Evaluating Hard Disk Encryption in an Academic Environment

Jonathan McIndoe Hunt
jmhunt@mit.edu
Senior Manager Software Services
Information Services & Technology

MIT Security Camp
August 15, 2006

Information Services & Technology

Massachusetts Institute of Technology

Today's Discussion

- What's the problem?
- Sensitive Data and the need for Disk Encryption Solutions
- Disk Encryption Pilot
- Wiki as a tool for evaluating solutions
- Discussion & Additional Questions

The Problem

- Too much sensitive data is stored and worked with locally on peoples desktops and laptops.
- Too many people don't realize that the data is sensitive and if they do aren't sure what to do about it.
- After a machine disappears it is too late.
- Too much unneeded sensitive data is collected.

The Solution

- Education
- Change the way work is done
- **Protect the data**
  - Encryption is only part

Sensitive Data - the brief view

What is Sensitive Data?

- Anything that requires special care or protection as a result of law or policy:
  - Social Security Numbers (with name)
  - Date of Birth (with name)
  - Medical Information (HIPAA)
  - Student Information (FERPA)
  - And much more!

Sensitive Data - the brief view

Why should you care?

- Most likely it is part of your job responsibility
  - MIT Policy 13.2.2
- They are handling your data

Recent Public Events

- 2 MIT data spills this year involving some SSNs early in 2006
- Diskettes with Veterans' information stolen from programmers house (lots of SSN and DoB)
- Credit Card companies

How does Disk Encryption fit?

- Protects against threats like laptops being stolen with sensitive data
- Raises awareness of dealing with sensitive data

Disk Encryption is not THE COMPLETE Solution

- Would not have prevented 2 most recent MIT spills
- Does NOT protect against weak passwords, network attacks, etc.
- Does NOT protect data in transit over networks
- Does mitigate some risks and is worth deploying

Current Evaluation of Operating System based Encryption

- Goals:
  - Easy to use
  - Transparent to the user
  - Recovery from forgotten passwords
  - Protect sensitive data from exposure on stolen equipment
  - Easy to setup
- FileVault - Mac OS X
- Encrypted File System (EFS) - Windows

FileVault - Advantages

- Easy to setup
  - Click a couple buttons and wait
- Protects everything in user's home folder
- Simple Recovery Agent with Master Password set
- Warns of blank account passwords and disables auto login
- Integrated with main login

FileVault - Disadvantages

- Long setup time
  - 4.5 hours on MacBook Pro - 28 GB of user data
- Backup requires special attention
  - No more incremental backup with SuperDuper!
- No granular control
  - Entire home folder or bust

Encrypted File System - Advantages

- Quick to setup
  - A few clicks and you have encrypted the file or folder
- Granular Control
  - Files or Folders can be encrypted using EFS
- Multiple Recovery Agents possible
- Integrated with main login

Encrypted File System - Disadvantages

- Does not warn for blank account passwords
- Granularity can confuse users as to where they should store their files
- Setting up Recovery Agents requires good understanding of certificates

Process in use for Evaluation

- Test group of tech savvy volunteers from MIT Community
- Wiki - Confluence based
  - Setup instructions
  - Test results (templates)
  - Exportable (PDF,XML,HTML) - HDEncrypt.pdf
  - http://confab.mit.edu/confluence/display/SWEVAL/Hard+Disk+Encryption+Evaluation

Discussion & Additional Questions

http://confab.mit.edu/confluence/display/SWEVAL/Hard+Disk+Encryption+Evaluation

Jonathan M. Hunt
jmhunt@mit.edu

Information Services & Technology

Massachusetts Institute of Technology