Future Trends in Flash Drive Encryption

Devesh Ahuja
Vijay Ahuja, Ph.D.
Cipher Solutions, Inc.

USB Host based security - NOW

HOST-BASED
USB access controlled through the host

Encryption material saved in the host

User needs to enter a secret/password to

- **Access the drive**
- **Decrypt the data**

STANDALONE DEVICE SECURITY
Password level security

- **Additional Measures to increase security**
  - **Token/ Cards for stronger authentication**

Flash Memory Security Issues

- Monitor/restrict files going to the Flash
  - Port Controls
  - Log meta data of files to and from the Flash
    - Need to maintain and secure the logs
- Authenticate the user
- Encrypt files to prevent disclosure
  - Need to maintain and secure the Keys and the Algorithms
  - Password-based keys commonly used

Future of Encryption

ENVIRONMENT OF INCREASING INSECURITY

- Expanding enterprise – home offices
- Increasing communication devices
- Mobility
- Growing email traffic
- Growing personal information
- Increasing storage sizes
- Social sites
- New and emerging threats to data

Future Trends in Encryption -

ENCRYPTION IS NEEDED EVERYWHERE…. BUT…

1. **Should be Simpler and Easier to use**
2. **Should Cost less**
3. **Should yield Higher performance – hardware?**
4. **Should comply with more and more of:**
   - **Government Regulations: GLBA, HIPAA, SB1386,…most states have regs for Privacy Protection**
   - **Industry Standards: NIST; ISO 11568-1, 11568-2, 11568-4; PCI; IEEE P1619; ..**

§ **Should be Ubiquitous – What about Interoperability?**

Cipher Solutions, Inc.

Key Management Issues – Keys needed for 10 or 20 or ?? Years

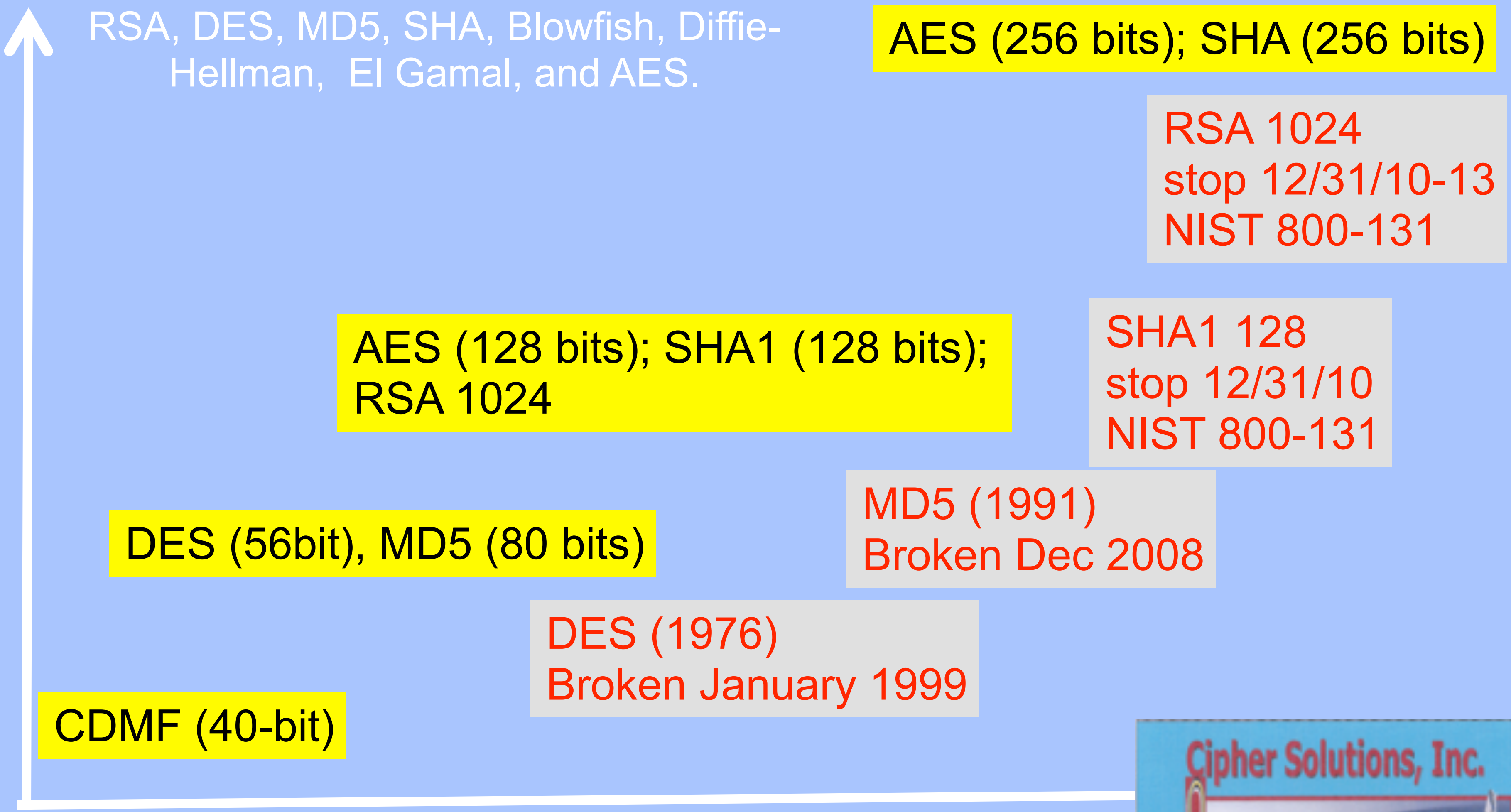
- Key retention for stored data – years
- Keys are NOT easy to upgrade
- Keys are not easy to be:
  - Secured
  - Available
  - Backed-up
- Key management technologies do not address the issue of aging
  - Key & Algorithm refresh every 5? Years
    - To resist brute-force attacks
- Secured keys are often as secure as passwords (+ Tokens!!)
- Backed up Keys help but introduce new issues
- Lost keys may be as bad as **losing data**

NIST 800-131

ALGORITHM	SIZES	EQUIVALENT STRENGTH
Two-key Triple DES Encryption	Acceptable through 2010 Restricted use from 2011 through 2015	80 bits
Two-key Triple DES Decryption	Acceptable through 2010 Legacy use after 2010	80 bits
Three-key Triple DES Encryption and Decryption	Acceptable	112 bits
SKIPJACK Encryption	Acceptable through 2010	80 bits
SKIPJACK Decryption	Acceptable through 2010 Legacy use after 2010	80 bits
AES-128 Encryption and Decryption	Acceptable	128 bits
AES-192 Encryption and Decryption	Acceptable	[illegible]
AES-256 Encryption	Acceptable	256 bits

Cipher Solutions, Inc.

Encryption Algorithms....moving targets



RSA, DES, MD5, SHA, Blowfish, Diffie-Hellman, El Gamal, and AES.

AES (256 bits); SHA (256 bits)

RSA 1024
stop 12/31/10-13
NIST 800-131

AES (128 bits); SHA1 (128 bits); RSA 1024

SHA1 128
stop 12/31/10
NIST 800-131

DES (56bit), MD5 (80 bits)

MD5 (1991)
Broken Dec 2008

DES (1976)
Broken January 1999

CDMF (40-bit)

NIST 800-131 Hash Function Transition

Hash Function	Usage
SHA 1	Digital Signature Generation: acceptable thru 2010; deprecated 2011-2013 Digital Signature verification: Acceptable thru 2010; legacy use after 2010 Non-digital signature generation
SHA-224,256,384,512	Acceptable for all hash function applications

Challenges for upgrading Keys

Example – PKI Certificate Signing Keys: SHA1 (128) -> 224/256 bits

- **If a CA signs a Certificate with SHA 2, and the Relying Party (e.g. Web Servers) cannot handle SHA 2, the authentication fails**
- **Need to test various combos of:**
  - **End user Certificate**
  - **CA's OCSP/CRL signing certificate**
  - **Issuing CA's End-entity Signing Certificate (Trust Chain to be all SHA2)**
  - **Relying Party's capability to verify SHA2 signatures**
- **DUE 12/31/2010**

Key Management – Cryptographic Key Storage

- Password-based keys => Security equals password security
  - Change passwords (keys) frequently
- Key Systems – Used for storing encrypted data
  - Secured Key Storage Devices
  - Key Management Servers
- Interact with Other Cryptographic Devices
  - Smart Cards
  - Memory Cards
- Storage of Keys Offline
  - Tape
  - Optical

Key Management – Protecting Keys

Non-Cryptographic Protection

- Time Stamps – Restrict Key Use to Specific Periods
- Sequence Numbering – Limit Re-Play Attacks
- Multiple key shares “k of N”

Cryptographic Protection

- Hardware Security Modules –
  - Secure cryptoprocessor
  - Targeted at managing digital keys
  - Accelerating in terms of digital signings
  - Providing strong authentication to access critical keys for server applications
- Companies that manufacture HSMs: Luna, Ncipher, Thales, HP, Safenet, etc.

Cipher Solutions, Inc.

PROVIDING IT SECURITY SERVICES SINCE 2001

Department of Defense — Largest Banks
Storage Networking Vendors — IT Security Vendors
Storage Security Vendors

IA Services for Federal/State Governments

- IT Security Design
- C&A using DIACAP
- Key Management; Data Security
- IPSec, SSL design

Application Security Services

- Security Design of large application
- PKI-usage and design for Key Management Application
- PKI-enabling of applications
- Security design for future Application Architectures

PKI Services

- PKI Design – from RFP/vendor-selection to delivery of Millions of certificates
- Develop CP, CPS and Sub Agreements
- Key Management Design and deployment
- Best Practices for Key Lifecycle Management ofPKI and Symmetric keys
- Support Web Trust Audit
- Digital Signature application design

Data Security Services

- Data Security newsletter
- Estimating Data Risk – Developed a new approach for computing Risk metrics
- Disaster Recovery plan
- Storage Security monthly newsletter
- Assessing Risk (metrics)

Cipher Solutions, Inc.

THANK YOU

Dr. Vijay Ahuja
President
Cipher Solutions, Inc.
vijay@CipherSolutions.com
1-919-848-3040