Larry Hines, Dale Hopkins, Jeff Kalibjian, Susan Langford, Steve Wierenga

Hardware Security Module Use in Banking and Electronic Commerce Applications

Hewlett Packard Corporation

Today's Presentation

- History of the Hardware Security Module (HSM) in Automated Teller Machine (ATM) Banking
  - The Problem/Solution
  - The Atalla Company
  - Tandem Atalla
  - Compaq Atalla
  - HP Atalla
    - What we do today
- HSM Essentials
  - Why Hardware Security?
  - Security Standards
  - Technology

Today's Presentation (cont.)

- HSM's in Banking Today
  - Data Flow
  - Initialization/Configuration
  - DES and Triple DES
  - Key Typing
- HSM Use Outside of Banking
  - Key Management
    - Commercial
    - Military
  - Other Sensitive Operations
    - Digital Signatures
    - Custom Functions

Making the Banking ATM Machine Happen

The ATM Problem

- ATM concept is very powerful
  - Bank customer independence from teller
  - Access to cash and potentially other banking services 24/7
- But, making it work was initially a challenge
  - When first systems deployed in mid 70's they were direct connect systems. A bank card only worked with your bank, not other banks
- But banks began to experience fraud around these systems. Why?
  - At first they utilized no encryption
  - Then utilized link encryption
  - Then software based encryption
- In all cases fraud still continued

The Solution

- The concept of bank customers being able to utilize other bank ATM machines made the solution clear:
  - PIN data, and customer information needed to be protected, always, since this information would be flowing over networks not necessarily controlled by the issuing bank
- Banks go to ANSI and suggest a national security standard
- The result…..

The ATM Solution

- PINs must ALWAYS remain encrypted after they are input and when they are stored for comparison
- Cryptographic keys used to encrypt PINs SHOULD NEVER be created or stored on conventional bank IT systems
  - No dual control for administrator or user access to system resources (e.g. memory, disk, etc).
- Cryptographic keys SHOULD ONLY BE created and stored on tamper resistant hardware devices.
- There must be a SEPARATION OF ROLES for individuals with access to the tamper resistant hardware device (e.g. administrator to care for the device, security officers to maintain key components placed into the device or configure policies for its use)

The ATM Solution (cont.)

- Operations performed with the cryptographic keys must ALWAYS be carried out inside the tamper resistant hardware (e.g. digital signature verification, PIN verification)
- A key created in a HSM CAN NEVER be exported from the tamper resistant hardware in the CLEAR. It MUST ALWAYS be WRAPPED with an appropriate STRENGTH Key Exchange Key (KEK)
- Keys MUST BE typed for usage to guarantee they will be used for only one purpose (e.g. data encryption key vs. PIN encryption key)

The Owners May Change, but to the Banks, it's Still *Atalla*

- The Atalla Company
  - Founded 1972
- Tandem Atalla
  - 1987-1997
- Compaq Atalla
  - 1997-2002
- HP Atalla
  - 2002-Present

HP Atalla Security Products

- Uniquely focused on transaction security and cryptographic performance
- Technology leader in hardware-based security module products
- Broad array of financial institution, third party processor and acquirer customers worldwide
- Prestigious RSA Award for its contribution to Industry (Netscape, Checkpoint, Gemplus, Symantec, MSFT)

HP Atalla is a Security Technology Provider

- 31 years experience in productizing, delivering, and supporting practical security solutions
- Expertise and experience in
  - End-to-end application layer security architectures
  - Cryptographic algorithms and standards
  - Hardware security standards (FIPS 140-2)
  - Security evaluation and certification processes
  - Working with security technology vendors (silicon, software)
- *Atalla* is a trusted brand, reputation
- Premium customer list in banking/finance industry

Examples of Atalla Products and Technologies in the Marketplace

- **Retail Banking** – protecting ATM/POS transaction networks worldwide
  - Rolling out Triple DES with Atalla Key Block IP
    - Adopted as ANSI X9 Standard and by industry partners
  - Protecting ATM/POS terminal key loading
    - Remote terminal re-key using public key technology
    - Secure printing component mailer solution
  - Protecting customer privacy and PINs
    - Secure printing PIN mailer solution
- **Protecting Microsoft's IP**
  - Atalla CAPI support, digitally signing all Microsoft object modules
- **Protecting eCommerce and Mobility**
  - Online payments – VISA/GlobeSet, Amex
  - AXL300/600, Proliant option, Apache, 600 SSLs/sec
  - All RSA toolkits enabled with Atalla MultPrime™ technology

Atalla Technologies Sampler

- Cryptographic System Secure Boot (Red/Black)
  - Precursor to TCPA, Palladium, others
- Secure Remote FPGA download
  - Patent issued, broad application, revenue potential
- AutoKey
  - Patent pending, broad applications
- MultiPrime
  - Patent issued, licensed, RSA toolkits, revenue
- Atalla Key Block
  - Market leadership, pending standard

Why Hardware Security?

Why Software Alone CANNOT be Secure!!

- Application/data vulnerable to other process access.
- Application/data vulnerable to single system administrator access.
- Application/data vulnerable to external electronic monitoring
  - Logic State Analyzer
  - EMI emission monitoring

Why Software Alone CANNOT be Secure (cont.) !!

- Application/data vulnerable to data dumps when crashes occur
  - Data in CPU registers/cache especially vulnerable
- Cryptographic (key material data) very easy to identify via histogram in large amounts of data.

Hardware Security Misconceptions and Reality

- Misconception:
  - Hardware is needed only to improve cryptographic performance
  - Security and trust can be achieved with software alone

- Reality:
  - Secure hardware platforms are essential for security and trust
  - If your security is based on software running on non-secure platforms, you are deluding yourself
  - Attacks will always succeed at the weak points, not the strong
  - Scan the headlines –
    - You'll see: "*Megasoft Security Vulnerability Exposed – Again*"
    - Or this: "*Ex-Employee Compromises Corporate Database*"
    - BUT NOT this: "*Keys Extracted from FIPS Rated Secure Hardware*"

Example: Consider a Document that Needs to be Protected

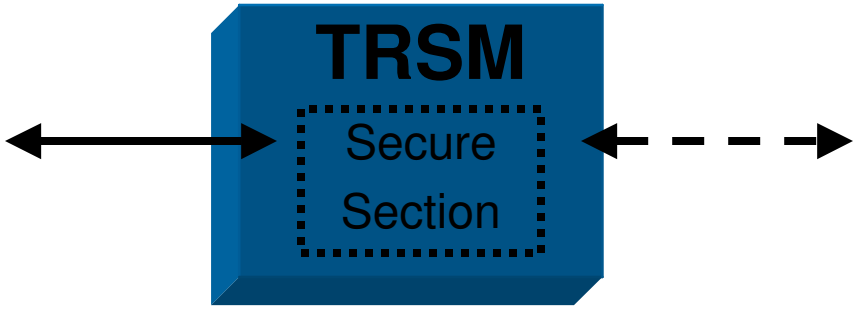
- How is the key (Kd) that encrypted the document being protected?
  - A user generated password is hashed and the result is utilized as a cryptographic key (Kp) that in turn is used in a cryptographic algorithm to encrypt the key (Kd).
  - Encrypted key (EKd) is then typically stored on disk for later access

The Perils of Software Based Encryption..

- The password utilized to derive the key (Kp) that encrypted Kd must be collected and temporarily stored in computer memory.
- After the password is hashed to derive Kp, the password maybe deleted, but then Kp must be stored temporarily in computer memory while it is being used to decrypt Kd
- Once Kd has been decrypted, Kp can be deleted from computer memory. Kd must re-main unencrypted in computer memory, until the entire document has been decrypted

Hardware-Based Security Principles - 1

- Physical Security
  - All cryptographic keys and sensitive data are protected inside a "secure section"
  - No secret information leakage (EMI, power, timing)
  - Tamper–resistant and –detecting physical perimeter
  - Active zero–ization of keys/secrets if tamper attempted
  - Hardware enforcement of the organization's logical security policy.
  - FIPS 140-2 standards and certification

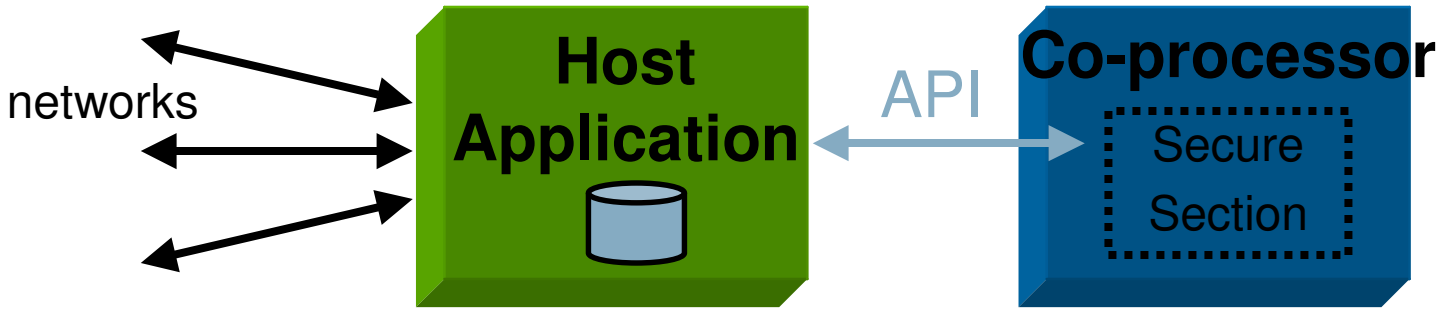


Hardware-Based Security Principles - 2

- Logical Security
  - Key Management
    - Strong key typing, use controls, hierarchy (master, KEK, working)
    - Key initialization processes/devices, remote keying
    - Lifecycle control and protection of keys
  - Carefully architected functionality and API
    - Sensitive information permanently out-of-reach from host applications, programmers, administrators, other insiders, outside attackers
    - End-to-end protection of data, identity, transactions, keys
    - Insecure functions (eg “decrypt and export key”) prohibited
  - Locked-down platform, OS, and application
    - Secure boot and encrypted image loading
    - No administrative/support/development “back doors”
  - Configure to support institution’s security policy
    - Functions enabled/disabled
    - Separation of roles, dual or multiple control

Today the HSM is Typically Utilized as a Co-processor

- Co-processor Class
  - Hardware Security Module with a carefully designed cryptographic services API, serving an external host-based application
  - protect keys and sensitive data from insider and outside attacks



What Banks Have Learned (the Hard Way)..

- Does not rely on applications software, OS, or individual people
- ANSI X9 standards that institutions must follow to connect into the payments network require secure HW
- Banks and transaction processors willingly deploy secure hardware to avoid fraud losses and liability
- Has protected PIN-based ATM/POS transactions and customer identity with secure hardware for over 25 years

FIPS 140-2 (Hardware)

- Federal Information Processing Standard (FIPS) that specifies the security requirements within a system protecting sensitive information
- Four increasing levels of security defined
  - Level 1 - No specific physical security mechanisms required.
  - Level 2 - Requires tamper evidence by utilizing tamper evident coatings or seals, role based authentication.
  - Level 3 – Requires strong enclosures or tamper detection and response circuitry that can zeroize sensitive data. Level 3 also requires identity based authentication mechanisms .
  - Level 4 – Level 3 protections plus protects against environmental condition changes such as temperature and voltage changes

Common Criteria (Software)

- Common Criteria is an ISO standard (15408) and has seven increasing Evaluation Assurance Levels (EAL)
  - EAL - 1 – Functionally tested. Evaluation of Target of Evaluation (TOE) is done with respect to the customer documentation.
  - EAL - 2 – Structurally tested. Evaluation of TOE is done with respect to developer design information and test results.
  - EAL – 3 –Methodically tested and checked. Evaluation of TOE is done at design stage.
  - EAL – 4 – Methodically designed, tested, and reviewed. Used when developers
  - EAL – 5 – Semiformally designed and tested. Rigorous commercial development tools and specialty security design techniques to design and implement TOE.
  - EAL – 6 – Semiformally verified design and tested. Security engineering techniques applied to an advanced development environment.
  - EAL – 7 – Formally verified design and tested. Advanced security engineering and development techniques that can be rigorously mathematically modeled and analyzed.

FIPS 140-2 Reality

FIPS 140-2 Rating	*Comments*
Level 1	Not Meaningful
Level 2	Not Meaningful
Level 3	Secure
Level 4	Very Secure

Common Criteria Reality

CC EAL Rating	*Comments*
EAL-1	Not Meaningful
EAL-2	Not Meaningful
EAL-3	Not Meaningful
EAL-4	Some Security re-implemented
EAL-5	Security Designed from the Start
EAL-6	Secure
EAL-7	Very Secure

HSM Essentials

How to Build a HSM

- Key Technologies
  - Packaging
  - Power dissipation
  - The boundary
    - Board vs. box
  - Custom chips sets vs. “off the shelf” chip sets
  - Tamper circuitry
  - Firmware/software
  - Logically Secure APIs

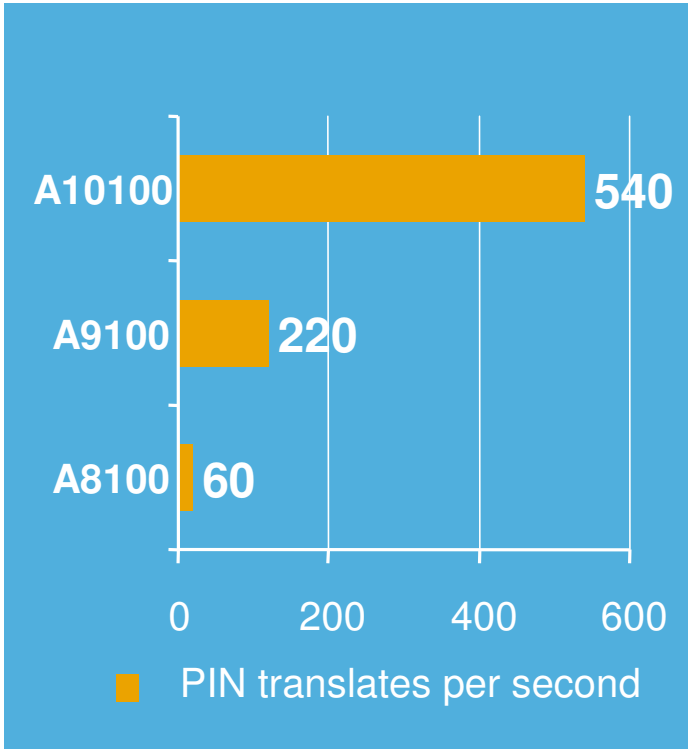
What They Look Like

- State-of-the-art, 1U rack-mountable form factor
- Dual locked front bezel

Performance Examples

- High-end Atalla 10100 NSP
  - Auto-sensing 10/100 Base-T Ethernet TCP/IP
- Midrange Atalla 9100 NSP
  - Auto-sensing 10/100 Base-T Ethernet TCP/IP
- Entry-level Atalla 8100 NSP
  - Auto-sensing 10/100 Base-T Ethernet TCP/IP
  - Async connection for compatibility with Atalla A8000

Triple DES Performance



FIPS 140-2 Validation Certificate for Atalla Cryptographic Engine

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. 296

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Atalla Cryptographic Engine (ACE) *by* Atalla Security Products of Hewlett Packard Corporation
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Designated Information* (Canada) within computer and telecommunications systems (including voice systems).

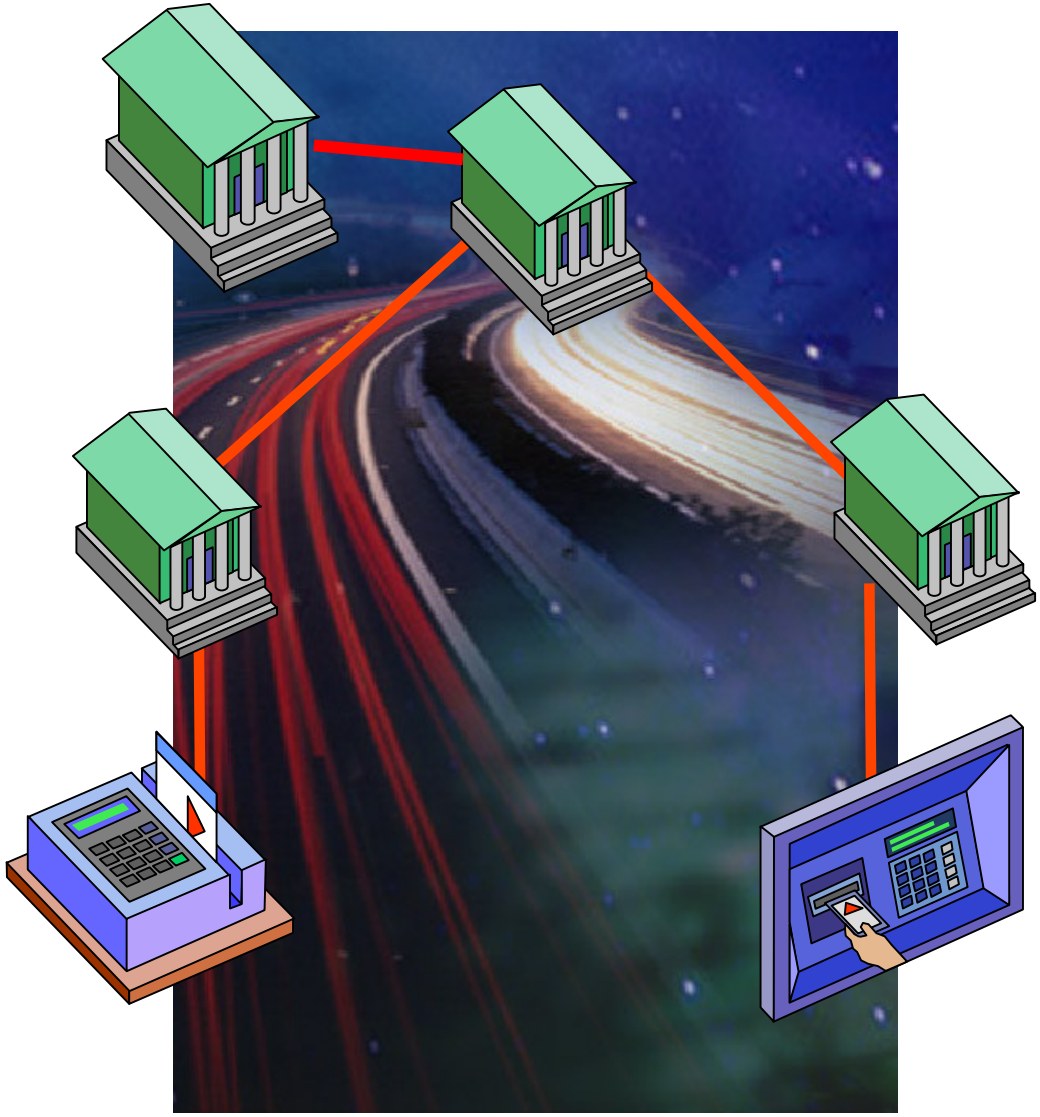
Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

HSM's in Banking Today

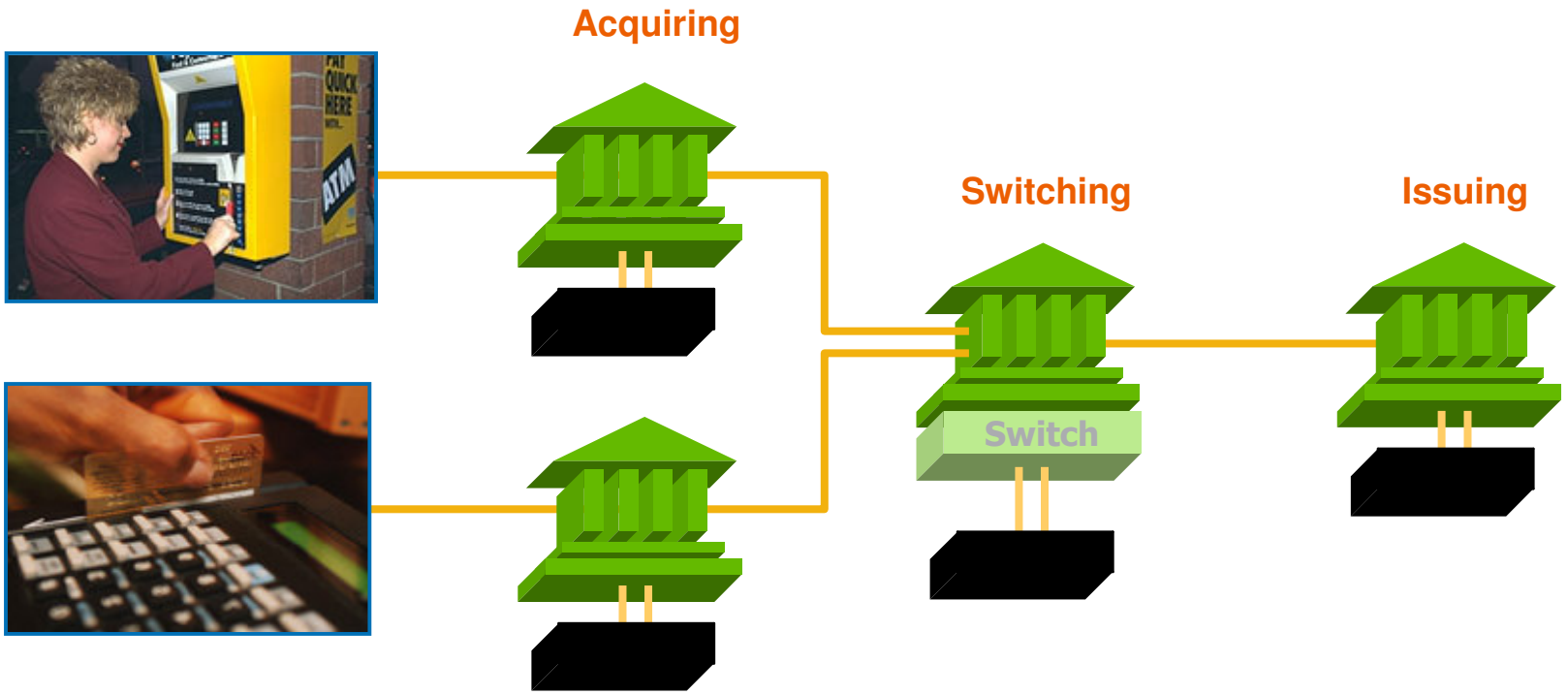
Financial Interchange Networks: The Power of Hardware-based Security

Proven, ubiquitous end-to-end secure network



A model network for high volume transaction processing

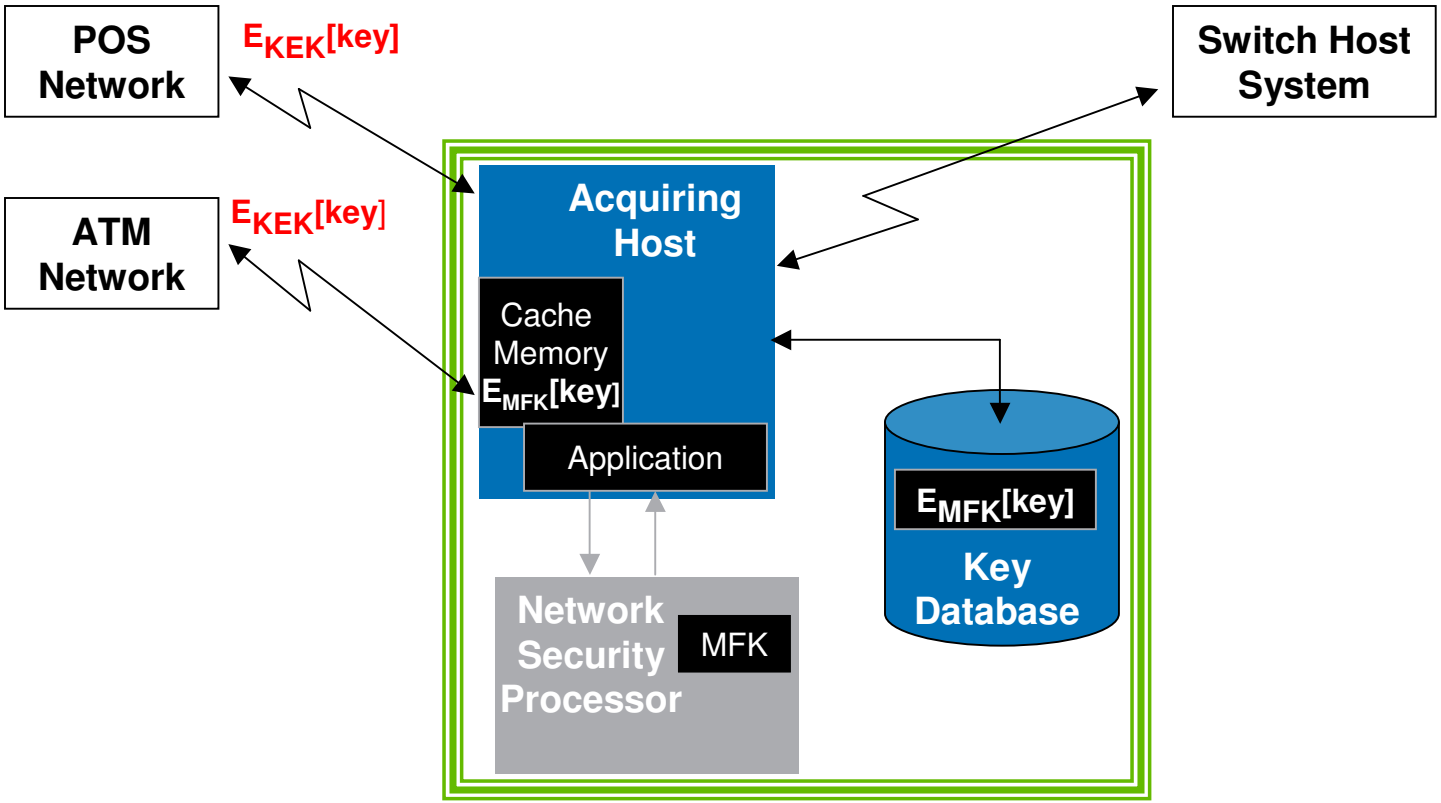
Financial Interchange Network



Configuring a HSM

- HSM's need keys to work
- Banks protect keys using a Master File Key (MFK)
  - Key to protect other keys
- No one person at a bank knows the Master File Key
- MFK split into components
  - Dual control
- Components are securely injected into HSM with a configuration device

Host and NSP work together for secure key management

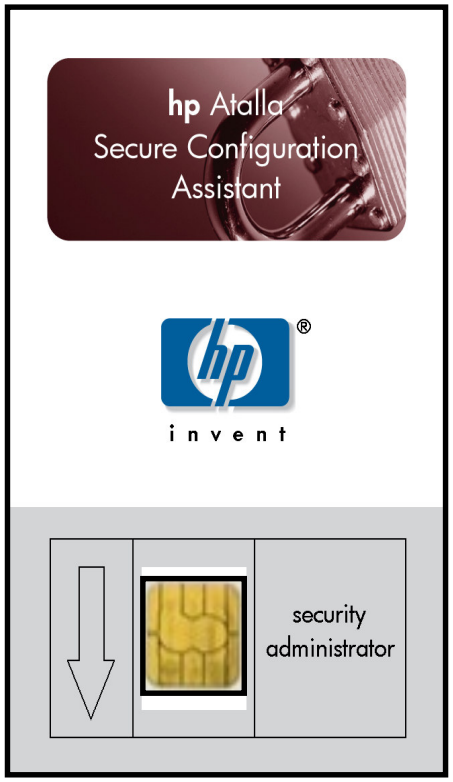


Configuration Device Example: The HP Atalla Secure Configuration Assistant (SCA)

- A secure configuration and key injection device based on the HP iPaq PDA with many security enhancements
- Custom FIPS 140-2 Level 3 SmartCards perform all cryptographic operations and store security-relevant data items
- Permits remote management of NSPs over the network

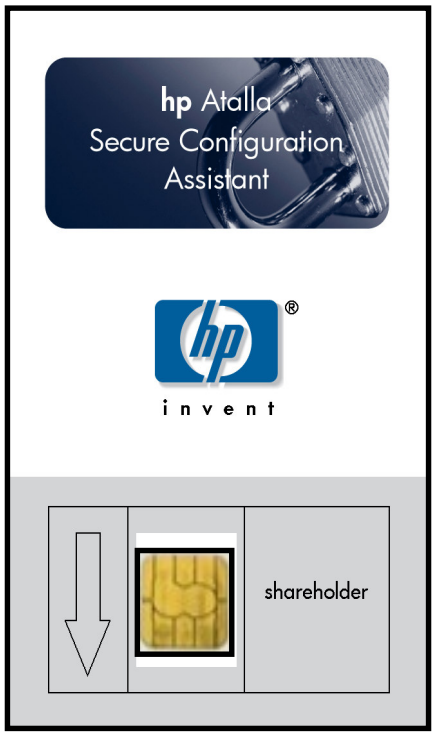
SCA: Security Administrators

- Personalize security administrator smart cards
  - Define card holder name and select PIN
- Define MFK key components
- Define SCA use policy
- Define NSP security policy
- Manage NSP audit information
- Create NSP initialization share data



SCA: Shareholders

- Personalize share SmartCards
  - Define card holder name and select PIN
- Receive configuration share data when authorized by security officers
- Initialize and update an NSP to a given configuration as specified in the share data



SCA Audit Logging

- NSP maintains record of configuration changes
  - NSP Factory resets
  - Association changes
  - Share card generation
  - Key loading (MFK, PMFK)
  - Generation of cryptograms
  - Enable/disable commands and options

Atalla SCA Benefit Summary

- Graphical user interface provides ease-of-use in a secure environment
- Ability to re-enforce your security policy
- Easily replicate desired configurations on multiple NSPs locally or remotely
- Save off cryptograms from SCA without having to hand copy
- Upload commands to transmit to NSP
- All security-related operations are logged by the NSP
- Only end-to-end secure key initialization solution to meet FIPS 140-2 Level 3 standard

Problem: Single-length DES is "Broken"

Knowing plaintext and ciphertext, test and compare for key

Takes only a 2^{56} key search

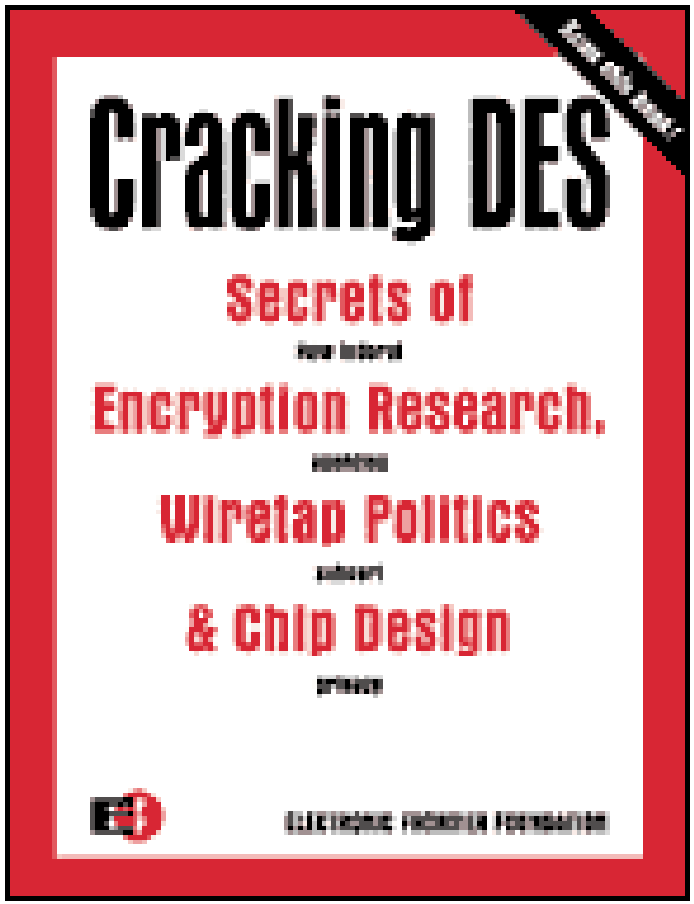
DES algorithm itself is strong

But the 56-bit key is too short

Key exhaustion attack by EFF breaks DES in only 22 hours

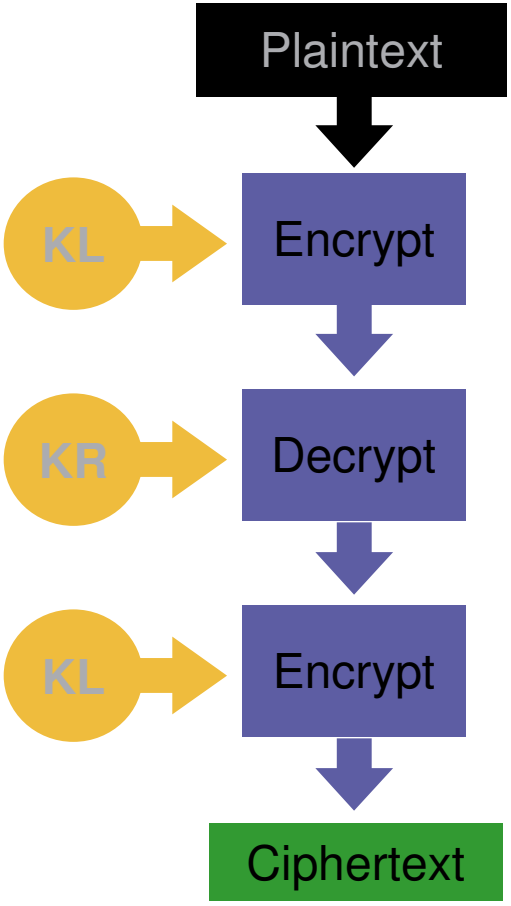
Today DES cracker machine sells on Web for under $995

Result: ATM and EFT/POS systems are in peril



Solution: Use Triple-DES Instead

- Triple-DES is three DES operations
- Triple-DES has longer, stronger keys
  - Two 56-bit keys, K=KL||KR
- To break Triple-DES requires a test and compare of 2^{112} keys
  - 2^{56} times 2^{56}
  - Approximately 200 trillion years!
- Vendors are implementing Triple-DES today
- Operationally, Triple DES is strong and adversary will attack elsewhere!

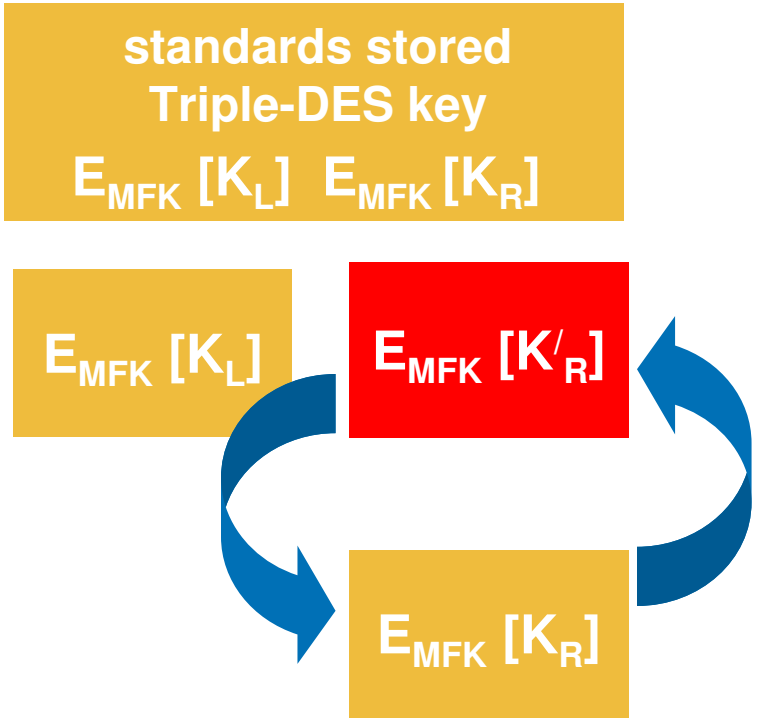


Financial Industry Encryption Mandates

Date	Standard	Mandating or Recommending Body
Now	Triple DES capable on new ATMs (Global)	MasterCard
January 2003	Triple DES capable on new ATMs (Global)	Visa
April 2003	All member and processor host systems to support 3DES (Global) for new ATMs	MasterCard
April 2005	Triple DES on all ATMs (Global)	MasterCard
No timeframe strongly encourage	Changing encryption keys	Visa/MasterCard
No outlined timeframe	Advanced Encryption Standard	US government National Institute of Science and Technology

Previous Standards Leave Triple-DES Implementations Vulnerable

- Two DES keys KL, KR stored independently, side-by-side
- Adversary will readily attack each encrypted stored key independently
- Result: Triple-DES keys remain vulnerable to a knowledgeable attacker in less than two days



Triple DES Attack Published (2001)

- Insider attacks published by researchers at the University of Cambridge
  - Well known HSM was made to expose its keys
  - Took 14 steps and approximately two days
  - That HSM was validated at FIPS 140-1 Level Four!
  - Attacked Triple DES keys while at rest
- Solution: “Type” Keys!!!

What is a “Key Block”?

- Data structure used to store or exchange cryptographic keys within hostile environments
- Bad key block design will leak key information
  - Attractive point of attack for knowledgeable adversaries
- Good key block design
  - Keys are encrypted using a secure algorithm with an appropriate key size
  - Control information allows hardware security modules to determine correct key usage
  - Secure mechanism detects any modification or manipulation of the control information and encrypted keys

Atalla Key Block (AKB)

Clear header

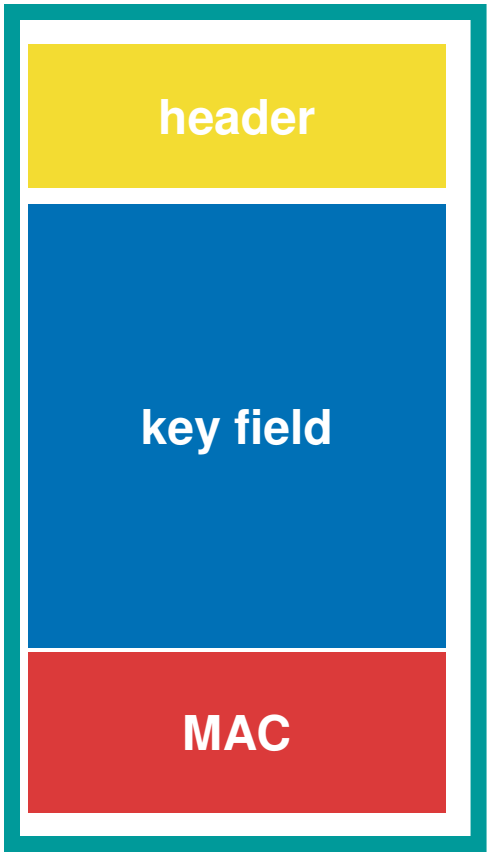
- controls key usage
- common attributes for all keys

Encrypted key field

- protects values
- Triple DES encrypted with specific master key
- variable length key field

MAC

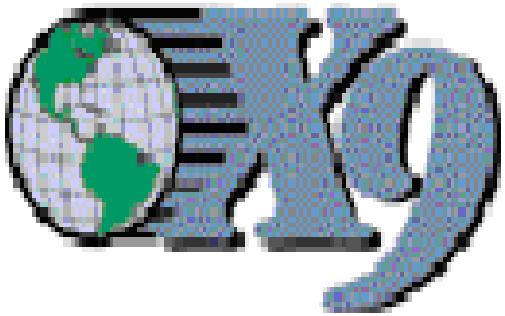
- binds key attributes to values
- Triple DES across the clear header and encrypted key field to prevent tampering



- Reviewed and adopted by standards committees

AKB has Driven Industry Standards

- Atalla offered the AKB to the financial security industry
  - X9.24: symmetric key management of symmetric keys
  - X9.52: Triple DES implementation



- Standards process can be slow and time-consuming
  - X9.24 Part 1 contains security requirements for a secure key block
  - 18 months in the making

  http://webstore.ansi.org/ansidocstore/product.asp?sku=ANSI+X9%2E24+%28Part+1%29%2D2002

- New Technical Report (TR-31) to consider how to implement a secure key block

Security Benefits of the AKB

- Attacker **cannot** change any attribute of any key
- Attacker **cannot** change any bits of any key
- Attacker **cannot** use part of a key as entire key
- Attacker **cannot** rearrange any part of a key
- Attacker **cannot** substitute parts of a key into another key
- Attacker **cannot** identify single-length keys

These 'benefits' are worded as 'requirements' in the latest ASC X.9 standards documents

HSM Use Outside Banking

HSM Use

- Hardware Security Modules in Finance
  - A consistently profitable segment of the security industry
  - The gold standard for secure IT infrastructure and interoperable security standards
  - Belief: hardware-based security will be required for new connections into the payments network, and will drive similar requirements into B2B commerce and other verticals
- Other entities use HSM's as well
  - Government
    - NSA, CIA, Military
  - Certificate Authorities
  - Business running commerce/information servers

HSM use in Government

- "Type 1" devices
  - Provide approved US government user with secure cryptographic products that are suitable for protection of classified information
    - Satellite data
    - Other data
    - Voice data
  - Goal(s):
    - Secure, reliable transport of information
    - Command and control

HSM use by Certificate Authorities

- Certificate Authorities
  - Sign business/user X.509 certificates
  - Root key is thus of great value
- Private key that signs certificate(s) must be protected
  - Locate CA in secure location (external threats)
  - Utilize FIPS 140-2 Level 4 key storage device (internal threats)

HSM use by Businesses Running Commerce/Information Servers

- The identity of high value servers (providing information or commerce services) is of great value.
- The private key representing that identity must be protected against inside and outside threats
  - FIPS 140-2 Level 3-4 key storage

HSM Future Trends

- More “off the shelf” vs. “custom”
- Gigabit cryptographic processing
- General cryptographic processing
- More of application will be moving into the HSM

Summary

- Software based security cannot meet existing and emerging requirements for secure application deployment
- IT systems can only be strongly secured with hardware based security
- Banks were the first commercial entities to make this realization
- HSM's are heavily used by the CIA, NSA, military and other government intelligence agencies to secure data and voice transmission
- HSM's have application outside the banking industry
- Legislated security mandates (e.g. HIPAA, SO, GLB, etc) will require the use of HSM technology.
- As HSM's advance, more of the application will be placed inside


hp
invent