience. In contrast to weekly online discussions that center on finite units of study, assigned postings and responses, and prescribed time limits, the community of practice supports ongoing dialogue, commitment, and respect in a collaborative atmosphere in which students share existing knowledge and new learning.

Presenter Bio:

Leslie Bowman is a career educator whose experience includes public schools and college teaching, instructional design, as well as training and professional development for online faculty. She is the author of *Online Learning: A User Friendly Approach for High School and College Students* and has presented topics in online teaching and learning at state and national conferences. She designs and teaches online courses in Criminal Justice, English, Educational Technology, Communications, and Writing.

An Overview of Learning Analytics and How We Can Use it To Predict Students' Performance

Beth Dietz-Uhler
Professor of Psychology
513-727-3254
uhlerbd@muohio.edu

Janet Hurn
Professor of Physics
513-727-3341
hurnje@muohio.edu

Miami University Middletown
4200 E. University Blvd
Middletown, OH 45042

Abstract:

At the start of a new semester, do you often have a hunch about which students will succeed in your class, and who will have difficulty? Of course, one could argue that acting on these hunches can create a self-fulfilling prophecy or possibly be considered "profiling". Likely, you probably have valuable data in your head, collected from semesters of experience, that can help you predict who will succeed and who will not based on certain data. But have you ever tried to formalize your hunches? Have you ever thought consciously if you have the data to support your hunches? And if you are correct, then do you also have the data to help all of your students succeed? Learning analytics promises to provide answers to these questions. Learning analytics is defined as "the measurement, collection, analysis, and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs" (Long & Siemens, 2011, p. 32). The purpose of this presentation is to provide a brief overview of learning analytics, including various tools to track, extract, and analyze data. We will also explore its uses and applications, goals, and examples. We will discuss why individual instructors will want to make use of learning analytics. Any discussion of learning analytics is not complete without a thorough discussion of the issues and concerns with the use of this type of data.

Presenters' Bios:

Beth Dietz-Uhler is a Professor of Psychology at Miami University. Her research focuses on computer-supported interaction, use of technology in teaching & learning, and scholarship of teaching and learning. She has taught online courses for more than 14 years.

Janet Hurn is the Coordinator of Regional eLearning Initiatives at Miami University. She has taught physics at the Middletown campus since 1990. She focuses her efforts on integrating technology in teaching and loves working with faculty interested in doing the same. She spends half her time working with faculty creating online and hybrid courses.

Using iPads and Verizon's Thinkfinity with Graduate Education Students: How Does it Affect Teaching and Learning?

Holly Gould
hgould@sbc.edu
434-381-6546

Tom Marcais
Academic Technology Trainer & Consultant
tmarcais@sbc.edu
434-381-6542

Sweet Briar College
134 Chapel Road
Sweet Briar, VA 24595

Abstract:

Today's PK-12 students regularly have access to SmartBoards, iPods, iPads, and other technological advances to which college students have had only brief contact, if any. College students who wish to become teachers need to be adept with technology that is commonly found in schools around the country if they are to use it effectively. Sweet Briar College's Education Department received a $20,000 grant from the Council of Independent Colleges and Verizon to teach preservice teachers to understand the potential of technology to maximize the learning experience for students. The training program developed to support the preservice teachers will be outlined. Examples will be shared of how graduate students have used the iPads and Thinkfinity resources, as well as data indicating changes in their comfort and proficiency in using the technology.

Presenters' Bios:

Holly Gould's professional experience includes eight years of teaching in Alaska. Her primary research interests include high potential, culturally diverse learners, differentiated instruction for all learners, gifted education and the professional development of novice teachers. She teaches courses in human development, teaching models and strategies, multicultural classes, gifted education and curriculum. She advises students interested in earning a teaching license and she supervises student teachers at the elementary and secondary levels.

Tom Marcais is the Academic Technology Trainer & Consultant at Sweet Briar College. He is responsible for developing and delivering classes, presentations, workshops and consulting for students, faculty and staff in computer applications and technology supported at Sweet Briar College.

Connecting students with technology so they can connect with each other

Wayland Harris
Spectrum Industries
wharris@spectrumfurniture.com
800-235-1262

William Jacocks
Troxell Communications
william.jacock@trox.com

Abstract:

Whether used in a classroom, library, or telepresence conference room, collaboration tables make it easy for people to practice active learning by gathering and sharing ideas. By utilizing collaboration tables of varying size and shape virtually any workspace can be transformed into an exciting, stimulating, and multi-faceted learning arena. There are many factors that go into the selection of the correct collaborative furniture for any space. The main considerations in selecting the proper configurations are learning group size, electronic sharing technologies to be deployed at each workgroup , level of learning systems integration needed, the curriculums that need to be supported, as well as the size of the learning space. The focus of this discussion will be to share cost effective and practical ways current learning areas can be transformed to collaborative learning spaces. We will thoroughly discuss with both a physical "hands on" demonstration and visual slides of existing spaces, spaces in process, and conceptual drawings of upcoming projects all with before and after photographs. The transformation of an existing conference room or classroom to an adaptive learning environment does not have to be either complex or costly. Furnishings and electronic sharing technology is available off the shelf today to facilitate this transformation.

Presenters' Bios:

Spectrum Industries, Inc. is based out of Chippewa falls WI and has been in business over 40 years. We are the largest manufacturer of lecterns, carts, and councils in North America, and the second largest manufacturer of mobile computing solutions (laptop carts). All of Spectrum products are covered by a 10 year warranty, and are made right here in the USA. Wayland Harris has been the Mid-Atlantic Territory Manager for 3 years. Prior to that, he has over 10 years experience in the design/build industry with core focuses on schools, universities, and medical facilities.

Troxell Communications is a South Carolina State AV Contract Vendor. offering Design, Supply and Integration. A few of our best products are Spectrum Furniture, Lumens Visual Presenters, Hitachi, Panasonic and NEC projectors, SMART and Hitachi Interactive products as well as professional audio and cameras. William Jacocks has been with Troxell Communications for 8 years and in the AV Industry for over 15 years.

Outcomes Assessment: Commercial System vs. Do-It-Yourself Apps

Kim Hunter
Director of Institutional Technology
College of Mount St. Joseph
5701 Delhi Road
Cincinnatti, OH 45233

Abstract:

After the discontinuation of a successful e-portfolio system to product sunset in 2009, assessment leaders at our small liberal-arts institution were forced back to the drawing board to find existing technology tools to support the general-education assessment process. Such tools included our learning management system for artifact collection, flash drives for artifact distribution to faculty raters, forms processing software for collecting assessment ratings, and Microsoft Excel for data reporting and curriculum mapping. Using existing campus technologies for assessment reduced our software budget, maintained the efficiency of the assessment process, increased the utilization of the software, and as an added bonus, resulted in faculty development relative to technology. We are now in the process of implementing the Blackboard Outcomes Assessment system. Using a licensed application for assessment will simplify the artifact collection and curriculum mapping processes as well as expanded the analytic reporting possibilities. This session will begin with an overview of the technology tools used to support the general education assessment process as well as an overview of the Blackboard Outcomes assessment system. A comparison of the homegrown and licensed system and the advantages and disadvantages of each will be discussed.

Presenter Bio:

Kim Hunter is the Director of Institutional Technology at the College of Mt. St. Joseph in Cincinnati, Ohio. Kim joined the Instructional Technology team after 20 years teaching in the Computer Information Systems programs at the College of Mt. St. Joseph and University of Toledo. Prior to teaching, Kim worked as a Senior Systems Analyst and programming consultant for several Fortune 500 firms. Kim has a MBA and BBA from the University of Toledo.

Could It Possibly Be...More Cool Tools!

Janet Hurn
Miami University Middletown Campus
4200 E. University Blvd
Middletown, OH 45011
513-727-3341
hurnje@muohio.edu

Abstract:

Come see what tools I have found this year to make your life more productive and your classroom more techified. I will share my favorite web apps and sites, iPad apps, software and hardware. This year I will add Chrome extensions to the list. Don't miss it! Bring your classroom problems and we will try to solve them with technology.

Presenter Bio:

Janet is a former board member of ASCUE and is currently the Coordinator of Regional E-Learning Initiatives for Miami University. She is also a Senior Instructor of Physics. Janet LOVES to integrate technology into the classroom, find new and innovative online technologies, and present Cool Tools at the ASCUE conference.

Creative Uses of Technology in Elementary Teacher Candidate Education in the Expressive Arts

Geraldine Jenny
Slippery Rock University
1 Morrow Way
Slippery Rock, PA 16057
Geraldine.jenny@sru.edu

Fred Jenny
Grove City College
100 Campus Drive
Grove City, PA 16127
724-458-2071
fjenny@gcc.edu

Abstract

Having taught a course for a number of years in the expressive arts taken by elementary education majors, I am finding more and more digital resources that augment and enrich student creative expression for their classroom use. This presentation will investigate and share those resources and share how they are used.

Presenter Bio:

Dr. Gerri Jenny has taught in the Pennsylvania State System of Higher Education for about 12 years after raising a family of three children. Prior to that she taught early childhood students in the public schools. She has been an ASCUE supporter and Ocean Creek groupie since the late '80s!

Longtime ASCUE attendee and 2-time president, Fred Jenny has taught at Grove City College for nearly 30 years.

Google Tools for the Education Major Professional Portfolio

Fred Jenny
Grove City College
100 Campus Drive
Grove City, PA 16127
724-458-2071
fjenny@gcc.edu

Abstract

Electronic portfolios have been a requirement of a course that I teach for a number of years now. Over the years that project has evolved from Frontpage sites on the Intranet to today's Google sites integrating Google Drive. We are also attempting to coordinate efforts with education courses and methods classes. This presentation will discuss the advantages and disadvantages of this strategy including the trials & tribulations. Sample portfolios will be highlighted. Google tools examples will be shown as well.

Presenter Bio:

ASCUE member since '80s. Repeat Offender as ASCUE Program Chair & President. Grove City professor in CS, education, & communication studies for nearly three decades.

Using TestOut's LabSim course in Avila's A+ course

Patrick Kopp
Avila University
11901 Wornall Road
Kansas City, MO 64145
816-501-3791
patrick.kopp@avila.edu

Abstract:

Avila University is a small school. We have limited funds and limited facilities. While students have access to computer labs and open labs, we do not have room for a dedicated hands-on lab for our certification courses. I have tried setting up and tearing down labs but this is too time-consuming, especially for classes that meet two or three times a week. We also do not have the money for up-to-date equipment and software to be used only in a dedicated IT lab. TestOut's LabSim course PC Pro consists of lectures, written text explaining key features and concepts, simulated labs and exams. At the end of the course, students are allowed to take the certification exam once. This demonstration will give a background of Avila's situation, show how students can set up an account and demonstrate the features of LabSim.

Presenter Bio:

I started teaching at Avila University January, 1986. I received a Master's in Education in 1993 from Avila University. The Fall semester 2012 will be our first semester offering our Bachelor of Science degree in Software Engineering. On a personal note, I was married on March 2, 2013.

Cloud Computing and UNOH

Jeffery Le Blanc
Vice President for IT
University of Northwestern Ohio
1441 N. Cable Road
Lima, OH 45805
419-998-3107
jalebran@unoh.edu

Abstract:

Cloud computing: What is it? How does it work? What can you do with it? Pros and cons? What is its future? This session is a non-technical overview (no computer degree required!) of the what's, why's, where's, how's, and what to look for when choosing a cloud computing based service. The use of cloud computing at UNOH will also be covered in order to give a better understanding of the many disparate systems that are used by faculty, staff, and students that are located both on campus and in the cloud. You're very likely already using cloud computing in some form or fashion and this session will help to uncover some of the mystery hidden behind that opaque silver lining.

Presenter Bio:

Jeff Le Blanc is the VP for IT at the University of Northwestern Ohio. He holds an M.B.A. in Organizational Leadership and International Business and currently leads the IT department that includes both administrative and academic computing at UNOH. He has also taught various IT courses over the years. He actively evangelizes, integrates, and supports the technology needs of faculty, staff, and students.

Designing Fool Proof Technology Classrooms for Faculty

Tom Marcais
434-381-6542
tmarcais@sbc.edu

M. J. Stinnette
mstinnette@sbc.edu

Sweet Briar College
134 Chapel Road
Sweet Briar, VA 24595

Abstract:

Faculty members on campus want to be able to walk into a classroom and just have the technology work. It needs to be reliable, consistent and easy to operate. The classroom also needs to be flexible enough to work suitably for diverse disciplines and teaching styles. Designing such a solution requires attention to installation, configuration and training. We've recently installed 7 new classrooms utilizing this concept with great success. Our session will describe our process and the challenges we encountered.

Presenters' Bios:

Tom Marcais is the Academic Technology Trainer & Consultant at Sweet Briar College. He is responsible for developing and delivering classes, presentations, workshops and consulting for students, faculty and staff in computer applications and technology supported at Sweet Briar College.

M J Stinnette is the Academic Technology Coordinator at Sweet Briar College. She is responsible for maintaining the AV equipment, hardware and software in all the classrooms and computer labs on campus.

Using Electronic Portfolios Based on National Standards to Assess Student Learning

Linda Novak
Instructor of Early Childhood Education
novakl@faytechcc.edu
910-678-0180

Belva Demendoza
Early Childhood Associate and School Age Education Department Chairperson
demendob@faytechcc.edu

Fayetteville Technical Community College
2201 Hull Rd
Fayetteville, NC 28303

Abstract

Fayetteville Technical Community College Early Childhood Associate Degree uses electronic portfolios to assess student learning based on National Association for the Education of Young Children Standards (NAEYC) for Associate Degree Programs. The presentation will include a demonstration of the electronic portfolio, and a summary of data gathered from course key assessments based on national standards. Participants will be able to see the process from student entering the assignment into the portfolio based on the key assessment rubric, to course data gathered, to success of meeting the NAEYC standards.

Presenters' Bios:

Linda Novak is an Instructor of Early Childhood Education at Fayetteville Technical Community College, a member of North Carolina Association for the Education of Young Children Board of Directors, campus based child development center director for 20 years, and past President of West Virginia Association of Young Children. She is currently part of NCCCS e-text pilot project.

Belva Demendoza is an Early Childhood Associate and School Age Education Department Chairperson at Fayetteville Technical Community College. She worked in higher education for 21 years on the University and Community College level as a classroom teacher with a specialization in Behavior Disorders. She is a member of Online Accessibility Committee for NCCCS and co-chair of SACS 5 year review committee at FTCC. She is currently part of NCCS e-text pilot project.

Project Management: Getting Things Done in IT

Mark Poore
540-375-2403
poore@roanoke.edu

Terri Austin
austin@roanoke.edu

Roanoke College
221 College Lane
Salem, VA 24153

Abstract:

During the 2012-2013 academic year, Roanoke College has formalized how new IT projects are requested, assessed, authorized and executed – all in a transparent and equitable manner. This session will describe our methodologies, the process of introducing this new procedure to campus, and lessons learned. We will also discuss our adventure to PMP certification and share pointers for those thinking of earning this credential.

Presenter Bio:

Mark Poore is the IT Projects Director at Roanoke College. He is responsible for overseeing all IT project requests and managing the IT project portfolio. Before coming to Roanoke College in 1997, he held several IT positions in software development companies. He holds a B.A. from Roanoke College and an M.S. from Baylor University. Mark was a Fulbright Scholar to Germany. He likes astronomy, camping and playing the cello, banjo & accordion.

Terri Austin is the Director of User Services at Roanoke College. In addition to supervising the User Services Team, her major duties are student assistant coordination, HelpDesk functions, one card system, Microsoft Team Sites, and user account management. Terri has worked at Roanoke College for 30 years and has a B.S. from Roanoke College. She likes sports, scrapbooking, & working out.

Expanding Technology Training & Integration with Online Learning

Julie Rayhorn
Senior Account Manager
Atomic Learning
320-631-5937
jrayhorn@atomiclearning.com

Abstract:

College professors and instructors are subject experts, not technology trainers. And, despite being called 'digital natives,' the majority of college students don't know how to EFFECTIVELY use technology. For many campuses, this creates a disconnect between the faculty's core competence and the students needs. Using an online technology training tool fills this void, allowing the instructor to focus on the content while providing students the tools they need to succeed.

Presenter Bio:

Julie Rayhorn is the Senior Account Manager at Atomic Learning, education's trusted training solutions provider. In his/her role at Atomic Learning, Rayhorn has helped hundreds of schools/campuses plan and implement effective technology training, support and integration initiatives. Rayhorn holds a BAS in Education from the University of Minnesota, Duluth. You may request to have your paper refereed if desired.

Mimio - A review of the latest Mimio Technology

Steve Schwartz
Senior Sales Manager for the SE
Mimio
704-999-1738
Steve.Schwarz@mimio.com

Abstract

Mimio has been a leader in educational technology for the past 18 years, providing affordable, easy-to-use, and effective solutions. Mimio technology empowers both educators and students in all forms of learning, to enable real understanding. The session will cover a brief summary of Mimio solutions with a deeper review of the MimioCapture and MimioMobile solutions. The participants are encouraged to download the MimioMobile iPad App or Android App to participate in the session.

Presenter's Bio:

Steve Schwarz is the Sr. Sales Manager for the SE at Mimio. He has worked in the K-12 and Higher Education market for 8 years. His background includes work with interactive solutions, IP based control systems and digital signage.

A More Effective Use of Faculty Office Hours with Student Appointment Scheduling Software

Jon Serra
Assistant Professor of Chemistry
The University of Pittsburgh Titusville
Titusville, PA 16354
814-827-4435
serra@pitt.edu

Abstract:

Student-teacher interactions outside of the classroom and outside of traditional business hours can be facilitated with web-based appointment scheduling software. Several freely available, cloud-based packages are compared that provide flexibility, integration, features and simplicity. Design and integration with common calendar software, course management systems, social media and mobile devices are investigated with the freely available cloud application from www.acuityscheduling.com. Uses discussed include: group collaboration and tutoring as well as virtual office hours, recitations and review sessions. Student usage data assembled by the software from www.acuityscheduling.com will be discussed as well as feedback from students.

Presenter Bio:

Jon is currently an Assistant Professor of Chemistry (hopefully soon to be Associate) at the University of Pittsburgh's Titusville campus where he teaches primarily organic and general chemistry. Jon enjoys introducing new methods to engage students in and out of the classroom using social media, mobile devices and cool gadgets, gizmos and techniques introduced at the ASCUE conference. .

Point, Click, Provision: Avoiding Campus "Move-in Day Blues"

Louis Simpson
Pre-Sales Systems Engineer
Meru Networks
614-570-3614
louissimpson@merunetworks.com

Abstract:

Today's students, faculty, administration and guests expect to be able to work, learn, and study whenever and wherever they want to. Wireless registration, authentication and access don't have to be cumbersome and complicated. In this presentation, you will learn how to take back control, and keep your users and visitors productive and happy, rather than complaining on social media about how the wireless is worse than the parking!

Presenter Bio:

Louis Simpson has over 25 years networking experience and is currently the Pre-Sales Systems Engineer for Meru Networks, covering North and South Carolina. Louis has extensive experience in routing and switching, as well as network security and content delivery. He has previously worked for Brocade, Nomadix, Alteon Websystems, Lucent Technologies and NationsBank (now Bank of America). Louis holds a BS in Computer Science from Appalachian State University.

How Roanoke College Reduced Their Data by 80% Leveraging De-Duplication and Compression Technologies

Randy Stubstad
Systems Administrator
Roanoke College
221 College Lane
Salem, VA 24153
540-375-2403
conference@ascue.org

Mike Taylor
Southeast Regional Sales Manager
Tegile
704-504-2575
mike@tegile.com

Abstract:

Learn how Roanoke College was able to reduce their data footprint from 36 TB's down to 8 TB's utilizing an innovative new Hybrid Storage Solution. This session will include a live demonstration of the technology in action and discuss basic things to consider before implementing a shared storage device. The demonstration will include creating volumes, CIF shares, NFS mounts, creating iSCSI LUNS, Snapshots, recovering from Snapshots, and demonstrate De-duplication and Compression savings in action. For those evaluating new Storage options, or looking into VDI - this will be a session you don't want to miss.

Moodlerooms joule + xpLor

Chris Vanderbosch
Regional Sales Executive
Moodlerooms, Inc.
317-669-2817
cvanderbosch@moodlerooms.com

Abstract:

Highlighting Moodlerooms joule Learning Management System combined with the new open standards based xpLor global advanced learning object repository. xpLor is not only a repository but a centralized authoring and editing environment incorporating crowd sourced and OER content. xpLor enables sharing and discovery of educational content with a rich metadata engine that enables copyright management with Creative Commons and derivative works.

Presenter Bio:

Regional Sales Executive, Moodlerooms, Inc

We virtualized the lab... Now what? BYOD access? Persistent faculty vm's?

Luke Van Wingerden
Director of Client Services
lvanwingerden@uscupstate.edu
864-503-5863

Kevin Hodges

USC Upstate
Spartanburg, SC 29303

Abstract:

Virtualization of the computer lab was a significant shift in how computer labs were managed, imaged and supported. Now that the computer lab has been virtualized, what's next? Do we stop there? Are there cost savings by virtualizing the user desktop or providing student access from their own device? USC Upstate has extended their SpartanGreenSky VDI past the computer lab which has increased support and response times, allowed students to access university owned software anywhere anytime, and reduce power and computer replacement costs. See how students, faculty and staff across the USC Upstate campuses have benefited from the SpartanGreenSky VDI.

Presenter Bio:

Luke VanWingerden is the Director of Client Services for Information Technology and Services at USC Upstate. Luke began his role at USC Upstate in the Summer of 2011. Luke started working in a higher education IT support environment in December 2005 serving in several capacities. Luke's primary focus is looking for ways to improve IT support and increase the services offered by Client Services to ensure a seamless and consistent technology experience.

What I've Learned: 200 Software Evaluations

Frank Vastola
Tech2Education
frank@tech2education.com
904-280-9797

Abstract:

Over the past 30 years I've had the opportunity to work in three very different roles involved in technology evaluation, selection and implementation. First as a higher education administrator (college admission, financial aid and enrollment management). Next as an account executive and sales manager with leading higher education technology vendors - including SCT/SunGard Higher Education and Datatel. Lastly, as a consultant - working with clients as they navigate through the steps toward selecting and implementing new technology solutions in line with the goals and objectives of their strategic plans. This session will present what I have learned from being involved in software evaluations at over 200 institutions while serving in these various roles.

Presenter Bio:

Frank Vastola began working with student information systems in the early 1980's while working in college admissions and serving on a team that implemented an SIS at a small private college in New York. He would go on to direct admissions, financial aid, enrollment management and alumni programs while also working as a member of teams that selected, implemented and managed CRM, ERP/administrative or learning management systems at each of three institutions over 14 years. In the mid-1990's, Frank joined the sales team at ABT, an administrative software provider to primarily small and mid-sized institutions. First as regional sales manager and eventually as a vice president, Frank was instrumental in the successful sales growth of ABT's PowerCAMPUS system by establishing over 50 new client partnerships up to and through the acquisition of ABT by SCT/SunGard Higher Education. Over 16 years, Frank assembled and coached sales and sales support teams, managed sales activities, proposals, contract negotiations and client relations at ABT, SunGard Higher Education (Banner and PowerCAMPUS) and Datatel (Colleague). While at Datatel, Frank managed all new account sales activity throughout the eastern U.S., eastern Canada and the Caribbean. He has worked with cabinet level and departmental administrators at hundreds of institutions. After the contract, he often served as the vendor's relationship manager throughout the implementation and beyond.

Presenters Index