Identity and Access Management

By: Anthony Maszeroski, Information Security Manager

Have you heard about the Identity and Access Management (IAM) initiative that is underway? Are you curious or confused about exactly what IAM is and what it means to you? If so, then this article is for you.

Microsoft’s Frederick Chong defines IAM as “the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources.” Still confusing?

Imagine that a trusted colleague, let’s call him Head Chef Fred, walks up to you and asks to borrow the key to a shared file cabinet that contains secret cookie recipes. Since you know Fred and you know that a cookie order is waiting to be fulfilled, you hand the key over to Fred and this enables him to retrieve the recipe he needs to make deluxe super-secret double-chocolate fudge cookies. In this scenario, the transaction that occurred depended on Fred’s identity, your ability to verify Fred’s identity, and the appropriateness of Fred’s request given his role. These same types of transactions happen constantly in the computer world, except the identities and resources involved are digital instead of tangible, and they can be located anywhere in the world where a network connection exists.

The framework of processes, technologies, and policies that allow these transactions to occur are collectively referred to as an Identity and Access Management Infrastructure (see page 2).

Please refer to the picture on page 2 while reading through this paragraph. At the University of Scranton, our sole Source System for identity information is BANNER. The system we are implementing to Manage Identity is called Oracle Identity Manager, or OIM for short. Most of our Systems and Services should already be familiar to you. These include email, the my.scranton portal (including embedded applications), RoyalDrive, Corptime Calendar, Cisco NAC, and so on. The surrounding business processes and policies, grouped into the categories of Policy and Governance, Group Management, and Privilege Management are what provide the foundation for and rules by which the technology components of IAM function. As you can see, it is critical that these components are tightly coupled and aligned with the institution’s needs, and nearly every individual fills some role in the IAM picture.

Exactly what your role is in the IAM initiative will become clearer as the project progresses. Some of you who participate in IMAC are aware of your data stewardship roles and how they factor in. Others have already met with our IAM integration partner, CampusEAI, to assist with phase one of this project. Many more will be involved as we establish processes to claim your digital identity, and as we solicit input on goals for the second phase of the project. So please do stay engaged and send any questions you may have to security@scranton.edu.

Why do we want to embark on such an initiative? First, it reduces overhead of service management. It simply isn’t practical for every information system to maintain its own identity store. Second, it increases security and privacy of stored information through a consolidated approach for managing identity (who you are), authentication (how we know who you are), authorization (what resources you’re entitled to access), and

Continued on Page 2
accounting (keeping track of who accesses what, on whose authority, and when -- a critical component of regulatory compliance). Third, it simplifies service access by allowing single or reduced sign to function (i.e., log in once, access many resources without having to log in again). Fourth, it allows us to meet contractual requirements for resources we license, such as software, library digital reserves, and clouded services. Last but certainly not least, IAM allows us to exercise good stewardship over the data that is entrusted to us by our community members and protected under law.

Faculty and Staff work at home rights for Microsoft Software

By: James Franceschelli, Director IT Services

As part of the Microsoft Campus Agreement, University of Scranton employees have the legal right to obtain Microsoft software such as Office 2010 Pro and Windows 7 Upgrade on your home computers for work-related purposes. The program provides all faculty and staff with exceptional discounts on Microsoft applications. We have enlisted our Microsoft software vendor, JourneyEd, to administer the Microsoft work at home rights program. The cost to obtain the software is $9.95 for the licensed download and $14.95 for the physical CD/DVD and can be ordered at http://www.journeyed.com/select/go/CAUSCRANTON. After you place the order online, you will be required to fax or email a copy of your Royal ID to JourneyEd. They will send you instructions for sending the verification by email once you have placed the order through their site. Once you have submitted your ID, you will receive either a license code and a link (download) or a physical CD media set.

Visit http://www.journeyed.com/select/go/CAUSCRANTON for a full listing of products and prices. This program is only available to faculty and staff.
The ERP Migration Project
By: Connie Wisdo, Director IT Development and Applications

What is it? What does it mean to me?

According to Wikipedia, “Enterprise resource planning (ERP) integrates internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, etc.” CIO magazine adds, “(ERP) attempts to integrate all departments and functions across a company onto a single computer system that can serve all those different departments’ particular needs.”

Here at the University of Scranton, our ERP is primarily composed of Internet Native Banner (INB) and Self-Service Banner (SSB), both from a company called SunGard Higher Education (SunGardHE). Banner was installed here nearly 20 years ago, and is now used by colleges and universities in 40 countries.

However, no single piece of off-the-shelf software can possibly serve every need of a university, so over the past 15+ years a team of developers here at the University have written hundreds of software applications that integrate with Banner, and our Oracle database, which is the data repository for the ERP. Some of these programs are interactive, and run from the my.scranton.edu portal (Employee Applications tab and SSB). Others are run automatically on a scheduler, using software called JAMS. Still others are reports that simply pull data from the Oracle database, and present it to our customers: printed reports, flat file listings, or Excel-format files. If you haven’t guessed by now, our ERP system is a critical component of the overall operation of the University!

About two years ago, Oracle and SunGardHE informed us that the OpenVMS operating system, upon which our database and ERP have been running, would not be supported after 2011. Therefore, it was necessary to select a different operating system for our ERP, and have the entire ERP up and running on this new operating system in 2011. In early 2010 the selection of Linux, a leading server operating system based upon the Unix operating system, was made.

Since last year, three PIR departments have been focusing on the serious, intensive effort to migrate the ERP to Linux: Systems & Operations, Database Systems & Data Processing, and IT Development and Applications (ITDA).

After much planning and close collaboration with the Data and Technology Coordinators and Printing Services, we have made significant progress.

While INB and SSB were migrated without too much difficulty or change, differences in the structure of Linux, along with a new version of Oracle, have forced our system administrators, DBAs and ITDA developers to make fundamental changes in the underlying architecture of custom-written programs, from the customer-facing menu structure, to the delivery of system output and reports.

As a customer, you may or may not notice any difference when we go “live” on Linux this summer. We’ve made some changes already. For example, the Employee Applications tab was launched late last year. Here you will find options from the old “Banner Reports Menu” as well as new reports developed in Argos. Along the way, we’re trying to improve ERP processes, incorporating key services that customers use every day, such as RoyalDrive, and improving the security of our information assets (i.e. data).

Please mark your calendars for the actual migration dates: 7/28/11-8/2/11. During that period nearly all IT services will be unavailable. Our team will make every effort to bring up services as they become available. We will use several different communication vehicles, but we’ll consistently use Personal Announcements on my.scranton.edu to communicate key information. Please stay tuned for further details as we get closer to the date.
P/IR Staff Updates
By: James J. Franceschelli, Director IT Services

The Planning and Information Resources division continues to evolve and to adapt our skill set to meet the demands of an ever changing industry.

David Rothrock has joined the IT Services staff as a Technology Support Center Analyst. David is a University of Scranton alumnus. He was previously employed in as a Geek Squad Agent for Best Buy and more recently as a Help Desk Agent at Siemens IT Solutions. David works at the TSC on second shift providing support to faculty, staff and students.

John Williams was recently transferred from the CGCE area into IT Services as the Information Technology Training Specialist. Prior to being assigned to IT Services as a trainer, Jack worked for the past 13 years as an instructor in Graphic Design, Web Design, and Photography for the Center for Professional Training and Development (formerly the Center for Continuing Education). Prior to his association with the University of Scranton, Jack managed several daily and Sunday newspapers in New York, Pennsylvania, and Rhode Island. Jack also owns and manages a design and promotion business, Williams Graphic Communications, and teaches graphics and photography part-time at an area vocational school. Jack will play a crucial role in providing user training as IT continues to roll out new initiatives.

Welcome to Derek Gelormini, a very capable student intern who recently joined the IT Development & Applications staff. Derek is currently a 4th year Computer Science major, but is simultaneously pursuing his M.S. in Software Engineering. Derek joined ITDA in mid-December, and is working on a variety of projects, most notably involving the University’s Web pages. If you’ve entered a Project Tracking request for a Web Project or CMS project lately, you’ve likely seen his name as the person who completed your request -- in a very timely manner! Derek also works as a Technical Consultant (TechCon) in the Center for Teaching and Learning Excellence, where he started as a freshman. We expect Derek to be with ITDA until May 2012, when he plans to graduate with his Master’s Degree.

Philip Erb was recently hired as a Systems Programmer / Administrator. Phil is a “computer guy” by trade and hobby. He often says that if he won the lottery, he would continue to work in Information Technology for the fun and challenges. Before coming to the University of Scranton, Phil worked for Towson University. There he managed the e-mail and file sharing services, desktop and server security software, and mobile device administration, among other tasks. Phil holds a Bachelor of Science degree in Information Technology from Pennsylvania College of Technology and is currently working toward a Master of Science degree in Applied Information Technology at Towson University. He has also attained certifications as a Microsoft Certified IT Professional - Server Administrator and a Microsoft Certified Professional on Windows XP and Windows Server 2003. When he’s not tinkering with a motherboard or some lines of code, Phil spends as much time outside as possible, camping and hiking with his wife, Theresa, and son, Adam.

In other staff news, several members of our IR division have continued to develop their skills through professional training and organizations. Jim Franceschelli, Connie Wisdo and Lorraine Mancuso completed the ITIL v3 Foundations course at New Horizons Computer Learning Center. ITIL is based upon a set of best practices used in the IT industry. The foundations course included a review of IT Service Management, IT Infrastructure Library, Service Lifecycle, Service Strategy, Service Design, Service Transition, Service Operation and Continued Service Improvement. Don McCall completed the Help Desk Institute (HDI) Support Center Analyst course and received his HDI Certification. Zack Coffey has successfully completed the Apple hardware and software certification tests and joins the ranks of Apple Certified technicians.

Please join us in extending a warm welcome to new employees and congratulating our staff on their recent certifications.
Mobile Malware ... It’s No Dream

By: Diane Jachmowicz, Senior Technology Services Analyst

March roared in like a lion and brought with it the most dramatic, widespread wave of malware on the Google Android mobile device platform. On Tuesday, March 1, 2011 the Android team became aware of a number of malicious, Trojan applications published to the Android Market that contained the Droid Dream malware rootkit. Droid Dream took advantage of known vulnerabilities that had been patched in Android versions 2.2.2 or higher. For affected devices, the Android team believed attackers were only able to gather device-specific information such as unique codes used to identify mobile devices (IMEIs/IMSIis) and the version of Android running on those devices. Given the nature of the exploits, attackers could access other data.

Google has since identified and removed as many as 60 malicious applications from the Android Market. Other steps Google has taken to protect Android mobile device users include:

- Suspending the developer accounts associated with the malicious applications;
- Contacting law enforcement about the attack;
- Remotely removing malicious applications from affected devices;
- Applying an Android Market security update to all affected devices that will repair the existing vulnerability.

The Android platform is loved by many because it is an open development platform. Openness, however, is a double-edged sword, inviting attackers to develop malicious applications to take advantage of platform vulnerabilities. For many, an Android smartphone is a life line to the outside world. It needs to be kept safe and information needs to be kept secure.

IT Services recommends that all Android, BlackBerry and Windows Mobile smartphone users download and install the free version of Lookout Mobile Security. Lookout Mobile Security provides security and privacy protection in the form of anti-malware protection, backup/restore options and find phone services. For more information, please refer to the Lookout Mobile Security website at https://www.mylookout.com/.

iPhone 4 now at Verizon

By: Diane Jachimowicz, Senior Software Analyst

IT Services Mobile Device Support Team has recently begun supporting Verizon Wireless’ (VZW) iPhone 4. This means that employees eligible for University provided wireless services may now select the VZW iPhone as a smartphone device instead of the more costly iPhone on AT&T. The monthly service for VZW is nearly half the cost of service on the AT&T network.

IT Services recommends that iPhone 4 (and iPad!) users install the free Find My iPhone app. The Find My iPhone app works with Apple’s MobileMe subscription service, but does not require a subscription. Once Find My iPhone is setup on a qualifying device and turned on the device can be located on a map, remotely locked or remotely wiped to permanently delete all data.

Find My iPhone can be installed from the App Store. Instructions for configuring Find My iPhone and MobileMe are available at apple’s website: http://www.apple.com/iphone/find-my-iphone-setup/.
The Technology Advisory Group (TAG) is a brand new initiative on campus that brings together faculty from each college with staff members from Information Resources and Academic Affairs in order to advance, promote, and propagate educationally appropriate technology at The University of Scranton. As two faculty members who are also heavy users of campus technology resources, we founded TAG in Fall 2010 with an initial goal of facilitating communication about and compromise between faculty needs and the capabilities of the University infrastructure. What exactly does this mean?

Faculty are increasingly using advanced technology not only to enhance their teaching but also to fulfill their service responsibilities and to achieve their research aims. As a result, faculty members are increasingly relying on Information Resources (IR) to provide a wide variety of technology tools, from classroom mediation equipment to specialized software to high speed wireless access.

However, all of these tools require resources (staff time, budget allocations, maintenance, etc.), and there are hundreds of faculty members with hundreds of different technological needs and wants. Furthermore, IR must balance the needs of faculty with the needs of the University’s students, staff, and administrators, and without unlimited resources, not every individual need or want can be met. So how can we reconcile what faculty want with the resources IR can provide?

This is where TAG comes in. A group of technology-savvy faculty and staff, TAG strives to “speak the language” of the faculty AND the language of IR and strives to facilitate communication between the two. TAG gathers feedback from faculty, identifying needs and explaining the “what” and “why” to IR, helping with prioritization of response. When IR can’t meet a faculty need, TAG brings an explanation and possible alternative resolutions back to the faculty.

While less than a year old, TAG has already had successes on several fronts. We’re working with IR to smooth the faculty’s transition to the new e-mail system. We’re keeping IR informed of faculty needs in the new science building. We’re gathering information about which faculty members use what classroom mediation equipment in which classrooms, so that IR can place equipment in the classrooms where it’s needed most. We’re informing the faculty about service downtime and the upgrades that IR is making to prevent them. And at every step of the way, the extremely supportive IR staff and administration have welcomed these interactions and have worked hard to respond to as many needs as possible.

So, who is TAG? Our group has grown to include twelve faculty members from twelve different departments, as well as Anne Marie Stamford from Academic Affairs, Eugeni Grigorescu from the Center for Teaching and Learning Excellence, and Jim Franceschelli as a representative for IR. Anyone interested in TAG’s efforts is welcome to visit our website at http://uofstechadvisory.wordpress.com, and all are invited to email us at tag-members@royallists.scranton.edu with questions, comments, or suggestions.

SECURITY TIP:

Do you have a lot of passwords to remember?

As time goes on, passwords will be more and more complicated and you will be required to change them on a regular interval. You might be thinking that there has to be an easier way to remember all of your passwords. Well there is!

With KeePass Password Safe you can store all of your passwords in a private database that is protected by a single password. New viruses are created every day that try to exfiltrate data, including passwords that are stored in plain text files, from personal computers. KeePass protects you from this type of data breach because it stores everything using encryption. Instructions for installing and using KeePass are in the Desktop Notices Channel in the Public Safety/IT Security tab in the My.Scranton portal.
The February IT Forum focused on the upcoming email conversion to Live@EDU. All users should be aware of the changes and updated time line. As announced in the fall, Live@EDU was selected to replace the current email and calendar system. This cloud solution will provide a more robust email & calendar system for all faculty, staff and students.

The Live@edu implementation time line has been adjusted to allow additional time for system configuration, testing, documentation, and developing training materials. The extended time line will provide users with more opportunity to clean up existing emails and to learn the new email and calendar system. Accounts for the new email system will be generated through a new identity and access management solution later this spring.

Testing the new Live@edu product has been very successful. P/IR has been able to successfully test a number of key concerns including the migration of address books as well as server and local email. Training materials are being developed and training will be made available in both an on-line and hands-on format in the near future.

A department by department approach will be used to convert staff and faculty email/calendar accounts. The process will begin with the conversion of P/IR division’s account in May 2011. IR plans to convert Staff email and calendar over the summer 2011, Students in August 2011, and Faculty in the fall 2011. At the time of conversion, a user’s server (RoyalMail) email will be moved to the Live@edu environment. Users will then be given tools and time to move their local email and address books to the Live@edu environment. The conversion process is scheduled to be completed by December 2011.

To prepare for the email conversion, all users should begin to organize their email. Users should retain emails that relate to official university business and delete personal or unnecessary email messages. In addition, IT Services will roll out a product (Identify Finder) to help users find and remove personally identifiable information (PII) from the desktop files.

Unified Science Center Update

By: Robert Kennedy, Instructional Technologies Supervisor

When it comes to the classroom technology in the new Science Center; The University of Scranton is sparing no expense. A total of forty-five learning spaces will be fully equipped with state of the art digital media technology including: Crestron digital media controls, high-definition ceiling mounted LCD projectors or wall mounted LCD monitors, High definition document cameras as well as video and audio inputs that can accommodate both traditional analog connections and digital interfaces found on the newest laptops and handheld devices.

Three rooms (including the Theater) will have lecture capture systems installed. These rooms include ceiling and/or wall-mounted cameras that have the ability to automatically follow an instructor wearing a special microphone so lessons can be easily captured and replayed on computers and mobile devices. The remaining forty-two mediated facilities will be able to utilize the lecture capture system by way of a mobile system that plugs into a panel at the back of the room which connects to the capture server.

The technology in all 45 mediated facilities will be continuously monitored by a central server that collects data on usage, tracks projector bulb life for proactive replacement, and enables remote assistance by the Office of Instructional Technology. This system will also provide the ability to remotely turn unused equipment off thereby saving electricity and excessive wear and tear on the equipment.

In terms of control, the touch panels are being designed in such a way that faculty can easily move from one room to another and instantly know how to operate the technology. Classes on the new equipment will begin being offered sometime in August.

Microsoft Live@edu Conversion Update

By: James Franceschelli, Director IT Services

The February IT Forum focused on the upcoming email conversion to Live@EDU. All users should be aware of the changes and updated time line. As announced in the fall, Live@EDU was selected to replace the current email and calendar system. This cloud solution will provide a more robust email & calendar system for all faculty, staff and students.

The Live@edu implementation time line has been adjusted to allow additional time for system configuration, testing, documentation, and developing training materials. The extended time line will provide users with more opportunity to clean up existing emails and to learn the new email and calendar system. Accounts for the new email system will be generated through a new identity and access management solution later this spring.

Testing the new Live@edu product has been very successful. P/IR has been able to successfully test a number of key concerns including the migration of address books as well as server and local email. Training materials are being developed and training will be made available in both an on-line and hands-on format in the near future.

A department by department approach will be used to convert staff and faculty email/calendar accounts. The process will begin with the conversion of P/IR division’s account in May 2011. IR plans to convert Staff email and calendar over the summer 2011, Students in August 2011, and Faculty in the fall 2011. At the time of conversion, a user’s server (RoyalMail) email will be moved to the Live@edu environment. Users will then be given tools and time to move their local email and address books to the Live@edu environment. The conversion process is scheduled to be completed by December 2011.

To prepare for the email conversion, all users should begin to organize their email. Users should retain emails that relate to official university business and delete personal or unnecessary email messages. In addition, IT Services will roll out a product (Identify Finder) to help users find and remove personally identifiable information (PII) from the desktop files.
Microsoft Forefront Client Security Deployment

By: Danielle Morse, Associate Director Desktop Services

In January 2011, IT Services began converting its windows antivirus software from McAfee to Microsoft Forefront Client Security, a unified malware protection product for Windows, which includes an integrated antivirus and antispyware engine, real-time protection, scheduled and on-demand scans, malware removal, and system recovery. All versions of McAfee must be removed from university owned computers by May 31, 2011 when our license expires.

Leveraging some of the capabilities of Kbox, IT Services is able to schedule tasks to run overnight to minimize disruption to faculty and staff during their busy work day. A process has been developed to uninstall McAfee, install Forefront, rename computers, and join computers to the Active Directory domain between 7:00pm and 4:00am the night your computer is scheduled.

To date, IT Services has replaced McAfee with Forefront on most staff/faculty computers in Brennan Hall, Ciszek Hall, DeNaples Center, Leahy Hall, McDade Center for Literacy and Performing Arts, McGurrin Hall, Ohara Hall, Smurfit, and Weinberg Memorial Library. Computer labs and classrooms were upgraded the week of Spring Break. The current deployment schedule to all remaining buildings continues through the end of May.

The campus was informed of the Forefront Conversion Project in many venues. There was an October 2010 IR Forum, it was featured in the Fall and Winter 2010 editions of IT Matters, discussed at the Data Technology Committee, and posted on the MyScranton portal in both the employee and security tabs. Our communication plan during the rollout includes:

1st Email - email to each individual with a computer in the targeted building approximately one week prior to the deployment date

2nd Email – a second email to each individual as the day of the deployment with specific instructions to reboot the scheduled computer before 7pm.

Department Secretaries – the day of the deployment a phone call and email goes out asking for assistance with any computers shared by the department, in conference rooms, work study use, faculty and staff not on campus, etc.

The morning after the deployment, members of IT Services will be available to troubleshoot any computer that didn’t receive Forefront overnight if the computer was rebooted as instructed.

In order for this rollout to be successful, EVERY computer in the scheduled department and building needs to be rebooted (not shutdown) prior to 7pm on the specified date. DO NOT log into the computer after it has been rebooted. Computers used in conference rooms, adjunct or part-time offices, work study, etc. also need to be rebooted. If you will not be on campus on the specified date, please make arrangements to have someone reboot your computer.

University owned laptop computers must be on campus, have Kbox installed, plugged into an electrical outlet, not set to hibernate or stand by, connected with a network cable to a wired network port (not wireless), and rebooted (not logged in). After the forefront install, users who take their laptops home for extended periods need to connect the laptop on campus on a regular basis to get all updates, patches, and security settings necessary to protect university data.

Desktop Tip

Log out of or lock your computer when stepping away, even for a moment: Forgetting to log out poses a security risk with any computer that is accessible to other people (including computers in lab facilities and offices), because it leaves your account open to abuse. Someone could sit down at that computer and continue working from your account, doing damage to your files, retrieving personal information, or using your account to perform malicious actions. To avoid misuse by others, remember to log out of or lock your computer whenever you leave it.
According to PandaLabs’ annual threat report, in 2010 cybercriminals created and distributed one-third of all existing viruses, creating 34 percent of all malware that has ever existed and been classified by the company. Essentially, that means that the cybercriminals are distributing malware at a pace that the antivirus companies aren’t able to keep up with, and as a result, antivirus products are only about 25% effective at preventing modern malware infections. So what does the average Jane do to protect her home PC?

The answer lies in adopting a layered defense strategy. That means, you need to beef up your home PC’s defenses so that there’s more obstacles for the cybercriminals to overcome before they’re able to get their clutches on your home PC and the valuable personal information stored within. By far the most common infection vector is your web browser and the programs that integrate with it, so that is where you should focus your security hardening efforts.

Here are my recommendations for doing so, based on my experiences with securing the personal computers of friends and family:

- Use the free OpenDNS Basic service (http://www.opendns.com/start/). This will help prevent your PC from contacting web sites known to host malicious material. It also allows you to set up web content filtering if you wish to limit what categories of web sites that you want your family to be able to visit.

- Patch your applications with the assistance of Secunia Personal Software Inspector Version 2 (http://secunia.com/vulnerability_scanning/personal/). This program will automatically keep your most critical applications up-to-date with security patches. It also provides an easy interface for you to manually patch all other applications.

- Make sure that the Windows firewall is turned on, and that Microsoft Update is enabled and functional. If you believe that Microsoft Update may be broken (i.e., it’s not prompting you to install updates on the second Tuesday of every month), try running the fixit tool located here (http://secunia.com/vulnerability_scanning/personal/)

- Use Mozilla Firefox or Google Chrome for the majority of your casual web browsing. Casual web browsing with Internet Explorer is akin to bathing in blood and jumping into a shark tank. For an added level of protection, install the Adblock Plus extension for Firefox and Chrome (http://adblockplus.org/en/). After installation, at a minimum, you should subscribe to the EasyList and the Malware Domains list (http://adblockplus.org/en/subscriptions)

Taking the steps above will help keep your PC safe without compromising its usability. If you’re an advanced user and want to go a little further:

- Install the NoScript extension in Firefox. This will keep you safer, but will break web pages until you train the program so that it knows what sites are safe and which aren’t. (http://noscript.net/)

- Use Keepass or Lastpass to store your passwords, and use different passwords for every site that you access. (http://www.keepass.info/-OR- http://lastpass.com/index.php)

- If you’re using a portable device, consider using full-disk encryption to protect your data in the event that your computer is lost or stolen. Truecrypt is a reliable, free solution (http://www.truecrypt.org/)

Please feel free to email security@scranton.edu with any questions or comments about this article.
Wireless Upgrade Project

By: Calvin Krzywiec, Network Engineer

In a previous IT Matters, I discussed the growing demand on the University’s wireless network and Network Infrastructure’s evaluation of products that can service this demand. Our evaluations focused on the products offered by Aruba Networks and Cisco Systems, both leaders in the wireless industry. We have since completed our evaluations and are in final negotiations with the two companies. We expect to announce our final decision to vendors by the end of March.

The purpose of this project is to overhaul our current wireless network and build one that meets the need of our users today, as well as their need in the future. While there were many technical focuses of the evaluations, there were several main goals of the project we look to achieve.

The first goal, mobility, will allow our users to access resources regardless of their connection medium. Today, access to some academic and administrative resources (e.g. Banner) is restricted from the wireless network. This is largely due to the fact that all users are treated the same on the wireless network and we cannot grant access based on a user’s role at the University (e.g. student, staff, faculty). It is also difficult for us to secure the connection from the wireless client to the wireless network. In order to achieve this goal of user mobility, we plan on deploying user-friendly wireless security (encryption) and role based access control.

Performance is, of course, our biggest focus. In order to provide the wireless throughput needed to meet the needs of our users, we plan on making several changes to our infrastructure. First, all existing wireless access points (WAPs) on campus will be upgraded to the newest technologies (802.11n). Second, we plan on increasing our total WAP count from 215 to 811. In addition, we plan on deploying 35 external access points to provide wireless coverage in green spaces and walkways throughout campus.

The timing of this project is still being determined however we currently predict a campus-wide upgrade to be complete within six to ten months. The first phase of the project will focus on the residential facilities, where the greatest demand for wireless services exists. We hope to have these areas complete before the start of the fall semester. Academic, administrative and outdoor spaces will follow, with a tentative completion date of January 1, 2012. New services will then be phased in throughout the spring semester.

As we finalize negotiations with the two companies, we are also working on finalizing funding for the project. As this process comes to a close, look forward to campus communications announcing the details of this project.