Towards an International Cryptographic Validation Program

Where Are We Now?

Clint Winebrenner Technical Leader, Global Certifications Team

May 18, 2017

What are we going to talk about?

- Introduction/background
- Shift?
- Algorithm testing and trust
- Internationally acceptable cryptographic validation program
- Summary

Introduction and Background

- Cryptographic algorithm validation - Integral part of product security evaluations
  - Verifiable assurance that active cryptographic algorithms are implemented correctly
- In years past
  - Different country, different requirements
  - Multiple evaluation efforts means we are testing the same product/service multiple times

Shift?

- Widespread Common Criteria Protection Profile evolution and adoption is changing how we scope cryptography gaps
- To only scope for FIPS crypto requirements has us playing catch up in the long run
- Common Criteria is driving crypto requirements, not FIPS

Previous Challenge

Trust the algorithm, but don’t trust the algorithm validation process.

Remediation

- ACAVP!

Previous 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?

- Have we made any progress on this?

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-256, SHA-384, SHA-512
- Authentication - *RSA-2048*, ECDSA-256, ECDSA-384
- Random number generation - AES-256 CTR-DRBG

Summary

- The CMVP and CAVP's move to automation
- International procurement requirements are not 100% solved through Common criteria
- Directly influences product, infrastructure security globally
- Challenges exist. Need for open dialog.
- Any questions or follow up please contact @CiscoCertTeam

Questions?

- tweet @CiscoCertTeam


CISCO