

# Security for Disk Drive Data at Rest ... Disk Drive Opportunities?

---

- **Gordon Hughes, CMRR**  
**gfhughes@ucsd.edu, 858-534-5317**
- **Protect data where it lies**
- **In the disk drives where it resides**
- **Why not evolve the ATA password system**  
**Into fully secure in-drive data encryption?**  
**and improve Secure Erase of disk drive user data**
- **Safes are locked, even in locked offices...**

# Years of Sloppy Losses of World's User Data

---

- **Repeated losses of SSN's, credit cards**
- **From lost or stolen laptop computers**
- **By sloppy credit card companies,**
- **By sloppy credit rating companies**
- **Tape backups lost to/from vaults**
- **Disk drives sent out for repair  
winding up on eBay instead**

# Sloppy is Now Illegal As Well

---

- **Five Federal laws now threaten fines and penalties for such releases of private information.**

**Health Information Act (HIPAA)**

**Personal Information Protection Act (PIPEDA)**

**Gramm-Leach-Bliley Act (GLBA)**

**California Senate Bill 1386**

**Sarbanes-Oxley Act (SBA)**

**SEC Rule 17a**

# All Computer Data is in Disk Drives

- **Today's computer data protection is not secure**
  - Many malware attack possibilities**
  - Unerased drives removed from computers & RAID arrays**
  - Users lose laptops regularly**
- **Why isn't all data securely encrypted by O/S?**
- **Because users demand transparent data availability**
- **Enterprise RAID storage: IT staff ditto**
- **Users only accept/allow automatic security**
  - Users do not voluntarily set up encryption**
  - (Some companies mandate their IT staff set it up)**

# Software Encryption

- **Known solutions: open source software encryption**  
PKC, PGP, DES, AES...
- **Windows 2000, XP & Vista offer encryption**  
But user transparency makes it default to “disabled”  
Transparency also weakens key security (travels with data)
- **Vista intended to be a Secure Platform**  
IF Trusted Platform technology is present & used
- **But Vista installation defaults initial user to insecure**  
Gets Administrator status, no password required
- **This means 99% of Vista users will be insecure**  
They get security only via the Windows password system
- **∴ Passwords will remain primary laptop loss protection**

# Virtually all Security is via Passwords

---

- **Some banks & governments mandate security**  
**Passwords plus smart cards or biometric devices**
- **Still, 99% of users only use passwords**
- **Solution: passwords plus “Trusted Platforms”**
- **Result: password-only transparent security!**  
**Password logs user on only if computer unaltered**  
**...Unchanged system board, disc drives, keyboard...**
- **TPs use TrustedComputingGroup.org rules**

# Trusted Computing Group

- **An open standards spec development group**  
**More than a hundred computer technology companies**  
Including Seagate, Western Digital, Hitachi, Fujitsu...  
**PCs, Processors, chips, system boards,**  
**Operating systems, peripherals...**
- **TP is based on “Trusted Platform Module”**  
**A chip on computer system board**  
Controls computer-wide trust process and encryption keys  
**Controls secure access to *Trusted* disk drives**
- **No access possible if drive leaves computer**  
**Except securely erasing all data - should open drive**

# Secure Trusted Platform

- **A computer meeting Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules standards FIPS 140-2**
- **Resistant to password/key & access attacks**
  - 1. Attacks across ATA/SCSI interface connector**
  - 2. Laboratory attacks**

Scopes and logic analyzers on DRAM pins, for example
  - 3. Exotic scientific instrumentation attacks**

MFM “bit read channels” (paranoid fears)

# Trusted Drives via TP

- **Full TP removes today's security flaws**
  - Most users don't/won't password their drives**
  - ATA Secure Erase helps, but has some security flaws**
- **TP issues:**
  - Needs T13.org ATA spec committee approval**
  - Then needs several year wait for all drives to comply**
  - Customers are slow to accept new disk drive features**
    - Beyond the basic half-century-old job of block write & read
- **But one TPM benefit is available today!**

# ATA Secure Erase via encryption

- **In-drive data encryption\*** is critical feature of TP
- **Allows Secure Erase via encryption – now!**
- **Securely erases drives by changing encryption key**  
**Takes microseconds instead of 30-60 minutes for ATA SE**  
**Drive erasable (only) by IT with a Master key/password**
- **Seagate now shipping encrypting mobile drives**  
**Evolves the ATA password system into TP**
- **TP securely handles drive key requests**  
**New key/keep data, new key/erase data...**  
**Keys should never leave drives**  
**IT may demand keys, but only needs Master PW SE**

\* G Hughes, “Wise Drives”, IEEE Spectrum, August 2002

# More About In-drive Secure Erase

---

- **Put into ATA & SCSI specs (t10.org, t13.org)**  
at CMRR's request ten years ago  
T13 included Secure Erase in ATA password system  
SE now universal in all ATA drives (CMRR tests)
- **SE only one part of data-at-rest security**
- **However, it has high Federal approval**  
Only degaussing and physical destruction higher  
NIST document 800-88

# Disc Drive Data Sanitization

---

- **Federal standards set by National Institute of Standards and Technology NIST 800-88:**
- **“Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed”**
- **Software block overwrite: Lowest security level**
- **Purging by ATA Secure Erase: Confidential data**
- **Drive destruction, disk shredding: Highest**

# Extending present Secure Erase to TP

---

**ATA SE command today has malware vulnerable**

**Single command will erase entire drive**

**Many BIOS chips prohibit SE**

**ATA Security Freeze command**

**Reassigned blocks may be unerasable**

**Servo defects, for example**

**SE can take up to an hour for large drives**

**Block overwrite 2X longer, like Norton Gov't Wipe**

**Means users won't bother to erase**

# Conclusions

---

- **Heavy public pressure for data security now**
- **Backed by new Federal and state laws**
- **SE drive command can help today**
- **Can also help acceptance of trusted drives**
- **First available TP feature**
- **Federal agencies back encryption**
- **Need Federal approval of in-drive encryption**