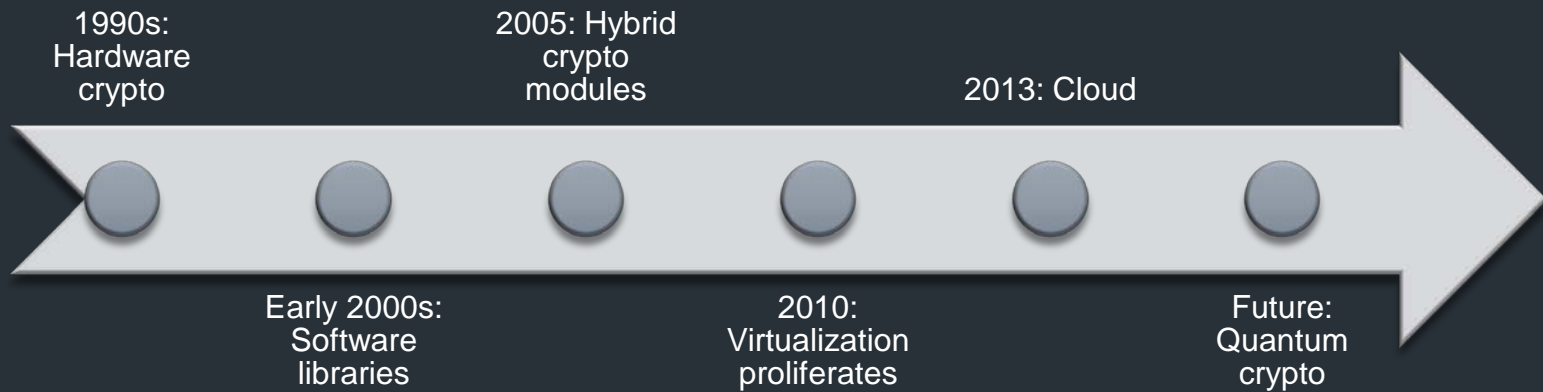




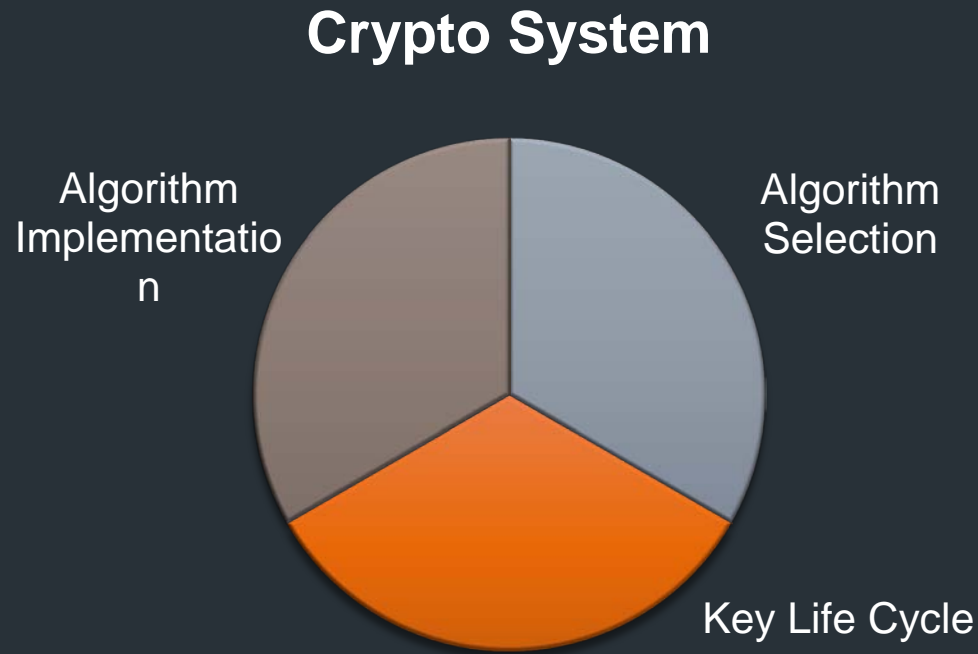
Cryptography and Common Criteria

Chris Brych and Ashit Vora
ICCC 2013

Evolution of Cryptography

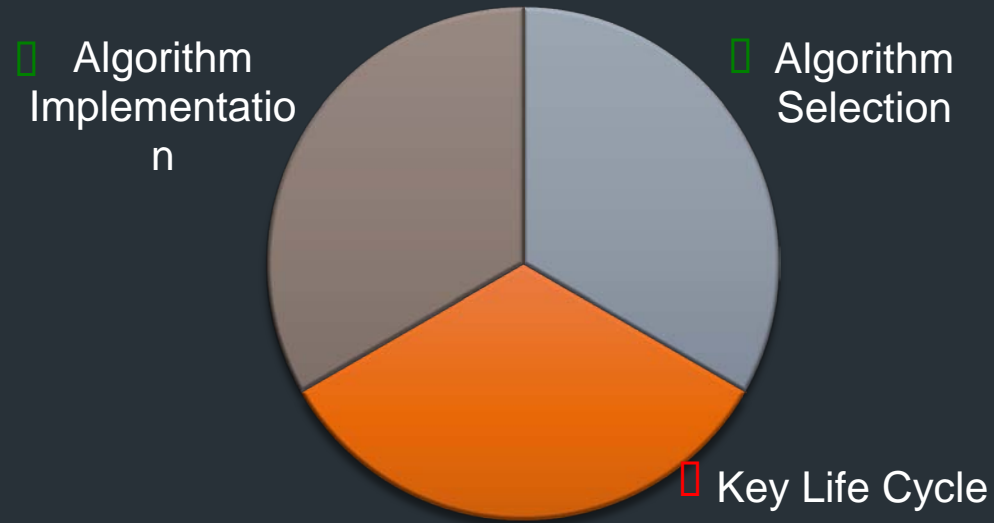


Anatomy of a good crypto system

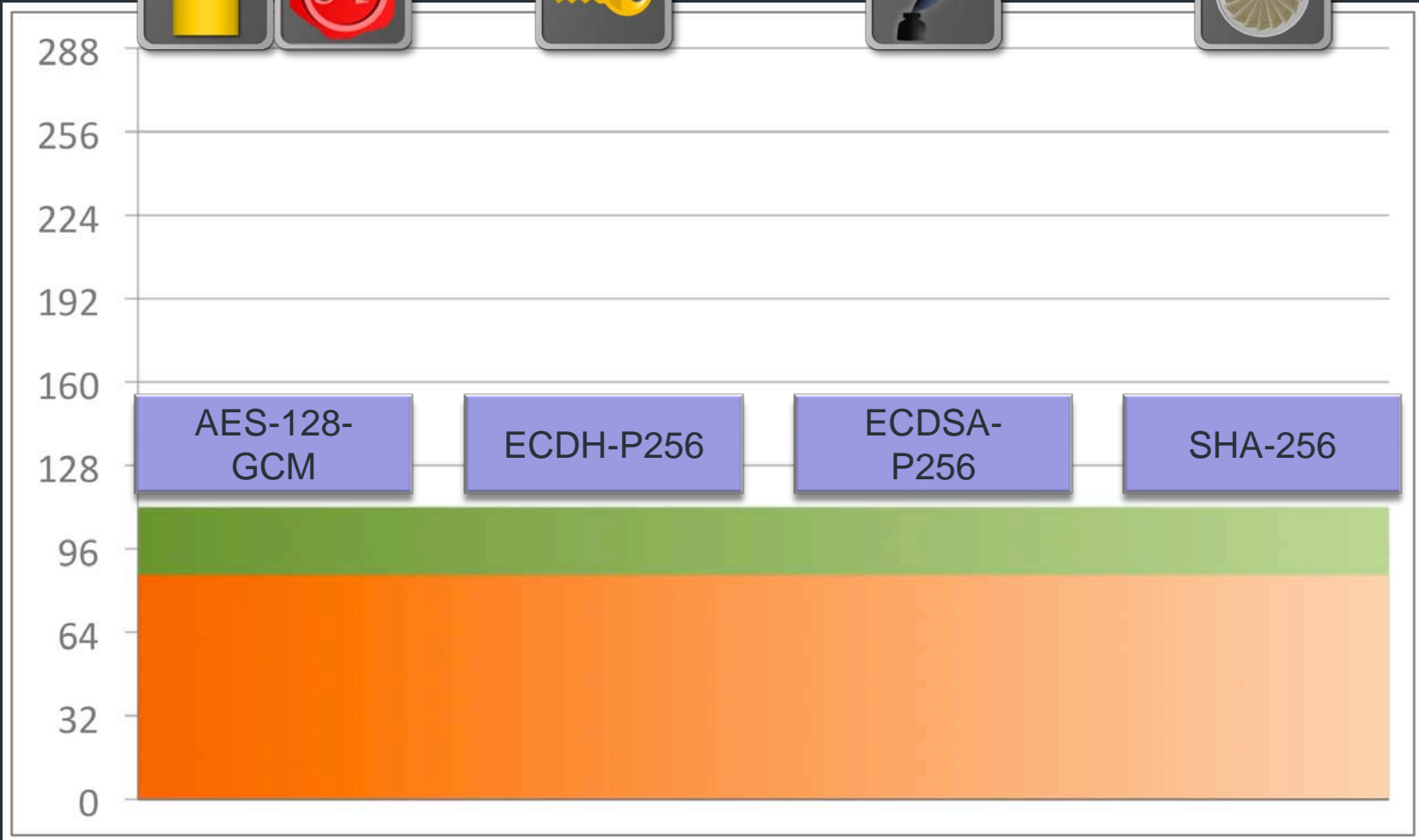


Anatomy of a good crypto system

Crypto System



Algorithm Selection: Right tools for the right job



Implementing Crypto Algorithms



Key Life Cycle

- Key Generation
- Key Access Control
- Key Transport / Key Establishment
- Key Storage
- Key Destruction

Key Generation

- Symmetric vs Asymmetric
 - Symmetric Key Generators
 - Pseudo Random Number Generators
 - Deterministic Random Bit Generators
 - Asymmetric Key Generators
 - FIPS 186-2 (ANSI X9.31)
 - FIPS 186-3 /4
- Key Strength Determined by the Generation of Entropy
 - Deterministic Entropy Sources
 - Non-Deterministic Entropy Sources

Key Access Control

- How do you control access to keys?
 - A. Create Multiple Roles
 - i. Admin Role
 - ii. Security Officer Role

 - B. Access Permissions
 - i. Key Identity
 - ii. Key Entity
 - iii. Key Type
 - iv. Key Usage
 - v. Key Access Control Rules
 - vi. Key Validity Time Period

Key Transport / Key Establishment

- Asymmetric
 - RSA Key Wrap (SP 800-56B)
 - Diffie-Hellman / EC Diffie-Hellman Key Exchange (SP 800-56A)
- Symmetric
 - AES Key Wrap
 - Triple-DES Key Wrap

Key Storage



- Ephemeral / Working Keys
 - Volatile RAM (plaintext)
- Secret / Private Keys
 - Non-Volatile RAM (encrypted)
- High Assurance
 - Hardware Security Module (HSM)
 - Security Processor
- Key Backup Strategies
 - Smart Cards or USB Tokens

Key Destruction

- Key Destruction Mechanisms
 - Overwrite key location in memory and on non-volatile storage
 - Tamper Response and Zeroization Circuitry
 - Factory Reset

Making Key Life Cycle Tractable

Two Suggestions

Use of secure
key store

Audit all actions
on keys

Secure Key Store




- Secure key store localizes keys there by making them easier to protect and manage
- All key related operations occur via a well defined API
- Access to keys can be granularly controlled
- HW as well as SW key stores exists
- HW key store is ideal but not practical for all situations

Auditing Key Access


- Audit Controls on Key / CSP Management
 - Log Creation of Keys
 - Usage of Keys
 - Tamper or Zeroization of Keys
 - Password Changes



Covered in
new PPs



Algorithm Selection
Algorithm Implementation
Key Generation
Key Transport/Establishment



Should be
covered in
new PPs



Key Storage

Key access control

Timely key destruction

Audit logging of all action on
keys

Cryptography has evolved significantly over the past decade



There are many cryptographic algorithms available

Implementing cryptography is easier than ever

Key Life Cycle remains a challenge especially with more complex product architectures

Common Criteria can help uplift the industry's approach to key life cycle by introducing relevant requirements



Thank You!

Questions?