Information Security 101

December 2013

Educational Institutions a Target for Hackers

The New York Times highlighted the increase in cyber-attacks against American research universities, in an article published in July 2013.

Universities are considered particularly vulnerable to attack due to the common culture of openness and information sharing in academia. Detection of these attacks is challenging, with many intrusions going undetected, and the majority of attacks being launched in China. This is difficult for research universities, where collaborating with others both inside and outside the university to share discoveries is the norm. University of Wisconsin cited they’ve seen a significant increase in hacking attempts to university systems to as many 100,000 per day. This increase has caused university officials to rethink the basic structure of their computer networks and modes of sharing, while resisting the temptation to create a digital fortress.

Universities develop intellectual property and sponsor research that can turn into valuable products and back political policies, but university systems are hard to secure in part because students and staff utilize their own devices on these networks. UC Berkeley IT security director shared that university IT security strategy is often opposite that of corpora­tions, whose networks are difficult to enter but easy to navigate once inside. Because of its open nature, overall Berkeley network is treated as just as hostile as the Internet outside.

As threats to academia continue to be on the rise, the Federal Bureau of Investigation has taken on a more active partnership to educate US Universities on a broad array of cyber threats and responses. The F.B.I. has a far reaching Bureaus College and University Security Effort (CAUSE) to partner with academia, which seeks to protect the integrity of research products and protect sensitive information from foreign intelligence threats. Every research university contacted for the recent article on education institutions as a target for hacking said it was in frequent contact with the F.B.I to mitigate threats. Universities have become more vigilant in response to increased incidents of international data theft by urging professors to follow federal rules that prohibit taking particularly vulnerable sensitive data abroad. In addition, University IT Security officials are urging the importance of installing software patches upon release. Doing so prevents becoming target for hacker groups that quickly design programs to take advantage of these security holes.

For more information:
http://www.fbi.gov/about-us/investigate/counterintelligence/us-academia
Securing Your Email: Threats & Tips

An email account is the first and primary component of your online identity and yet it’s often the most unguarded. Regular email is sent in the clear, making users susceptible to eavesdropping, identify theft and even invasion of privacy.
When you use e-mail software such as Microsoft Outlook or Thunderbird (without using account credentials) messages are sent in cleartext from your computer, over the local network and Internet. If you are using a web-based only email service such as Gmail or Yahoo, there are also client-server security concerns, and your messages and login information can be compromised. Maintaining updated antivirus definitions and allowing antivirus to scan email attachments prior to opening are a few best practices. Below are additional tips and best practices protect both work and personal email.
Use secure email:
One free secure email option, Safe Gmail: A free extension of Google Chrome that allows you to send encrypted emails to anyone https://chrome.google.com/webstore/detail/safegmail/Lmkjkmphdmbieffonjmgmfmk-bed

Email Security Tips:
- Keep software up to date; install patches, and enable the operating system automatic update function
- Use digital signatures to identify legitimate messages
- Don’t open attachments you aren’t expecting, (attachments are a common source of viruses)
- Use Spam filters
- Avoid clicking on links in the body of an email message

For more information on safe communication and protecting email: http://www.us-cert.gov/ncas/tips

Stay Secure While on Holiday Travel

The holiday travel season is upon us! As we head out to visit friends and family, or for a holiday getaway, how do we ensure protection and security of our devices that store so much of our personal information while traveling? Here are some tips to keep your devices secure.

Before You Go:
1. Backup. Be sure to backup contacts and data stored on your device. If lost, stolen, or dropped in the pool, the ability to easily transfer data to a new device key to less stress and more fun.
2. Helpful apps. Download an app that adds contact info to the lock-screen or one with GPS technology to locate a phone, and transmit location data to the owner via email.
3. Screen lock. Enable a screen lock code that can’t be easily guessed. 15% of iPhone users have one of the 10 most popular codes (1234, 0000, etc.). Choose a non-sequential passcode longer than 4 digits to protect your data.
4. Remote wipe. If your device is gone, this type of app allows for remote erase of data. Many smartphones come with this installed.

After Arriving:
Connecting to unknown, open wireless networks can be risky. If only unsecured networks are available, take extra care with these steps:
1. Disable the "automatically connect to non-preferred networks" setting.
2. Turn off file and printer sharing.
3. Switch off your wireless card and or Bluetooth when not in use.
4. Use only VPN or other encrypted tunnels for business.
5. Always log out of social media, bank accounts or other password-protected websites.

It’s Gone! Now What?
1. If missing, track it. Activate the GPS tracker app which may include a beacon function, and will sound a loud alarm when activated. This will be useful if your phone is hiding under the hotel bed or rental car seat.
2. If stolen, report it. If all hope is lost on finding your device, it’s time to implement the remote wipe app.
3. Contact your service provider to disable the account.

15% of iPhone users have one of the 10 most popular screen codes.
Revision 4 of NIST SP 800-53 Released

On April 29th, NIST released Revision 4 of Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. This marks the most extensive revision yet and included the first public call for review and comments. Revision 4 was driven by factors including:

- the evolving threat landscape
- availability of empirical attack data
- gaps in insider threat, application security, and advanced persistent threat
- trustworthiness and assurance of information systems, during development and during operations via continuous monitoring

Changes included in Revision 4 support the federal information security strategy of “Build It Right, Then Continuously Monitor” and are directly linked to the current threat space and the attack data collected and analyzed over a substantial period of time. This update emphasizes security controls to increase the reliability, trustworthiness, and resiliency of information systems, system components, and information system services. Significant changes include:

- New security controls and control enhancements addressing the advanced persistent threat (APT), supply chain, insider threat, application security, distributed systems, mobile and cloud computing, and developmental and operational assurance;
- Clarification of security control language;
- New tailoring guidance including the fundamental assumptions used to develop the security control baselines;
- Significant expansion of supplemental guidance for security controls and enhancements;
- Streamlined tailoring guidance to facilitate customization of baseline security controls;
- New privacy controls and implementation guidance based on the internationally recognized Fair Information Practice Principles;
- Updated security control baselines;
- New summary tables for security controls and naming convention for control enhancements to facilitate ease-of-use;
- New mapping tables for ISO/IEC 15408 (Common Criteria);
- The concept of overlays, allowing organizations and communities of interest to develop specialized security plans that reflect specific missions/business functions, environments of operation, and information technologies; and
- Designation of assurance-related controls for low-impact, moderate-impact, and high-impact information systems and additional controls for responding to high assurance requirements.

SP 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. This “Build It Right” strategy is coupled with a variety of security controls for “Continuous Monitoring” to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.

Information Assurance Working Group Update

2013 IAWG meetings were a continued success, with collaborative participation across the Arctic IT service provider community resulting in:

- Arctic Privacy Policy vetted, approved, and published in the ARC Information Security Handbook
- Arctic System and Services Acquisition policy review
- Implementation of Security Warning Banner for Arctic Systems
- Collaboration on execution of the July 2013 Security Control Assessment on Arctic systems and operations at Toolik Field Station, Barrow, Alaska, Fairbanks, Alaska, and Denver, Colorado locations