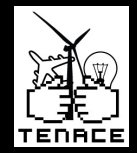
UNIVERSITY OF TRENTO

SECONOMICS



Research ideas

Attacker economics for Internet-Scale risk Assessment

Luca Allodi
University of Trento, Italy
http://disi.unitn.it/~allodi

Research objectives

- I aim at enabling decision makers in making statements like:
  - "If we fix vulnerabilities in this group, the risk of cyber attacks against our costumers will decrease by 55%"
  - Risk is not measured by $\frac{\sum_{v \in machines} CVSS(vuln)}{\sum machine} - \int firewalls \pm ..$
- Focus on un-targeted attacks against the general population
  - Google: 80% of risk comes from these attacks

Research Plan

- Three tracks:
  1. Characteristics of (non)interesting vulnerabilities (CVSS-based)
  2. Context characteristics for interesting vulnerabilities
  3. Trends in attacks enabled by attack tools

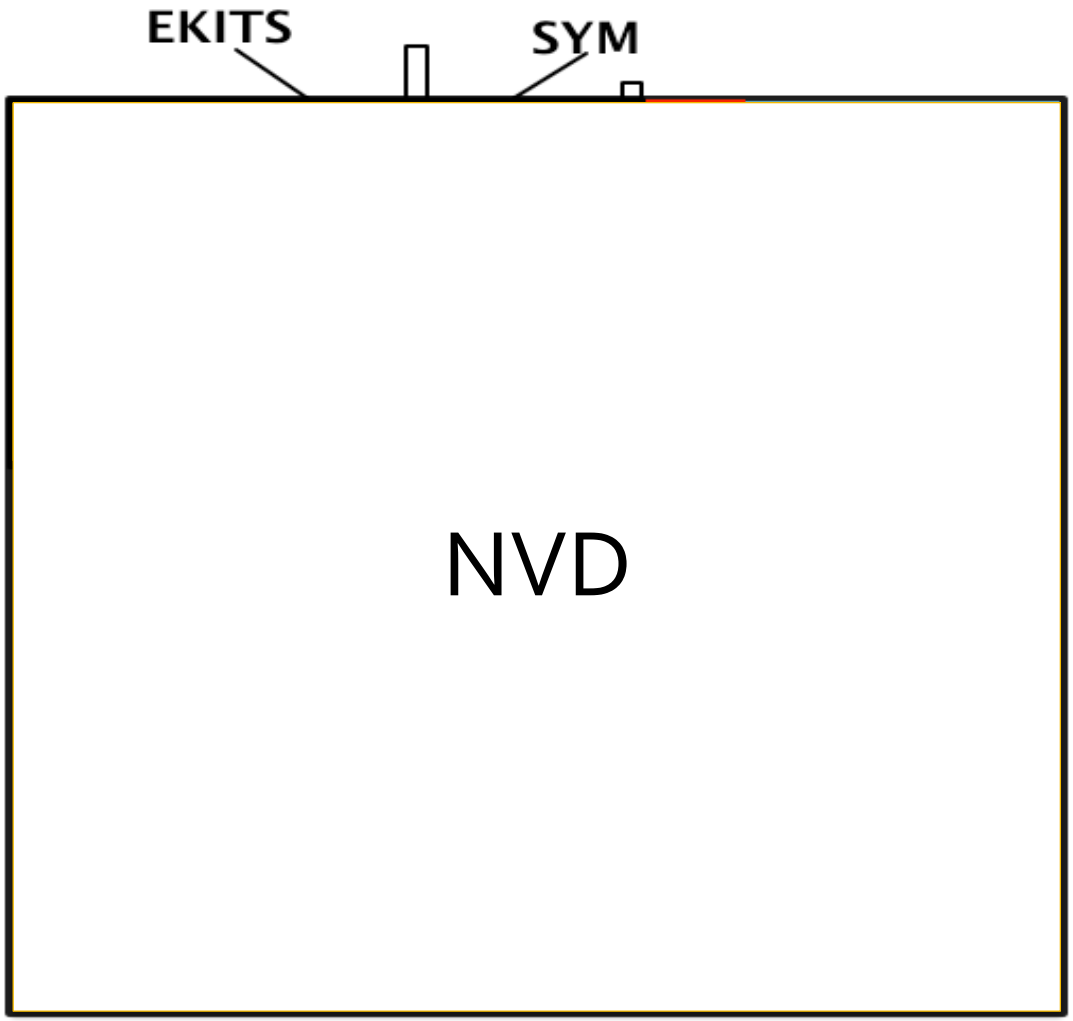
Track1: Characteristics of (non)interesting vulns

- CVSS is a composition of *expert judgments* on vulnerability characteristics
- Some combinations may be good indicators for "likelihood of exploitation"
  - E.g. High complexity, low-medium Impact vulnerabilties → **not interesting for exploitation**
- Differentely, the *final CVSS score may not correlate with (non)exploitation*
- → Empirical research: need the data

Empirical research

- Datasets
  - NATIONAL VULNERABILITY DATABASE: NVD
    - The universe of vulnerabilities
  - WHITE MARKETS OF EXPLOITS: EXPLOIT-DB
    - Proof-of-Concept exploits published by security researchers
  - ACTUAL EXPLOITS IN THE WILD: SYM
    - Symantec / Kaspersky Threat reports
    - Vulnerabilities actually exploited in the wild
  - RECORD OF ATTACK IN THE WILD WORLDWIDE: WINE
  - BLACK MARKETS FOR EXPLOITS: EKITS
    - Exploit advert from the bad guys in an exploit kit
    - 90+ exploit kits from the black markets
- Usage: economic modeling of exploitation, correlation market cost/popularity in the wild, controlled experiments, testing of blackhat tools, ..

What vulnerabilities do attackers exploit?



LOW CVSS<6

6≤MEDIUM CVSS<9

HIGH CVSS ≥ 9

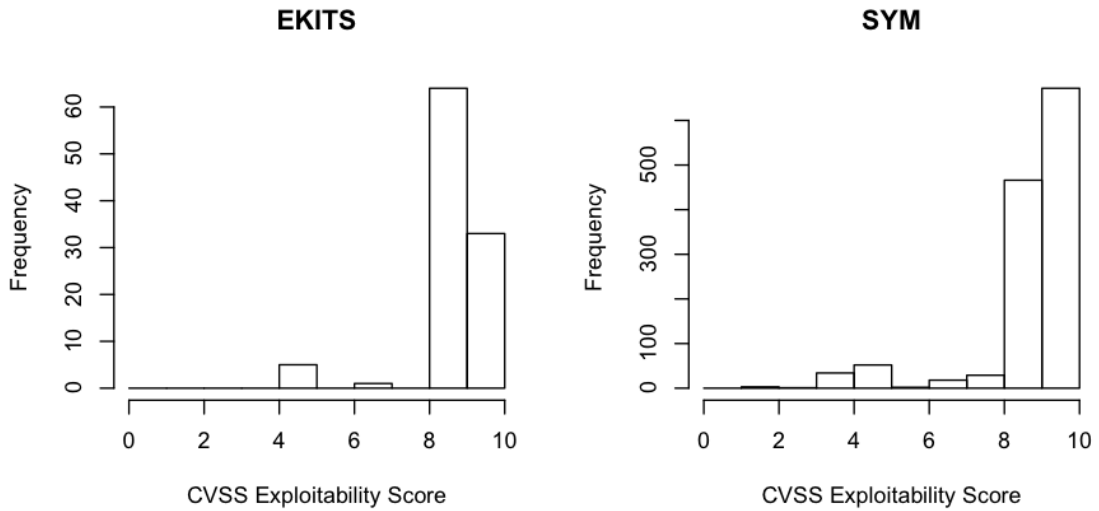
Areas are proportional to no. of vulns

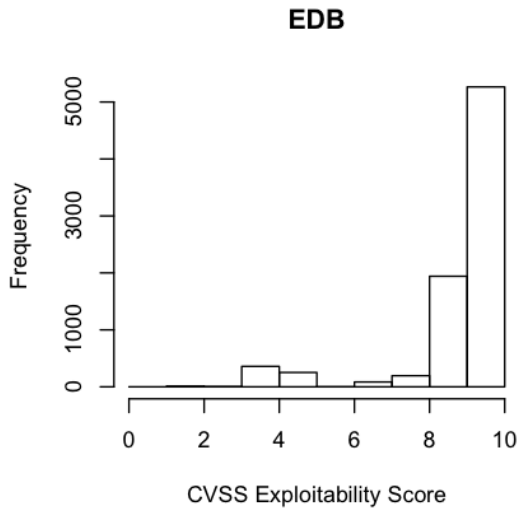
Is CVSS a good marker for exploitation?

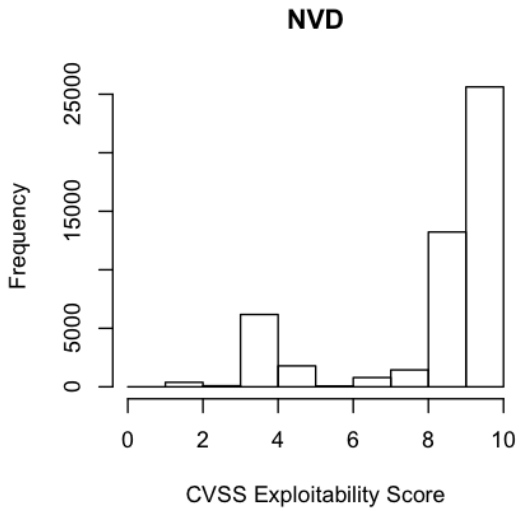
- Sensitivity → true positives vs all attacked vulns
  - HIGH→ the test correctly identifies exploited vulns
  - LOW → lots of exploits undetected
- Specificity → true negatives vs all non-attacked vulns
  - HIGH → the test correctly identifies non exploited vulns
  - LOW → lots of non-exploited vulns flagged

Test for Patching	Sensitivity	Specificity
CVSS High+Med	91%	23%
CVSS + PoC in EDB	97%	22%
CVSS + EKITS	94%	50%
3BT: Down Syndrome	69%	95%

Why CVSS does not work?







- Risk (CVSS)= Impact x Likelihood
  - CVSS Likelihood = Exploitability
- Everything is exploitable → CVSS lacks of a real characterization of likelihood of exploitation

Track2: Context variables for exploitation

- Look at the exploitation from an Expected Utility perspective
  - Among a set of vulnerabilities $v_1 \ldots v_j$
  - High risk = max(EU(v_1), EU(v_2)…, EU(v_j))
- Example hypotheses

1. If other exploits exists for that software, other vulns represent lower risk
2. Among a set of vulnerabilities, the attacker is most likely to attack that with highest pay-off
3. Persistence of the vulnerability in time

- ..Will keep you posted

Track3: Trends in attacks enabled by attacker tools

- Black markets trade tools to perform automated attacks
- Collaboration with symantec WINE Project
- Correlation with data in EKITS from the black markets
- →assessment of black market trends for final user security

Questions?

Thanks to
Vadim Kotov, Fabio Massacci, Viet H. Nguyen,
Julian Williams, Woohyun Shim

luca.allodi@unitn.it
http://disi.unitn.it/~allodi
http://securitylab.disi.unitn.it

Track3: Trends in attacks enabled by attacker tools