Open Web Application Security Project

Commercial Cryptographic Transitions and Web Application Key Management

Mr. Jeff Stapleton
CTO, Innove LLC
jeff.stapleton@innove.biz
(210) 568-3823
(636) 448-5775 mobile

Innové

Agenda

Cryptography Transitions

- Technology Issues
- Transition Principles
- Transition Life Cycle
- Case Studies

Key Management for Web Applications

- Standards Bodies
- Payment Card Industry (PCI)
- Key Management Principles
- Web Server Environment

Cryptography Transitions

IEEE 2006 Region 5 Technical, Professional, Student Conference – San Antonio TX

Definition: ***Managing the transformation from one cryptographic architecture to another cryptographic architecture in a methodical approach that is consistent with prudent business practices and security guidelines.***

1. Introduction

2. Technology Issues

2.1 Key Life Cycle

2.2 Algorithm Life Cycle

2.2.1 Differential Cryptanalysis

2.2.2 Integer Factorization

2.2.3 Quantum Computing

2.3 Product Life Cycle

3. Transition Principles

3.1 Business Requirements

3.2 Cryptographic Hardware

3.2.1 Tamper Resistant Security Module

3.2.2 Interoperability

3.2.3 Reliability

3.2.4 Certification

3.3 Application Management

3.3.1 Algorithm Independence

3.3.2 Security Architecture

3.3.3 Enterprise Management

3.3.4 Security Guidelines

4. Transition Life Cycle

4.1 Vulnerability Assessment

4.2 Impact Analysis

4.3 Implementation

4.4 Reconciliation

5. Case Studies

5.1 Healthcare Industry Study

5.2 Financial Industry Study

5.3 Government SBU Study

5.4 DoD Crypto Modernization

6. Summary

Technology Issues

- **Key Life Cycle**
  - **Advancements in raw computing power (Moore's Law) has increased risk to shorter cryptographic keys**
- **Algorithm Life Cycle**
  - **Advancements in mathematical research (Frequency Analysis, Differential Cryptanalysis, Number Field Sieve, Differential Power Analysis) can increase risk to existing algorithms**
- **Product Life Cycle**
  - **Hardware and/or Software lose vendor support such that products are no longer maintainable or available**

Transitional Principles

- **Business Requirement Principle**
  - **Overarching principle (and some common sense)**
- **Cryptographic Hardware Principles**
  - **Tamper Resistant Security Module (TRSM)**
  - **TRSM Interoperability**
  - **TRSM Vendor Reliability**
  - **TRSM Certification**
- **Application Management Principles**
  - **Algorithm Independence**
  - **Security Architecture**
  - **Enterprise Management**
  - **Security Guidelines**

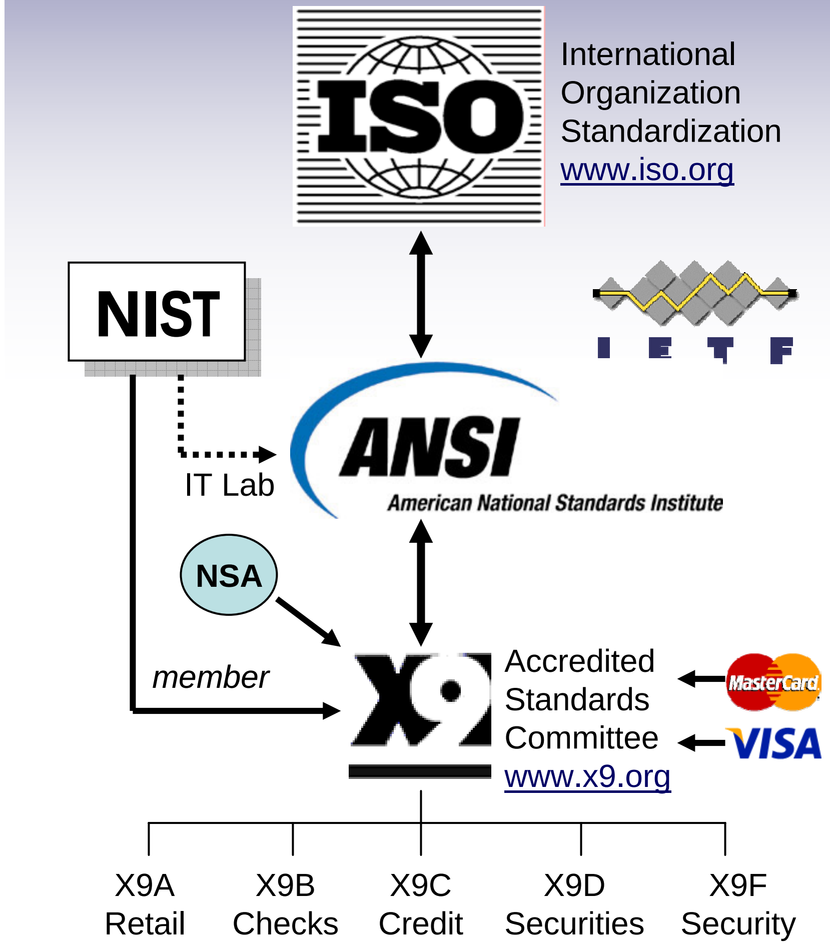
Transition Life Cycle

- **Vulnerability Assessment**
  - Legacy System Requirements
  - New System Requirements
  - Infrastructure Requirements
  - Risk Assessment
- **Impact Analysis**
  - Inventory Assessment
  - Dependency Analysis
  - Jurisdictional Issues
  - Migration Issues
- **Transition Implementation**
  - Development Plan
  - Test Plans
  - Quality Assurance Plan
  - Deployment Plan
- **Transition Reconciliation**
  - Conduct Post mortem
  - Monitor Program
  - Transitions are Cyclic

Case Studies

- **Healthcare Case Study**
  - HIPAA as driver; transition E-mail system from no encryption to password-based encryption to PKI
- **Pharmaceutical Case Study**
  - HIPAA as driver; transition anonymous prescription data feeds from multiple sources to centralized data mining facility
- **Financial Services Case Study**
  - Protecting Personal Identification Number (PIN) was driver
  - Transition ATM and POS from Tables to DES to TDES
- **Government SBU Case Study**
  - Protecting Sensitive But Unclassified (SBU) data was one driver
  - Cost reduction and wider availability were additional drivers
  - Transition from government proprietary cryptography to DES to TDES to AES
- **DoD Cryptographic Modernization**
  - Drivers include maintainability, cost containment, information assurance, and enhanced functionality
  - Transition legacy equipment to modern equipment

Standards Bodies



International Organization Standardization
www.iso.org

NIST

IT Lab

NSA

member

Accredited Standards Committee
www.x9.org

X9A Retail

X9B Checks

X9C Credit

X9D Securities

X9F Security

- ISO has ~100 member bodies & over 200 technical committees
  - TC 68 Financial Services Industry
  - ISO / IEC Joint Technical Committee One (JTC1)
- ANSI is the US national standards body to ISO
  - Accredits standards organizations
- X9 is an ANSI accredited standards body for the Financial Services Industry
  - US TAG to TC 68
- NIST is responsible for the Federal government, including commerce
  - NIST, NSA members of X9
  - NIST chairs ISO JTC1 SC 37 Biometrics
  - NSA is a US expert to ISO TC 68
- Payment Industry
  - MasterCard, Visa, AMEX, Discover members of X9
  - MasterCard, Visa liaison members to ISO TC 68
- IETF is an independent, unaffiliated, “international” standards body
  - Web services are based on IETF and W3C specifications
- *Disconnect* between financial services and the Internet community

Payment Card Industry (PCI) Data Security Standard

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored data

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Requirement 3: Protect stored data

Address data management

- 3.1 Keep cardholder information storage to a minimum
- 3.2 Do not store sensitive authentication data subsequent to authorization
- 3.3 Mask account numbers when displayed
- 3.4 Render sensitive cardholder data unreadable

Address key management

- 3.5 Protect encryption keys against both disclosure and misuse
- 3.6 Document and implement all key management processes and procedures

3.5 Protect encryption keys against both disclosure and misuse

3.5.1 Restrict access to keys to the fewest number of custodians necessary.	**X9.24 Retail Key Management** – ***Avoid "super-user" syndrome***
3.5.2 Store keys securely in the fewest possible locations and forms.	**X9.24 Retail Key Management** – **Originated as input from MasterCard** – ***Initial direction was to restrict keys to two entities (sender & receiver)*** – **Infeasible for POS environment & especially important for the Internet environment with multiple Web servers**

3.6 Document and implement all key management processes and procedures

3.6.1 Generation of strong keys	**X9.80 RNG (draft)**
3.6.2 Secure key distribution	**X9.24 Retail Key Management** – **X9.42 D-H, X9.44 RSA, X9.63 ECC**
3.6.3 Secure key storage	**X9.24 Retail Key Management**
3.6.4 Periodic key changes	**X9.24 Retail Key Management**
3.6.5 Destruction of old keys	**X9.24 Retail Key Management**
3.6.6 Split knowledge and dual control	**X9.24 Retail Key Management**
3.6.7 Prevention of unauthorized substitution of keys	**X9.24 Retail Key Management**
3.6.8. Replacement of known or suspected compromised keys	**X9.24 Retail Key Management**
3.6.9. Revocation of old or invalid keys (RSA keys)	**X9.57 Certificate management**
3.6.10 Form for key-custodian responsibilities	

Requirement 4: Encrypt transmission

4.1 Use strong cryptography (at least 128 bit)

- Secure Socket Layer (SSL)
- Point-to-Point Tunneling Protocol (PPTP)
- Internet Protocol Security (IPSEC)

4.1.1 For wireless networks

- Wi-Fi Protected Access (WPA) if WPA capable
- Virtual Private Network (VPN)
- Secure Socket Layer (SSL) at 128-bit

Negative Requirements

- Never rely exclusively on Wired Equivalent Privacy (WEP) to protect confidentiality and access to a wireless Local Area Network (LAN). Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

4.2 Never send cardholder information via unencrypted e-mail

Still need to deal with key management – X9.24

Key Management Principles

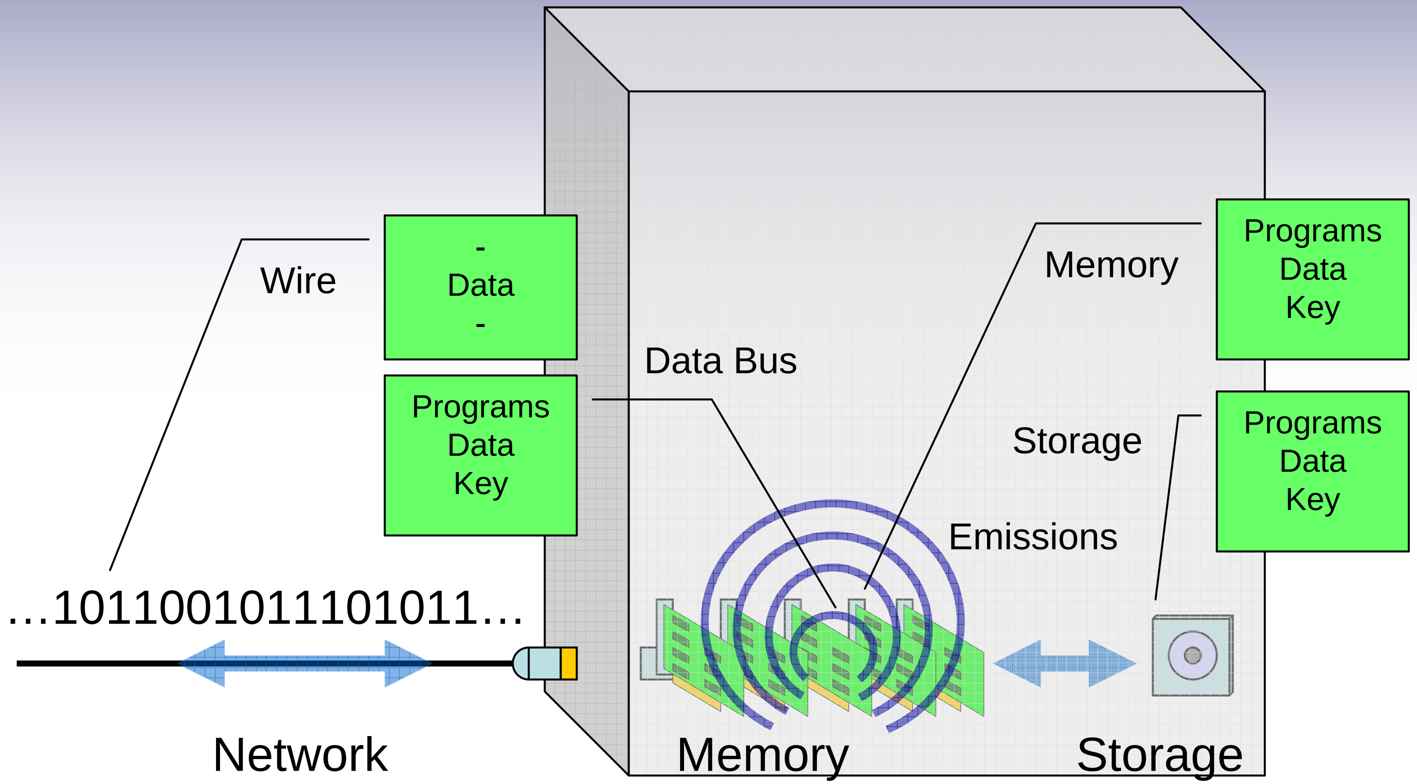
American National Standard X9.24-2006

Retail Financial Services Symmetric Key Management

- Symmetric keys and Asymmetric private keys (*secret*)
  - Inside a Tamper Resistant Security Module (TRSM)
  - Encrypted outside a TRSM
  - Key components (key shares) employing dual control and split knowledge
- Asymmetric public keys (*public*)
  - Any form that a private can exist
  - Embedded in a public key certificate (digital signature)
  - Protected with a message authentication code (MAC)

    [a cryptographic checksum using symmetric cryptography]
- Financial network audit requirements codified in Guideline for Financial Services (TG-3-2004) Retail Financial Services Compliance Guideline or “TG-3”
  - 60% dedicated to key management; 24 of 39 compliance statements

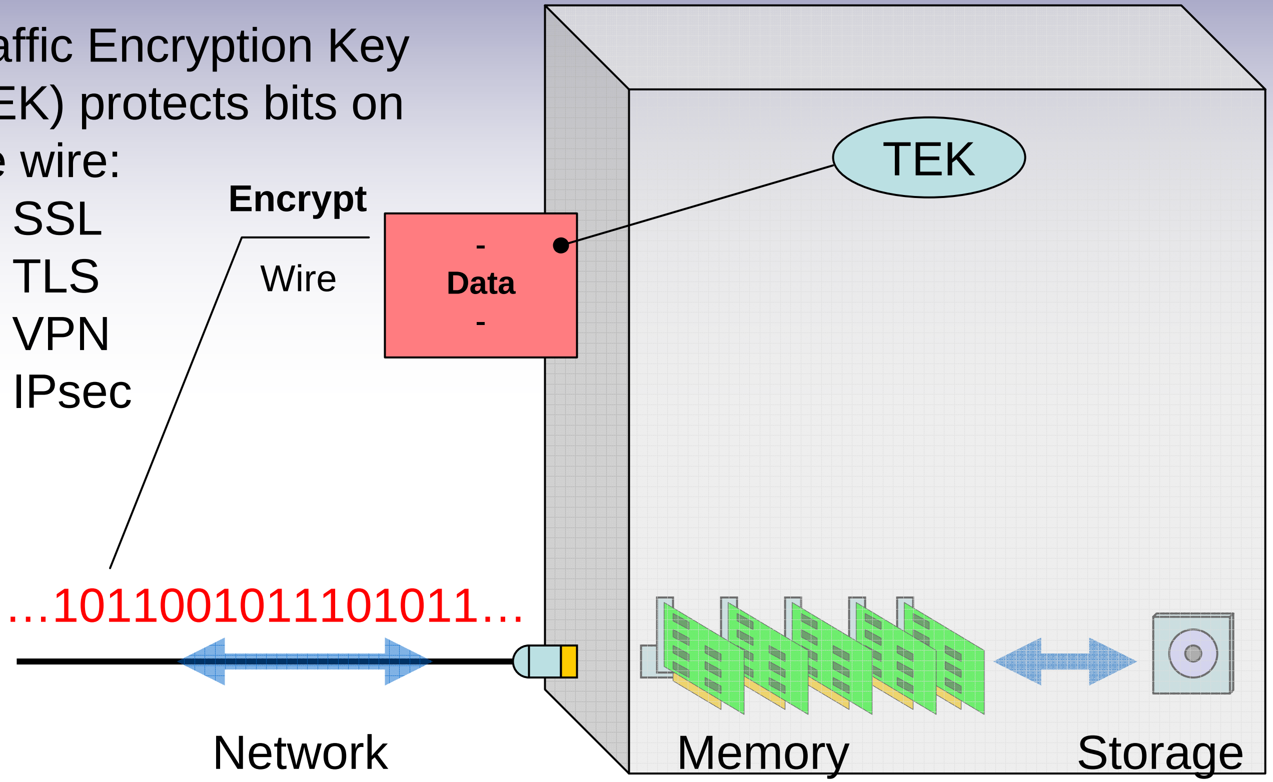
Web Server Environment



Traffic Encryption Key

Traffic Encryption Key (TEK) protects bits on the wire:

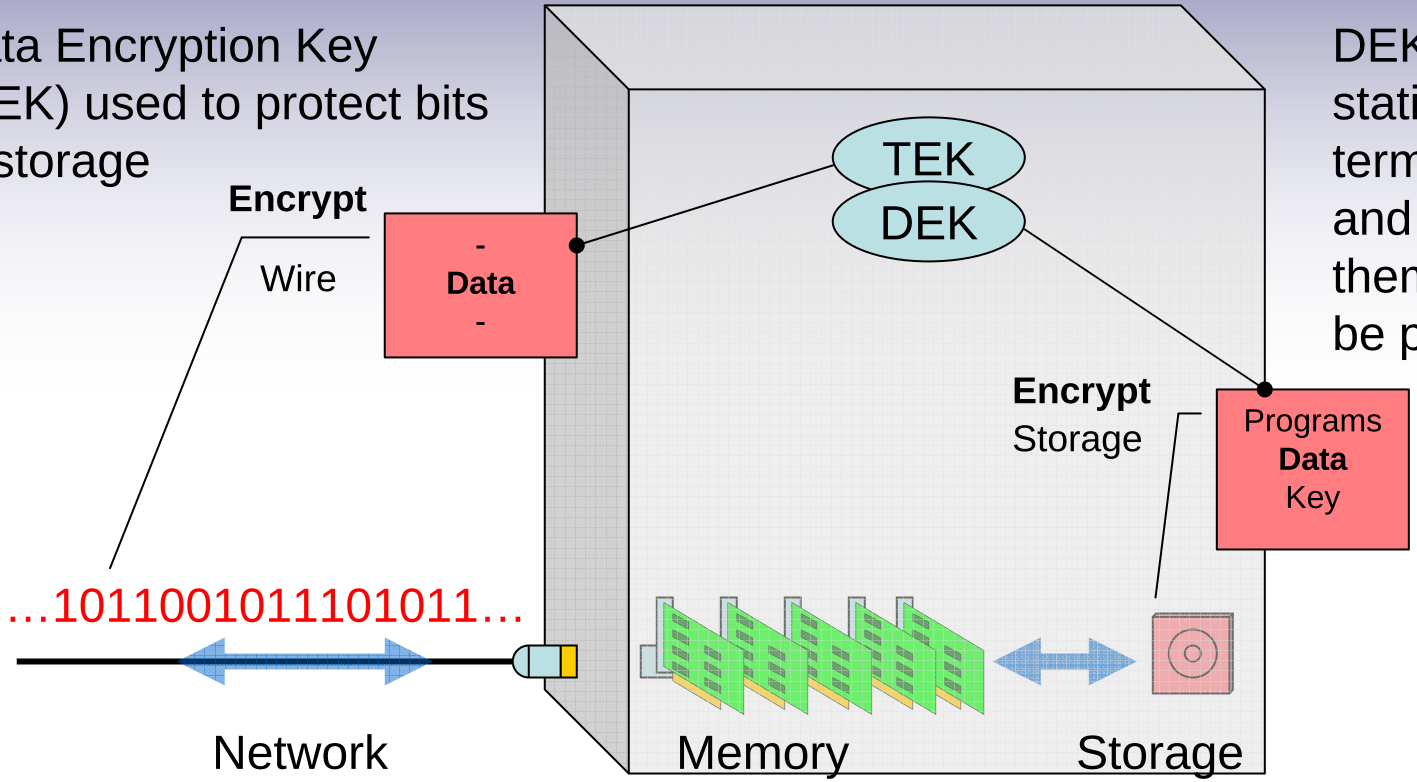
- SSL
- TLS
- VPN
- IPsec



TEKs are temporal, established per session, then they go away – low risk situation

Data Encryption Key

Data Encryption Key (DEK) used to protect bits in storage

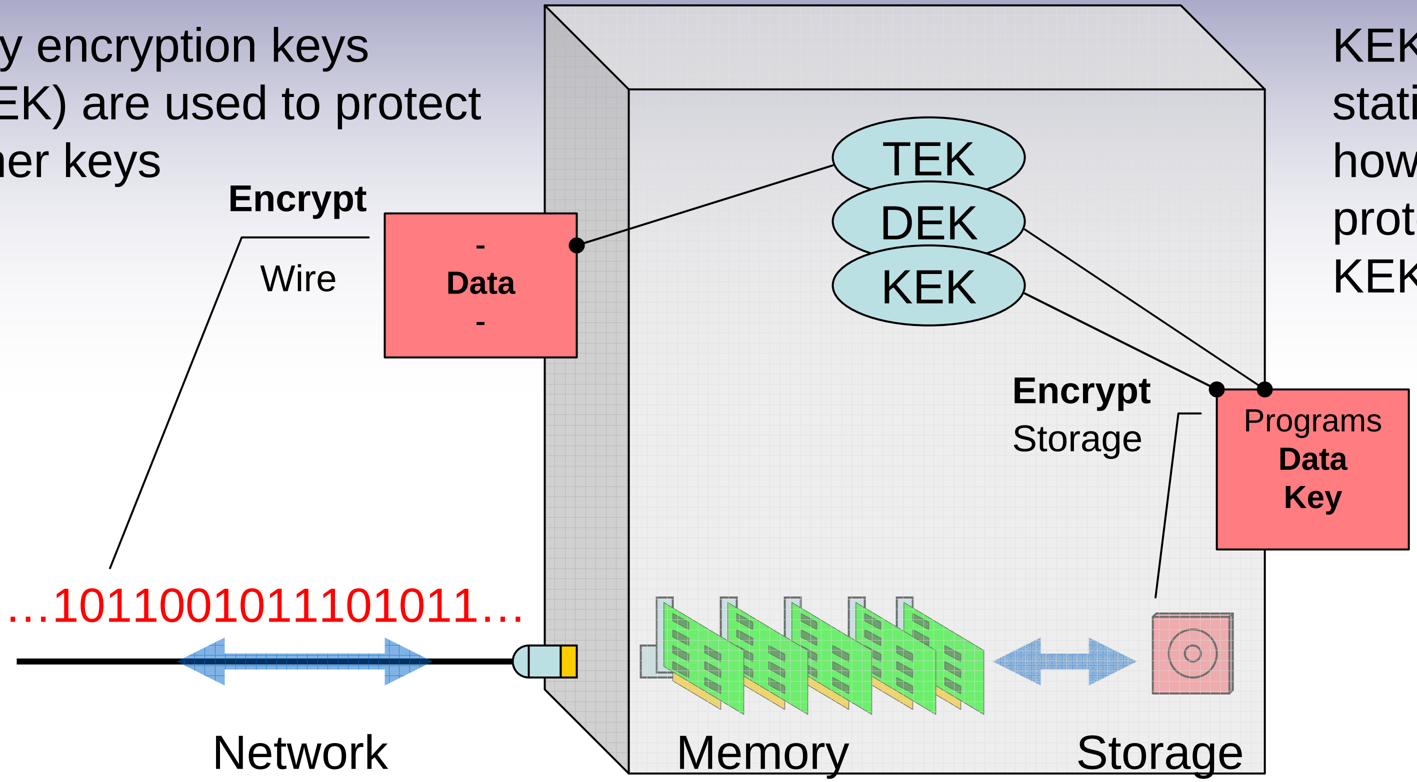


DEKs are static, long-term keys and must themselves be protected

Unprotected stored data is a hacker’s gold mine…

Key Encryption Key

Key encryption keys (KEK) are used to protect other keys



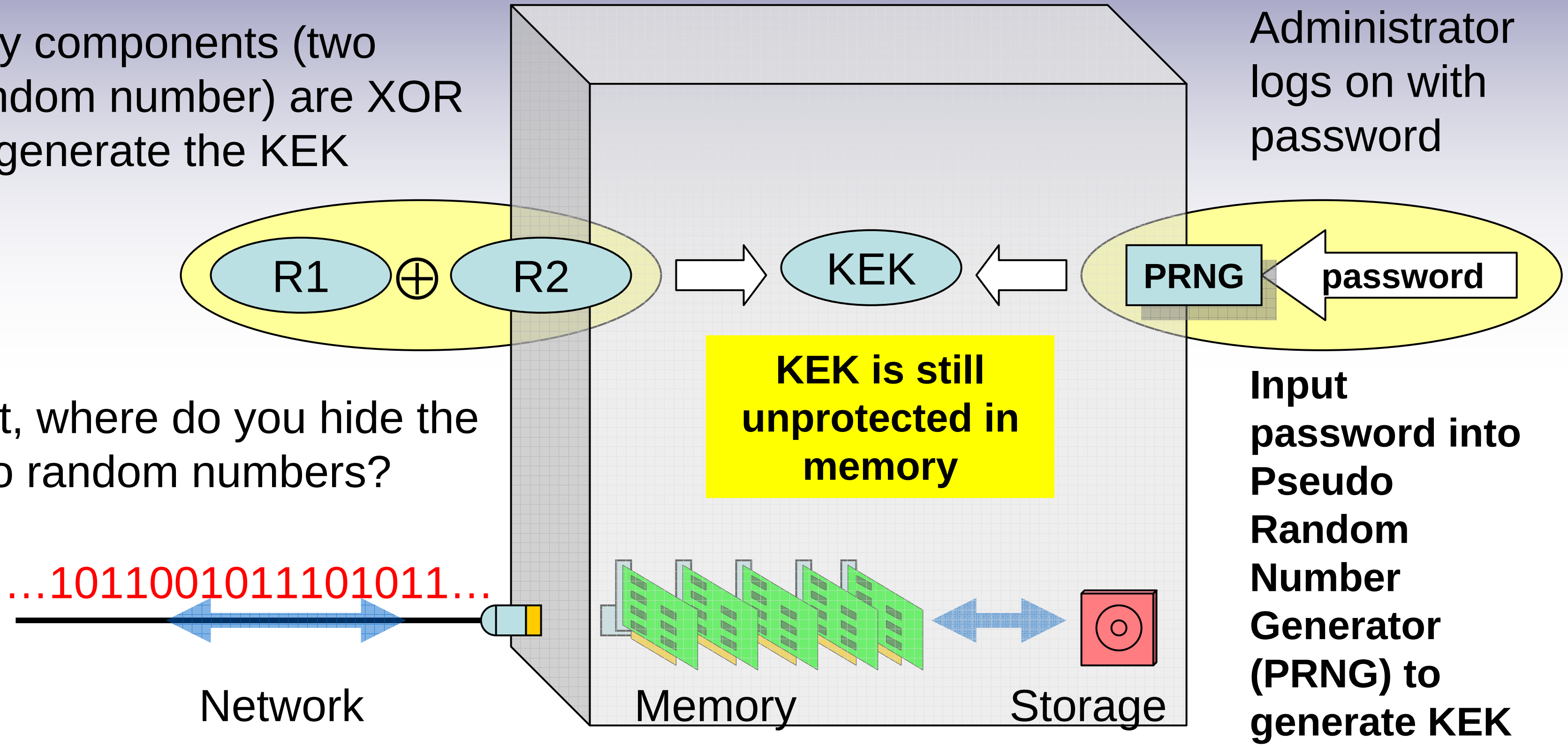
KEKs are static, but how to protects the KEK?

Protecting KEK (and others)

Key components (two random number) are XOR to generate the KEK

But, where do you hide the two random numbers?

Administrator logs on with password

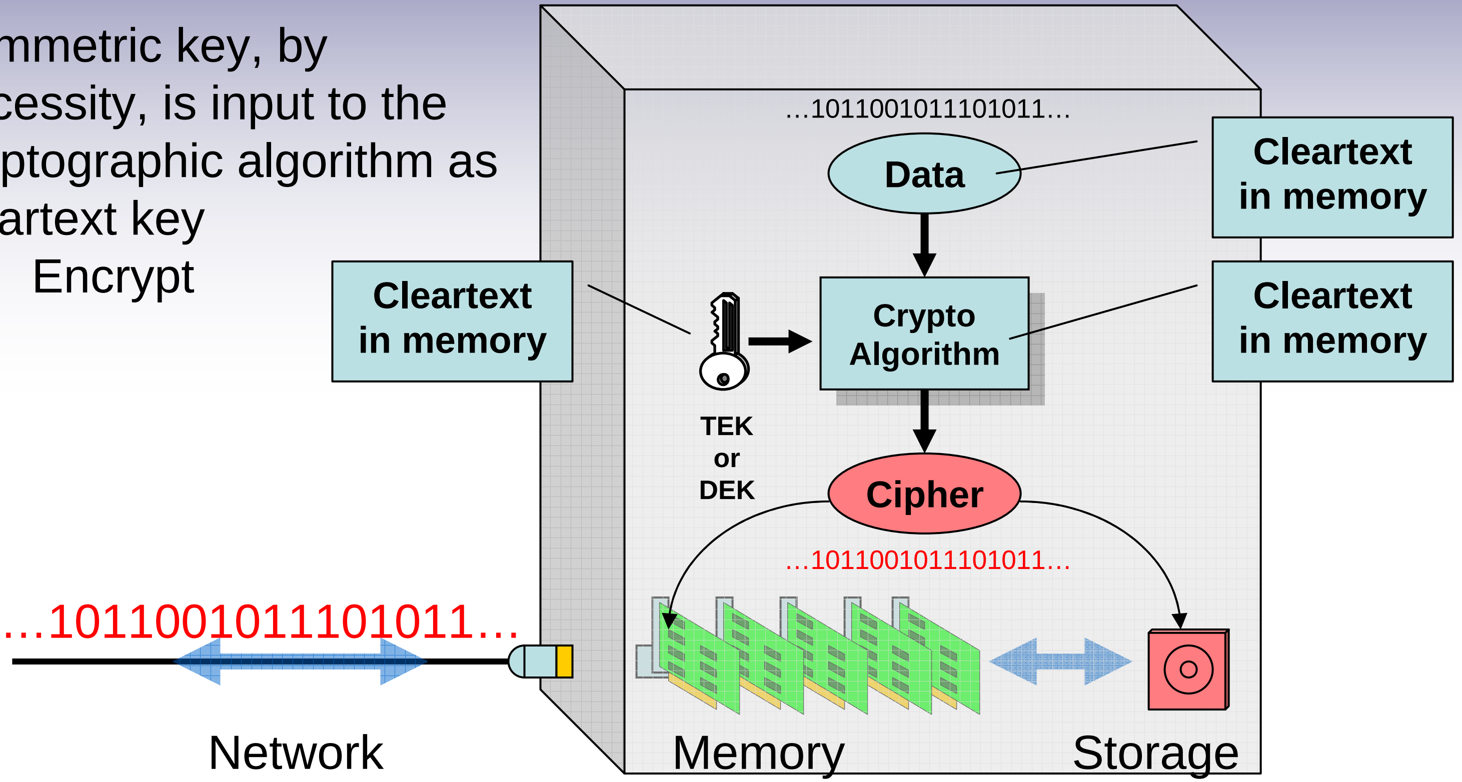


Input password into Pseudo Random Number Generator (PRNG) to generate KEK

Think Inside the Box…encrypt

Symmetric key, by necessity, is input to the cryptographic algorithm as cleartext key

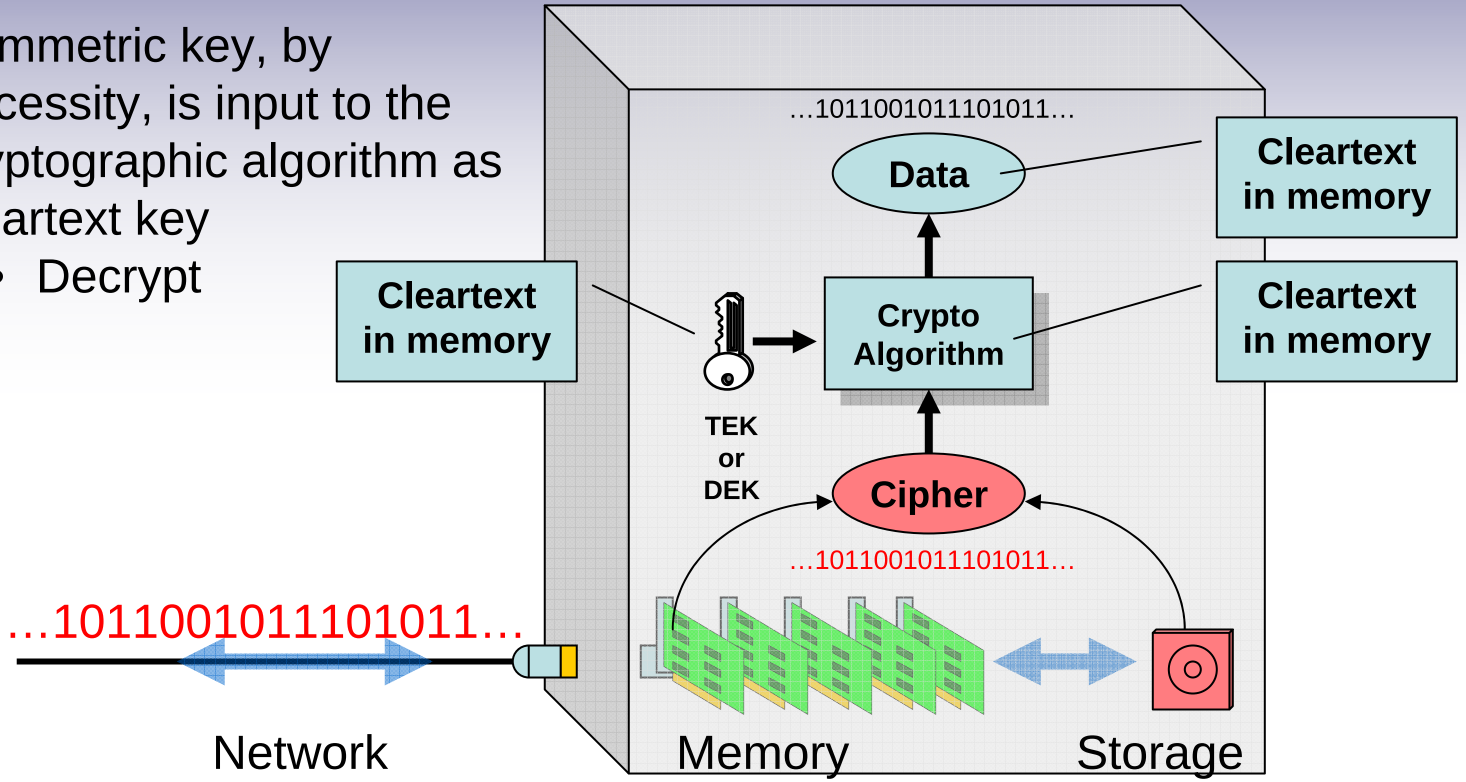
- Encrypt



Think Inside the Box…decrypt

Symmetric key, by necessity, is input to the cryptographic algorithm as cleartext key

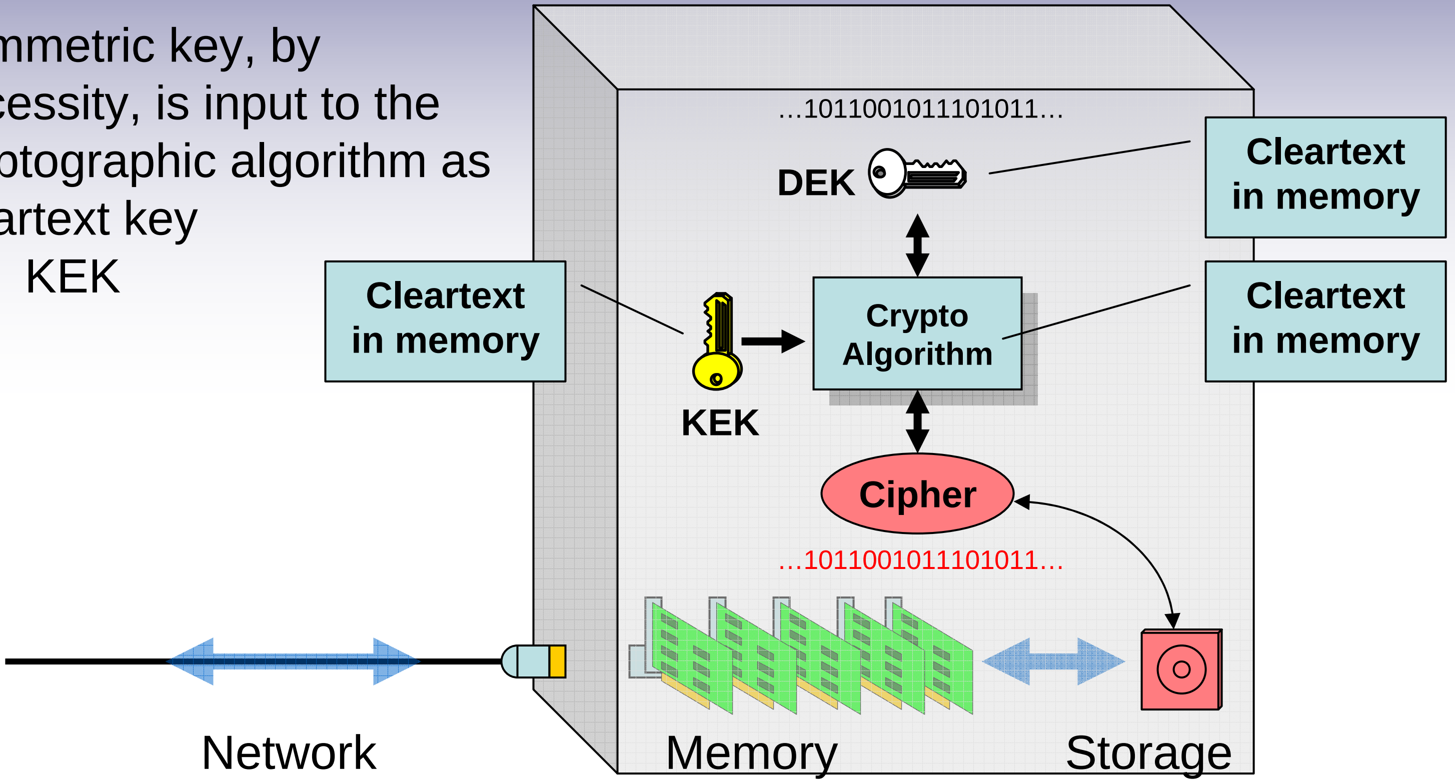
- Decrypt



Think Inside the Box…KEK

Symmetric key, by necessity, is input to the cryptographic algorithm as cleartext key

- KEK



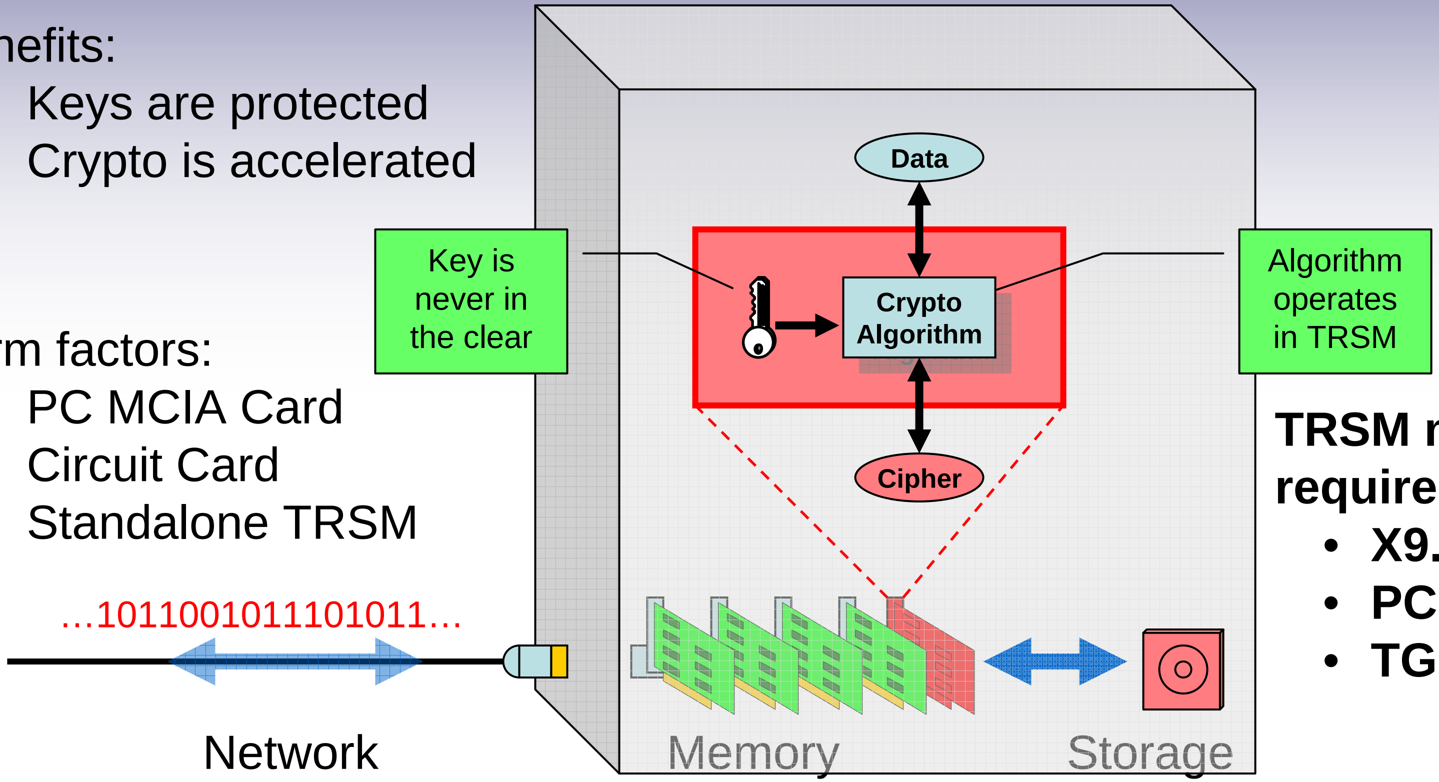
Think Inside the Box…TRSM

Benefits:

- Keys are protected
- Crypto is accelerated

Form factors:

- PC MCIA Card
- Circuit Card
- Standalone TRSM



Key is never in the clear

Algorithm operates in TRSM

TRSM meets requirements:

- **X9.24**
- **PCI**
- **TG-3**

NOTE: TRSM key management is specific to TRSM manufacturer

Summary

- Cryptography Realizations
  - Cryptography transitions are inevitable, require planning, challenging, feasible and worth doing well…
  - Cryptography is about protecting data
  - Key management is about protecting cryptographic keys
- TRSM (hardware) is the optimal solution
  - PCI does not specifically call for hardware (politics)
  - Associations mandate TRSM for PIN protection
  - Association do not (yet) mandate TRSM for data protection
- Political Realizations
  - Associations (MasterCard, Visa) have direct influence to financial institutions (Issuers - Cardholders, Acquirers - Merchants)
  - Associations have influence of merchants and cardholders
  - IMHO, PCI is a simplified rehash of the **SET** Secure Electronic Transaction Specification Book 1: Business Description Version 1.0 May 31, 1997
- **Questions?**