

Information Assurance Best Practices for Faculty

2007 Professional Development Day

Christophe Veltsos, Ph.D.

Assistant Professor
Department of Computer & Information Sciences
Minnesota State University, Mankato

Speaker Background

Not your average paranoid faculty

- 1998, Ph.D. in Computer Science (focus on highly complex systems and Petri Nets).
- Joined MSU in 1998
- Relevant teaching portfolio:
 - Intro to Data Communications & Networking (taught for 6 years)
 - Communication Protocols (helped create and taught twice)
- 2005-2006 Sabbatical at Iowa State U. to pursue a Grad. Cert. in Information Assurance.

Outcomes

What's in it for me?

- I want to help you become aware of:
 - what can happen (and how easily)
 - the threats you face
 - the threats you pose and cause
 - what you can do
 - who you can turn to
 - how things change (MSU ITS, OS Patches, new attacks and defenses)

Security – A perspective

When the past can become the future

- Sun Tzu – The Art of War:
 - You can be sure of succeeding in your attacks if you only attack places which are undefended.
 - So in war, the way is to avoid what is strong and to strike at what is weak.
 - Do not repeat the tactics which have gained you one victory, but let your methods be regulated by the infinite variety of circumstances.

Source: <http://www.chinapage.com/sunzi-e.html>

Why Security? Why care?

Because it can change your life!

1. It can happen to you
2. An ounce of prevention...
3. Impact on your courses and research
4. Behave as you would have others behave
5. Spread the word – profess your new religion

Why Now?

Security: a bad dream?

- Security is on everyone's mind and MSU would rather not be in the news.
- Security problems won't go away anytime soon:
 - People and machines
 - Behavior and technology
- An increasing amount of data is at stake and there are plenty of ways to get at it.
- Security breaches will incur increasing penalties.

The Vulnerable Ivory Tower

Where anything (but security) goes

- Faculty office doors left open
- Loose password/access procedures
- Grade posting practices not followed
- Backups (What backups?)
- Removable media (a USB what?)
- Emails out of control (send me your SSN)

The Faculty Member's Treasure Trove

Open sesame

- Student data which is protected by [FERPA](#) and [MGDPA](#).
 - admissions, financial aid, transcripts, graded exams and papers, work study records, and more.State employees have a legal responsibility to protect the privacy of student educational records under their control, including access within the institution.
Source: [MSU FERPA](#) and the [MGDPA](#)
- Other private/confidential data:
 - as a reviewer: papers, book manuscripts
 - as a researcher: confidential data and IP

The Faculty Mindset

Not bred for privacy

- As faculty, we are used to
 - sharing with colleagues
 - sharing with students (sometimes even sharing office space)
 - sharing with large audiences (classes, conferences)
- in other words,
 - sharing with the world

Security Monsters

Searching for your identity in a world of PII

- PII versus Public
 - PII – Personally Identifiable Information
 - Public or directory information
- Be vigilant with data, as a faculty, as a student, as an employee
 - Why do you need it?
 - How do you use it?
 - How will you protect it?

MSU Directory Information

What you thought might be private just might not be...

1. Name
2. Date and place of birth
3. Local and permanent address
4. Major field of study
5. Local and permanent telephone number
6. Dates of attendance
7. Previous college/university attended
8. Degrees received
9. E-mail address
10. Awards and honors
11. Height and weight information for athletic participants
12. Performance records and participation in competitive events
13. Participation in officially recognized activities, sports and organizations

Source: www.mnsu.edu/registrar/DATAPRIV.html

Monster Mayhem

Identity Theft

- Large # of people affected.
- Need to be vigilant for a long time.
- Level of disclosure hard to accurately assess.
- More states crafting disclosure laws (sometimes with minimum standards regarding time to disclose).

Information Assurance Primer

Be scared, be very scared; you will never be the same

Information Assurance

Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Source: US Intelligence Community - www.intelligence.gov/0-glossary.shtml

Information Assurance Primer – cont.

IA versus Information Security

In addition to defending against malicious hackers and viruses, IA includes other corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery.

Source: Wikipedia - http://en.wikipedia.org/wiki/Information_assurance

The CIA Triad

A one-slide indoctrination

- Confidentiality
- Integrity
- Availability
- Accountability
- Non-Repudiation
- Authentication

Screen tips information from Wikipedia

Malware Threats

Malware, malware, everywhere

- Virus
- Trojan
- Worm
- Spyware
- Advanced malware:
 - Exploits
 - ZDA
 - Rootkits

Security Monsters

Malware – is there a ghost in the machine?

- If your data had been compromised, would you know it?
- If your machine had been hijacked, would you know it?
- How quickly would you realize it?
- What steps would you take to recover?
- How quickly would you recover?

Social Engineering Threats

Give me your PIN and I'll give you happiness

- Spam
 - Email overload leads to wasted time, inattention, or loss of information. Combines with phishing.
- Phishing
 - "Congratulations, you've won \$500. Simply give us your account so that we can deposit your prize."
- Pretexting
 - "Hi, I'm Jane, can I have my grade please."
 - The problem of large classes and an inadequate student record system - Paint me a picture.

Online Security - Overview

What you don't know can expose your data

- The internet is built atop a set of flawed assumptions about users, hosts, and networks.
- Worse, many application programs have flaws which expose the core of the machine to attacks from the outside.

Online Security – Communication Basics

On the meaning of being "online"

- You are "online" when you can send/receive data – and you usually need to do both.
- Application programs use the operating system to send data via the network to the internet.

Online Security – Communication Basics

On the meaning of being “online”

- You are “online” when you can send/receive data – and you usually need to do both.
- **Application programs** use the **operating system** to send **data** via the **network** to the **internet**.
 - IE uses Windows to send data via Ethernet to the Internet.
- Many points of attack due to flawed assumptions and implementations.

Online Security – Web Dangers

Getting yourself in a web of trouble

- Browser flaws
- Sites with hostile content
 - pop-ups
 - message boxes
 - downloads
- Data in plaintext – i.e. not encrypted
- Cookies – just another crumb

Online Security – Email Dangers

Getting yourself in a web of trouble

- Tech ids floating into thin air
- Data in plaintext – Except
 - Except when over VPN (the tunnel itself is an encrypted communication medium).
 - Except over encrypted MAVMail (starts with HTTPS)
 - Emails coming/going off-site however will travel unencrypted!
- Mail from Santa – Mail sender/receiver cannot be trusted, especially off-site
- Mail clients have flaws – MS Outlook

Online Security – Wireless Dangers

Opening a can of flying worms

- Danger of simply being online
 - Makes your machine visible on the network – now vulnerable to attacks using unpatched security holes.
 - November/December Broadcom Driver flaw that affected Windows machines.
- Choosing your security options:
 - Unencrypted
 - WEP
 - WPA

Online Security – Other Programs

No one is safe, not even Firefox

- Microsoft Office Suite (Outlook, Word, Excel, Access, PowerPoint)
- Firefox (alternate web browser)
- Instant Messaging tools
- Any type of service (which accepts and responds to requests): web server, file sharing, peer-to-peer.

Physical Security – Work Environment

On security when every door has at least 3 keys

- Would you leave your checkbook/credit card in your office with the door open or unlocked?
- Too many keys: master keys, sub-master keys, GAs/RAs/TAs
- Office break-ins at critical times; any exams laying around?

Monster Sightings

MSU's Own Experience during the Fall 2006

From official MSU talking points

- Situation: Two laptop computers used by faculty were stolen from Minnesota State University in the Fall 2006. The computers contained final grades for over 800 students.
- Worst-case Scenario: Minimal. No student information on either laptop can be used for identity theft.
- Remedy: All students affected have been notified by mail, as per federal law when grades are involved.

Physical Security – Machines & Media

Give me a machine and I'll give you access

- Physical access to unencrypted media means unauthorized access.
- Physical access to a machine can lead to unauthorized access in a matter of minutes; breach of CIA.
- USB Storage devices are small in size, big in capacity. Should the data it contains be encrypted?

Physical Security – At Home

Is your data feeling secure at home?

- Keep other people off.
- Keep FERPA data private.
- Watch what you do/send/receive.
- A virus/worm in one machine could spread to others rapidly.
- Wireless – yes, but with caution.

Physical Security – On The Road

On The Road Again

- Don't leave valuables (including MSU property) in plain sight.
- Don't connect to wireless network unless you are fully patched and running both Antivirus and Firewall.
- Do consider encrypting PII or sensitive data.

Encryption

The art of hiding in plain sight

- the process of obscuring information to make it unreadable without special knowledge...
Source: Wikipedia - <http://en.wikipedia.org/wiki/Encryption>
- FDE – Full Disk Encryption
 - MSU trial of PointSec
 - Few free options for multi-platforms
 - [CompuSec](#) (CEInfosys) is free (Win/Lin)
- File-level encryption
 - [AxCrypt](#) (Win only)
 - [TrueCrypt](#) (Win/Lin)
 - [FreeOTFE](#) (Win but can read Linux)
 - [GPG4Win](#) (Win wrapper for GnuPG)

Beyond Security – Recovery & Continuity

A backup is worth a thousand hours

- Backups
 - Frequency
 - Type
 - Location & Protection
- USB Drives – play it safe.
- MavDisk - an untapped resource for disaster recovery and business continuity.

ITS & Information Security

Relax, the manager is here!

- Kevin Thompson, MSU's new Information Security Manager is busy improving our security
 - Tools like FDE
 - Policies, Procedures, Standards, Guidelines
 - Investigations of incidents
 - Shoring up defenses

Best Practices

Making the grade

- Practice physical security, access control.
- Practice operations security: need-to-know, labeling/handling sensitive data, backup, antivirus, malware control.
- Use secure communications when dealing with sensitive data.
- Use encryption when needed: protect data at rest or in travel.

Free Security Tools

No one size fits all, but that's the price of free!

- Antivirus: [AVG](#), [Comodo](#), [AntiVir](#)
- Antispyware: [MS Windows Defender](#), [Ad-Aware Personal](#), [Spybot - Search & Destroy](#)
- Firewalls: MS Windows Firewall (built-in), [Comodo](#), [Zone-Alarm](#)
- Syncing/Backups: [MS SyncToy](#), [Comodo](#), [SyncBack Freeware](#)
- Web Browsers: MS IE (built-in), [Firefox](#), [Opera](#)

Thank You

I'm done crying wolf!

Ponderables

- Where do we go from here?
- Where does it stop?
- Where do I start?