Metrics Suite for Enterprise-Level Attack Graphs

Center for Secure Information Systems
George Mason University
Steven Noel, PhD

September 16, 2013
Team Profile

Fairfax, VA
GMU Center for Secure Information Systems

Northport, NY
Secure Decisions

Bethesda, MD
ProInfo

Information Visualization

Technology Transfer

9/16/2013
Customer Need

• Understand impact of combined topology, policy, and vulnerabilities on security posture
  – Prioritize critical problems
  – Compare options for risk mitigation
  – Measure security trends over time
• Attack graphs via Cauldron show all multi-step vulnerability paths through enterprise networks
• Lacks quantitative scores that capture overall security state at a point in time
• Metrics that can be compared
  – Over time
  – Across organizations
• Simple, practical, efficient, well organized, and clear
Approach: Attack Graph Metrics

Network Topology

Firewall Rules

Host Vulnerabilities

Attack Graph Analysis

Metrics Engine

Metrics Dashboard
Approach: Metrics Hierarchy

- **Network Score**
  - **Overall**
  - **Metrics Family**
    - **Victimization**
      - Existence
      - Exploitability
      - Impact
    - **Size**
      - Vectors
      - Machines
    - **Containment**
      - Vectors
      - Machines
      - Vuln Types
    - **Topology**
      - Connectivity
      - Cycles
      - Depth

9/16/2013
Approach: Topology Family

**Connectivity**
Relative number of (weakly) connected components

1 component
Metric $= 10 \left( 1 - \frac{1-1}{11-1} \right) = 10$

4 components
Metric $= 10 \left( 1 - \frac{4-1}{11-1} \right) = 7$

5 components
Metric $= 10 \left( 1 - \frac{5-1}{11-1} \right) = 6$

**Cycles**
Relative number of (strongly) connected components

4 components
Metric $= 10 \left( 1 - \frac{4-1}{11-1} \right) = 7$

5 components
Metric $= 10 \left( 1 - \frac{5-1}{11-1} \right) = 6$

10 components
Metric $= 10 \left( 1 - \frac{10-1}{11-1} \right) = 1$

**Depth**
Minimum of all-pairs shortest path

Shortest path 3/8
Metric $= 10 \left( 1 - \frac{3}{8-1} \right) = 5.7$

Shortest path 4/8
Metric $= 10 \left( 1 - \frac{4}{8-1} \right) = 4.3$

Shortest paths 2/3 and 1/5
Metric $= \frac{10}{2.8} \left[ 3 \left( 1 - \frac{2}{3-1} \right) + 5 \left( 1 - \frac{1}{5-1} \right) \right] = 2.3$
In general, for \( n \) scores, the combined score \( S \) is

\[
S = 10 \cdot \frac{\sqrt{\sum_{i=1}^{n} (w_i s_i)^2}}{\sqrt{\sum_{i=1}^{n} (w_i s_i)^2 + (w_i w_i)^2}} \in (0,10)
\]

where \( w_i \) is the weight for the \( i \)-th score, \( s_i \) is the score, and \( w_i \) is limited to \( 0 < w_i < 1 \).

For individual score \( s_i \) with weight \( w_i \), the unit vector is

\[
\frac{(w_i s_i)}{\sqrt{(w_i s_i)^2 + (w_i w_i)^2}} \in (0,1)
\]
Approach: Metrics Dashboard

Line Graph
Historical Details

Bar Graph
Summary Trends
Benefits

- Numeric measures are simple to understand, organized into families of related metrics
- Quickly determine if the situation is improving over time
- Tedious error-prone work is automated
- All metrics linear complexity with respect to graph size
- Practical for large networks
- Comparable across different organizations and networks
- Huge volumes of disparate data reduced to concise business intelligence
Competition

• Metrics
  – There are many metrics but for the most part they are qualitative
  – Quantitative measures such as CVSS and SANS Top 10 vulnerabilities lack context of specific network environment
• There is no automated tool in the market place
Current Status

- Type III (one year)
- Q1: requirements, design, interfaces, mockups
- Q2: Prototype implementation, user feedback
- Q3-Q4: Production implementation
- 9 development sprints
- 70+ customer briefings
- Customer evaluations
- Final software packaging, documentation, reporting
Next Steps

- Cauldron commercialization through Mason Tech Transfer (GMIP) and ProInfo/CyVision partnership
- Cauldron deployed in a variety of customer settings
- Significant IP, protected by patents and copyrights
- Available under GSA scheduling
- Marketing through direct sales and a network of resellers, strategic partners, and OEM relationships
- Strategic partners for services and complementary technologies
- Cauldron+Metrics (C+M) as software, C+M as service
Contact Information

Prof. Sushil Jajodia
jajodia@gmu.edu

Dr. Steven Noel
snoel@gmu.edu

Center for Secure Information Systems
George Mason University
Fairfax, Virginia