Quantitative assessment of risk reduction with cybercrime black market monitoring

Luca Allodi, Woohyun Shim, Fabio Massacci
University of Trento
Trento, Italy

IWCC 2013, IEEE SS&P 2013
24 May, San Francisco, CA, U.S.A.

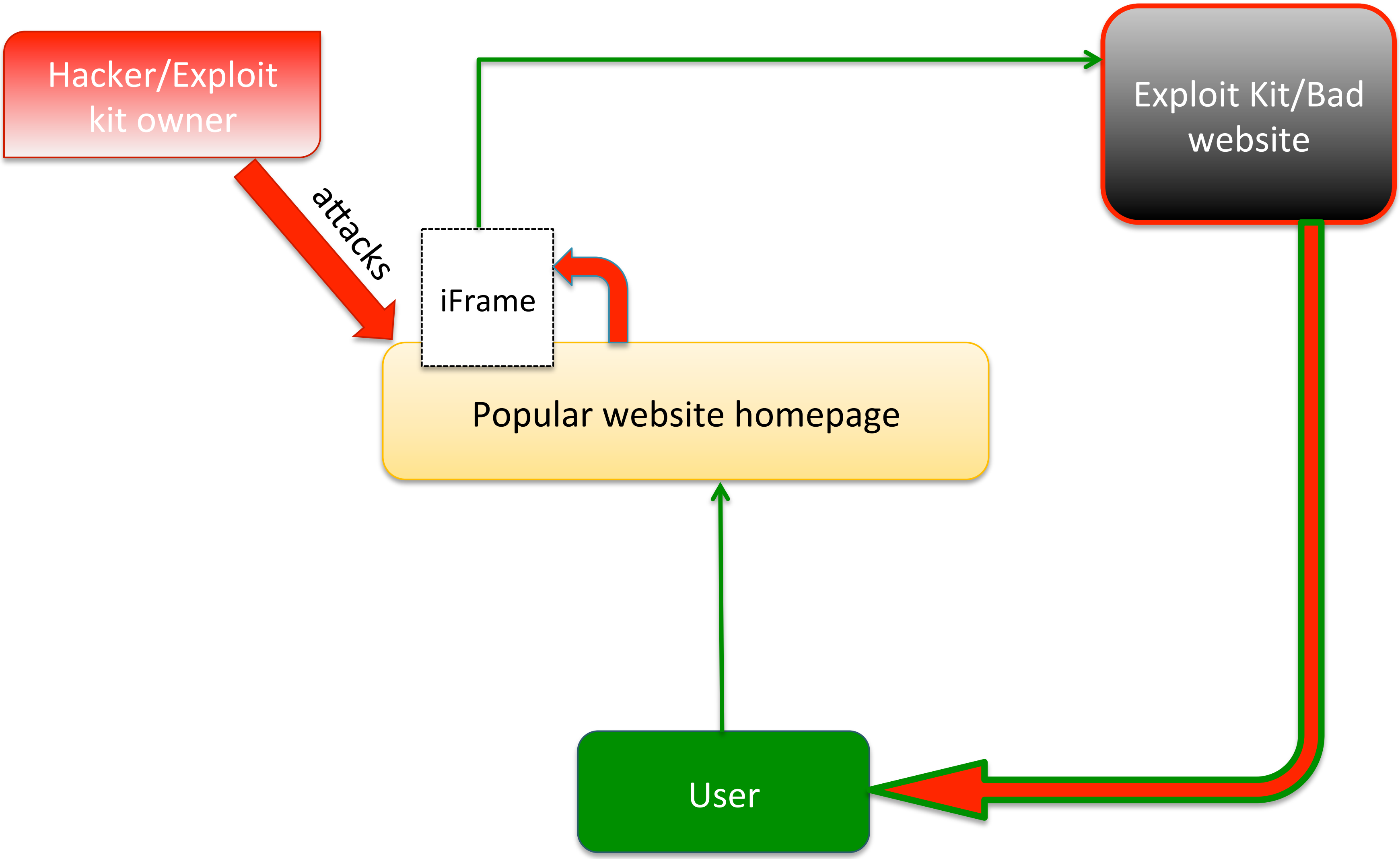
Outline

- Motivation
- Questions
- Data
  - Attacks
  - Black markets
- Preliminary observations
  - Vulnerability risk score (CVSS) vs attacks
  - Black market vulnerabilities vs attacks
- “Effectiveness” of patching policies
  - Methodology
  - Results
- Conclusions

Motivation

- Software vulnerabilities are main vector for attacks against the users
- Patching is critical
  - Too many, users are bothered
  - How to prioritize?
- Patches priorities by means of CVSS scores
  - High score -> vulnerability is attacked
  - Low score -> ignore for now
- Observation: Drive-by-downloads responsible for 70% of infections [Google 2011]
  - Cybercrime black markets trade very popular drive-by-infection tools: Exploit kits

Drive-by-download attacks



Hacker/Exploit kit owner

attacks

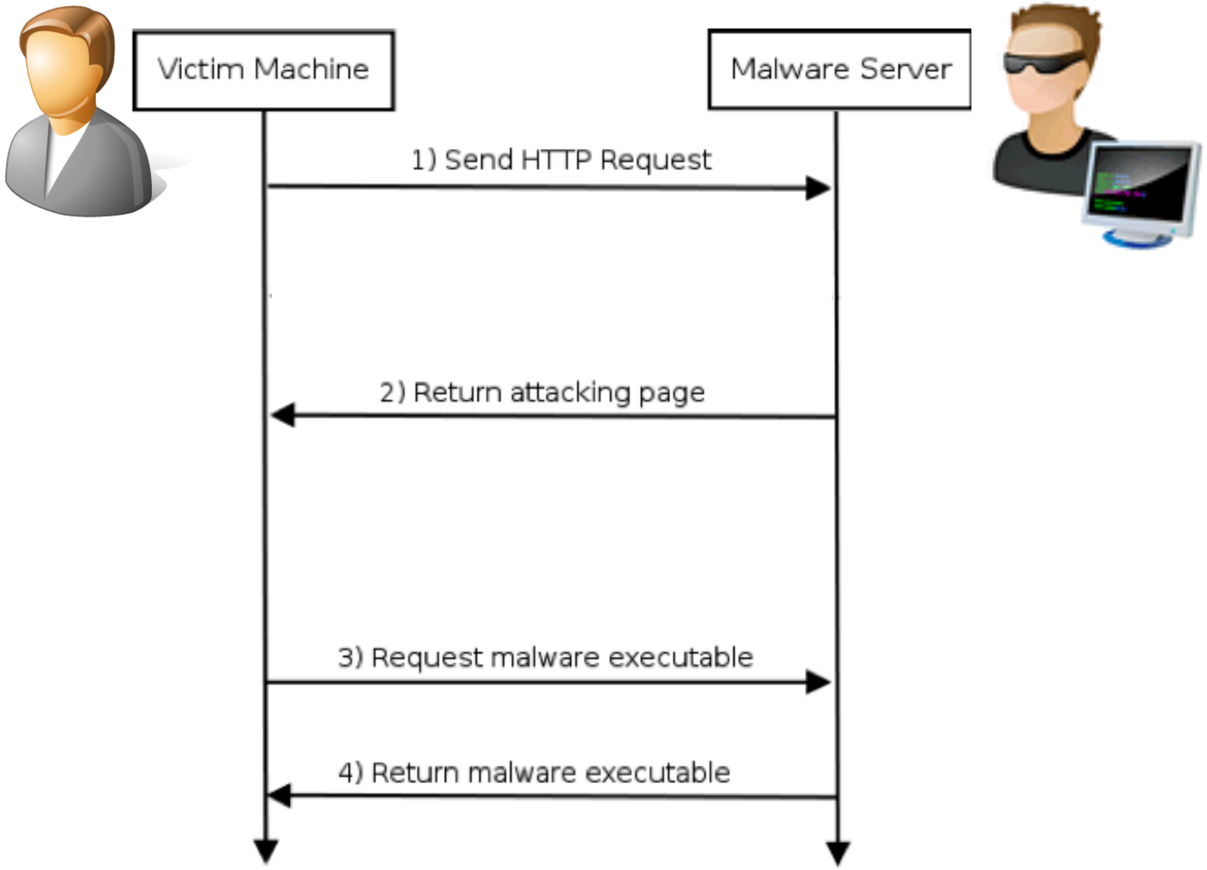
iFrame

Popular website homepage

Exploit Kit/Bad website

User

Drive-by-download attacks



Our question(s) here

- Are black markets relevant for the final user security?
- Does it make sense to use vulnerability information from the black markets to design patching policies?

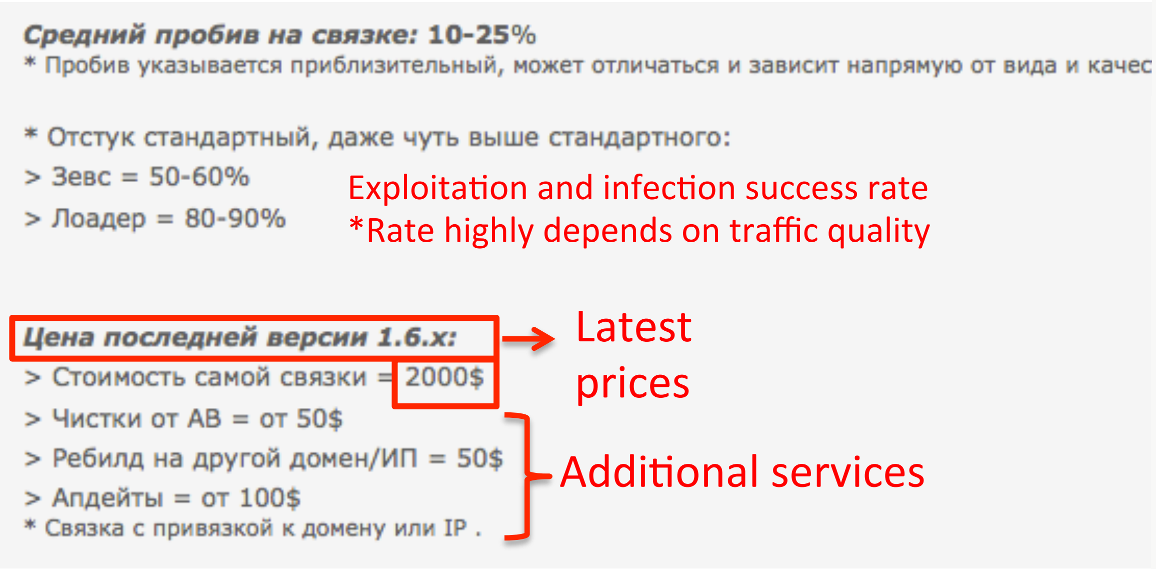
- Two-steps:
  1. Check for relevance of exploit kits vulnerabilities in the general attack scenario
  2. Develop a model to estimate the reduction in risk by using a typical CVSS-based strategy and a BlackMarket-based strategy.

Databases

- NVD: National vulnerability database, universe of vulnerabilities
- EKITS: vulnerabilities traded in the black markets
  - Made in Italy (University of Trento)
  - Substantial expansion on Contagio's Exploit Pack Table
  - Semi-automated retrieval of vulnerability data

Databases

- NVD: National vulnerability database, universe of vulnerabilities
- EKITS: vulnerabilities traded in the black markets
  - Made in Italy (University of Trento)
  - Substantial expansion on Contagio's Exploit Pack Table
  - Semi-automated retrieval of vulnerability data



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

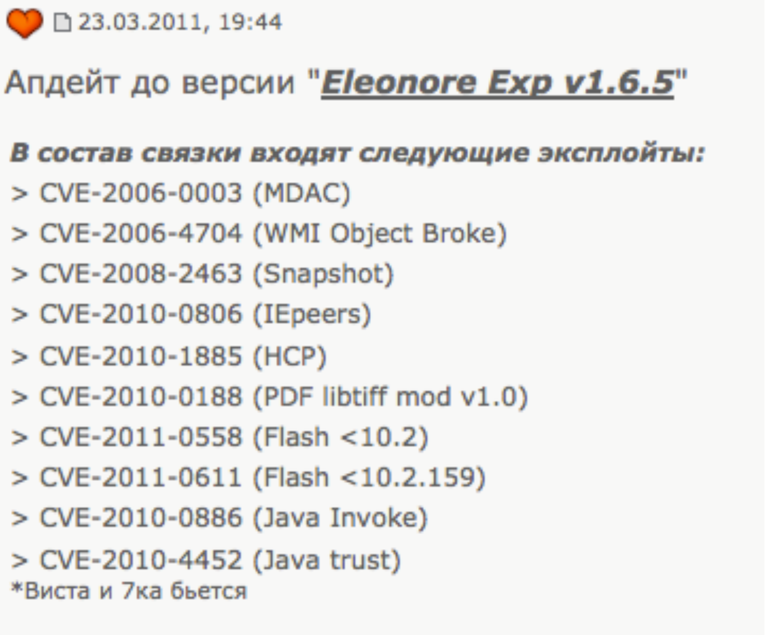
* Отстук стандартный, даже чуть выше стандартного:
> Зевс = 50-60%
> Лоадер = 80-90%

Цена последней версии 1.6.х:
> Стоимость самой связки = 2000$
> Чистки от АВ = от 50$
> Ребилд на другой домен/ИП = 50$
> Апдейты = от 100$
* Связка с привязкой к домену или IP .

Exploitation and infection success rate
*Rate highly depends on traffic quality

Latest prices

Additional services



23.03.2011, 19:44

Апдейт до версии "**Eleonore Exp v1.6.5**"

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

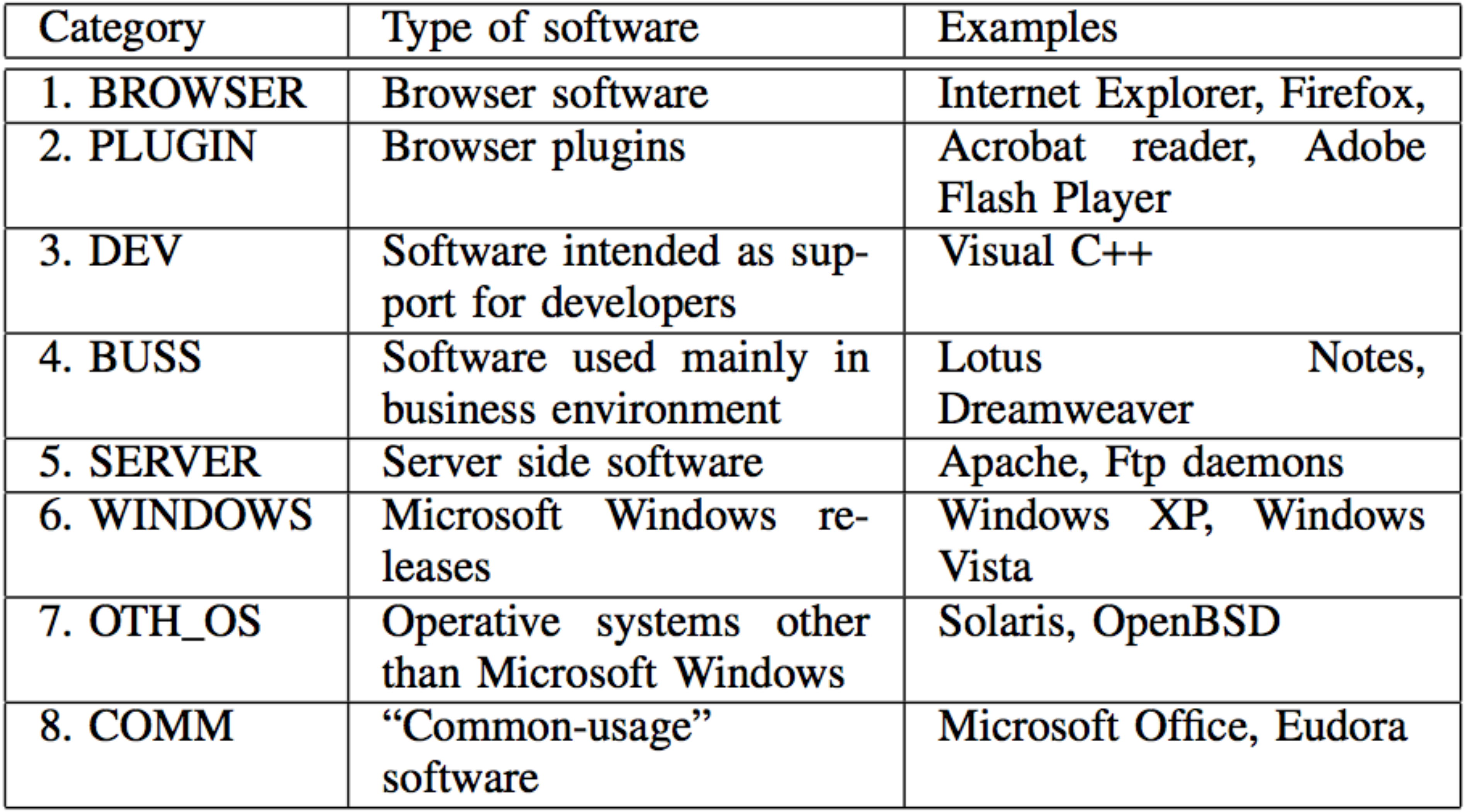
Databases

- NVD: National vulnerability database, universe of vulnerabilities
- EKITS: vulnerabilities traded in the black markets
  - Made in Italy (University of Trento)
  - Substantial expansion on Contagio's Exploit Pack Table
  - Semi-automated retrieval of vulnerability data
  - Monitoring 90+ exploit kits, 1.5yrs
  - 126 vulnerabilities growing

Databases

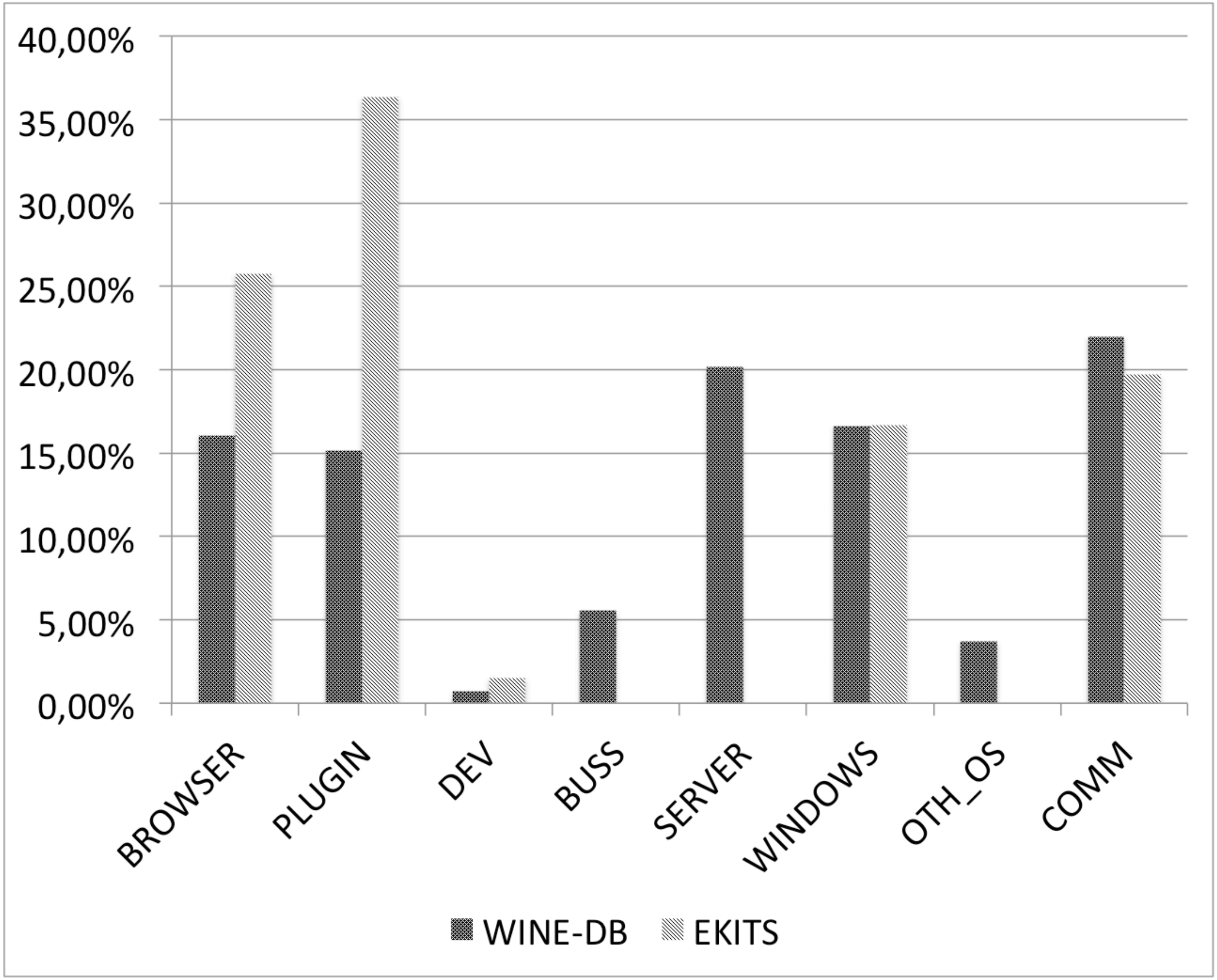
- NVD: National vulnerability database, universe of vulnerabilities
- EKITS: vulnerabilities traded in the black markets
  - Made in Italy (University of Trento)
  - Substantial expansion on Contagio’s Exploit Pack Table
  - Semi-automated retrieval of vulnerability data
  - Monitoring 90+ exploit kits, 1.5yrs
  - 126 vulnerabilities growing
- WINE-DB: attacks delivered in the wild
  - Collaboration with Symantec WINE data sharing programme
  - 600+ exploited vulnerabilities
  - ~10^8 attacks recorded
  - .. However, we have no data on users’ software configurations (other than the OS)

Data categorization

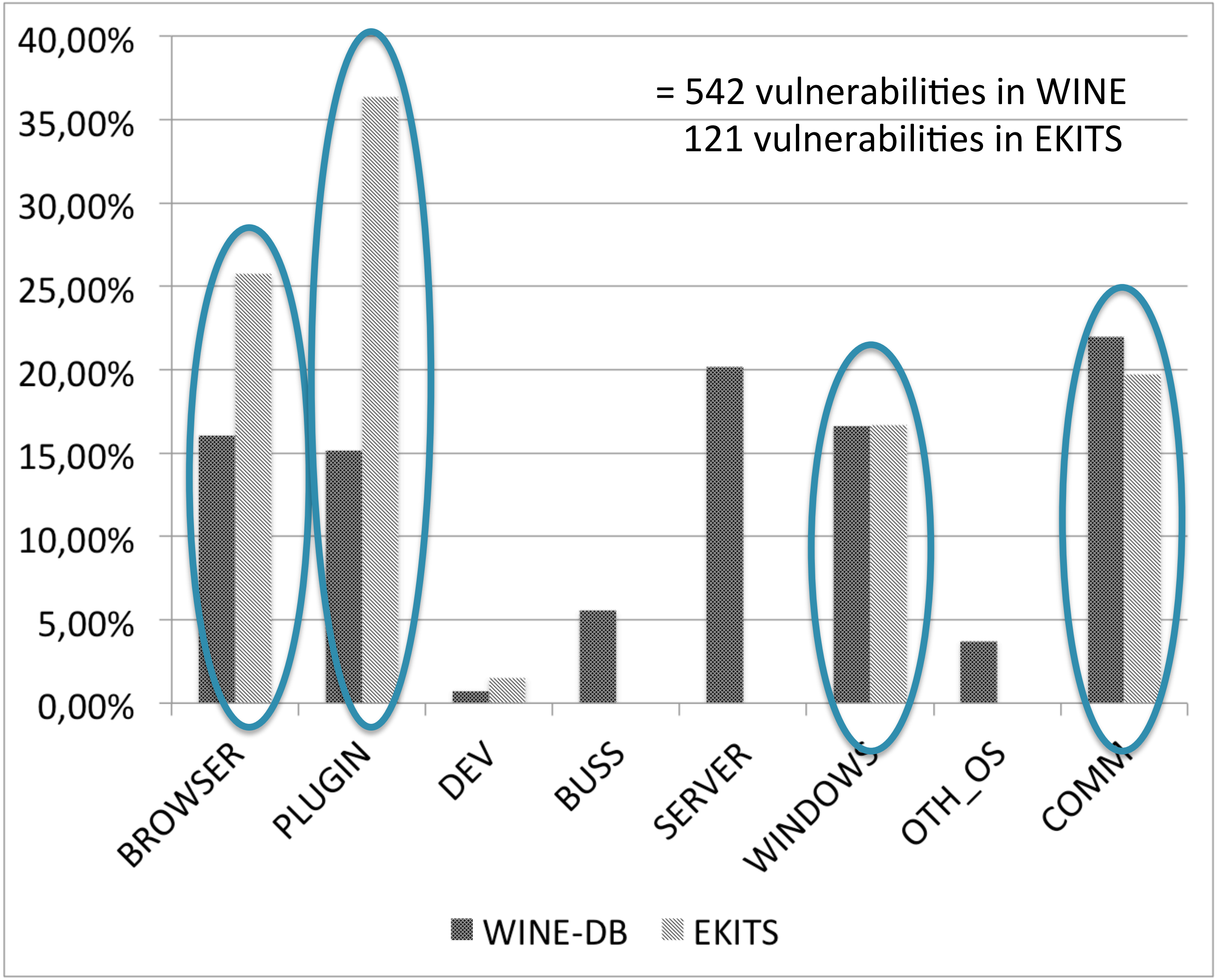


Category	Type of software	Examples
1. BROWSER	Browser software	Internet Explorer, Firefox,
2. PLUGIN	Browser plugins	Acrobat reader, Adobe Flash Player
3. DEV	Software intended as support for developers	Visual C++
4. BUSS	Software used mainly in business environment	Lotus Notes, Dreamweaver
5. SERVER	Server side software	Apache, Ftp daemons
6. WINDOWS	Microsoft Windows releases	Windows XP, Windows Vista
7. OTH_OS	Operative systems other than Microsoft Windows	Solaris, OpenBSD
8. COMM	"Common-usage" software	Microsoft Office, Eudora

Data categorization



Data categorization

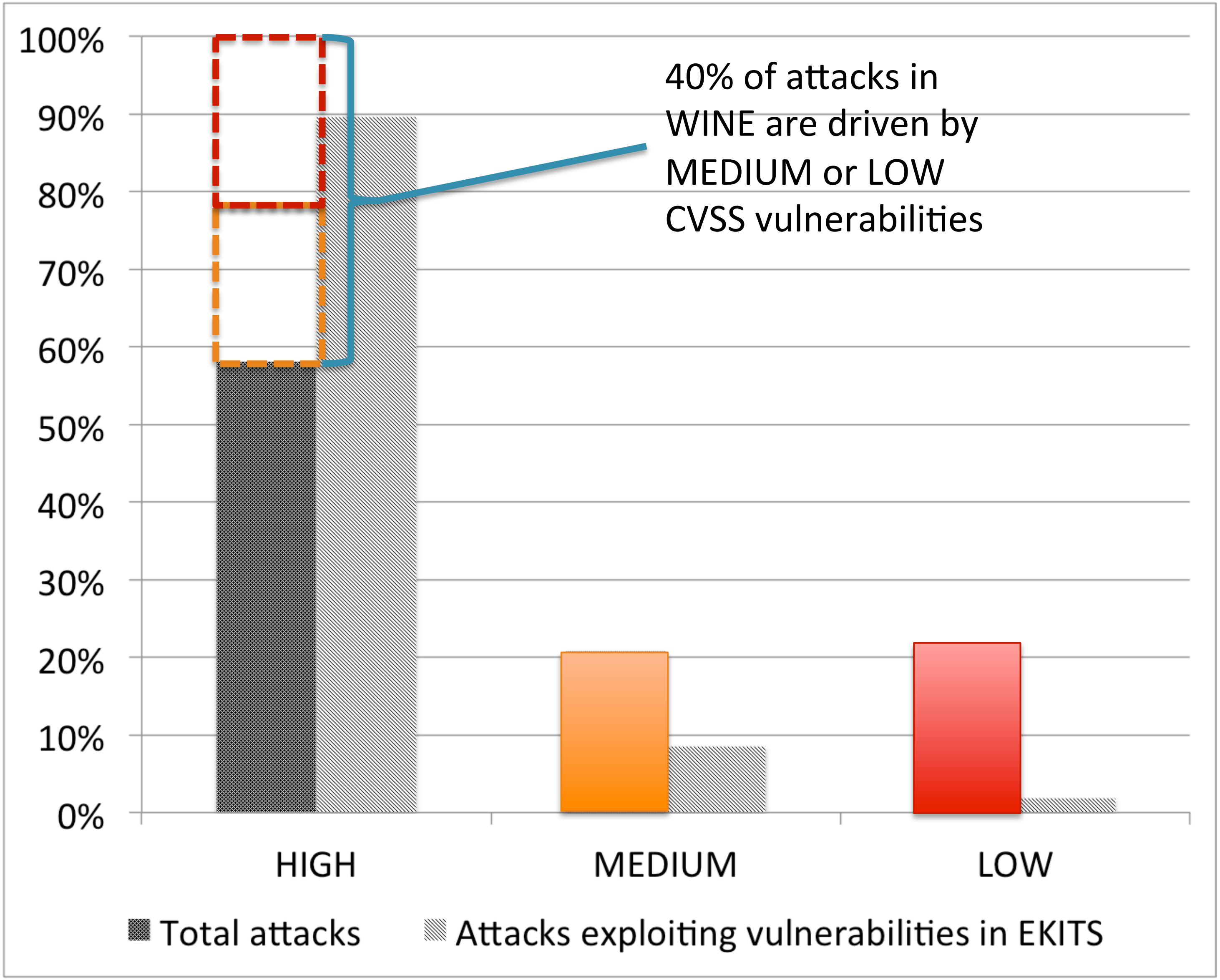


= 542 vulnerabilities in WINE
121 vulnerabilities in EKITS

1. Observational analysis of data

Preliminary: Does CVSS look good?

Preliminary: Does CVSS look good?

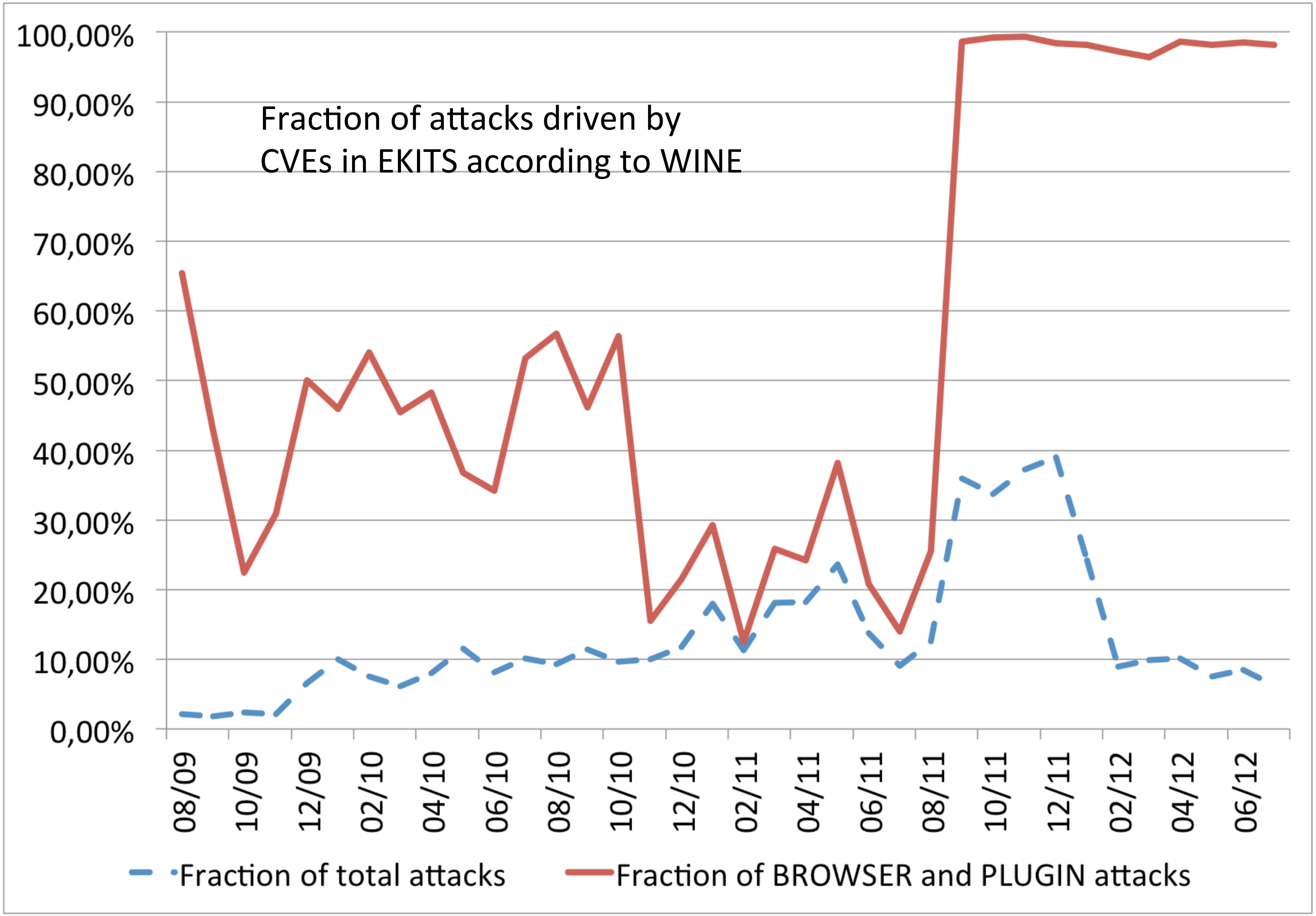


40% of attacks in WINE are driven by MEDIUM or LOW CVSS vulnerabilities

Preliminary: Do ekits look interesting? (1)

- Fraction of attacks driven by CVEs in EKITS according to WINE
- Relative probability of receiving an attack by means of a vulnerability in EKITS rather than one NOT in EKITS

Preliminary: Do ekits look interesting? (1)



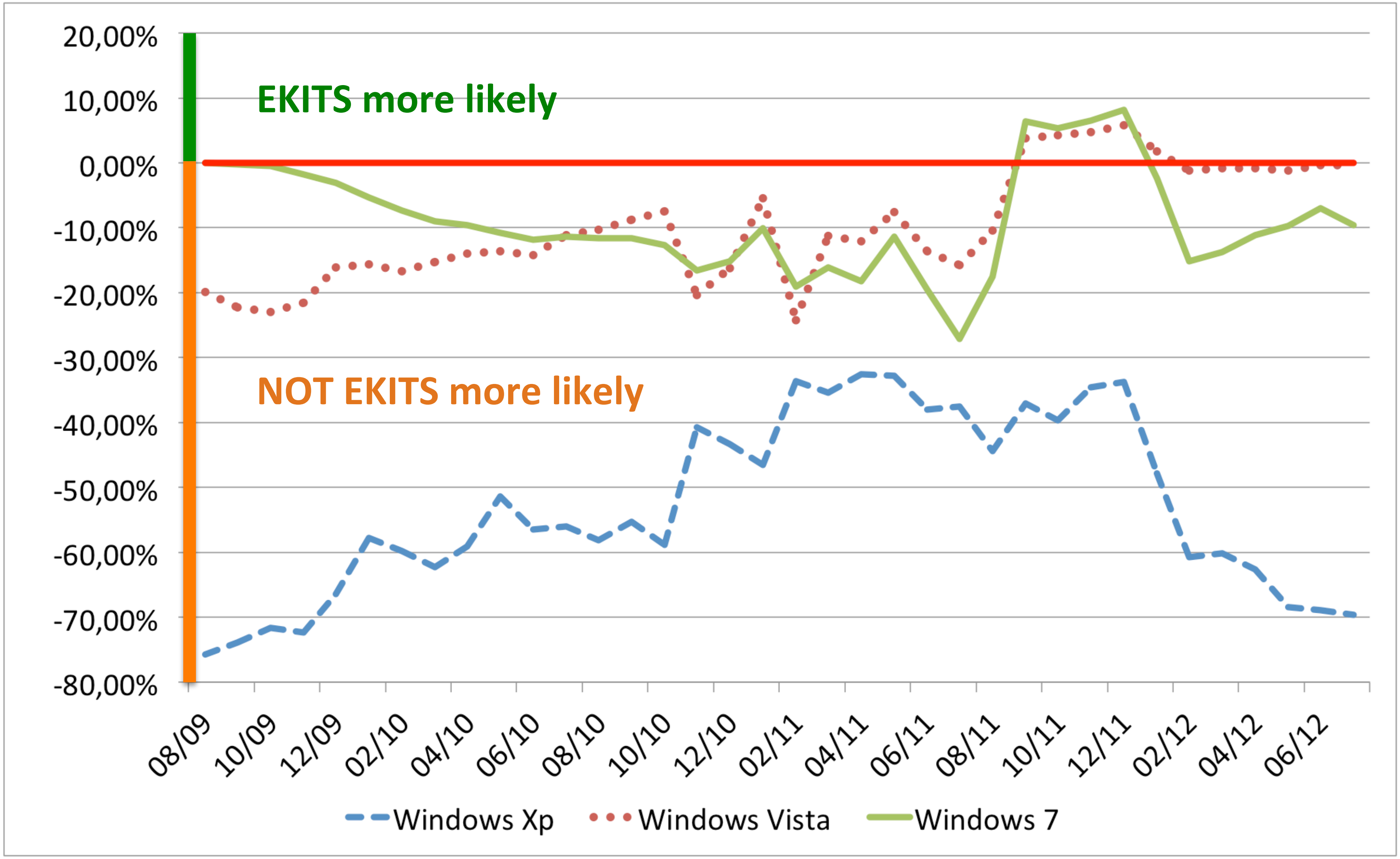
Preliminary: Do ekits look interesting? (2)

- Fraction of attacks driven by CVEs in EKITS according to WINE
- Relative probability of receiving an attack by means of a vulnerability in EKITS rather than one NOT in EKITS
  - Breakdown by operating system

$$\Pr(v \text{ in EKITS} \mid \text{attack}) - \Pr(v \text{ not in EKITS} \mid \text{attack})$$

Preliminary: Do ekits look interesting? (2)

Relative probability of receiving an attack by means of a vulnerability in EKITS rather than one NOT in EKITS



Preliminary conclusions

- CVSS does a good job but leaves 40%+ of the attacks uncovered
- Vulnerabilities in exploit kits drive between 10% and 40% of attacks received by the final users
- Exploit kit vulnerabilities dominate the scenario for attacks against browsers and plugins
- Probability of exploitation of vulnerabilities in EKITS (121) is comparable to ~EKITS (421)

2. Does it make sense to use vulnerability information from the black markets to design patching policies?

The method

- A patching strategy is like safe belt usage
  - Does not assure you do not die in a car accident
  - But decreases your chances of dying by X% (seatbelts: ~43% according to [Evans 1986])

- We paraphrase and adapt Evans' methodology
  - Strategy to select vulnerability to be fixed -> wearing seatbelt
  - You receive an attack -> you have a car crash
  - You are not patched and get infected -> crash is fatal

The method (1)

- “Patching effectiveness” = decrease in attacks if policy A is enforced instead of policy B
  - A = High risk vulnerabilities are patched
  - B = Low risk vulnerabilities are patched

- CVSS case:
  A. High risk = vulnerability has HIGH CVSS
  B. Low risk = vulnerability has LOW+MEDIUM CVSS

- EKITS case:
  A. High risk = vulnerability is in the black markets
  B. Low risk = vulnerability is not in the black markets

The method (2)

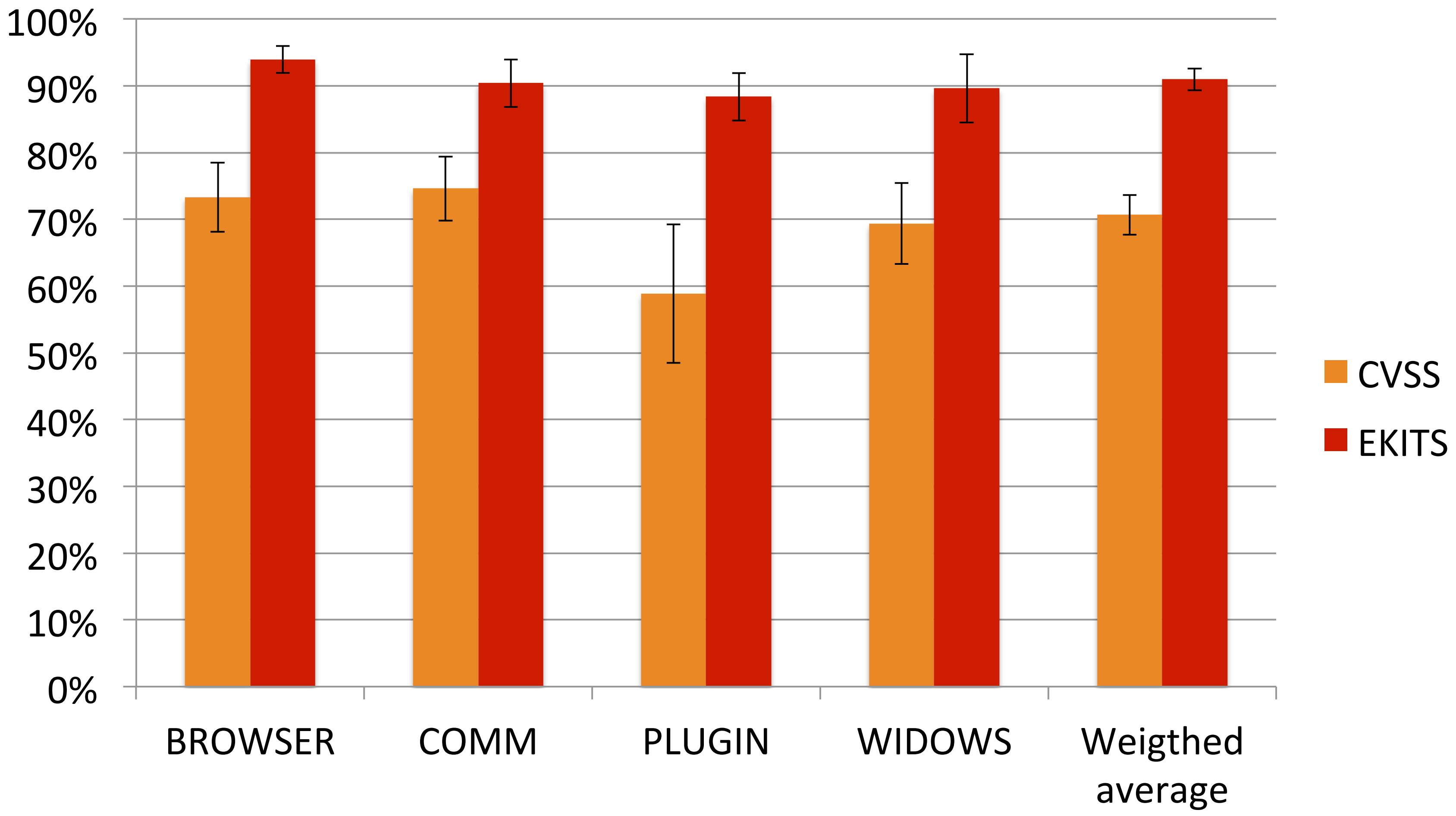
- “If I were to enforce patching policy A, how many less attacks than with B would I receive?”

- General formulation:

$$\Pr(attack \mid risk.type = B) / \Pr(attack \mid risk.type = A)$$

- Two assumptions
  - A user may be affected by any vulnerability in NVD
  - WINE-DB includes all exploits in the wild, that can be used by any attacker with the same probability

Results: Effectiveness



Conclusions

- Cybercrime black markets are an important source of risk for the final user
- Active and efficient monitoring of the markets may lead to more efficient patching strategies
- Efficacy of patching strategies seems to vary with the "category" of the vulnerable software
  - There may be a need for "ad-hoc" policies for different software products

Questions

If you have any further enquiry / comment:

allodi@disi.unitn.it
massacci@disi.unitn.it
shim@disi.unitn.it

http://securitylab.disi.unitn.it

Thanks