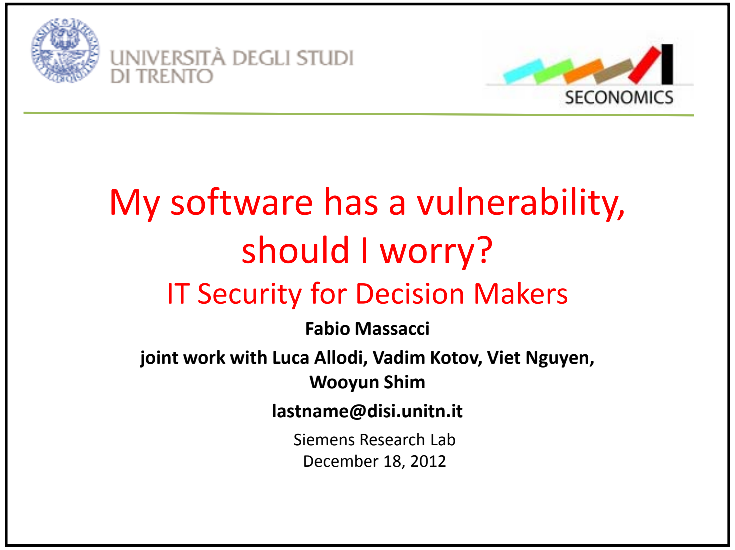


UNIVERSITÀ DEGLI STUDI DI TRENTO

SECONOMICS

My software has a vulnerability, should I worry?

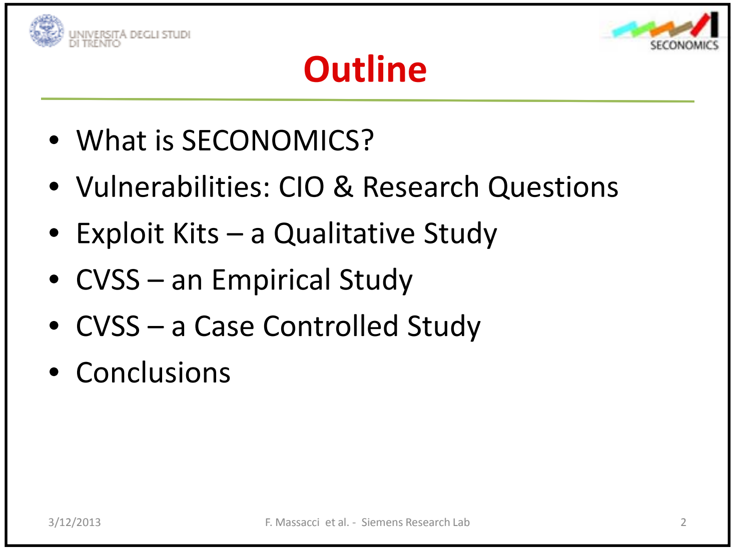
IT Security for Decision Makers

Fabio Massacci

joint work with Luca Allodi, Vadim Kotov, Viet Nguyen, Wooyun Shim

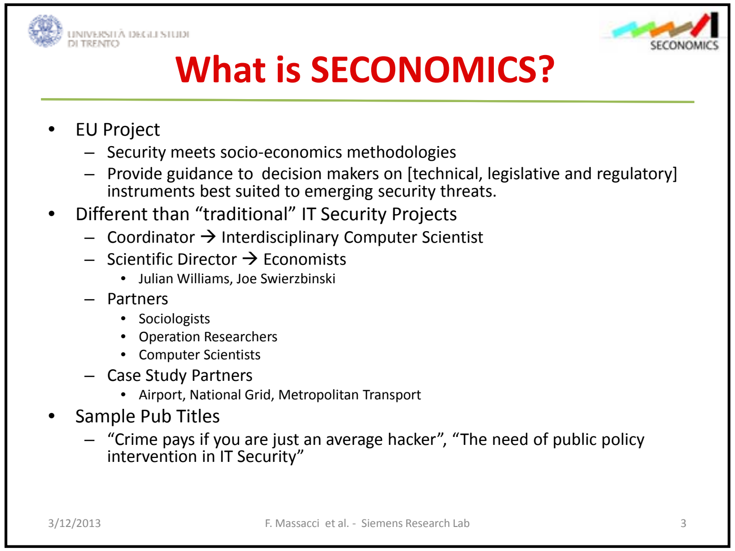
lastname@disi.unitn.it

Siemens Research Lab
December 18, 2012



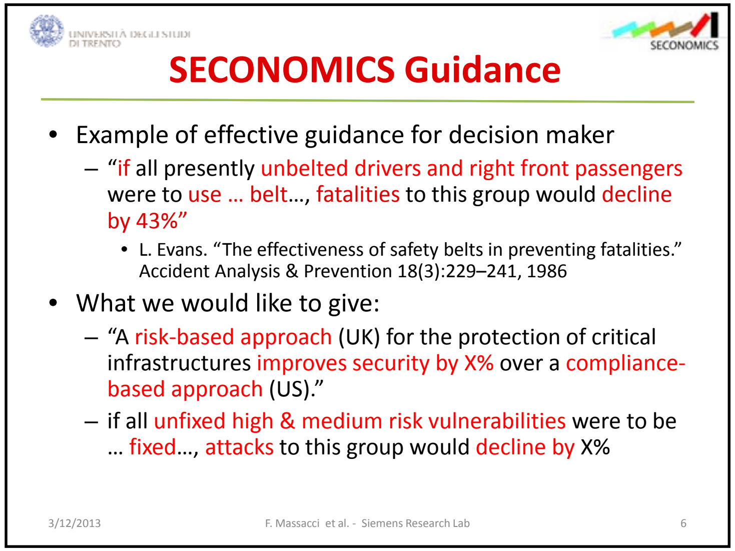
Outline

- What is SECONOMICS?
- Vulnerabilities: CIO & Research Questions
- Exploit Kits – a Qualitative Study
- CVSS – an Empirical Study
- CVSS – a Case Controlled Study
- Conclusions



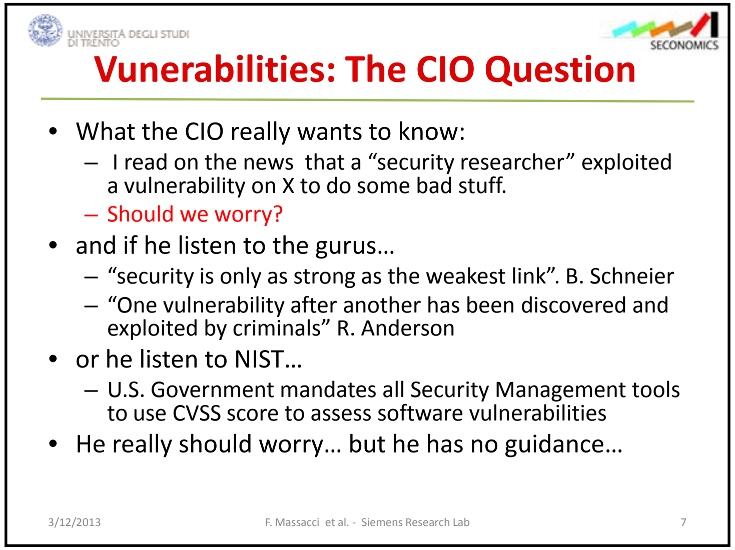
What is SECONOMICS?

- EU Project
  - Security meets socio-economics methodologies
  - Provide guidance to decision makers on [technical, legislative and regulatory] instruments best suited to emerging security threats.
- Different than "traditional" IT Security Projects
  - Coordinator → Interdisciplinary Computer Scientist
  - Scientific Director → Economists
    - Julian Williams, Joe Swierzbinski
  - Partners
    - Sociologists
    - Operation Researchers
    - Computer Scientists
  - Case Study Partners
    - Airport, National Grid, Metropolitan Transport
- Sample Pub Titles
  - "Crime pays if you are just an average hacker", "The need of public policy intervention in IT Security"



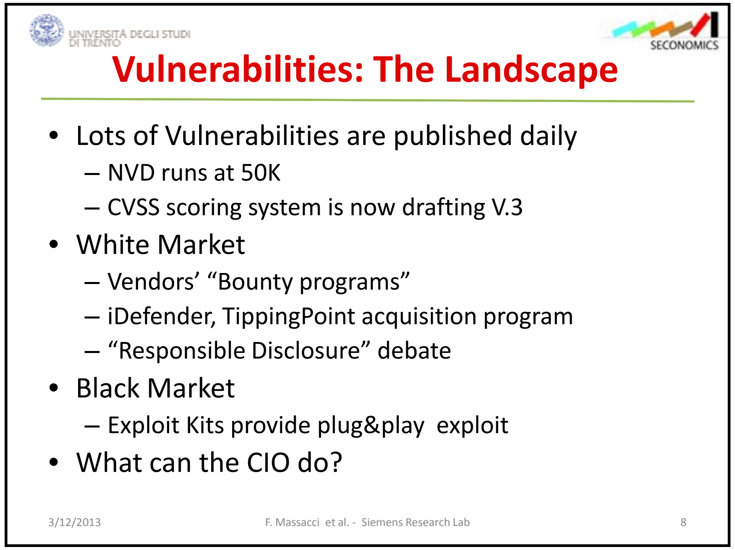
SECONOMICS Guidance

- Example of effective guidance for decision maker
  - "if all presently unbelted drivers and right front passengers were to use … belt…, fatalities to this group would decline by 43%"
    - L. Evans. "The effectiveness of safety belts in preventing fatalities." Accident Analysis & Prevention 18(3):229–241, 1986
- What we would like to give:
  - "A risk-based approach (UK) for the protection of critical infrastructures improves security by X% over a compliance-based approach (US)."
  - if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by X%



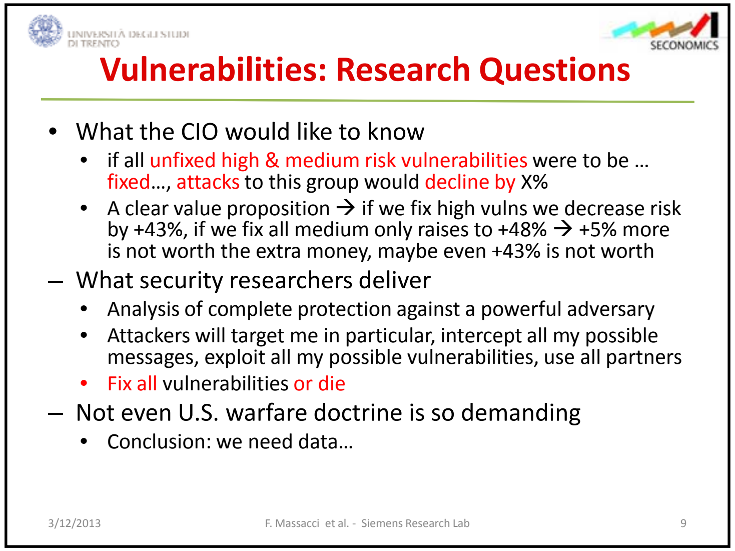
Vunerabilities: The CIO Question

- What the CIO really wants to know:
  - I read on the news that a “security researcher” exploited a vulnerability on X to do some bad stuff.
  - Should we worry?
- and if he listen to the gurus…
  - “security is only as strong as the weakest link”. B. Schneier
  - “One vulnerability after another has been discovered and exploited by criminals” R. Anderson
- or he listen to NIST…
  - U.S. Government mandates all Security Management tools to use CVSS score to assess software vulnerabilities
- He really should worry… but he has no guidance…



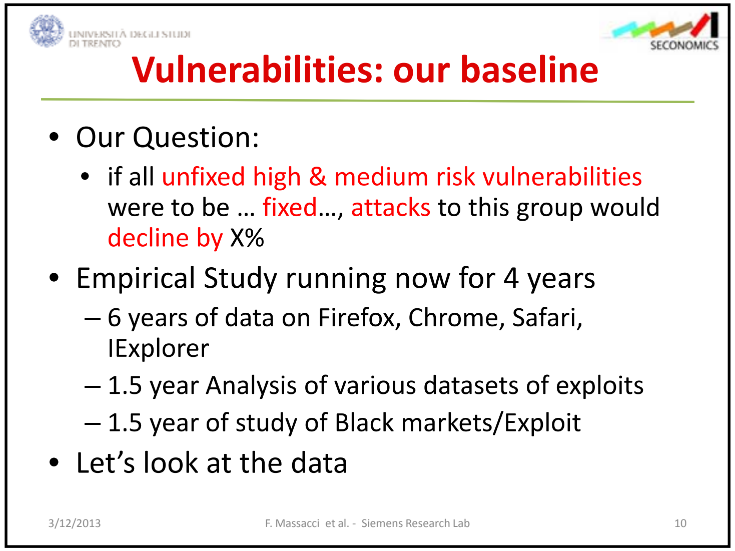
Vulnerabilities: The Landscape

- Lots of Vulnerabilities are published daily
  - NVD runs at 50K
  - CVSS scoring system is now drafting V.3
- White Market
  - Vendors’ “Bounty programs”
  - iDefender, TippingPoint acquisition program
  - “Responsible Disclosure” debate
- Black Market
  - Exploit Kits provide plug&play exploit
- What can the CIO do?



Vulnerabilities: Research Questions

- What the CIO would like to know
  - if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by X%
  - A clear value proposition → if we fix high vulns we decrease risk by +43%, if we fix all medium only raises to +48% → +5% more is not worth the extra money, maybe even +43% is not worth
- What security researchers deliver
  - Analysis of complete protection against a powerful adversary
  - Attackers will target me in particular, intercept all my possible messages, exploit all my possible vulnerabilities, use all partners
  - Fix all vulnerabilities or die
- Not even U.S. warfare doctrine is so demanding
  - Conclusion: we need data…



Vulnerabilities: our baseline

- Our Question:
  - if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by X%
- Empirical Study running now for 4 years
  - 6 years of data on Firefox, Chrome, Safari, IExplorer
  - 1.5 year Analysis of various datasets of exploits
  - 1.5 year of study of Black markets/Exploit
- Let’s look at the data

Vulnerabilities: a closer look

- “A vulnerability is discovered” has many meanings
- CVE entry mentioned in NVD
  - somebody (vendor, researcher etc.) told NIST the software has a vulnerability
- Its exploit code appears in the Exploit-DB
  - Somebody actually constructed a proof-of-concept code that exploits it
- Mentioned in Symantec/Kaspersky Threat-Explorer
  - Somebody actually used the vulnerability to run an attack
- Advertised in an Exploit Kit
  - Bad guys packaged its exploit into a “PnP” platform

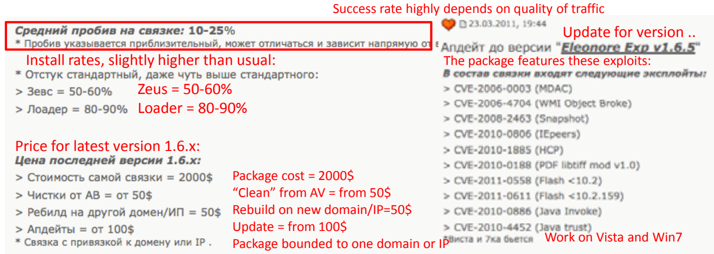
Vulnerabilities: numbers speak

- “A vulnerability is discovered” has many meanings
- CVE entry mentioned in NVD - **49.624**
  - somebody told NIST the software has a vulnerability
- Exploit by sec. researchers in Exploit-DB - **8.189**
  - Somebody constructed a proof-of-concept that exploits it
- Symantec/Kaspersky Threat-Explorer - **1.289/1.321**
  - Somebody actually used the vulnerability to run an attack
  - Browser/Plugins 14% – Server 22% – App. 24%
- Exploit advert by bad guys in an Exploit Kit - **103**
  - Bad guys packaged its exploit into a “PnP” platform
  - 2/3 of client threaths according Google (2011)

Exploit Kits Study: a closer look

- Do bank robbers manufacture their own guns?
  - just buy them from somebody
- Top threat according to Google + AV Vendors

Exploitation success rate: 10-15%
Success rate highly depends on quality of traffic



Средний пробив на связке: 10-25%
* Пробив указывается приблизительный, может отличаться и зависит напрямую от

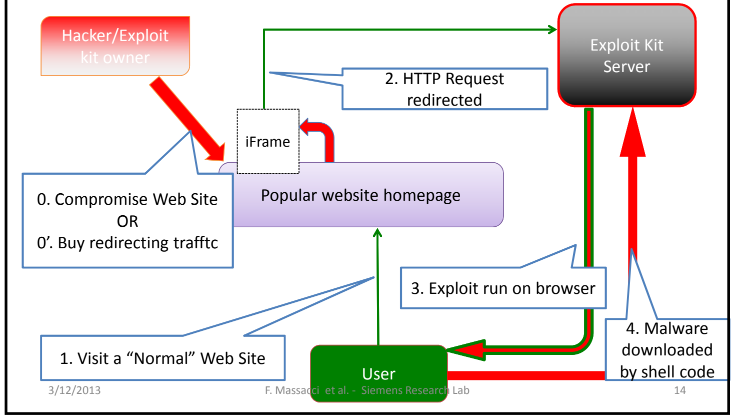
Install rates, slightly higher than usual:
* Отстук стандартный, даже чуть выше стандартного:
> Зевс = 50-60% Zeus = 50-60%
> Лоадер = 80-90% Loader = 80-90%

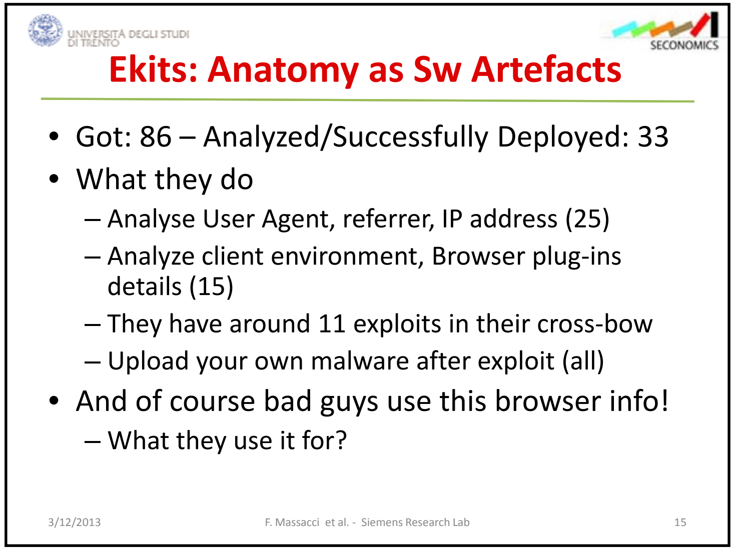
Price for latest version 1.6.x:
Цена последней версии 1.6.x:
> Стоимость самой связки = 2000$ Package cost = 2000$
> Чистки от АВ = от 50$ “Clean” from AV = from 50$
> Ребилд на другой домен/ИП = 50$ Rebuild on new domain/IP=50$
> Апдейты = от 100$ Update = from 100$
* Связка с привязкой к домену или IP . Package bounded to one domain or IP

23.03.2011, 19:44

Update for version ..
Апдейт до версии "***Eleonore Exp v1.6.5***"
The package features these exploits:
В состав связки входят следующие эксплойты:
> CVE-2006-0003 (MDAC)
> CVE-2006-4704 (WMI Object Broke)
> CVE-2008-2463 (Snapshot)
> CVE-2010-0806 (IEpeers)
> CVE-2010-1885 (HCP)
> CVE-2010-0188 (PDF libtiff mod v1.0)
> CVE-2011-0558 (Flash <10.2)
> CVE-2011-0611 (Flash <10.2.159)
> CVE-2010-0886 (Java Invoke)
> CVE-2010-4452 (Java trust)
*Виста и 7ка бьется Work on Vista and Win7

EKit Study: infection dynamics

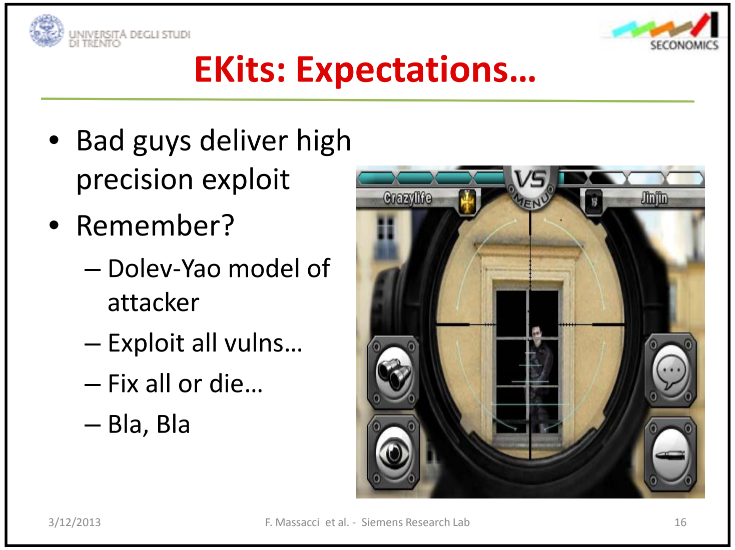

Hacker/Exploit kit owner
Exploit Kit Server
2. HTTP Request redirected
iFrame
0. Compromise Web Site OR 0’. Buy redirecting trafftc
Popular website homepage
3. Exploit run on browser
4. Malware downloaded by shell code
1. Visit a “Normal” Web Site
User



UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

Ekits: Anatomy as Sw Artefacts

- Got: 86 – Analyzed/Successfully Deployed: 33
- What they do
  - Analyse User Agent, referrer, IP address (25)
  - Analyze client environment, Browser plug-ins details (15)
  - They have around 11 exploits in their cross-bow
  - Upload your own malware after exploit (all)
- And of course bad guys use this browser info!
  - What they use it for?

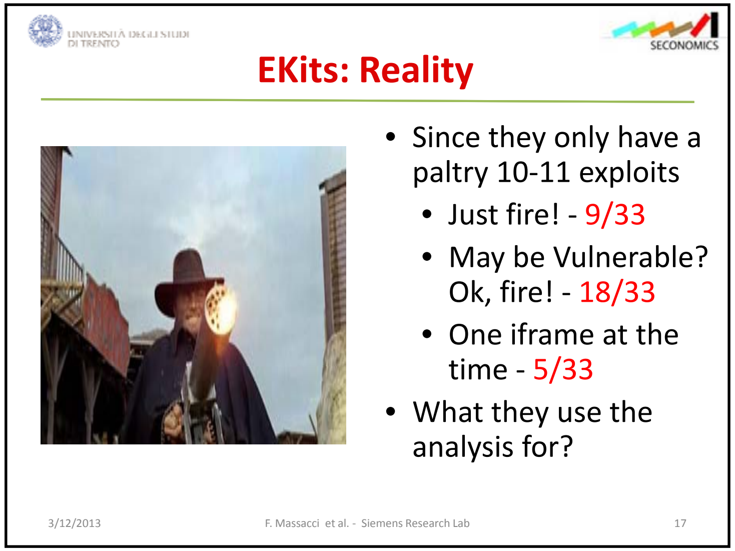


UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

EKits: Expectations…

- Bad guys deliver high precision exploit
- Remember?
  - Dolev-Yao model of attacker
  - Exploit all vulns…
  - Fix all or die…
  - Bla, Bla

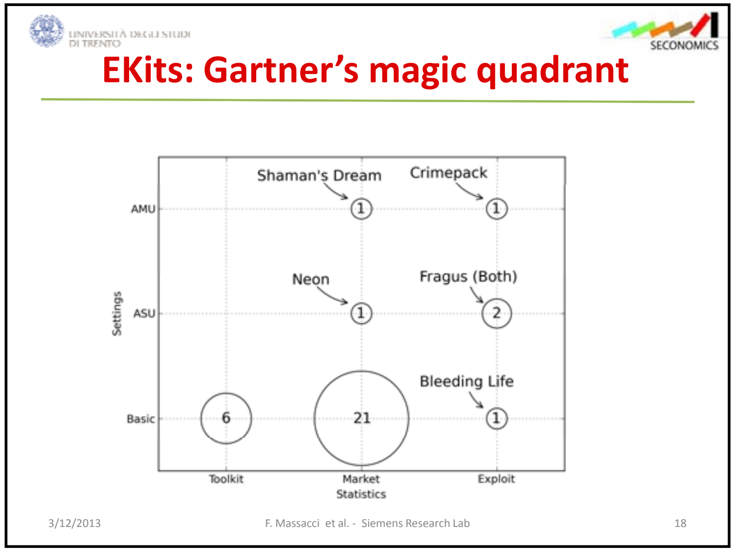
Crazylife
VS
MENU
Jinjin



UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

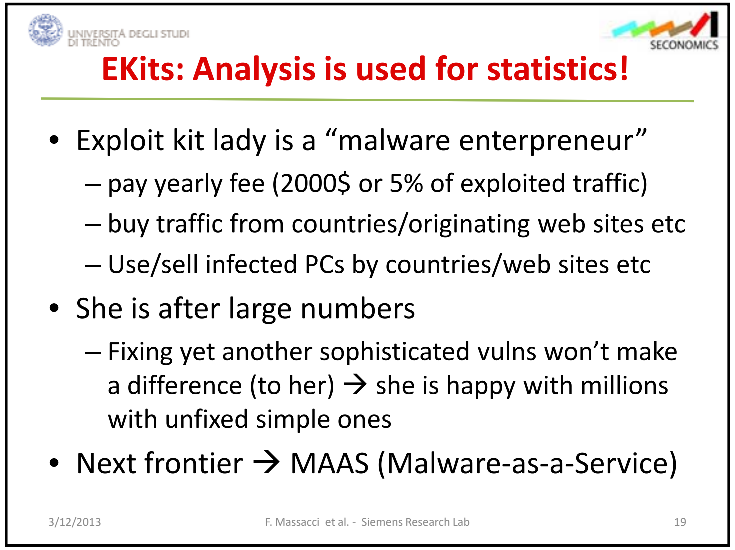
EKits: Reality

- Since they only have a paltry 10-11 exploits
  - Just fire! - 9/33
  - May be Vulnerable? Ok, fire! - 18/33
  - One iframe at the time - 5/33
- What they use the analysis for?



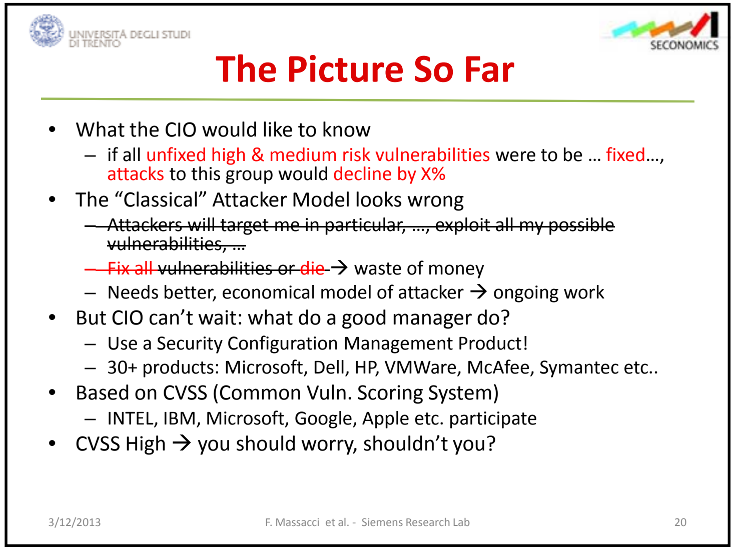
UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

EKits: Gartner's magic quadrant



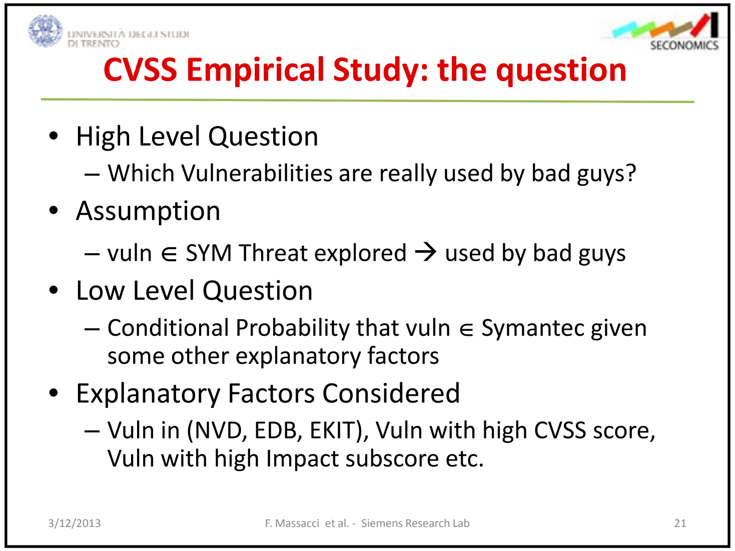
EKits: Analysis is used for statistics!

- Exploit kit lady is a “malware enterpreneur”
  - pay yearly fee (2000$ or 5% of exploited traffic)
  - buy traffic from countries/originating web sites etc
  - Use/sell infected PCs by countries/web sites etc
- She is after large numbers
  - Fixing yet another sophisticated vulns won’t make a difference (to her) → she is happy with millions with unfixed simple ones
- Next frontier → MAAS (Malware-as-a-Service)



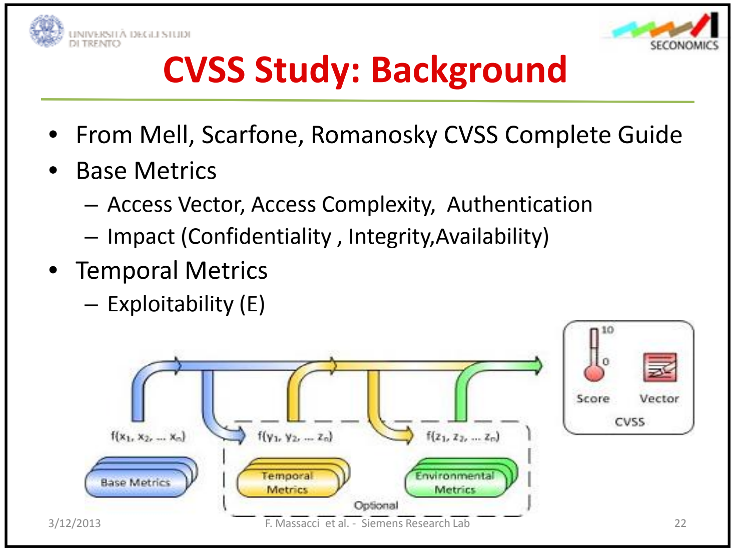
The Picture So Far

- What the CIO would like to know
  - if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by X%
- The “Classical” Attacker Model looks wrong
  - ~~Attackers will target me in particular, …, exploit all my possible vulnerabilities, …~~
  - ~~Fix all vulnerabilities or die~~ → waste of money
  - Needs better, economical model of attacker → ongoing work
- But CIO can’t wait: what do a good manager do?
  - Use a Security Configuration Management Product!
  - 30+ products: Microsoft, Dell, HP, VMWare, McAfee, Symantec etc..
- Based on CVSS (Common Vuln. Scoring System)
  - INTEL, IBM, Microsoft, Google, Apple etc. participate
- CVSS High → you should worry, shouldn’t you?



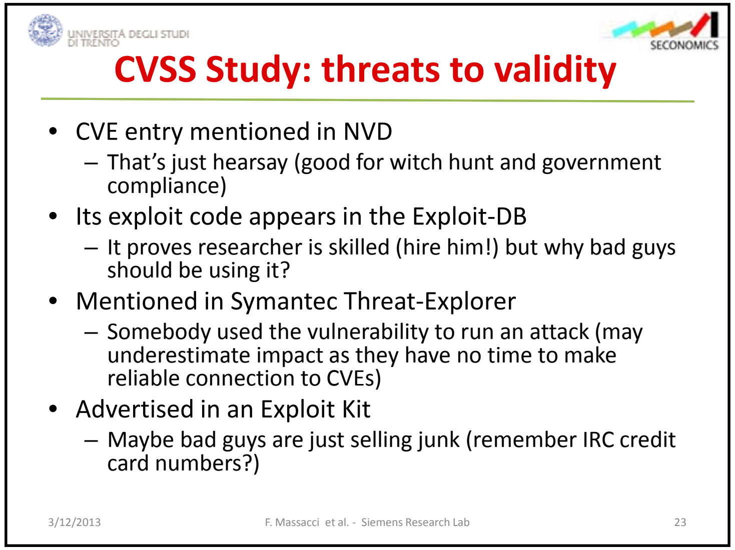
CVSS Empirical Study: the question

- High Level Question
  - Which Vulnerabilities are really used by bad guys?
- Assumption
  - vuln ∈ SYM Threat explored → used by bad guys
- Low Level Question
  - Conditional Probability that vuln ∈ Symantec given some other explanatory factors
- Explanatory Factors Considered
  - Vuln in (NVD, EDB, EKIT), Vuln with high CVSS score, Vuln with high Impact subscore etc.



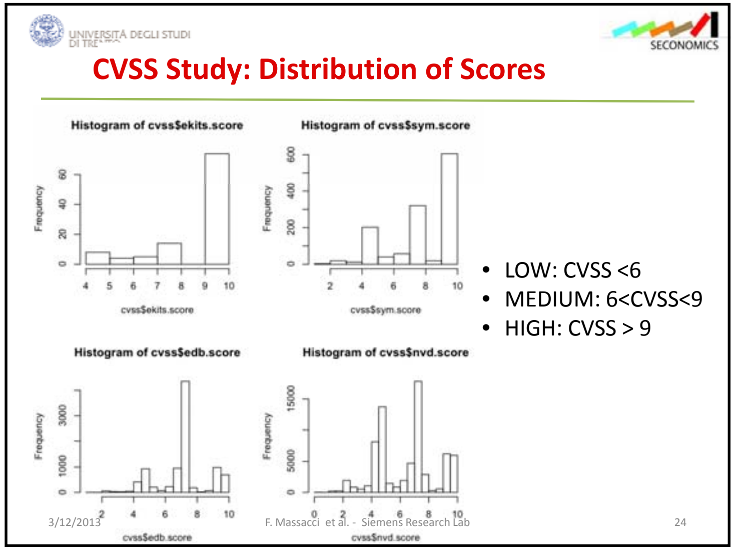
CVSS Study: Background

- From Mell, Scarfone, Romanosky CVSS Complete Guide
- Base Metrics
  - Access Vector, Access Complexity, Authentication
  - Impact (Confidentiality , Integrity,Availability)
- Temporal Metrics
  - Exploitability (E)



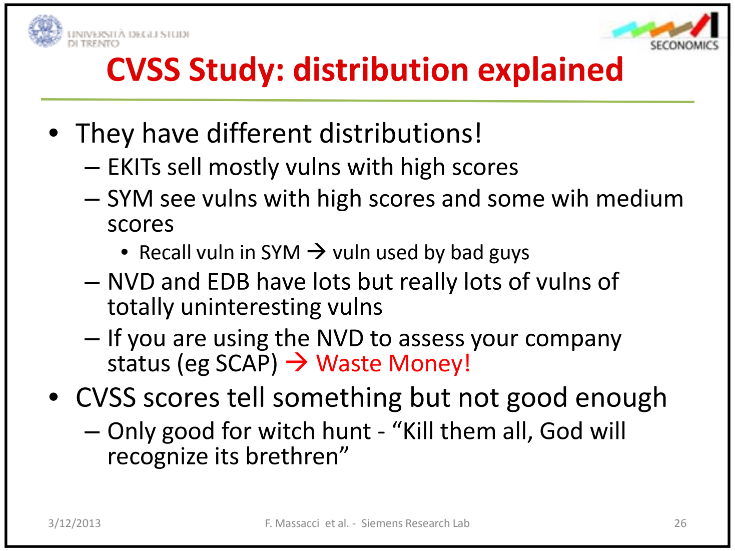
CVSS Study: threats to validity

- CVE entry mentioned in NVD
  - That’s just hearsay (good for witch hunt and government compliance)
- Its exploit code appears in the Exploit-DB
  - It proves researcher is skilled (hire him!) but why bad guys should be using it?
- Mentioned in Symantec Threat-Explorer
  - Somebody used the vulnerability to run an attack (may underestimate impact as they have no time to make reliable connection to CVEs)
- Advertised in an Exploit Kit
  - Maybe bad guys are just selling junk (remember IRC credit card numbers?)



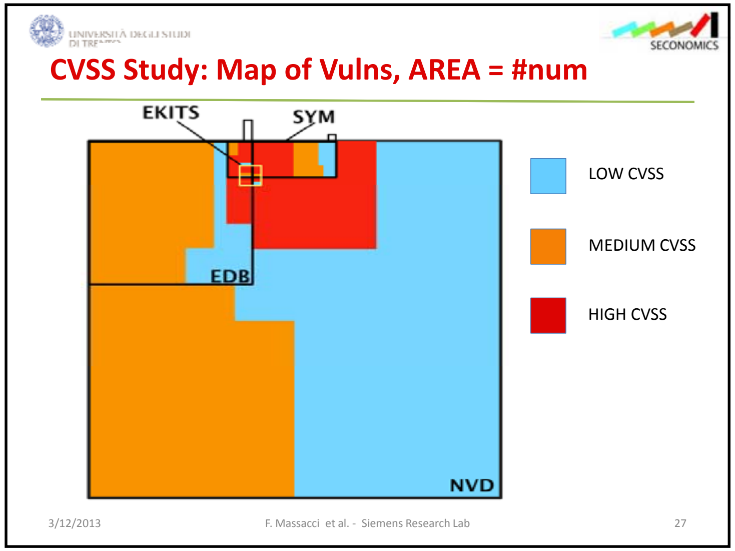
CVSS Study: Distribution of Scores

- LOW: CVSS <6
- MEDIUM: 6<CVSS<9
- HIGH: CVSS > 9

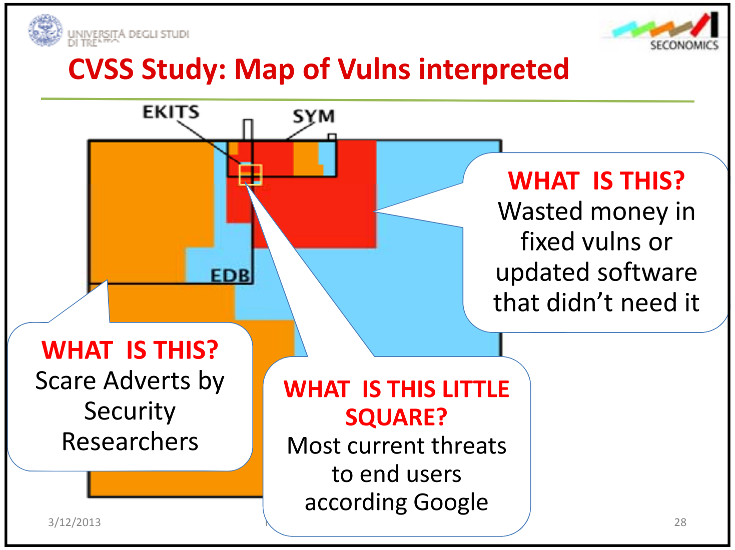


CVSS Study: distribution explained

- They have different distributions!
  - EKITs sell mostly vulns with high scores
  - SYM see vulns with high scores and some wih medium scores
    - Recall vuln in SYM → vuln used by bad guys
  - NVD and EDB have lots but really lots of vulns of totally uninteresting vulns
  - If you are using the NVD to assess your company status (eg SCAP) → Waste Money!
- CVSS scores tell something but not good enough
  - Only good for witch hunt - “Kill them all, God will recognize its brethren”



CVSS Study: Map of Vulns, AREA = #num

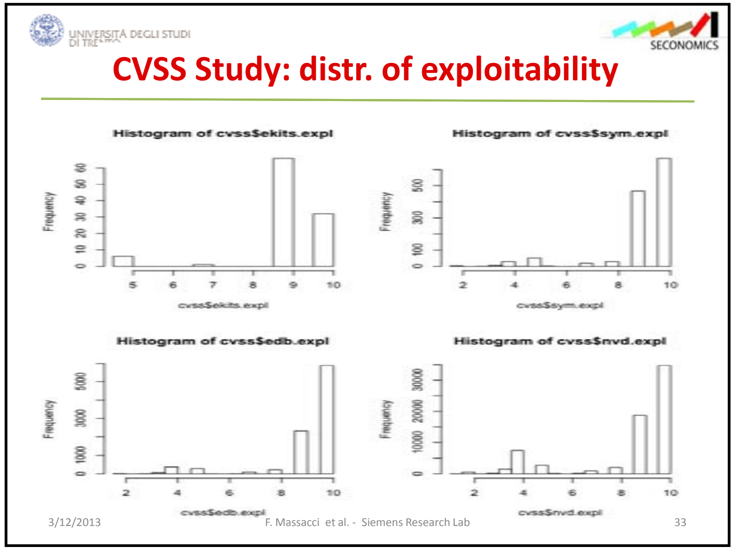


CVSS Study: Map of Vulns interpreted

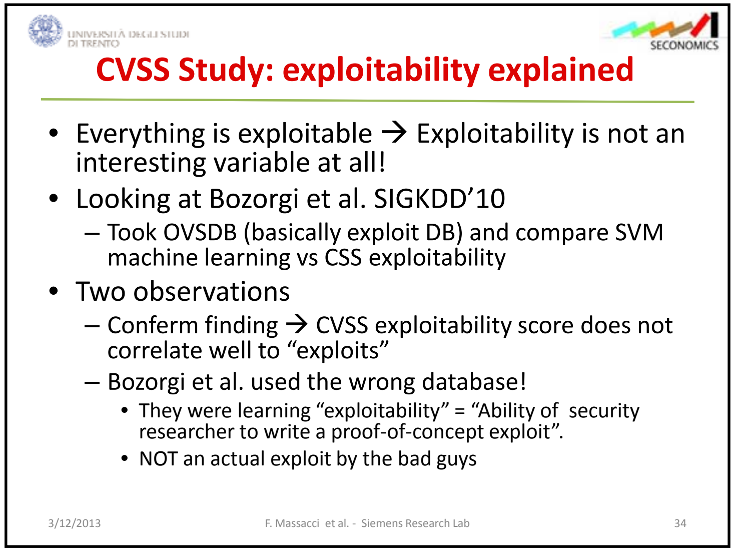
WHAT IS THIS? Wasted money in fixed vulns or updated software that didn't need it

WHAT IS THIS? Scare Adverts by Security Researchers

WHAT IS THIS LITTLE SQUARE? Most current threats to end users according Google

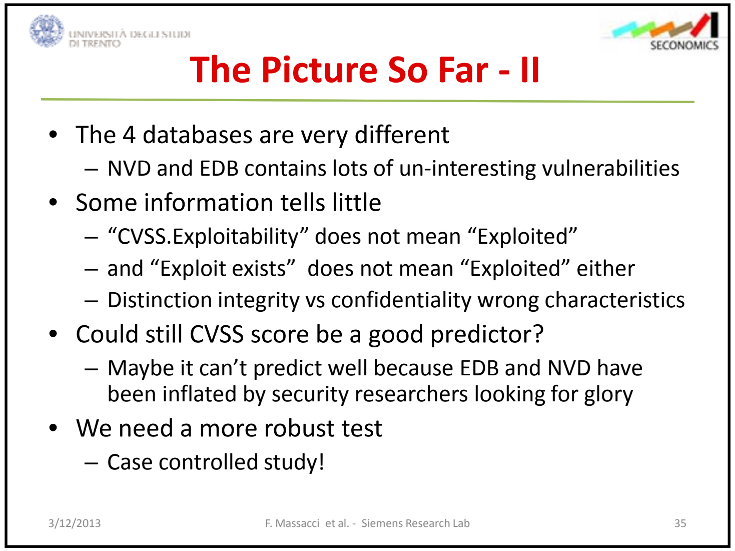


CVSS Study: distr. of exploitability



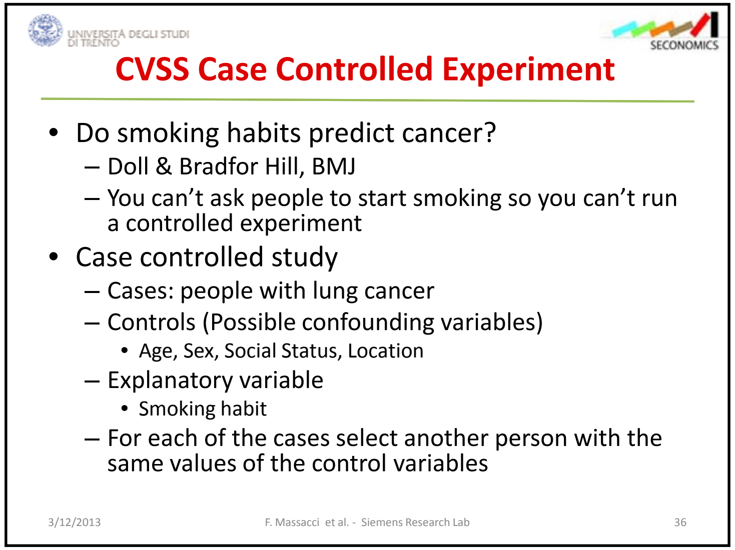
CVSS Study: exploitability explained

- Everything is exploitable → Exploitability is not an interesting variable at all!
- Looking at Bozorgi et al. SIGKDD'10
  - Took OVSDB (basically exploit DB) and compare SVM machine learning vs CSS exploitability
- Two observations
  - Conferm finding → CVSS exploitability score does not correlate well to "exploits"
  - Bozorgi et al. used the wrong database!
    - They were learning "exploitability" = "Ability of security researcher to write a proof-of-concept exploit".
    - NOT an actual exploit by the bad guys



The Picture So Far - II

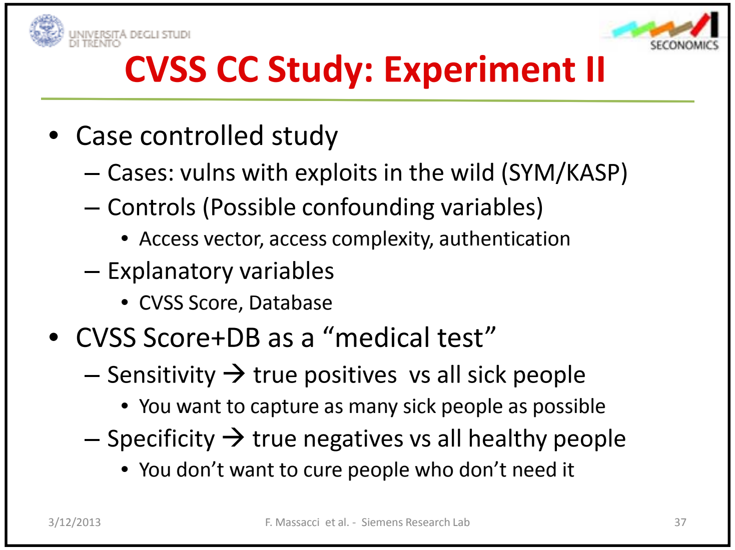
- The 4 databases are very different
  - NVD and EDB contains lots of un-interesting vulnerabilities
- Some information tells little
  - "CVSS.Exploitability" does not mean "Exploited"
  - and "Exploit exists" does not mean "Exploited" either
  - Distinction integrity vs confidentiality wrong characteristics
- Could still CVSS score be a good predictor?
  - Maybe it can't predict well because EDB and NVD have been inflated by security researchers looking for glory
- We need a more robust test
  - Case controlled study!



UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

CVSS Case Controlled Experiment

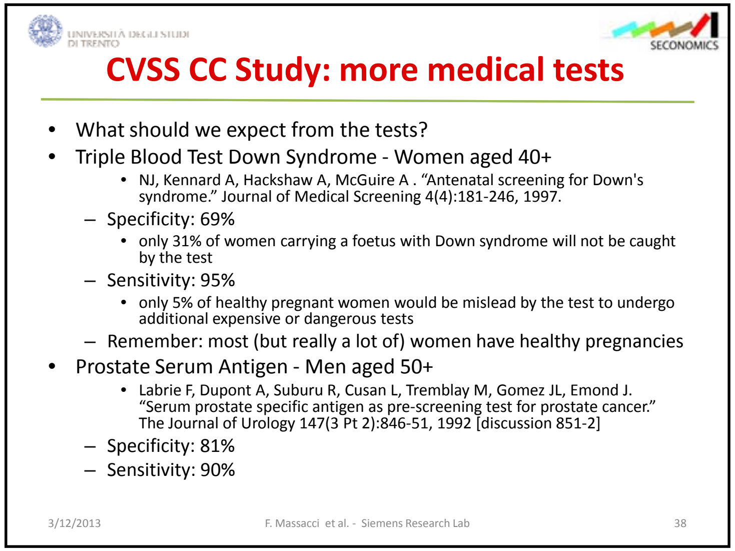
- Do smoking habits predict cancer?
  - Doll & Bradfor Hill, BMJ
  - You can't ask people to start smoking so you can't run a controlled experiment
- Case controlled study
  - Cases: people with lung cancer
  - Controls (Possible confounding variables)
    - Age, Sex, Social Status, Location
  - Explanatory variable
    - Smoking habit
  - For each of the cases select another person with the same values of the control variables



UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

CVSS CC Study: Experiment II

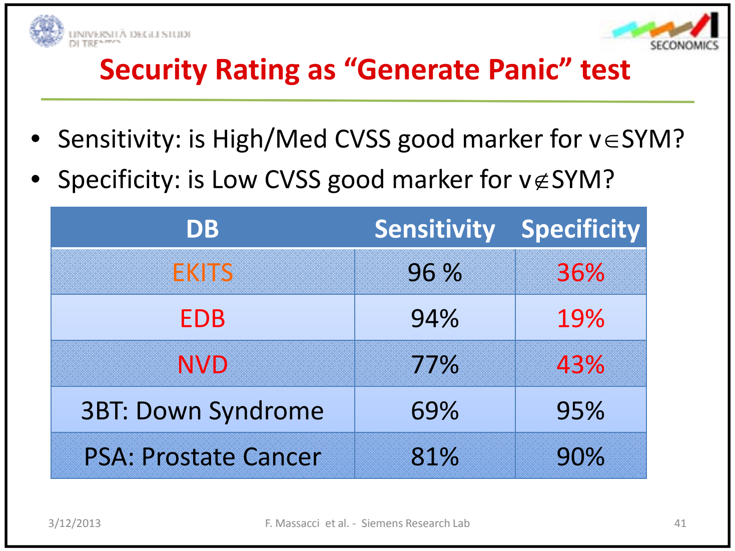
- Case controlled study
  - Cases: vulns with exploits in the wild (SYM/KASP)
  - Controls (Possible confounding variables)
    - Access vector, access complexity, authentication
  - Explanatory variables
    - CVSS Score, Database
- CVSS Score+DB as a "medical test"
  - Sensitivity → true positives vs all sick people
    - You want to capture as many sick people as possible
  - Specificity → true negatives vs all healthy people
    - You don't want to cure people who don't need it



UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

CVSS CC Study: more medical tests

- What should we expect from the tests?
- Triple Blood Test Down Syndrome - Women aged 40+
    - NJ, Kennard A, Hackshaw A, McGuire A . "Antenatal screening for Down's syndrome." Journal of Medical Screening 4(4):181-246, 1997.
  - Specificity: 69%
    - only 31% of women carrying a foetus with Down syndrome will not be caught by the test
  - Sensitivity: 95%
    - only 5% of healthy pregnant women would be mislead by the test to undergo additional expensive or dangerous tests
  - Remember: most (but really a lot of) women have healthy pregnancies
- Prostate Serum Antigen - Men aged 50+
    - Labrie F, Dupont A, Suburu R, Cusan L, Tremblay M, Gomez JL, Emond J. "Serum prostate specific antigen as pre-screening test for prostate cancer." The Journal of Urology 147(3 Pt 2):846-51, 1992 [discussion 851-2]
  - Specificity: 81%
  - Sensitivity: 90%

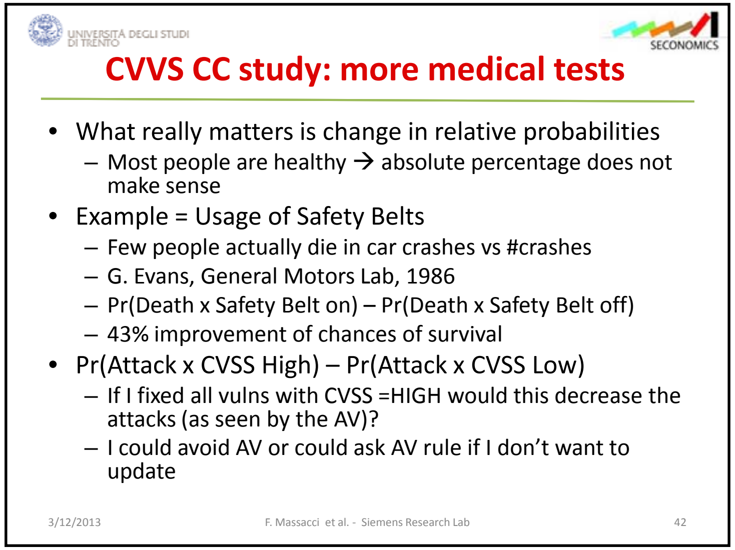


UNIVERSITÀ DEGLI STUDI DI TRENTO — SECONOMICS

Security Rating as "Generate Panic" test

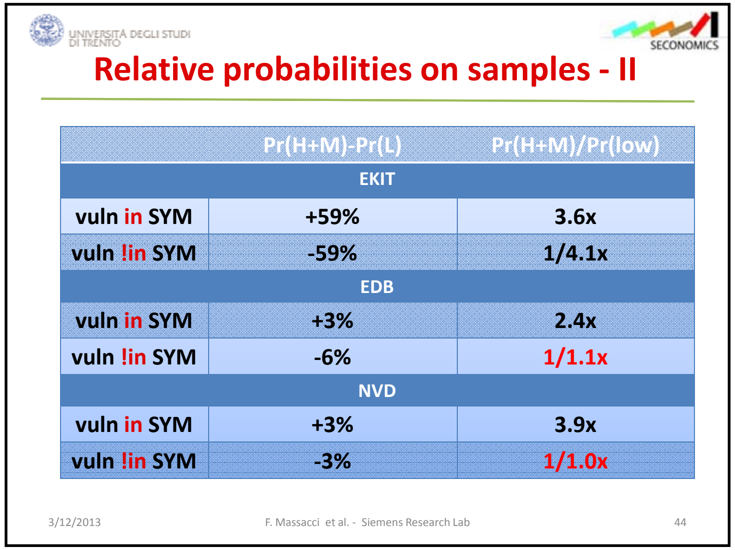
- Sensitivity: is High/Med CVSS good marker for v∈SYM?
- Specificity: is Low CVSS good marker for v∉SYM?

DB	Sensitivity	Specificity
EKITS	96 %	36%
EDB	94%	19%
NVD	77%	43%
3BT: Down Syndrome	69%	95%
PSA: Prostate Cancer	81%	90%



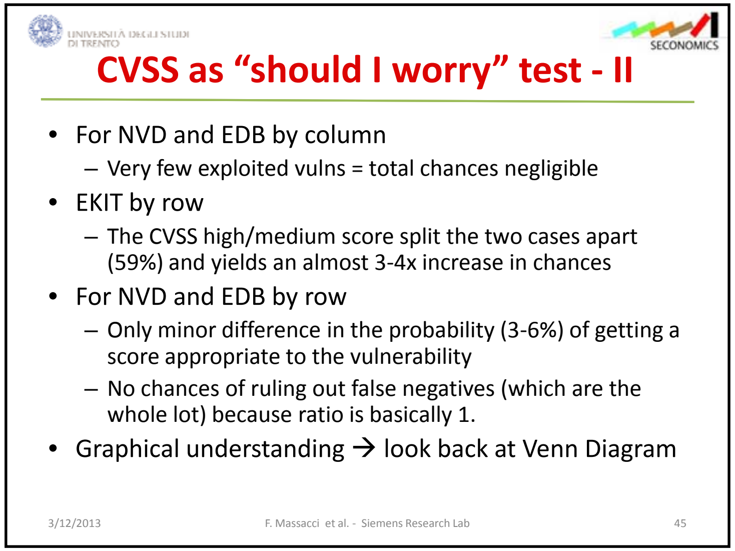
CVVS CC study: more medical tests

- What really matters is change in relative probabilities
  - Most people are healthy → absolute percentage does not make sense
- Example = Usage of Safety Belts
  - Few people actually die in car crashes vs #crashes
  - G. Evans, General Motors Lab, 1986
  - Pr(Death x Safety Belt on) – Pr(Death x Safety Belt off)
  - 43% improvement of chances of survival
- Pr(Attack x CVSS High) – Pr(Attack x CVSS Low)
  - If I fixed all vulns with CVSS =HIGH would this decrease the attacks (as seen by the AV)?
  - I could avoid AV or could ask AV rule if I don't want to update



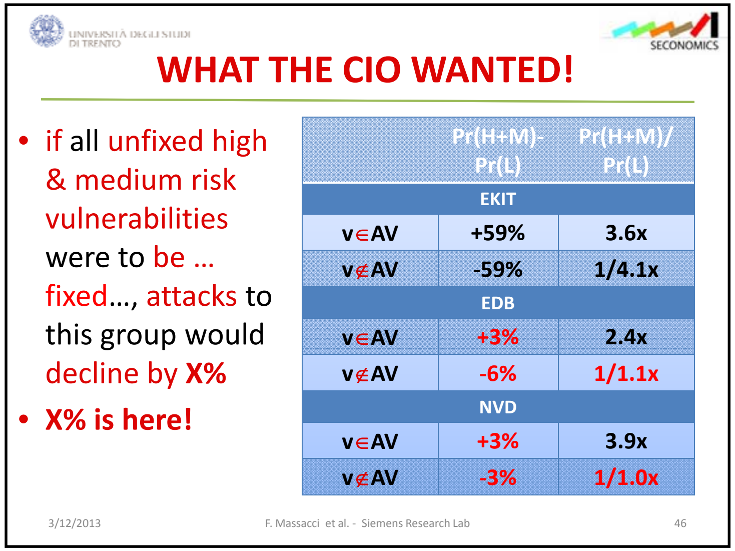
Relative probabilities on samples - II

	Pr(H+M)-Pr(L)	Pr(H+M)/Pr(low)
EKIT		
vuln in SYM	+59%	3.6x
vuln !in SYM	-59%	1/4.1x
EDB		
vuln in SYM	+3%	2.4x
vuln !in SYM	-6%	1/1.1x
NVD		
vuln in SYM	+3%	3.9x
vuln !in SYM	-3%	1/1.0x



CVSS as "should I worry" test - II

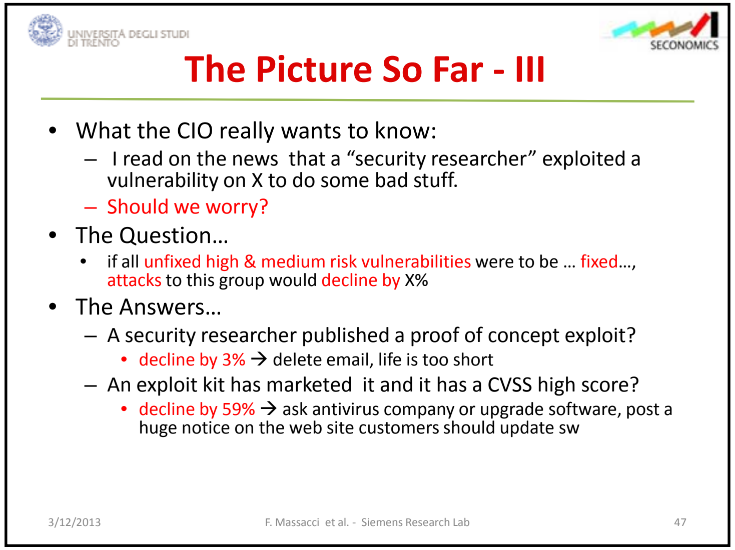
- For NVD and EDB by column
  - Very few exploited vulns = total chances negligible
- EKIT by row
  - The CVSS high/medium score split the two cases apart (59%) and yields an almost 3-4x increase in chances
- For NVD and EDB by row
  - Only minor difference in the probability (3-6%) of getting a score appropriate to the vulnerability
  - No chances of ruling out false negatives (which are the whole lot) because ratio is basically 1.
- Graphical understanding → look back at Venn Diagram



WHAT THE CIO WANTED!

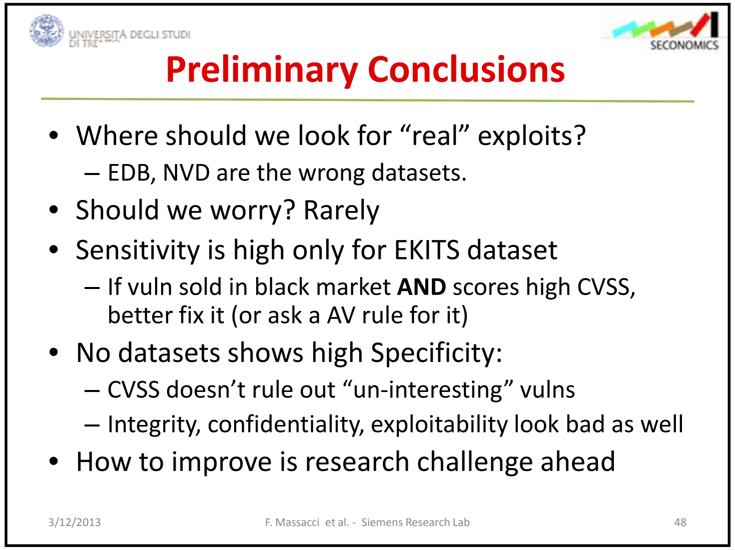
- if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by **X%**
- **X% is here!**

	Pr(H+M)-Pr(L)	Pr(H+M)/Pr(L)
EKIT		
v∈AV	+59%	3.6x
v∉AV	-59%	1/4.1x
EDB		
v∈AV	+3%	2.4x
v∉AV	-6%	1/1.1x
NVD		
v∈AV	+3%	3.9x
v∉AV	-3%	1/1.0x



The Picture So Far - III

- What the CIO really wants to know:
  - I read on the news that a “security researcher” exploited a vulnerability on X to do some bad stuff.
  - Should we worry?
- The Question…
  - if all unfixed high & medium risk vulnerabilities were to be … fixed…, attacks to this group would decline by X%
- The Answers…
  - A security researcher published a proof of concept exploit?
    - decline by 3% → delete email, life is too short
  - An exploit kit has marketed it and it has a CVSS high score?
    - decline by 59% → ask antivirus company or upgrade software, post a huge notice on the web site customers should update sw



Preliminary Conclusions

- Where should we look for “real” exploits?
  - EDB, NVD are the wrong datasets.
- Should we worry? Rarely
- Sensitivity is high only for EKITS dataset
  - If vuln sold in black market **AND** scores high CVSS, better fix it (or ask a AV rule for it)
- No datasets shows high Specificity:
  - CVSS doesn’t rule out “un-interesting” vulns
  - Integrity, confidentiality, exploitability look bad as well
- How to improve is research challenge ahead