Pitfalls of Vulnerability Rating

or: The ERNW Rapid Rating System

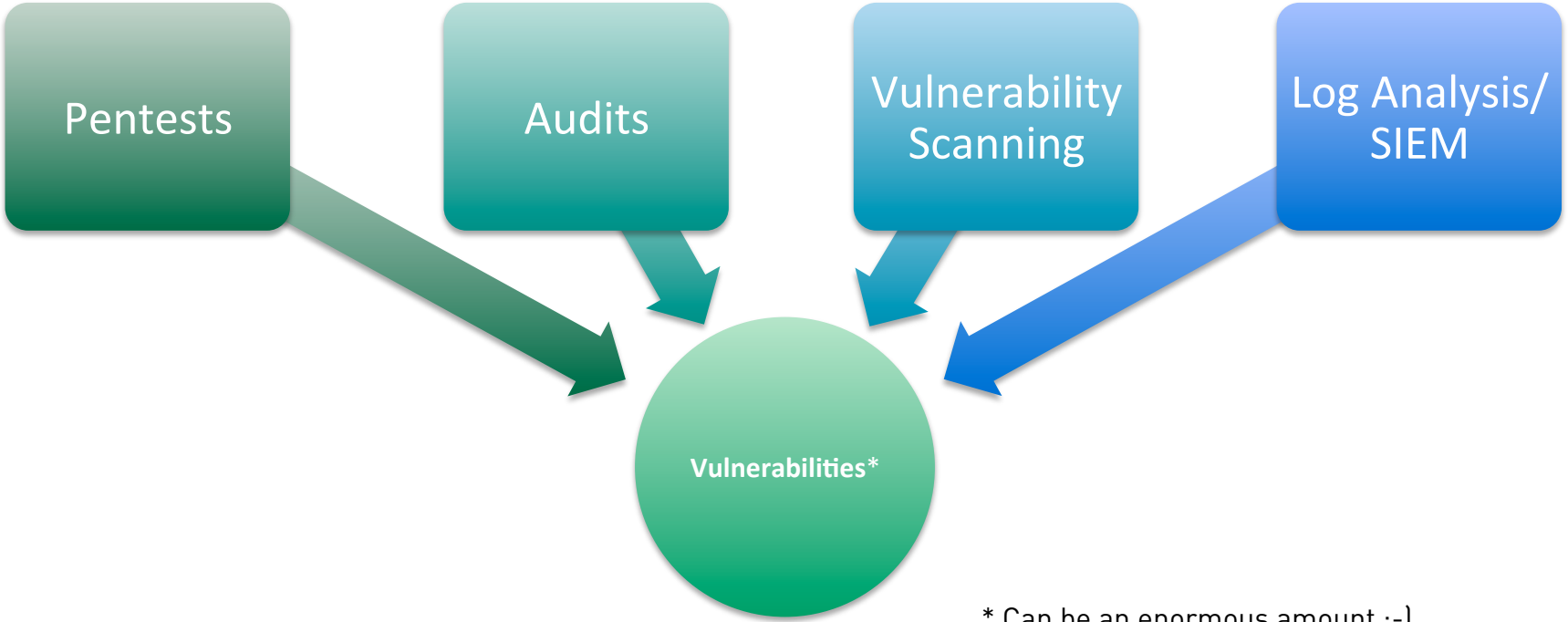
Michael Thumann [mthumann@ernw.de]
Matthias Luft [mluft@ernw.de]

Agenda

- Problem Statement
- Existing Approaches
- New Directions

Problem Statement

Goal: You want to make the world (or your company ;-) a safer place.



* Can be an enormous amount ;-)

Problem Statement:

Vulnerabilities*

* Enormous amount

Problem Statement

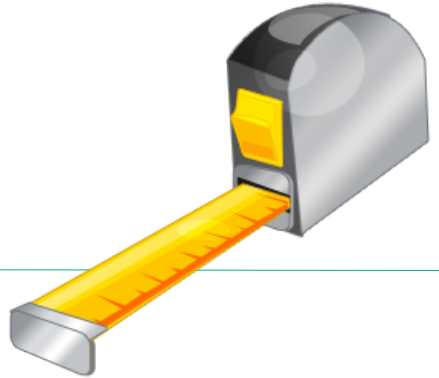
- Typical associated problems:
  - Lack of resources to manage all items immediately.
  - Lack of information about vulnerabilities
  - Cooperation/interaction between different departments necessary.

Still...

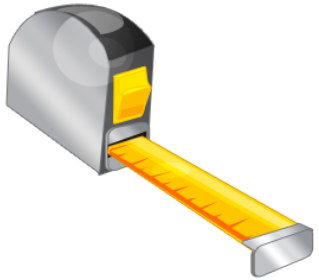
- You have to make a decision.
- No matter how much you wish there would be more (reliable) information, more resources, or clear responsibilities, again, you have to make a decision.

- We want to discuss two (most interesting, in our opinion ;)) aspects of these decisions:
  - *Prioritization*
  - *Answering all relevant (customer) questions.*

Existing Approaches



Rating Approaches



- CVSS
- CWSS
- Risk-based
- Custom Excel-Sheets ;)
  - Sometimes even databases

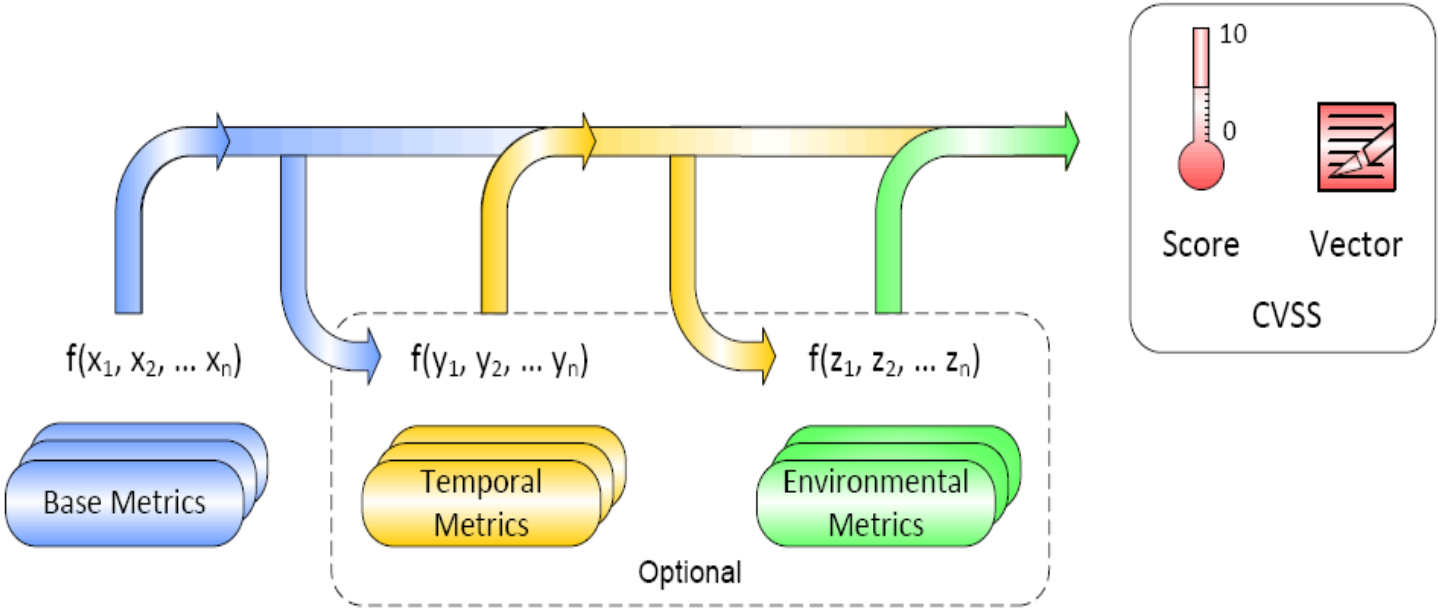
ERNW
providing security.

CVSS

http://www.first.org/cvss

- *C*ommon *V*ulnerability *S*coring *S*ystem
- Widespread use
- Main idea: Patch relevance
  - => Strong focus on vulnerabilities in software products
- E.g.
  - Impact
  - Target Distribution
  - “Chains & Composites”

Basic Categories



Parameters


Base
Metric Group
Access Vector
Confidentiality Impact
Access Complexity
Integrity Impact
Authentication
Availability Impact
Temporal
Metric Group
Exploitability
Remediation Level
Report Confidence
Environmental
Metric Group
Collateral Damage Potential
Confidentiality Requirement
Target Distribution
Integrity Requirement
Availability Requirement

Demo!

CWSS

http://cwe.mitre.org/cwss/

- *C*ommon *W*eakness *S*coring *S*ystem
  - Currently version 0.8 (work in progress)
  - No news since 2 years
- Allows automated scoring processes
- Includes characteristics of the weakness
- Integration of stakeholder concerns
- Environmental requirements

Base Finding Group

- Technical Impact
- Acquired Privilege
- Acquired Privilege Layer
- Internal Control Effectiveness
- Finding Confidence

Attack Surface Group

- Required Privilege
- Required Privilege Layer
- Access Vector
- Authentication Strength
- Authentication Instances
- Level of Interaction
- Deployment Scope

Environmental Group

- Business Impact
- Likelihood of Discovery
- Likelihood of Exploit
- External Control Effectiveness
- Remediation Cost
- Prevalence

3 Metric Groups

Rating

- Assignment of values to each factor
- Resulting in a value ranging from 0 to 100
- 100 is most critical
- Each factor has four categories

ERNW
providing security.

Rating Categories

- Unknown
  - Not enough information/not assessed
  - 0.5 for all factors, lowers overall score
- Not Applicable
  - Marked as “to be ignored at the moment”.
  - 1.0 for all factors,
- Quantified
  - Regular scoring, 0.0 – 1.0
  - Scale defined for each factor
- Default
  - Labeled for later modification
  - Each factor has a default value, which typically complies to the quantified value which is assumed to be *default*.

Finding Confidence

Value	Code	Weight	Description
Proven True	T	1.0	The weakness is reachable by the attacker.
Proven Locally True	LT	0.8	The weakness occurs within an individual function or component whose design relies on safe invocation of that function, but attacker reachability to that function is unknown or not present. For example, a utility function might construct a database query without encoding its inputs, but if it is only called with constant strings, the finding is locally true.
Proven False	F	0.0	The finding is erroneous (i.e. the finding is a false positive and there is no weakness), and/or there is no possible attacker role.
Default	D	0.8	Median of the weights for Proven True, Proven Locally True, and Proven False.
Unknown	Unk	0.5	
Not Applicable	NA	1.0	This factor might not be applicable in an environment with high assurance requirements; the user might want to investigate every weakness finding of interest, regardless of confidence.
Quantified	Q		This factor could be quantified with custom weights. Some code analysis tools have precise measurements of the accuracy of specific detection patterns.

Risk-based

ISO/IEC 13335-1:2004

- Threat:

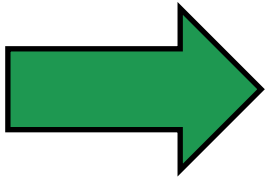
  a potential cause of an incident that may result in harm to a system or organization

- Vulnerability:

  a weakness of an asset or group of assets that can be exploited by one or more threats

Risk

- Risk: threat “viewed by some dimensions”
  - How likely is it going to happen? [*Likelihood*]
  - Are we susceptible if it happens? [*Vulnerability (Factor)*]
  - What harm is caused in case it hits us? [*Impact*]



- Talking about *threats* does not make too much sense
  - At least not when it’s about conclusions & actions…

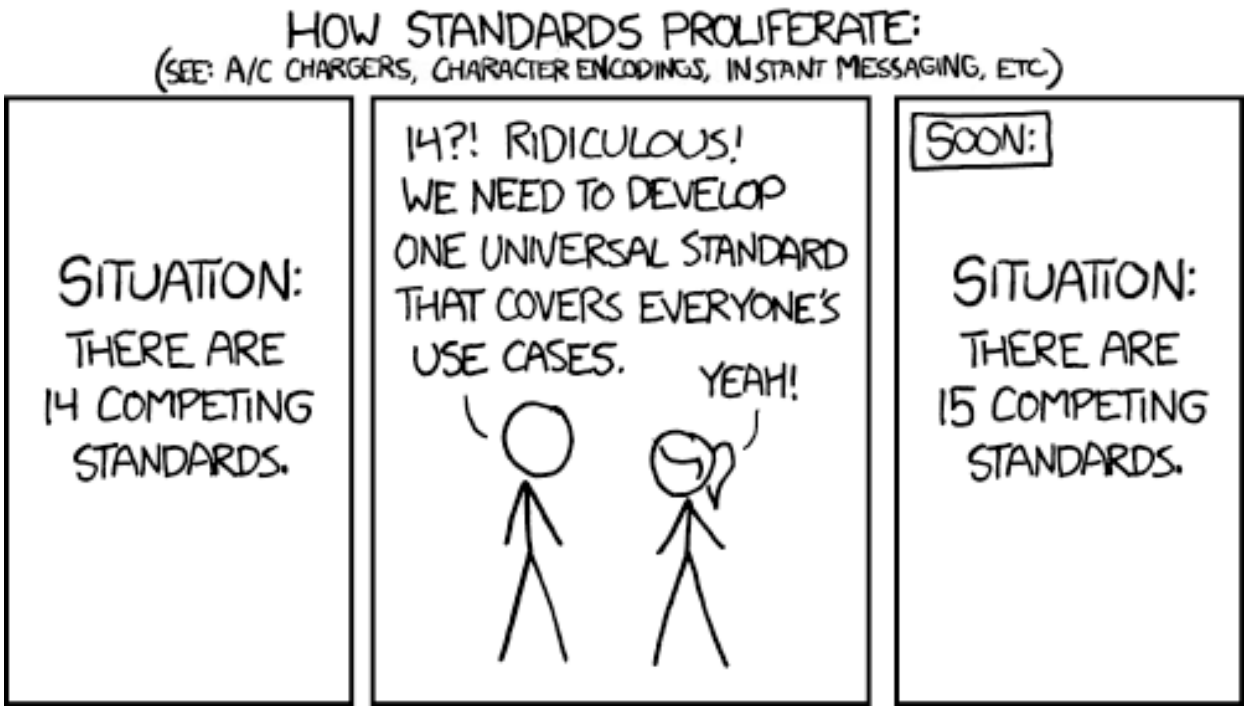
Custom Approaches

- Different approaches developed for individual environments.
  - Usually resulting from the need for “some qualification”.
- Or developed for dedicated ecosystems:
  - Qualys 1-5 Score
  - NIPC low, medium, high

General Problems

- Entropy
  - The lack of information on e.g.
    - context
    - impact
- What to rate?
  - Findings, vulnerabilities, threats, risks…?
  - The differences affect the metric usage in a significant way!
- Who is filling it in?
  - Internal GRC vs. Pentesters vs. Auditors vs. Admins vs. …
- Who wants to get value out of it?
  - Internal GRC vs. Pentesters vs. Auditors vs. Admins vs. …

New Directions


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Yet another...

Design Goals

- Main idea: Provide a severity rating
  - Which can be used for prioritization
- Addressing the mentioned problems
- Lightweight
- Clear questions/parameters
  - Suitable for different areas of application (pentest vs. audit)
  - Easy (& efficient) to answer!

Categories

Characteristics

Exploitability

Impact

Mitigation

Environment

Characteristics

- Access Vector
- Required Privilege
- Compromise Level
- Qualified PoC?

Exploitability

- Required Skill Level
- Time to Exploit
- Financial Effort
- Enabling Vulnerability present [if required]?
- Insider KnowHow required?

Impact

- Is the *Confidentiality* of the asset affected?
- Is the *Integrity* of the asset affected?
- Is the *Availability* of the asset affected?

Mitigation

- Mitigation Effort
- Mitigation depends on 3rd party?
  - E.g. vulnerability in COTS, outsourced development.

Environment

- Trust Level of Accessing Entities
- Data Classification
- Is the Target a Critical/Core Business Service?
- Can an one hour outage be tolerated?
- Are there external law/compliance requirements?

Factor Weight

- 1-5
  - 5 = very important
  - 1 = not important
- Some examples:
  - Compromise Level: 5
  - Access Vector: 2
  - Required Skill Level: 3
  - C,I,A: 3
  - Mitigation Effort: 1
  - Data Classification: 3

Formula

$$\frac{\sum_{i=1}^{n}(weight(i) * result(i)) * 100}{\sum_{i=1}^{n}(weight(i) * maxresult(i))}$$

Demo!

One Metric to Rule Them All!

One Metric to Rule Them All?

Lessons Learned

- There are different categories of findings.
  - And we don't mean that in the obvious way as "critical and less critical ones".
  - Pentest vs. Audit or "directly exploitable" vs. "not directly exploitable"
- (Good) Metrics are hard ;-)
- Having the questions that both sides want to answer/get answered in mind (always) helps.

Conclusions

- (Good) Metrics are hard ;-)
- We provided a 0.9 metric that
  - is likely to have broader applicability than CVSS.
  - is likely to be more intuitive than CWSS.
  - can provide inspiration or serve as an alternative for internal/custom metrics.
  - likely still has some rough edges.
  - hence is worth to get some field experience.
- Tools & Publications will follow soon!

Questions & Discussion

mthumann@ernw.de
mluft@ernw.de