UW Security Policy and Implementation

12 May 2011
TINFO 340: Information Assurance

Stephen Rondeau
Institute of Technology
Labs Administrator
Policy Agenda

- Data Issues
- Key Security Concepts
- Sampling of Laws
- Complying with the Law
- Consideration of Ethics
- Consequences
- References
Data Issues

• Sensitivity: public or confidential
  – public: still needs protection
  – confidential
    • minimal, more sensitive, most sensitive
    • owned by someone
    • specific statements for access, distribution, storage, disposal and penalties for disclosure

• Criticality: importance of data to function
Key Security Concepts

• Must protect:
  – Services/Use
    • Functionality: perform function or use device
    • Availability: device or data is ready for use on demand and at operational speed and capacity
  – Data
    • Confidentiality: prevent unauthorized disclosure
    • Integrity: prevent alteration and spoofing
Sampling of Laws

- International, federal, state, UW
  - statutes and regulations
- Federal
  - privacy, wiretapping, fraud, disclosure, surveillance, counterterrorism
  - grant-related policy
- WA State
  - privacy, malicious mischief, public records, spam, disclosure
- UW Administrative Code
  - student and general conduct, records access
Complying with the Laws

• Comply: take action to conform
• Law => Policies + Standards + Guidelines
• Policies state what needs to be done
• Standards define how to implement the policy (via procedures)
• Guidelines are strongly-recommended practices to assist in adhering to standards
Roles and Responsibilities

- System owners and operators
  - comply with laws, policies, guidelines
  - maintain confidentiality of sensitive data
  - grant access based on “least privilege” and “separation of duties” principles
  - report security incidents and perform incident response
- Data Custodians
  - manage data access, storage, transmission and usage
- Users
  - protect and maintain UW information systems/data
Policies

- Monitor user accounts, files and access as needed
- Understand nature of data on systems, and manage it appropriately
- Provide logical and physical access control and logging
  - commensurate with sensitivity and criticality of computing devices, networks and data
- Document procedures for issuing, altering and revoking access privileges
- Implement minimum computer and network measures and practices
Consideration of Ethics

• Ethics: principles of conduct that are harmonious with society
  – arguably higher than policy
  – notable examples
    • whistleblowing
    • preventing conflicts of interest
    • protecting life
• Use of university resources; data sensitivity
Consequences

• Loss of privacy
• Loss of research, funding, reputation
• Malware infections
• Unauthorized use
• Information theft
• Vandalism
• Cheating
References

• UW Information Systems Security Policy
  – http://www.washington.edu/admin/rules/APS/02.01TOC.html

• UW Guidelines for Implementing Systems and Data Security Practices
  – http://passcouncil.washington.edu/securitypractices/

• UW Minimum Computer Security Standards
  – http://www.washington.edu/computing/security/pass/MinCompSec.html

• UW Minimum Data Security Standards Policy
  – http://www.washington.edu/admin/rules/APS/02.10TOC.html

• UW Electronic Information Privacy Policy
Implementation Agenda

• UW Minimum Computer Security Standards Summarized
• Examples using Windows XP
• Example using Group Policy
Minimum Computer Security Standards: Goals

• “The focus [...] is on protecting computing devices from misuse and is intended to [...] prevent subject devices from:
  • being accessed or used by unauthorized entities.
  • causing harm to other UW computers or computers at other organizations.
  • causing harm to the UW network or other networks.”

• Does not address “information security”
  • i.e., protecting the information on those devices
Minimum Computer Security Standards: Applicability

- Applies to one or more of the following:
  - owned by the UW
  - directly connects to the UW network
  - accesses UW network via:
    - the UW dial-in service
    - a wireless access point attached to UW network
    - a Virtual Private Network (VPN), such that the device is effectively part of the UW network and capable of sending arbitrary packets to any UW computer.

- Doesn't apply to:
  - non-UW computers connected from non-UW locations via secure protocols
Minimum Computer Security Standards: Audience

• All applicable computing devices:
  – will have, explicitly or implicitly, an individual or group responsible for the configuration and management of that device
  – If the device lacks a professional system administrator, the owner or end-user is responsible for implementing this standard by whatever means possible
Standards for Servers, Desktops, Laptops: Part I

- restrict physical and logical access to authorized users
- provide login control to the device through the use of good passwords transmitted only across a secure (encrypted) network link
- disable and/or block all unnecessary network services. For servers, only allow essential incoming or outgoing traffic. For desktop or laptop computers: block unsolicited incoming connections.
- use only operating system and application software versions for which security updates are readily available; otherwise, restrict access to vulnerable services
Standards for Servers, Desktops, Laptops: Part II

• enable software auto-patching

• do not install any software that grants unauthorized users access to non-public data stored on, or accessed through, subject devices.

• counteract malicious and other prohibited software that may infect computers by installing auto-updating defensive software (e.g., anti-virus and anti-spyware)
Standards for Servers, Desktops, Laptops: Part III

• **enable logging**: periodically review server logs and keep client logs for audit or diagnostic purposes. Log at least authentication failures and security setting changes.

• when installing (or re-installing) a computer operating system or other software packages that require multiple steps, and using the network to obtain software updates, **ensure that the system is safe during the update process**
Standards Examples: Part I

- restrict access to authorized users
  - create user accounts and groups
  - assign file/directory permissions to groups
- provide login control
  - set password policy via Local Security Policy
- disable and/or block unnecessary services
  - use services.msc to see
  - use Windows firewall to block incoming
- use only operating system and application software versions for which security updates are readily available
Standards Examples: Part II

• enable software auto-patching
  • turn it on via the Control Panel

• do not install any software that grants unauthorized users access to non-public data
  • nothing to configure

• counteract malicious/prohibited software
  • http://www.washington.edu/uware/sophos
Standards Examples: Part III

- enable logging; log at least authentication failures and security setting changes
  - eventvwr.msc
  - Local Security Policy/Local Policies/Audit Policy

- ensure that the system is safe during the update process
  - get service packs beforehand
    http://support.microsoft.com/sp
Standards Example: Group Policy for Many Computers

- Active Directory with one client computer
  - Windows 7 client
  - Joined to domain
- Look at existing password length for client
- Group Policy (GP)
  - Set a password length policy for domain
  - Possibly force GP update
- Look at current password length for client
Conclusion

- **Bruce Schneier wrote:**
  - "Security is a chain; it's only as secure as the weakest link."
  - “Security is a process, not a product.”
- Everyone is responsible for it
- Only have a *better* chance if you follow best practices and standards to implement policies, to conform to laws
- Always think about what you are doing