Flash Security – Future Trends in Technologies and Standards

Devesh Ahuja
Vijay Ahuja
CIPHER SOLUTIONS, Inc.

Flash Memory – Security Topics

- Authentication
- Data Encryption
- Access Control
  - Port Controls
  - Audit Logs
- Intercept Malware !!!!! – both ways
  - Download updates on real-time basis (Ex: Windows)

Flash Memory – Authentication

- Authenticate the User, the Server, the device
  - Strong Authentication
  - 2-Factor
    - SecureID
    - Biometrics:
      - Thumbprint
      - Signatures
      - Retina
    - Phone Factor
  - PKI based authentication – later

Encryption

- Encryption Algorithms
  - Code base
  - Upgrading algorithms in the field
- Key Management
  - Key Renewal
  - Key Backup
  - Key Recovery
  - Secure Key Storage
- Key lengths
  - Moving targets

Mostly Certificates have a validity period of 1 or 2 years

Flash Keys have a life cycle of 4-5 Years?

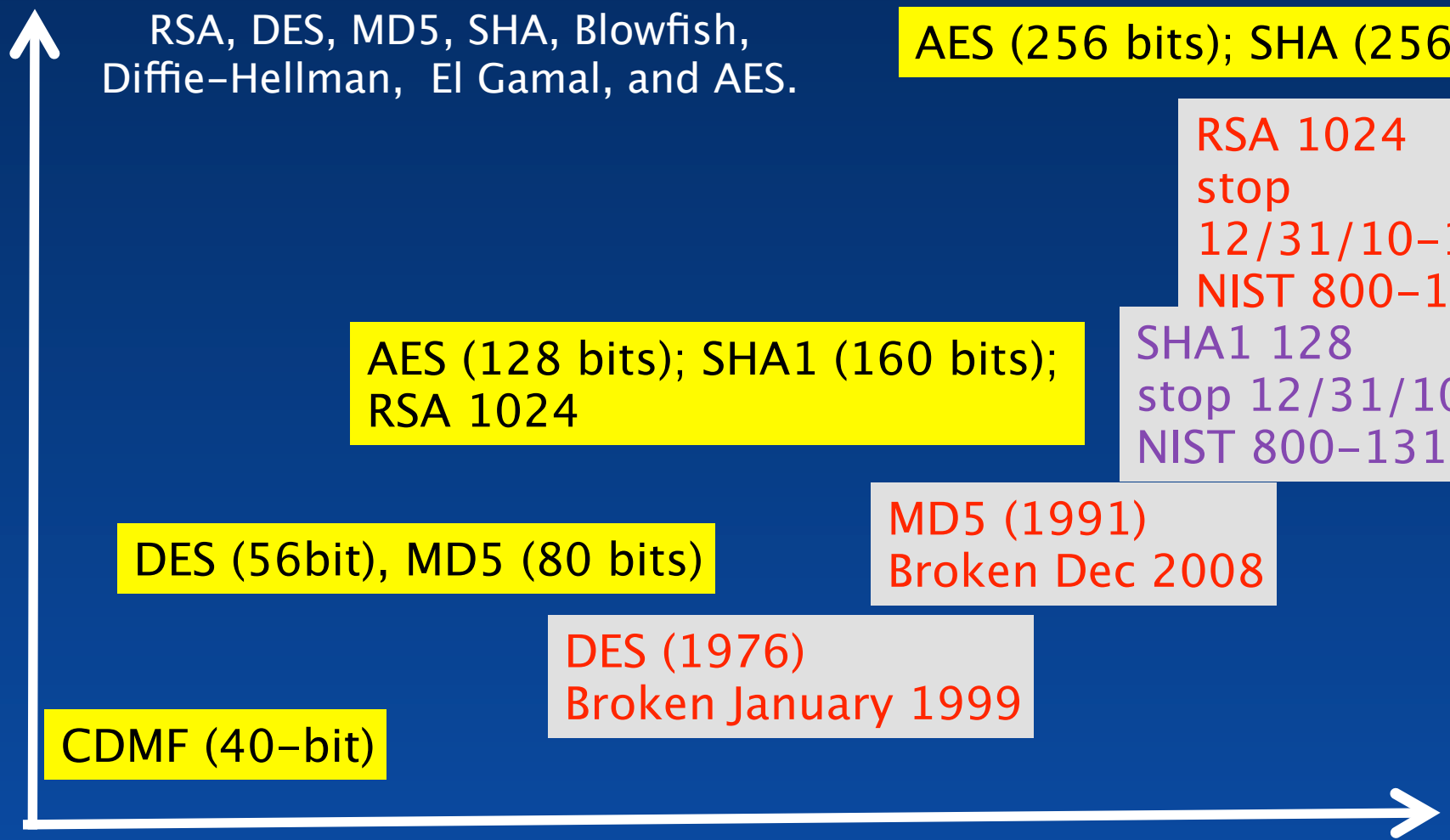
Key Management Issues – Keys needed for many Years

- Key retention for stored data – years
  - Even after the Algorithm is deprecated
- Keys are NOT easy to upgrade
- Keys are not easy to be:
  - Secured
  - Available
  - Backed-up (HSM usage)

Audit Logs to be available for 7 years
Mortgage records for 30 years

- 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**

Flash Drives – Upgrading Encryption Algorithms



NIST 800-131A February 2011

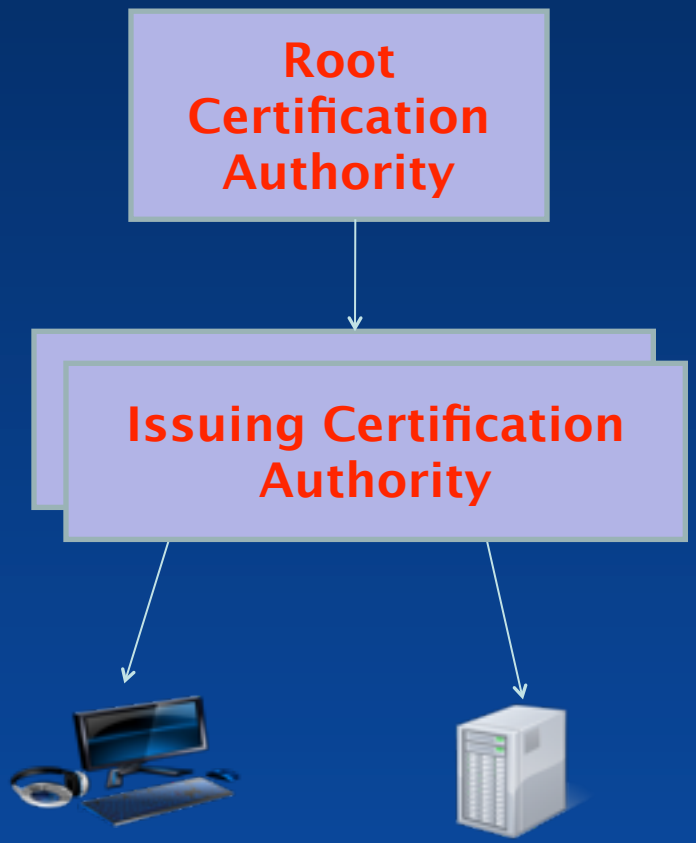
ALGORITHM	SIZES	EQUIVALENT STRENGTH
RSA	Acceptable through 2010 Deprecated 2011-2013 Disallowed after 2013	1024 bits
Two-key Triple DES Encryption	Restricted use from 2011 through 2015	80 bits
Two-key Triple DES Decryption	Acceptable through 2010 Legacy use after 2010	80 bits
Three-key Triple	Acceptable	112 bits
SKIPJACK Encryption/	**WAS** Acceptable through 2010	80 bits
AES-128 Encryption and Decryption	Acceptable	128 bits
AES-192 Encryption and Decryption	Acceptable	192 bits
AES-256 Encryption and Decryption	Acceptable	256 bits

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**
- **Confusion between 224 and 256 bit SHA 2 !!!**

PKI: Public Key Infrastructure for Flash



Certification Authorities issue digital Identity (Certificates) that can be used for client/server authentication or data encryption

– Client authenticates Server
-Server authenticates client

.

PKI Infrastructure – Uses in Flash

- Support Strong Authentication
  - Private Key-based
  - Verify the Trust-chain
  - Verify the Certificate Issuer
  - Verify the Certificate status (CRL/OCSP)
- Means to exchange encrypted data between entities
  - Using Public/Private Keys
    - Exchange Symmetric Keys use Public/Private Keys (e.g. SSL)
- Communicate within your Trust Anchor
- Communicate outside your Trust Anchor
  - Trust Stores
  - Cross-Certification
- Signing Code/Updates for distribution using Certificates

Steps to Implement PKI – Cipher

1. Trust Requirements
2. Design Trust Hierarchy
3. Deploy Secure environment for PKI
4. Develop CP and CPS
5. Document Certificate Profiles, Procedures
6. Implement Prototype and Production – Record Process
7. Ensure auditability

Thank You

Cipher Solutions, Inc.

"Securing Storage for last 10 Years"

www.CipherSolutions.com

info@CipherSolutions.com

919-848-3040