Cryptography and Common Criteria

Establishing a Representative List of Internationally Acceptable Approved Security Functions in ISO/IEC 19790

Sonu Shankar – Technical Leader, Trust Strategy and Clint Winebrenner Technical Leader, Global Certifications Team

November 5, 2015

Questions?

- tweet @CiscoCertTeam

Introduction and Background

- Cryptographic algorithm validation - Integral part of product security evaluations
  - Verifiable assurance that active cryptographic algorithms are implemented correctly
- ISO/IEC 19790
  - International standard specifying security requirements for cryptographic modules
  - Specifies list of approved security functions (cryptographic algorithms)
  - Huge global impact with widespread adoption of ISO/IEC 19790

Problem Statement

How do we establish a common internationally acceptable cryptographic evaluation process?

Problem Statement… details

- What challenges do we face today in the area of cryptographic validation and the establishment of a representative list of algorithms?
- Is there a reference recommended list of cryptographic algorithms covering encryption, integrity, authentication, random numbers?

Trust

- Customer ⟷ Vendor
- Vendor ⟷ 3rd Party Test Lab
- 3rd Party Test Lab ⟷ Certification Body

... But Verify?

- Evidence based verification of cryptographic algorithm implementation
- Scalable, repeatable validation methods for each approved cryptographic algorithm
- Submit algorithm implementation information, receive test vectors, submit responses, verify responses, publish cert

Challenge #1

Don't trust the algorithm?

Remediation

- Engage experts from the industry and academia
- Critically analyze design from both a security and performance perspective
- Propose effective, scalable alternatives

Challenge #2

Trust the algorithm, but, don't trust the algorithm validation process?

Remediation

- Modify existing process for algorithm validation?
- Introduce methods to verify a sub-set of the effort?
- Share more evidence?
- Publish detailed algorithm validation results?

Challenge #3

Trust the algorithm, trust the validation process, but, don't trust the algorithm use cases in protocols?

Remediation

- Share information re: IUT's protocol implementation
- Verify algorithm initialization details via source code reviews
- Verify platform algorithm integration

Cisco's “Next Generation Encryption” Recommendations

- Choosing algorithms considering advances in computing and cryptanalysis
- Focus on security, efficiency (low-power endpoints), scalability
- Encryption - *AES-CBC mode*, AES-GCM mode
- Integrity - *SHA-1* (legacy), SHA-256, SHA-384, SHA-512
- Authentication - *RSA-2048*, ECDSA-256, ECDSA-384
- Random number generation - AES-256 CTR-DRBG

Summary

- Opportunity to establish new internationally acceptable evaluation process
- Significant impact on industry from business perspective; ability to rapidly deliver state of the art solutions
- Directly influences product, infrastructure security globally
- Challenges exist. Need for open dialog.
- Any questions or follow up please contact @CiscoCertTeam


CISCO