UNIVERSITY OF TRENTO

SECONOMICS

TENACE

My software has a vulnerability, I need a medic.

Or: How vulnerability research can leverage from medical sciences

http://securitylab.disi.unitn.it

@secscientist

Luca Allodi, Fabio Massacci
University of Trento, Italy.

GEORGE MASON UNIVERSITY

accenture

black hat USA 2013
JULY 27 - AUGUST 1, 2013
CAESARS PALACE | LAS VEGAS, NV
WWW.BLACKHAT.COM

22nd USENIX Security Symposium
AUGUST 14-16, 2013
WASHINGTON, D.C.
www.usenix.org/sec13

Introduction

- My research focus is on vulnerability exploitation: "what makes sense for the attacker to exploit in the majority of cases?"
  - → "what makes sense for you to patch so you are safe against the majority of attacks?"
- In this presentation:
  - Vulnerability assessment and management: what we can learn and do by leveraging from medical sciences

BTIA: Call for discussion

You should select just one paper so that it relates to one of the main topics of the school (i.e., the topics that will be discussed in the lectures) and its topic is within your current research interests.

- "The Economics of Information Security Investment" *Lawrence A. Gordon, Martin P. Loeb. University of Maryland. TISSEC 2002.*

- What's their contribution?
  - Model to quantify optimal amount of investment in security (i.e. patching, hardening, etc)
  - **They provide a clear proposition:** Invest **at most** 37% of what you expect to lose
  - → the model applies to **limited** monetary losses
    - → not for critical assets / governmental assets where the "*loss could be catastrophic*"

Their approach

- The model adds up to the pre-existing layer of vulnerability management
  - → you have a set of vulnerabilities that you know and can assess → "*fix as much as you can (CIO view) but spending more than 37% of your loss makes no sense (CEO view)*"
  - Foundational "Security metrics" problem remains open:
    - Which vulns does the CIO have to worry about?
    - How better is the CEO off with a certain security investment?

- Limitations of their study (excerpts from the paper):
  1. **[…]** Second, there is no simple procedure to determine the **probabilities of the threat** and the vulnerability associated with an information set.
  2. **[…]** A fourth limitation .. is that we have not modeled how **conflicts of interest between [CEO] and the [CIO]** would affect the derivation of the optimal amount to invest in information security.

- So (1) the CIO chooses what vulns to fix.. → **needs a way to measure criticality of solution**
- ..but (2) still needs the CEO to sign the check → **needs a way to evaluate the solution investment**

A different research goal

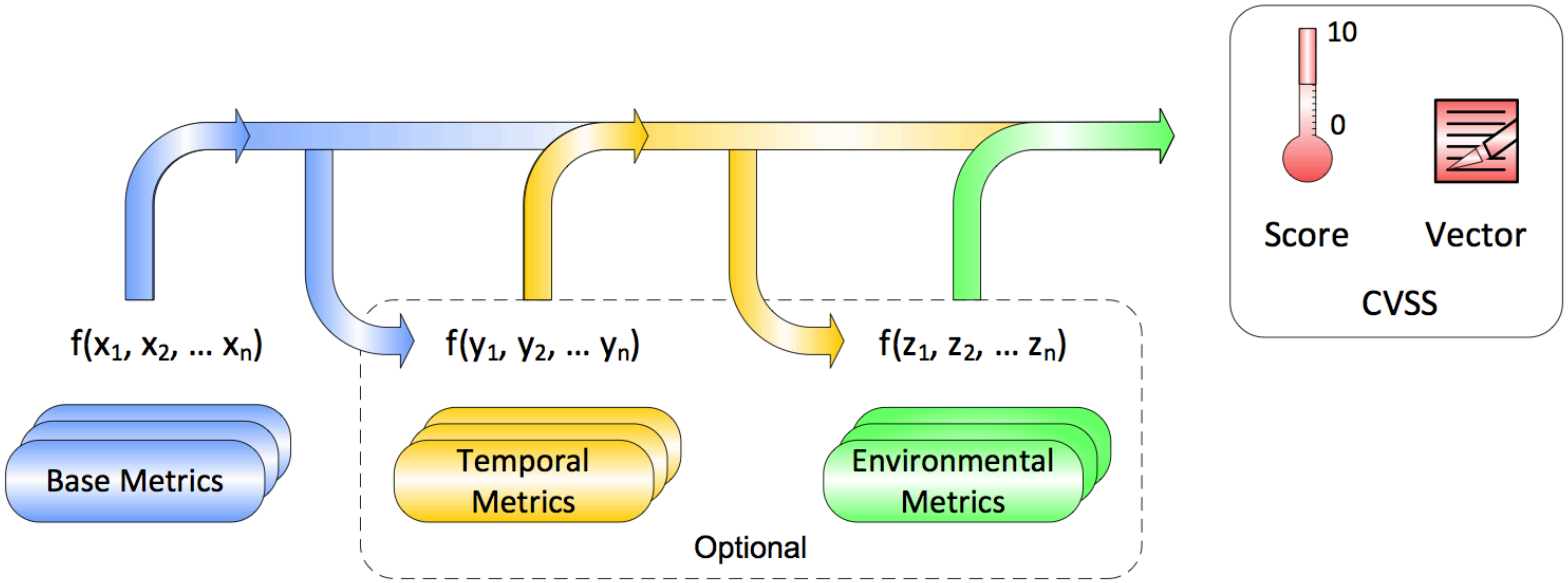
- *"If we fix this group of vulnerabilities, risk of attacks decreases by 85%"*
- No theorem here: not "classical" computer science
- **We need a different approach**
  - Think of car accidents:
    - You **can't prove** that if you wear a safety belt you will not die
    - But still, they **improve your chances of surviving** [Evans 1986]
  - Same with vulnerabilities:
    - Fixing a vulnerability will **not** assure you you will not be hacked (not even **fixing ALL vulnerabilities you know of does**)
    - But this **improves** your chances of **not being** hacked
- Make sense only for non-catastrophic "accidents" (as in Gordon et al. model) → in that case statistics do not make sense → no black swan attacks, targeted attacks, governmental attacks
- But how to get there? Let's start from the.. start

This is a practical problem

- U.S. NIST SCAP Protocol v1 (May '10) -> v1.2 (Draft Jan '12)
  - *"Organizations should use **CVSS base scores** to assist in prioritizing the remediation of known security-related software flaws based on the relative severity of the flaws."*
- PCI-DSS v2 (June '12)
  - *"Risk rankings should be based on industry best practices. For example, criteria for ranking —High // risk vulnerabilities may include a **CVSS base score of 4.0** or above"*
- U.S. Government Configuration Baseline (USGCB)
  - Supported by the industry
  - Rapid7, Telos, VmWare, Symantec.. → SCAP, PCI compliance

What is CVSS?

- CVSS is an assessment of vulnerability "system impact"
- Based on expert assessments to evaluate:
  - **Base Score *[0..10]***
  - Temporal Score
  - Environmental Score



Let's see this from a different perspective

- CVSS is a test by clinical expertise..

- I have a sw with a vulnerability…
- Is it easy to access?
- Is it high impact?
- Your CVSS doctor says HIGH Risk → patch
  - ✓ Of course please…

- I see double…
- Both eyes involved?
- Primary gaze impacted?
- Your CVSS doctor says HIGH risk → brain surgery
  - Ehm are you sure…

..But how informative is it?

Tests and Risks: a practical question

- A clinical test must be matched to the risk
  - Binocular diplopia AND intracranial lesion → 0% recovered without treatment
  - Binocular diplopia and no additional evidence → 42% recovered ***without*** treatment
    - Nolan "Diplopia" B. J. Ophtalm. 1966

- What the CIO would like to know:
  - IF HIGH CVSS listed by Sec. Config. Manager and Metasploit finds it → fix it and decrease risk of successful attacks by +15%
  - IF fix all remaining HIGH listed by Sec. Config. Manager but no additional evidence → risk decreses only by 3%
  - → Is +3% worth the extra money?

Vulnerabilities: data collection

- NATIONAL VULNERABILITY DATABASE: NVD – 49.624 vulns
  - The universe of vulnerabilities
- WHITE MARKETS OF EXPLOITS: EXPLOIT-DB – 8.189 vulns
  - Proof-of-Concept exploits published by security researchers
- ACTUAL EXPLOITS IN THE WILD: SYM – 1.274 vulns
  - Symantec / Kaspersky Threat reports
  - Vulnerabilities actually exploited in the wild
  - Conservative approach: SYM represents the existence of an attack
  - Browser/Plugins 14% – Server 22% – App. 17% - Windows 13%
  - Other OS 5% - Developer 5% - Business 7% - Unclassified 17%
- BLACK MARKETS FOR EXPLOITS: EKITS – 114 vulns
  - 2/3 of client threaths according Google (2011)
  - Exploit advert from the bad guys in an exploit kit
  - 90+ exploit kits from the black markets expanding Contagio's exploit pack table

Leveraging on cancer research

- Do High CVSS scores predict exploitation?
- Do smoking habits predict cancer?
  - → You can't ask people to start smoking so you can't run a controlled experiment → same here
- Case controlled study
  - Cases: people with lung cancer
  - Controls:
    - People with characteristics similar to the cases (Confounding factors)
    - Age, Sex, Social Status, Location
  - Explanatory variable
    - Smoking habit
- For each of the cases select another person with the same values of the control variables
  - Doll & Bradfor Hill, British Medial Journal 1950

CVSS Case Controlled Experiment II

- Case (attacked vulnerability):
  - CVE-2010-3962 (use-after-free vulnerability in MS IE 6,7,8)
  - Year=2010
  - Confidentiality =C, Integrity=C, Availability=C
  - Vendor=Microsoft, Software = ie
- Control (vulnerabilities similar to attacked ones):
  - Select 1 out of:
    - 5 from EKITS
    - 7 from EDB
    - 37 from NVD
- Repeat for all cases of attacked vulnerabilities
  - See what values of CVSS we get
  - See how many times you find an attacked vulnerability

CVSS Risk reduction: answer to the CIO

- Is wearing a seat belt any useful?
  - Pr(Death x Safety Belt on) – Pr(Death x Safety Belt off)
  - Yes it is→ 43% improvement of chances of survival
    - L. Evans, Accident Analysis and Prevention 1986
- Is patching HIGH score any useful?
  - Pr(Attack x CVSS High) – Pr(Attack x CVSS Low)

You Fix	Your Risk Reduction
+93 Vulns with H/M CVSS score used by Exploit Kits	**+61%** (c.i. 61%-61%)
+801 Vulns with H/M score also with a disclosed proof of concept by security researchers	**+9%** (c.i. 7%-11%)
+6480 Vulns with H/M score and no other evidence than SCAP says you should	**+2%** (c.i. 0%-4%)