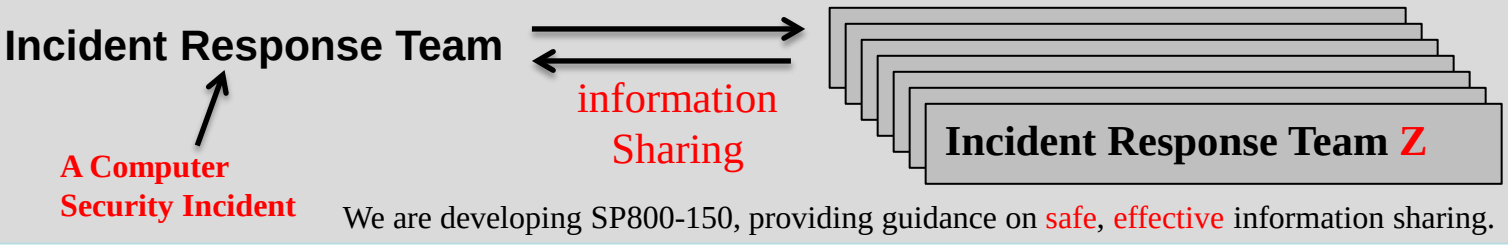
Security Components and Mechanisms

Lee Badger

June. 4, 2013

Major Thrust Areas

1 Incident Coordination (Lee Badger and David Waltermire)



We are developing SP800-150, providing guidance on safe, effective information sharing.

2 Algorithms for Intrusion Measurement (Peter Mell)

Network tainting
Bounding Internal Attack Propagation

Scan detection
Improving Scan Detection Techniques

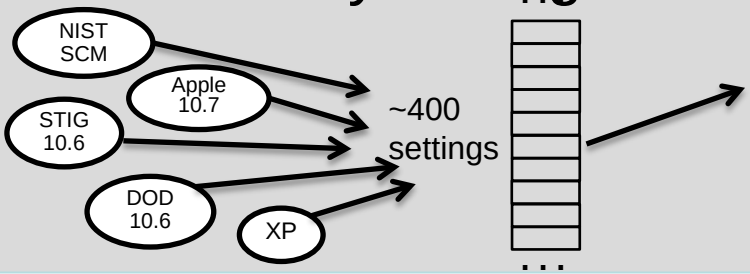
Log aggregation
Efficient Alert Aggregation With Optimization of Data Element Cardinality

3 IPv6 Profile and Testing (Sheila Frankel)

1. IPsec interactive tester
2. SP 800-119: Guidelines for the Secure Deployment of IPv6
3. SP 500-267: A Profile for IPv6 in the US Government
4. USGv6 IPv6 Test Program: tests IPv6 conformance and interoperability
5. NIST IPv6 Deployment Monitor

Major Thrust Areas

4 OSX Security Configuration (Kathy Ton-Nu)



Common Configuration Enumeration (CCE)

↓

Open vetting process

↓

OSX Hardening Guide

5 Continuous Monitoring Architecture (David Waltermire)

Defines:

Workflows – How information moves through the system?

Subsystems – What components comprise the a CM system?

Interfaces – How components communicate and what data is exchanged?

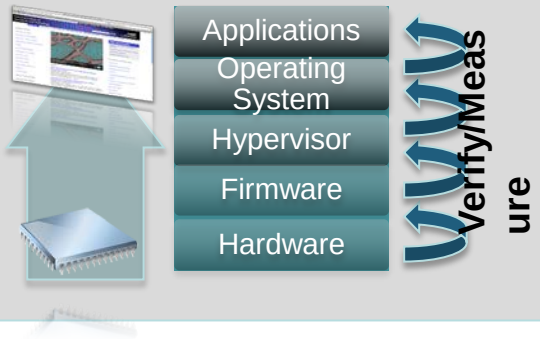
Working with DHS and NSA on overall architectural approach.

6 Roots of Trust (Andrew Regenschneid)

Perform a vital function.

resistant to tampering
isolated and trusted env.
small, simple
limited attack surface

E.g.
- RoT for Storage
- RoT for Integrity
- RoT for Reporting
- RoT for Measurement
- RoT for Verification



Major Thrust Areas

7 Security Content Automation Protocol (David Waltermire)

Facilitate transition of specs to SDOs.

8 Biometric Standards & Conformance Testing (Fernando Podio)

Key Objectives & Impact

- Increased adoption of technically-sound biometric standards (e.g., DoD, DHS, Spain, …)
- Test tools are being required by users (e.g., government agency) and are being used by testing labs and vendors worldwide.
- Developed the set of conformance test assertions for a Conformance Testing Methodology (CTM) for the ANSI/NIST-ITL 1-2011 standard.

9 Combinatorial Methods in Software Testing (Rick Kuhn)

34 switches -> 2^{34} = 1.7 x 100000000000 tests.

But errors tend to cluster in interactions with small numbers of variables.

Considering only 3=4-way interactions, only need **85** tests.

Enhancing testing effectiveness, measuring testing effectiveness.