Evidence-Based, Good Enough, and Open

Karen Scarfone
Computer Security Division
National Institute of Standards and Technology (NIST)

Outline

- Motivation
- Security Content Automation Protocol components
- Host score generation
- Future work

Overview

- Difficult to measure host security quantitatively
  - Complex, network attack-focused models
  - Multiple vulnerability classes to measure
- Framework for host security measurement
  - Evidence-based
  - “Good enough” answers
  - Reliance on open standards and specifications that facilitate automation

Applications for framework

- Compare a host’s security to a baseline configuration/policy
- Plan security policies and controls
  - Quantify policy strength, compare policies
  - Determine effect of policy change
  - Select security controls (limited resources)
- Provide data for attack/threat modeling
- Assess and quantify risk
  - Estimate mean time to exploitation

Security Content Automation Protocol (SCAP): Existing Components

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Extensible Configuration Checklist Description Format (XCCDF): automatically collecting data and performing scoring
- Open Vulnerability and Assessment Language (OVAL): definitions of host checks
- Common Vulnerability Scoring System (CVSS): documenting software flaw characteristics

CVSS Characteristics

- Base Exploitability: Access Vector, Authentication, Access Complexity
- Base Impact: Confidentiality, Integrity, Availability
- Temporal: Exploitability (Exploit Availability), Remediation Level, Report Confidence
- Environmental: Collateral Damage Potential, Target Distribution, Security Requirements (Impact Bias)

Possible Future SCAP Components

- Common Configuration Scoring System (CCSS): documenting security configuration characteristics
- Common Misuse Scoring System (CMSS): documenting software feature/trust relationship misuse characteristics
- CxSS example—use IM to transfer unwanted files (malware) to the user's host
  - CVSS: Coding flaw in IM client permits such transfers
  - CCSS: IM client is configured to permit such transfers
  - CMSS: Social engineering tricks user into permitting such transfers; user mistakenly accepts transfer request; IM client does not offer a configuration option for restricting transfers

Create standardized host profiles

- Host security component definitions
  - Vulnerabilities
  - Security controls
  - Security configuration settings
- Host interdependencies
- Host security baseline
- Expressed using XCCDF, with checks and data from OVAL, CVE, CCE, CVSS, CCSS, CMSS…

Determine weightings

- Vulnerability and attack data
  - Operational
  - Experimental
- Initially base on CVSS, CCSS, CMSS elements and other characteristics
  - CVSS, CCSS, and CMSS intended as a starting point
  - Study correlations between CxSS characteristics and actual exploitation

Develop host scores

- Apply security state data and weightings to host profile
- Determine how individual scores should be rolled up for each host, including how scores should be grouped, and which scoring scales would be most useful
  - Numeric scales (0-10, 0-100); mean time to exploitation; rankings; etc.
  - Need multiple scales to accomplish different purposes
- Determine if scores from multiple hosts can be combined into network or enterprise scores

Future work

- Finalize CCSS and CMSS
- Revise CVSS temporal and environmental variables
- Identify relevant attack & vulnerability characteristics
- Develop and validate scoring definitions
- Integrate the components and test the entire framework
- Long-term effort (at least 5 years)

Additional Information

- NVD: http://nvd.nist.gov/
- SCAP: http://scap.nist.gov/
- CVSS: http://www.first.org/cvss/
- CCSS: Scarfone, K. and Mell, P, Draft NIST Interagency Report 7502: *The Common Configuration Scoring System (CCSS)*, May 2008, http://csrc.nist.gov/publications/PubsNISTIRs.html
- General: Scarfone, K. and Grance, T., “A Framework for Measuring the Vulnerability of Hosts”, *Proceedings of the 1st International IEEE Conference on Information Technology*, Gdansk, Poland, May 2008

karen.scarfone@nist.gov