

Key Management & Mobile Computers in the Government

Bill Burr
NIST

IEEE KEY MANAGEMENT SUMMIT 2008

NIST

- National measurement laboratory
 - Laboratories:
 - Physics, Chemistry, Electronics, Nanotech, Buildings & Fire, Manufacturing, Materials, **Information Technology**
- Information Technology Laboratory (ITL)
 - Divisions:
 - Math & Computational Sciences, Networking, Information Access, Software Diagnostics & Testing, Statistics, **Computer Security**
- Computer Security Division
 - Groups:
 - Research, Management & Assistance, Security Testing, **Security Technology (crypto)**

Security Technology Group

- SecTech does several things
 - Standards (FIPS) & recommendations for crypto
 - Apply directly only to US Fed. Gov
 - For protection of sensitive, unclassified data
 - Voluntary standards work for crypto & protocols
 - Mainly in IEEE 802, IETF & X9
 - Various mandated (law, Pres. or OMB) projects
 - Voting standards (Help America Vote Act)
 - E-Gov initiative/ e-Authentication
 - PIV (HSPD-12) – now mainly just the crypto
 - Inter-agency cooperation – too many committees
- Personnel
 - 16 (+1) professional staff, 4 guest researchers

OMB M-06-16

- “I am recommending all departments and agencies take the following actions:
 1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
 3. Use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
 4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.”

OMB M-07-16

- “Within the framework set forth in the attachments, agencies may implement more stringent policies and procedures reflecting the mission of the agency. While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as:
 - reducing the volume of collected and retained information to the minimum necessary;
 - limiting access to only those individuals who must have such access; and
 - using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals. “

Full Disk Encryption (FDE)

- The term “full disk encryption” does not occur in M-06-16 or M-07-16
- Nevertheless many agencies are asking for full disk encryption in response to M-06-16.
- What is FDE?
 - Apparently any method that encrypts an entire hard drive, except for some initial boot record
 - May be entirely software, could be in the drive controller, or could use assist hardware (e.g. TPM)
 - User typically enters a password at boot time

FDE – Key Management

- Key or password backup is a big issue
 - otherwise loose the key or password and you often loose all the data on the disk
 - To the extent you don't loose all the data, you probably don't have very good FDE
- Many FDE “solutions” have some provision for managing and backing up keys and passwords

FDE – how useful is it?

- A good FDE system gives protection when a system/drive is lost or stolen.
 - May also provide “instant erase” or “sanitization”
- Protects swap files, temp. files, deleted files
- FDE subject to network or malware attacks
 - If the drive is in use then malware has access too.
- Activated, “sleeping” or recently turned off software systems may be vulnerable to attack
 - “Lest we remember:”
<http://citp.princeton.edu/memory/>

All software FDE

- An “all software” FDE solution may fall to a password dictionary attack if a drive/system is lost, stolen or imaged
 - Attacker has everything needed for an offline password attack
 - Need high entropy passwords
 - Nothing between attacker and plaintext except the entropy of the password
 - Don't make users change these passwords frequently

FDE – at least 5 variants

- Pure software
 - Key is on the encrypted laptop drive
 - Plaintext key in laptop DRAM when drive is active
- Store key on separate device
 - Key can be removed from laptop
 - Plaintext key in laptop DRAM when drive is active
- Trusted hardware to secure keys (TCG/TPM)
 - Trusted chip on motherboard to secure keys & boot process
 - Plaintext key in laptop DRAM when drive is active

FDE – at least 5 variants

- Removable crypto module
 - Key is never in laptop memory
 - Module can be separated from the data
- Encryption built into disk drive controller
 - No performance hit for encryption
 - Key is never in laptop memory
 - But key is always bundled with the data on the drive
 - Extracting raw ciphertext from drive is laboratory scale problem
 - Extracting the key is probably an even harder lab problem
 - FIPS 140-2 validation issues for single chip controller

Plaintext keys in laptop DRAM

- Modern CPU is fast crypto engine
 - Small performance hit – seems attractive
- Malware is obvious problem
- “Lest We Remember: Cold Boot Attacks on Encryption Keys”
 - Keys can be recovered for some time after power off
 - Capacitive memory decays gradually
 - Key schedule also in DRAM
 - Makes an effective key error correction code
 - <http://citp.princeton.edu/memory/>
 - Not the end of the earth, but
 - Need to wait a while after you turn you laptop off before you leave
 - Don't leave your encrypted laptop in “sleep mode”

Other solutions

- Volume, file or application level encryption have other advantages
 - Key is less likely to be activated exposing the key or data to malware
 - Sensitive data that isn't often used is less exposed
 - Everything doesn't have to be encrypted under the same key

Verify Extract Erased Within 90 Days

- NIST FAQ
 - <http://csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf>
- Probably a business opportunity here for a good solution
- Problem seems related to DRM
 - And for similar reasons really hard
 - Probably largely a key management problem
- Ephemerizer – Radia Perlman
 - http://research.sun.com/techrep/2005/smli_tr-2005-140.pdf
- My guess is that some kind of trusted hardware is required

Questions?

IEEE KEY MANAGEMENT SUMMIT 2008