



Tutorial T1A: Introduction to Flash Memory

Security and Flash Memory Tutorial

Presenter: John Geldman
Lexar Media
jgeldman@lexar.com

Security and Flash Memory Tutorial

- Protection against Data Loss
 - Loss & Host-originated Attacks
- Protect the Host against Flash-originated Attacks
- Six Tools of Cryptography
- Security != Cryptography
- Password Protocols
- PKI & Certificate Protocols
- Conclusion



Protection against Data Loss

Santa Clara, CA USA
August 2007

Flash Memory Summit A/V Sponsor: **Seagate** 

Protection against Data Loss

- **Data Capacity is rising**
 - New functionality in Flash device's allow your whole environment to be portable (Lexar's PowerToGo)
 - How much information about you is in your whole environment?
- **Transient Storage is growing** (Gartner 2006)
 - ~100 Million USB Flash Devices (UFDs) will be sold in 2007
 - ~25 Million will be used in an Enterprise domain
- **An incredible number of storage devices are lost**
 - In one six month period over 100K storage devices were found in Chicago taxis alone (Pointsec Mobile Technology 2005)
- **Transient Storage (Flash Cards and UFDs) are the easiest target**
 - Laptops (SSDs and HDDs) are another major target
- **Prediction**
 - Security will be embedded in all transient storage within 5 years
 - Most general purpose storage will include hardware encryption (FDE) within 5 years

Protection against Data Loss

- Data/Device Loss & Theft Scenarios
 - Simple Loss
 - Targeted Theft (for resale)
 - Targeted Theft (for data)
- What data was lost?
 - Non-existent or un-enforced Data Policies
- Security protocol design guidelines

Know what you are protecting, know the threats and know the attackers to protect data appropriately

 - As developers, we can't even know what our users will save
 - As IT, we can implement Data Tracking software tools



Protect the Host against Flash-originated Attacks

Santa Clara, CA USA
August 2007

Flash Memory Summit A/V Sponsor: **Seagate** 

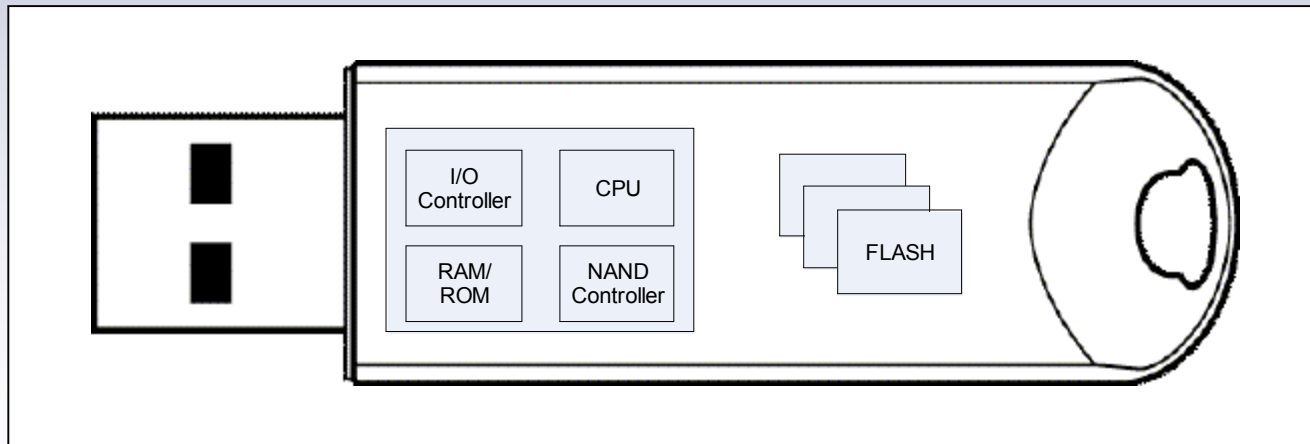


Protect the Host against Flash-originated Attacks

- Simple Attacks – Device is “seeded” with malware
 - As Autorun/Autoplay programs
 - Varied usability over different device types, different OS, versions of an OS, and configurable autorun/play policies
 - CD spoofing
 - Good because it enables greater usability in limited cases
 - Bad as it is easily hacked (this talk is about security...)
 - http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=266990&intsrc=news_ts_head
 - As Infected pictures/documents
- Anti-virus/Anti-rootkit/Anti-Spyware software may detect these

Protect the Host against Flash-originated Attacks

- Anatomy of a Flash Device (or Flash Card)
 - A complete computer is inside
 - CPU (8051, 80186, ARM, ARC,...)
 - RAM/ROM
 - Firmware (can be held in FLASH)
 - I/O (USB, SD, CF, MMC, MemoryStick, ...)



Protect the Host against Flash-originated Attacks

- Not-so-Simple Plug n' Play “active” attack
 - Most devices have firmware update capabilities
 - Plug n' Play Devices & drivers are tested for together for functionality
 - Plug n' Play Devices load drivers based on Class or Vendor IDs
 - USB uses Class ID, SubClass ID, Vendor ID, Product ID, etc.
 - It is easy for a hacked device to “choose” its driver, and target an attack on that driver
 - But it takes a lot of skill & knowledge about both the device & driver to execute this
 - May or may not be detected by anti-malware software



Six Cryptographic Tools

Santa Clara, CA USA
August 2007

Flash Memory Summit A/V Sponsor: **Seagate** 

Six Cryptographic Tools (and that's all)

- One-way hash functions
- Random Number Generators
- Symmetric Encryption
- Message Authentication Codes (MAC)
- Public Key Encryption (Asymmetric Encryption)
- Digital Signatures

Six Cryptographic Tools

- Cryptographic hash functions
 - Magic algorithms with special properties
 - One-way functions
 - Easy to compute digest from data
 - Very hard to compute data from digest
 - Small data changes produce large digest changes
 - Very hard to produce and predict collisions (duplicate collisions)
 - Effectively produces small chunks of data that positively identify larger pieces of data
 - SHA-256, SHA-384, SHA-512, ..
 - SHA-1, MD5 have known collision weaknesses
 - NIST 180-2

6 Cryptographic Tools

- Random Number Generators
 - Can be based on Deterministic Random Bit Generators (DRBGs), also known as Pseudorandom Number Generators
 - NIST SP 800-90
 - NIST SP 800-22 (testing requirements)
 - Can be based on Non-deterministic Random Bit Generators (NRBGs), also known as "True" Random Number Generators
 - NRBGs are often used as seeds for DRBGs
 - Many physical circuits have voltage & temperature weaknesses
 - There are no approved NIST methods!

Six Cryptographic Tools

- Symmetric Encryption
 - Data is encoded with a secret shared key
 - Block ciphers which require block-cipher modes for large messages
 - AES, 3DES, ...
 - NIST SP800-197, SP800-67

- Message Authentication Codes (MAC)
 - Used to ensure authentication (secret key) & integrity (cryptographic hash)
 - HMAC-SHA-xxx, HMAC-MD5, ...
 - NIST SP800-198a, SP800-57

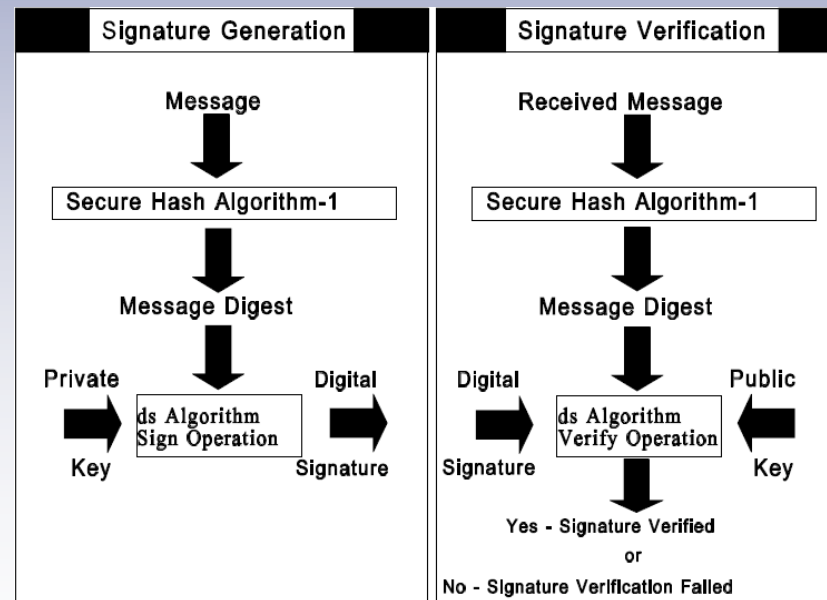
Six Cryptographic Tools

- Public Key Encryption
 - Sender & receiver each have related public & private keys
 - The relationships are based on two mathematical problems
 - Differential Logarithms
 - Elliptical Curves
 - For Asymmetric encryption:
 - the sender encodes the data with the receiver's public key
 - the receiver decodes the data with the receiver's private key
 - For Elliptical Curve Cryptography, it is more complicated:
http://en.wikipedia.org/wiki/Integrated_Encryption_Scheme
 - Used in PGP & S/MIME
 - Specified by RSA (PKCS #7) , IETF, IEEE 1363

6 Cryptographic Tools

- Digital Signatures

- DSA – Digital Signature Algorithm (FIPS186-2 Change 1)
- RSA – Rivest, Shamir, Adelman Algorithm (ANSI X9.31)
- ECDSA – Elliptical Curve Digital Signature Algorithm (ANSI X9.62)



From FIPS186-2

6 Cryptographic Tools

■ Suite B

- The NSA has published algorithm strength requirements for government purchases starting in 2010
 - Highly classified data is to protected by Suite A, which is, classified
 - http://www.nsa.gov/ia/industry/crypto_suite_b.cfm?MenuID=10.2.7
- Public Key schemes must use Elliptical Curve Algorithms
 - RSA/DH key sizes have grown to impractical sizes
- 128-bit Strength Equivalents
 - AES-128, SHA-256, ECDSA with NIST P-256, ECDH or ECMQV with NIST P-256, (RSA/DH equivalent is 3072)
- 192-bit Strength Equivalents
 - AES-256, SHA-384, ECDSA with NIST P-384, ECDH or ECMQV with NIST P-384 (RSA/DH equivalent is 7680)

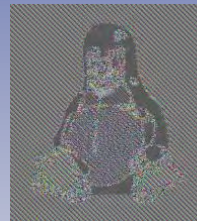


Security != Cryptography

Security != Cryptography

- Cryptography isn't a cure-all:

AES-ECB



AES-CBC



- Algorithms are measured by how long they have gone without being broken, not by any one expert's analysis
- Be very careful with non-standards-based cryptography
- Key Management is “key”
 - The strengths of most algorithms can be assessed
 - How the keys & secrets are held is the critical question
- Look for security in depth
 - Such as password protected encrypted data
- “Security through Obscurity” doesn't work



Password Protocols

Santa Clara, CA USA
August 2007

Flash Memory Summit A/V Sponsor: **Seagate** 

Password Protocols

- Plain Passwords
 - The password is passed as plain text
 - Vulnerable to snooping and filter drivers
- Challenge Handshake Authentication Protocol (CHAP)
 - The device gives a random number to the host, the host computes a hash of the random number & the secret
 - Don't repeat the random number!
- PKI protected Password
 - Strong encryption protects the weak password

Password Protocols

- Simple Taxonomy of Host-based Attacks
 - Simple Password protected
 - Break the password (Dictionary Attack)
 - Steal the password (Social Engineering)
 - Go around the password (Hack)
 - PKI Protected
 - Break it (Computational attack)
 - Steal it
 - Go around it
 - Encrypted Data
 - Break the key
 - Steal the key
 - Go around the key

Password Protocols

- Password Protection
 - Dictionary Attack
 - How hard is it to guess your password?
 - Don't use: "secret", "password", birthday, ...
 - There are common password dictionaries available
 - The attack can be a simple program that tries these sequentially or simply tries random letters/numbers/symbols
 - These programs are easily available
 - Dictionary attack countermeasures include
 - Password Complexity Policies (# char, case, numbers, symbols)
 - Limit the rate of attempts (linear or exponential)
 - Limit the number of attempts (per power cycle or to a brick point)
 - Configurability of these countermeasures



PKI & Certificate Protocols

Santa Clara, CA USA
August 2007

Flash Memory Summit A/V Sponsor: **Seagate** 

PKI & Certificate Protocols

- PKI or Public Key Infrastructure-based systems are typically designed to use Digital Certificates
- Digital Certificates are electronic documents which include a digital signature, a public key, an identity and information about the issuer
 - IETF x.509 specifies a common format for certificates
- There will be several Digital Certificates for a Flash Storage device
 - Owner/Administrator
 - Manufacturer
 - User

PKI & Certificate Protocols

- X.509 Certificates include at least the following information
 - Version
 - Serial Number
 - Algorithm ID
 - Issuer
 - Validity
 - Not Before
 - Not After
 - Subject
 - Subject Public Key Info
 - Public Key Algorithm
 - Subject Public Key

PKI & Certificate Protocols

- PKI is currently used or proposed in
 - IEEE 1667 (RSA)
 - IPSEC (RSA)
 - TCG Storage WG proposal (RSA & ECC)
 - OS's (RSA & ECC)
 - SSL/TSL (RSA & ECC)
 - S/MIME (RSA & ECC)
 - OpenPGP (RSA & ECC)



Conclusion

Conclusion

- Security will be an integral part of all portable storage
- Look for solutions based on standard cryptography
- There will be many different levels of security
- Security solutions must be targeted to market and threat requirements




Questions?

John Geldman
Lexar Media
jgeldman@lexar.com



References


Suggested Crypto Reading

 Practical Cryptography, Niels Ferguson,
Bruce Schneier (Wiley)

- How security is built from cryptography







 Applied Cryptography, Bruce Schneier
(Wiley)

- Cryptography implementation

 Handbook of Applied Cryptography, Alfred J.
Menezes, Paul C. van Oorschot, Scott A.
Vanstone (CRC Press Series)

- A handbook & textbook

Suggested Specifications

-  ATA-Lock <http://www.t13.org>
 - Plain text passwords w/BIOS dependency
-  IEEE 1667 <http://grouper.ieee.org/groups/1667>
 - Mutual Authentication using CHAP – proposal in process
 - RSA Certificate
-  NIST <http://csrc.nist.gov/CryptoToolkit/>
 - Guided introduction to NIST standards & guidance's
-  RSA <http://www.rsa.com/rsalabs/node.asp?id=3122>
 - Specifications on RSA PKI & OTP
-  TCG <https://www.trustedcomputinggroup.org/groups/storage/>
 - A comprehensive approach to secure storage
-  USB MSC-Lock <http://www.usb.org>
 - Plain text password protocol to protect against loss & theft