National Institute of Standards and Technology
U.S. Department of Commerce

Assurance Architecture Through Testing

International Cryptographic Module Conference
17 May 2017

Michael Cooper, Manager
Security Testing, Validation and Measurement Group
Computer Security Division, NIST

Welcome

National Institute of Standards and Technology
U.S. Department of Commerce

- This is the 5th ICMC
- Thank You
  - to all of the people that have planned this conference over the past 5 years
- This Conference has become a model for collaboration between government and industry

CSD vs Security Testing Group Mission

National Institute of Standards and Technology
U.S. Department of Commerce

- CSD
  - The Computer Security Division (CSD), a division of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) is responsible for developing cybersecurity standards, guidelines, tests, and metrics for the protection of non-national security federal information systems. CSD's standards, guidelines, tools and references are developed in an open, transparent, traceable and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted globally.

CSD vs Security Testing Group Mission

National Institute of Standards and Technology
U.S. Department of Commerce

- STVMG
  - CSD operates several validation programs that help provide a level of assurance that products meet established security requirements and conform to published specifications. To that end, the Security Testing, Validation, and Measurement Group (STVMG) develops test suites and test methods; provides implementation guidance and technical support to industry forums; and conducts education, training, and outreach programs.

Current Validation Programs

National Institute of Standards and Technology
U.S. Department of Commerce

- Cost and Time
- No integration testing
- No ability to know what product of the validated module
- How do I know if the product that I am using is validated
- Migration of validation to similar operating environments

NIST Metrology

National Institute of Standards and Technology
U.S. Department of Commerce

- Metrology − the study of measurement science
- NIST is a Metrology research agency
- What are the appropriate measures for cybersecurity?
  - Vulnerabilities?
  - Software errors?
  - Size and complexity of the system?
- Testing provides measurements…

Information Assurance

National Institute of Standards and Technology
U.S. Department of Commerce

- This was the predominant term used for many years to describe what most people mean when the use the term “cybersecurity” today
- Cybersecurity more focused on ethical hacking, threats, vulnerabilities, risk assessment, indicator sharing, remediation, reporting, etc.
- Assurance is more focused on how to build provably secure systems

Science vs Architecture vs Engineering

National Institute of Standards and Technology
U.S. Department of Commerce

- Types of engineering – Civil, Systems, Software
- Composition vs decomposition
  - Unit / back-box testing vs integration testing
  - Cryptographic system stack
- The value of automation
- The value of objective results and artifacts to show conformance to standards
- Use cases – not all requirements in the standards are of equal importance for all expected implementations.
- The role of the agency CIO/CISO?

NIST/NIAP

National Institute of Standards and Technology
U.S. Department of Commerce

- NIAP originally focused on the goal of building systems with a known provable level of assurance, which is a good goal.
- The work that is being done in the development of the many protection profiles are the most relevant security guides for the subject technologies.
- cavp/cmvp -> NIAP PP -> NIST 800-53 -> CyberSecurityFramework

RSA

National Institute of Standards and Technology
U.S. Department of Commerce

- RSA – Whitfield Diffie – cryptographers panel
  - https://www.rsaconference.com/events/us17/agenda/sessions/7580-the-cryptographers-panel
- “Build Better Systems”

Final Thoughts

National Institute of Standards and Technology
U.S. Department of Commerce

- More testing is better
- Faster and lower cost testing is better
- Automation helps accomplish more/better/faster
- Integration testing of each layer builds an assurance case
- Transparent public/private partnership will produce best results