Carnegie Mellon

Common Vulnerability Scoring System

Sasha Romanosky

February 07, 2006

Carnegie Mellon
Information Security Policy & Management
Heinz School

What is CVSS?

- Is a way of scoring vulnerabilities and prioritizing them based on the impact to any organization
- In other words…

What is CVSS?

- Is a way of scoring vulnerabilities and prioritizing them based on the impact to any organization
- In other words…
- Identifies the **actual RISK** posed by a vulnerability to an organization

Why do we need CVSS?

- Consider all these different players…
  - Researchers who discover vulns
  - Software vendors who respond to notifications
  - CSIRTs who gather and distribute vuln advisories
  - Security vendors that perform scanning, present results
  - Users have to react to vulns
- Each with their own motivations, priorities, information…
- Combine with multiple, incompatible scoring systems (microsoft, CERT, sans, vendors, etc)

- All this leads to uncertainty and confusion on how to address vulnerabilities

- **We need a common way to communicate!**

Brief History

Initially

•Conceived by the National Infrastructure Advisory Council (NIAC), a group of industry leaders who provide the DHS with recommendations for IT security of critical infrastructures

• Core Team: Cisco, Qualys, Symantec (security focus), eBay
• CVSS 1.0 was accepted by the DHS Oct 2004

Now

• Under the custodial care of FIRST (Forum of Incident Response and Security Teams)

• Involves: CERT/CC, NIST NVD, Mitre, ISS, ArcSight, Tenable, IBM, JPCERT, AusCERT, netForensics, Skybox, Unisys, etc

What CVSS is not

- A threat rating system (DHS colors, Sans Internet Storm Center)
- Vulnerability database (bugtraq, OSVDB)
- Vulnerability classification / taxonomy (CVE, Plover)

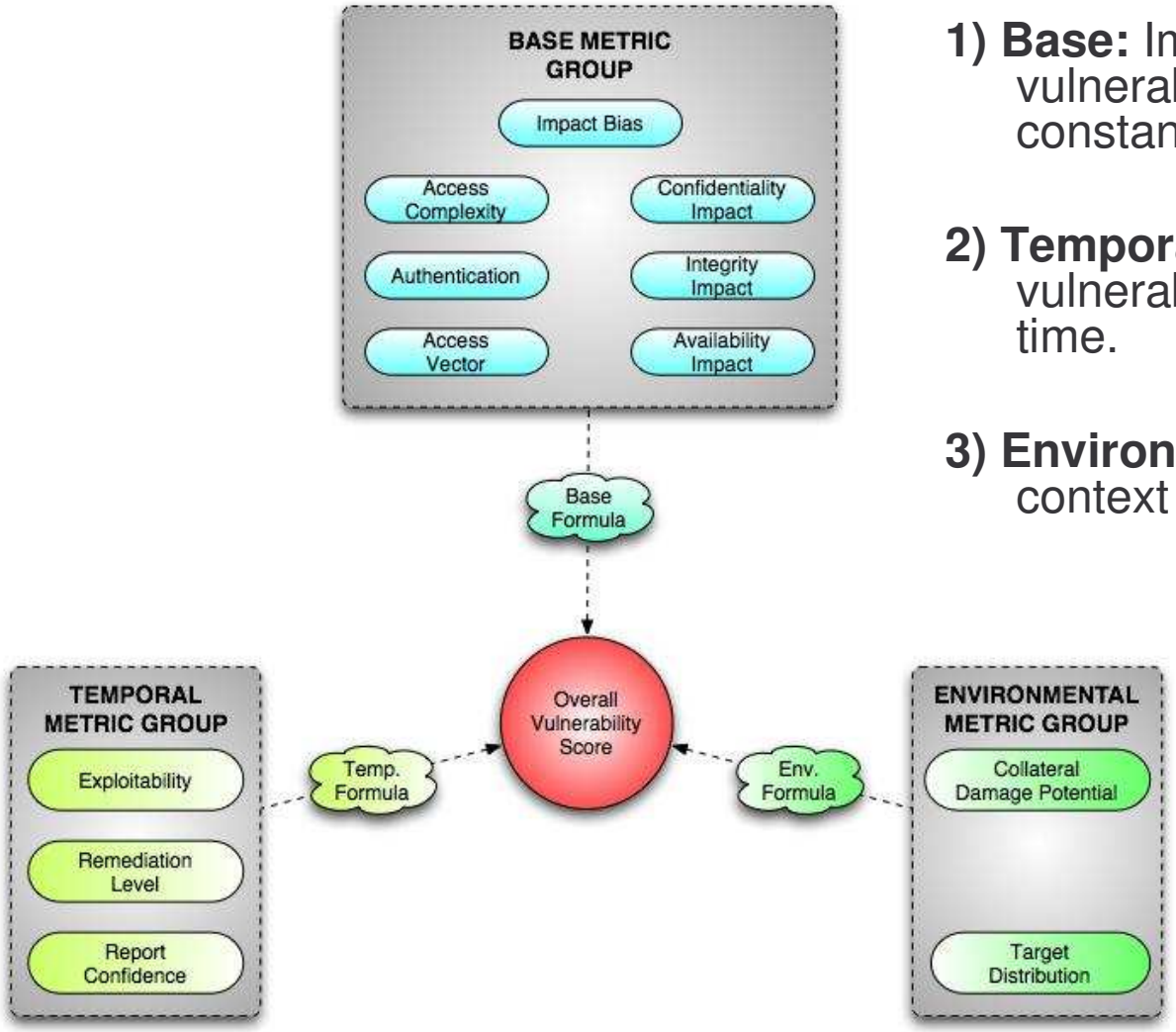
How does CVSS work?

It uses a bunch of metrics, that combine with formulas, to create a score

Final score = [0 – 10]

That's all!

CVSS Metric Groups

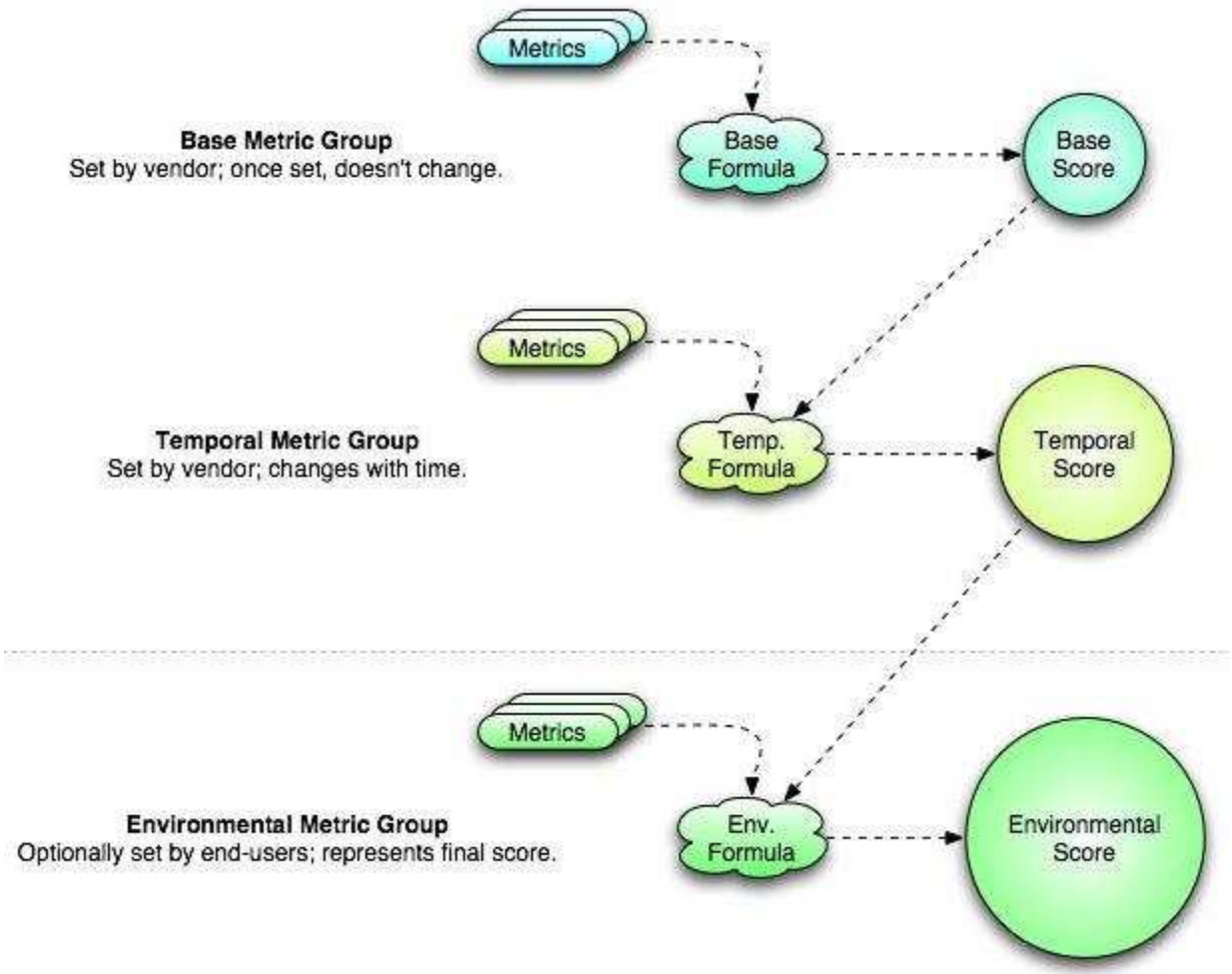


1) Base: Immutable characteristics of the vulnerability. These properties are constant over time and across systems

2) Temporal: Properties of the vulnerability that may change over time.

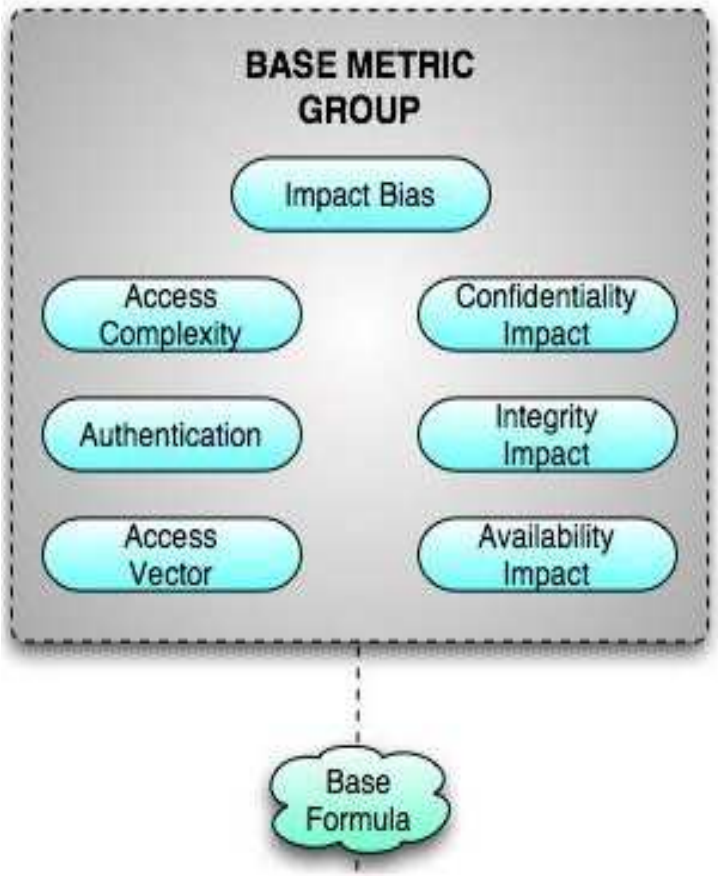
3) Environmental: Provide environmental context for the vulnerability.

CVSS Scoring



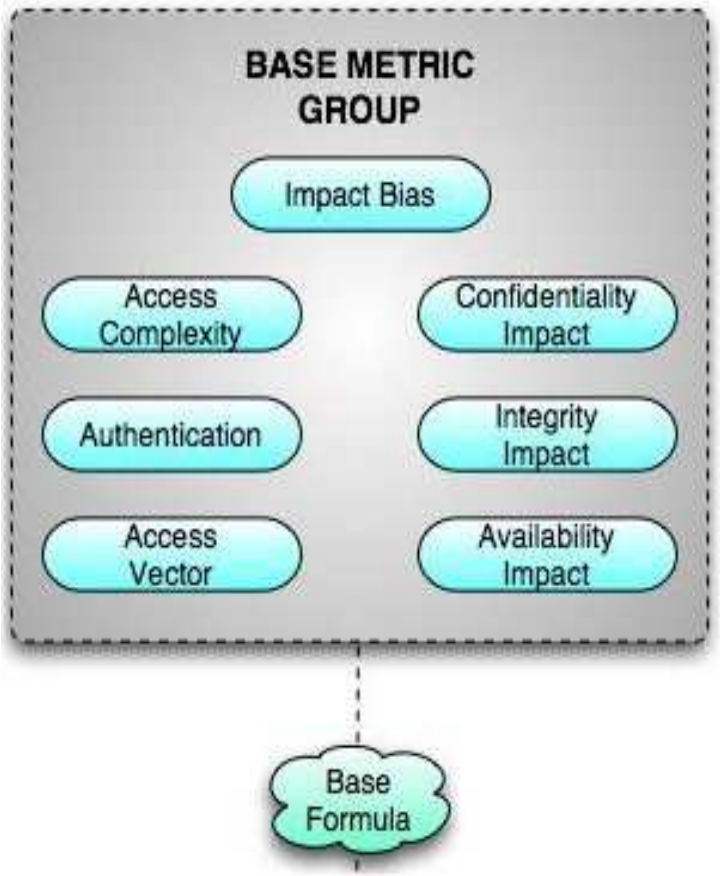
- The base score is computed first
- Temporal metrics modify the base score
- Environmental components further modifies the score

Base Metrics



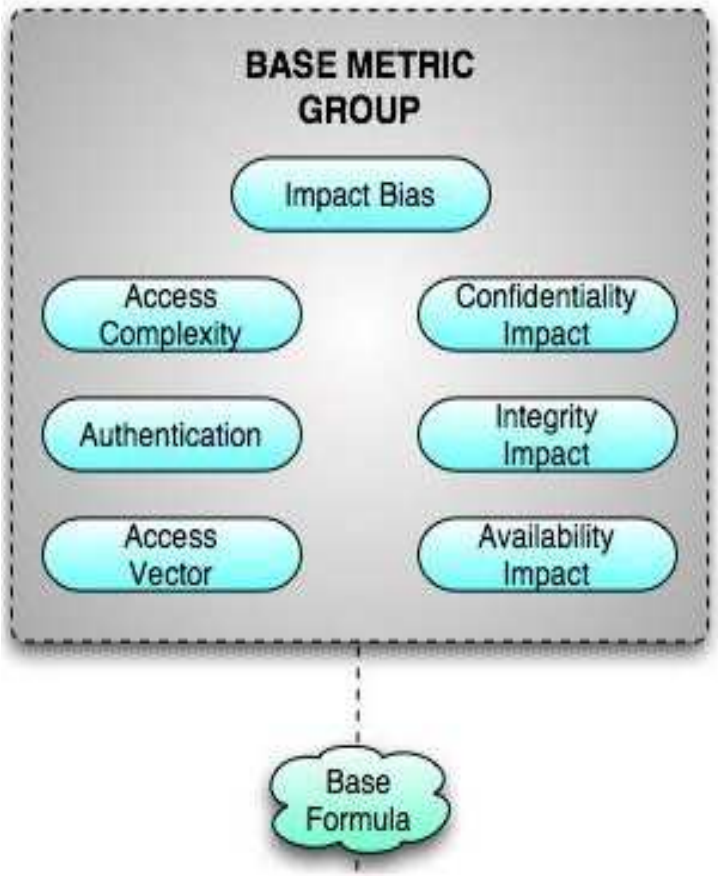
- **Access Vector**: measures whether the vuln is exploitable locally or remotely. [Local, Remote]
- **Authentication**: measures whether an attacker needs to be authenticated to a system in order to exploit the vuln. [Required, Not-Required]

Base Metrics (2)



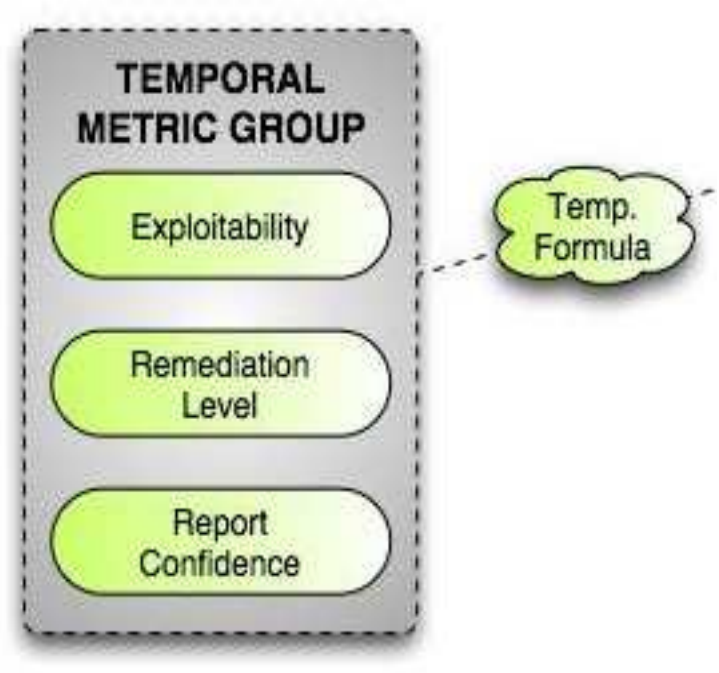
- **Access Complexity**: measures whether special circumstances are required in order to exploit the vuln (e.g. social engineering) [High, Low]
- **Confidentiality Impact**: measures the degree of loss of information [None, Partial, Complete]
- **Integrity Impact**: measures degree of unauthorized modification to data [None, Partial, Complete]

Base Metrics (3)



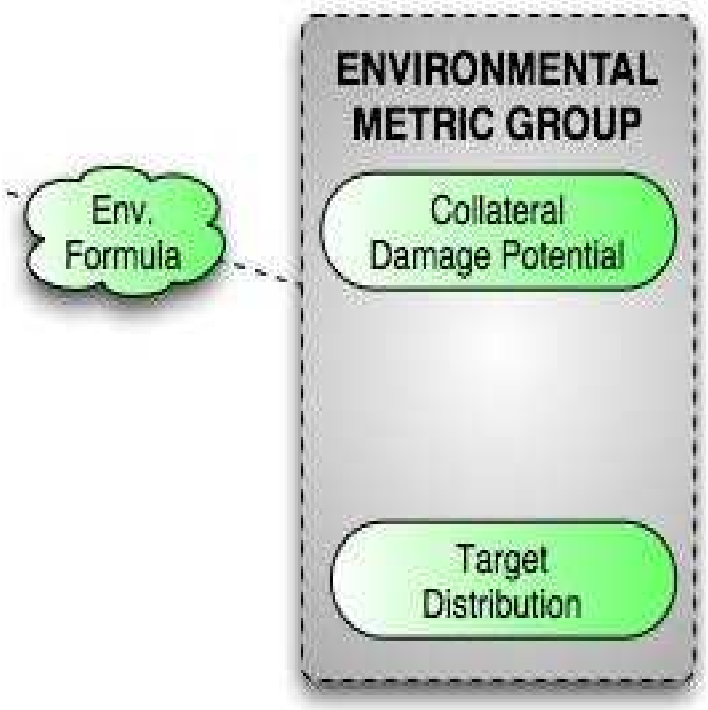
- **Availability Impact**: measures degree of loss of (yes) availability to the system [None, Partial, Complete]
- **Impact Bias:** allows the score to convey greater weighting to one of C,I,A metrics [Normal, Confidentiality, Integrity, Availability]

Temporal Metrics



- **Exploitability**: measures the current state (or ease) of exploitability of the vulnerability [Unproven, Proof of Concept, Functional, High]
- **Remediation Level**: represents the level of mitigating controls that currently exist for the vulnerability [Official Fix, Temporary Fix, Workaround, Unavailable]
- **Report Confidence**: measures the credibility of the details of the vulnerability [Unconfirmed, Uncorroborated, Confirmed]

Environmental Metrics



- **Collateral Damage Potential**: measures the degree of loss to information, systems or people [None, Low, Medium, High]
- **Target Distribution:** measures the percentage of systems that could be affected by the vulnerability [None, Low, Medium, High]

Let's Score!

- Cisco Ipsec malformed IKE packet vulnerability
- Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows (zotob)
- Buffer overflow in NOD32 allows local users to execute arbitrary code

We have a score, now what?

- What does a CVSS score of 7.0 mean to me?
- What action am I supposed to take..?

We have a score, now what?

- That's what Vulnerability Management and Security Policies are for. A policy might say something like this:

CVSS Score	Remediation
0-3	No impact – wait for service pack
4-6	Address in next patch cycle
7-8	Fix within 7 days
9-10	Holy Crap, fix it now!

- It's clear and simple to follow.
- The big advantage is that if all your vulnerabilities come with a CVSS score, then you know how to react in every situation!.

Next Steps

- Expand Environmental Metric Group
  - Provide greater ability to match various environments
  - Module/plug-in architecture
  - Include additional metrics like asset value
- Increased community adoption (help us with scoring!)
- Ability to score large (massive!) groups of vulnerabilities at once
- Seamless integration between CVSS, product security vendors and customer vulnerability management processes

More information

- Tenable: http://www.nessus.org/plugins/index.php?view=newest
- NIST: http://nvd.nist.gov/cvss.cfm (avg 5.38, stdev 2.32, n=13k)
- FIRST: http://www.first.org/cvss
  - Monthly calls,
  - Mailing list: cvss-info@first.org

http://explodingdog.com/rocketguy.gif