TRADE-OFFS IN SECURE FLASH DESIGN

Kevin Vlasich, CISSP at Imation

THE RISK OF REMOVABLE STORAGE

UK Study: 17,000 USB sticks were left behind in 2010 in clothes left to be dry cleaned

(Source: www.credant.com on 3/1/2011)

DESIGNING A SECURE FLASH MEMORY DEVICE

- **Security Objectives**
  - Confidentiality
  - Integrity
  - Legal compliance
- **Other objectives**
  - Portability
  - Performance

SECURITY: SOFTWARE OR HARDWARE?

SOFTWARE ADVANTAGES

- Faster development
- Ability to tune performance and features post-release
- Easier to evaluate for security correctness

SOFTWARE DISADVANTAGES

- Key management
- Offline attacks possible
- Performance

HARDWARE ADVANTAGES

- **Increased Security**
  - Ability to protect crypto keys in hardware
  - Security critical decision in hardware
- **Faster performance**
- **Higher level certifications possible (e.g. FIPS 140-2 Level 3)**

HARDWARE DISADVANTAGES

- **Cost**
  - Longer development cycles
  - Limited COTS options

- **Little or no updates after release**

HYBRID SOFTWARE/ HARDWARE SOLUTIONS

- **Use hardware for what it does best**
  - Protecting cryptographic keys
  - Encryption

- **Use software for what it does best**
  - Central Management
  - Auditing & Reporting
  - End user applications

THE SECURE ERASE PROBLEM

- **Problem: Erasing data from flash based memory is problematic at best**

- **Solution:**
  - All data should automatically be encrypted
  - Ability to delete crypto keys

AUTHENTICATION OPTIONS

- Password
- PKI
- Biometric

PASSWORD

- **Password authentication advantages**
  - Easiest to implement
  - Integration into Active Directory

- **Password disadvantages**
  - Not very secure
  - Help Desk costs

BIOMETRICS

- **Advantages**
  - Ease of use
- **Disadvantages**
  - Cost
  - False positives

PKI

- **Advantages**
  - Security
    - No private keys are transmitted
  - Convenience

- **Disadvantages**
  - Initial overhead of setup
  - Possible reoccurring cost

STRONG AUTHENTICATION

Santa Clara, CA
August 2011
15

KEY BACKUP

- **Should devices allow for cryptographic keys to be backed up?**
  - Why Yes
    - Recovery of data
  - Why No
    - Complicates security

Questions?