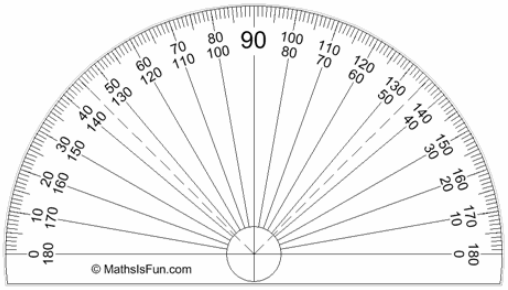
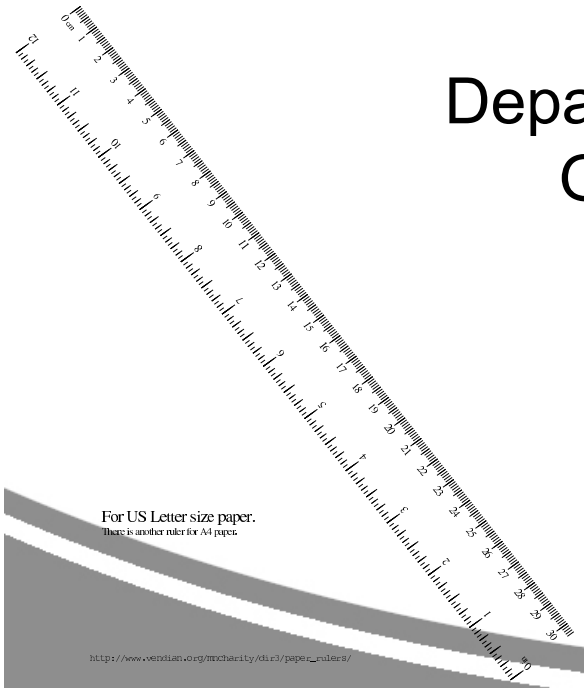


Ontologies for Modeling Enterprise Level Security Metrics

Duminda Wijesekera
Department of Computer Science
George Mason University



with assistance from
Paul Ngo, DHS
Anoop Singhal, NIST
Samuel Singapogu, GMU

Why Security Metrics?

- How can I plan on security investments so the system can achieve a certain level of security?
- What Risk postures am I willing to endure at what cost?
  - What are my perceived threats?
  - How secure are system with given configurations?
  - How much security does a new configuration provide?
  - Which countermeasures or controls provide the greatest risk reduction?
- We need a common nomenclature (ontology) to discuss Enterprise Level Security Metrics.

Challenges in Creating Security Metrics

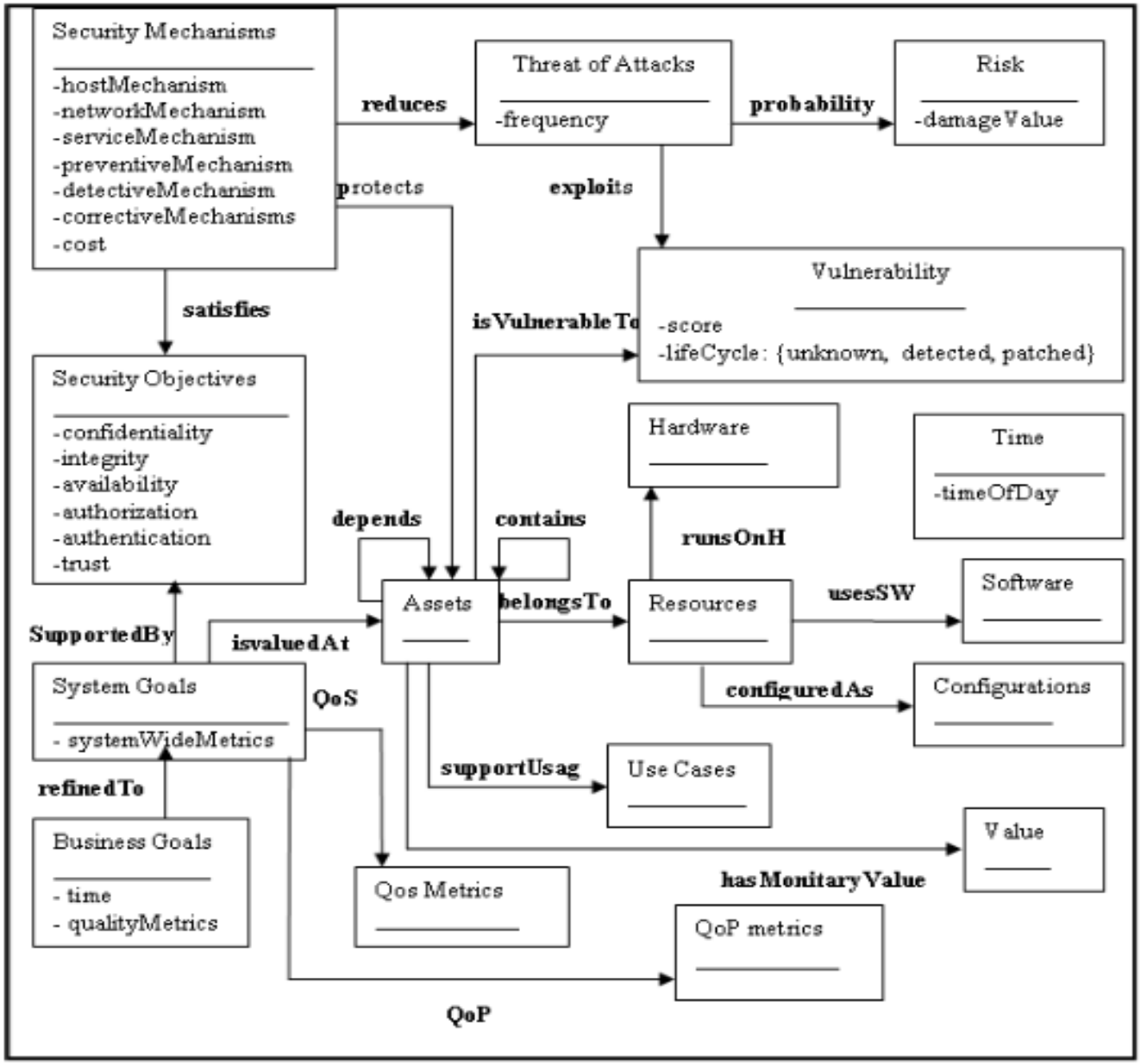
- Metric for individual vulnerabilities already exists
  - Impact, exploitability, temporal, environment, etc.
  - E.g., the Common Vulnerability Scoring System (CVSS) v2 released on June 20, 2007*
- How to we compose individual measures for the overall security of a system?

* Common Vulnerability Scoring System (CVSS-SIG) v2, http://www.first.org/cvss/

Common Terms used in Security Metrics

- Threats
- Vulnerabilities
- Countermeasures
- Assets
- Risks
- Security Objectives
  - Business Goals
  - Use Cases to be provided
  - Misuse Cases to be avoided
- Tredeoffs

An Ontology for Security Metrics (cont.)



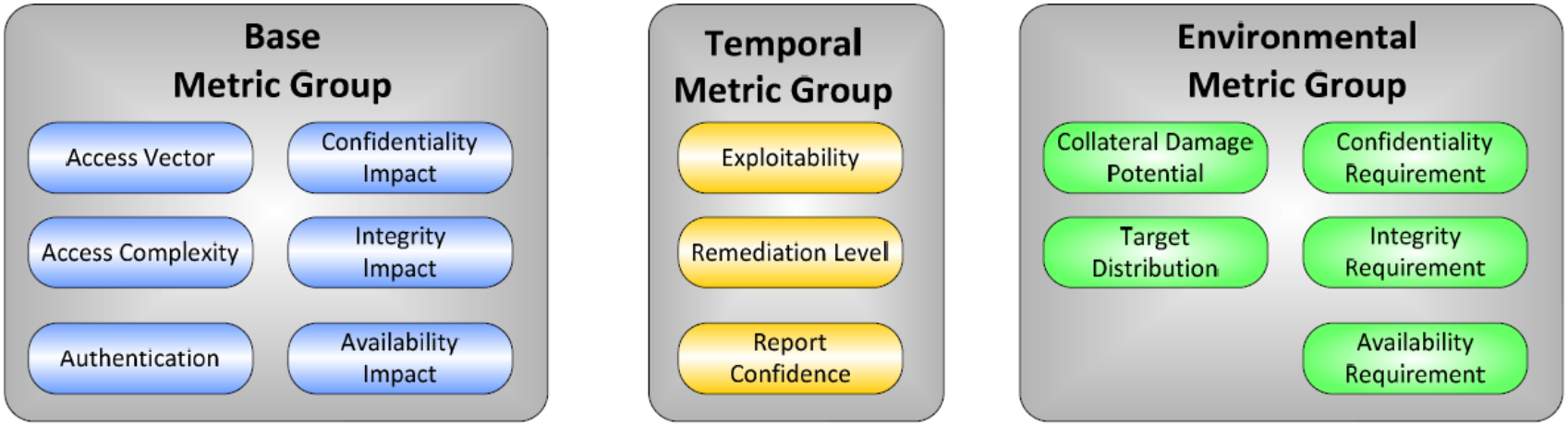
Properties of Asset Class

```
<rdf:Property rdf:ID="value">
   <rdfs:domain  rdf:resources="Asset"/>
   <rdfs:range      rdf:resources=&xsd:integer/>
</rdf:Property>
<rdf:Property rdf:ID="depends">
   <rdfs:domain  rdf:resources="Asset"/>
   <rdfs:range      rdf:resources="Asset"/>
</rdf:Property>
<rdf:Property rdf:ID="contains">
   <rdfs:domain  rdf:resources="Asset"/>
   <rdfs:range      rdf:resources="Asset"/>
<rdf:Property rdf:ID="isVulnerableTo">
   <rdfs:domain  rdf:resources="Asset"/>
   <rdfs:range      rdf:resources="Vulnerability"/>
<rdf:Property rdf:ID="belongsTo">
   <rdfs:domain  rdf:resources="Asset"/>
   <rdfs:range      rdf:resources="Resource"/>
<rdf:Property rdf:ID="monitaryValue">
   <rdfs:domain  rdf:resources="Assets"/>
   <rdfs:range      rdf:resources="Value"/>
<rdf:Property rdf:ID="supportUsage">
   <rdfs:domain  rdf:resources="Assets"/>
   <rdfs:range      rdf:resources="Use Cases"/>
</rdf:Property>
```

CVSS

- Stands for Common Vulnerability Scoring System
- An open framework for communicating characteristics and impacts of vulnerabilities
- Consist three metric groups: Base, Temporal, and Environment
  - Base metric: constant over time used environment
  - Temporal metric: change over time, constant w.r.t. environment
  - Environmental metric: unique to user environment

CVSS



- Each metric group has sub-matrices
- Each metric group has a score associated with it
- Score is normalized to the range of 0 to 10

Access Vector

This metric measures how the vulnerability is exploited

- Local
- Adjacent Network
- Network
- Remote

Access Complexity

This metric measures the complexity of the attack required to exploit the vulnerability

- High: Specialized access conditions exist
- Medium: The access conditions are somewhat specialized
- Low: Specialized access conditions do not exist

Authentication

Measures the number of times / ways in which an attacker must authenticate to a target to exploit a vulnerability

Number:

- Multiple: The attacker needs to authenticate two or more times
- Single: One instance of authentication is required
- None: No authentication is required

Ways:

- Login /password/
- must solve a puzzle/ biometric
- Need remote attestation

Confidentiality Impact

This metric measures the impact on confidentiality due to the exploitation.

- None: No Impact
- Partial: There is a consideration information disclosure
- Complete: There is a total information disclosure

- Similar things for the Integrity and Availability Impacts.

Base Score

Base Score = roundTo1Decimal(((0.6*Impact +(0.4*Exploitability)-1.5)*f(Impact))

Impact = 10.41*(1-(1-ConImp)*(1-IntImp)*(1-AvailImpact))

Exploitability =

20*AccessV*AccessComp*Authentication

F(Impact) = 0 if Impact=0, 1.176 otherwise

Base Score Example CVE-2002-0392

Apache Chunked Encoding Memory Corruption

BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complex.	[Low]	(0.71)
Authentication	[None]	(0.704)
Availability Impact	[Complete]	(0.66)

Impact = 6.9

Exploitability = 10.00

Base Score = (7.8)