

Online security or insecurity: The current threat landscape

Nikolaos Tsalis

November 2015

Online security or insecurity: The current threat landscape



Nikolaos Tsalis (ntsalis@aueb.gr)

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business

Background Info

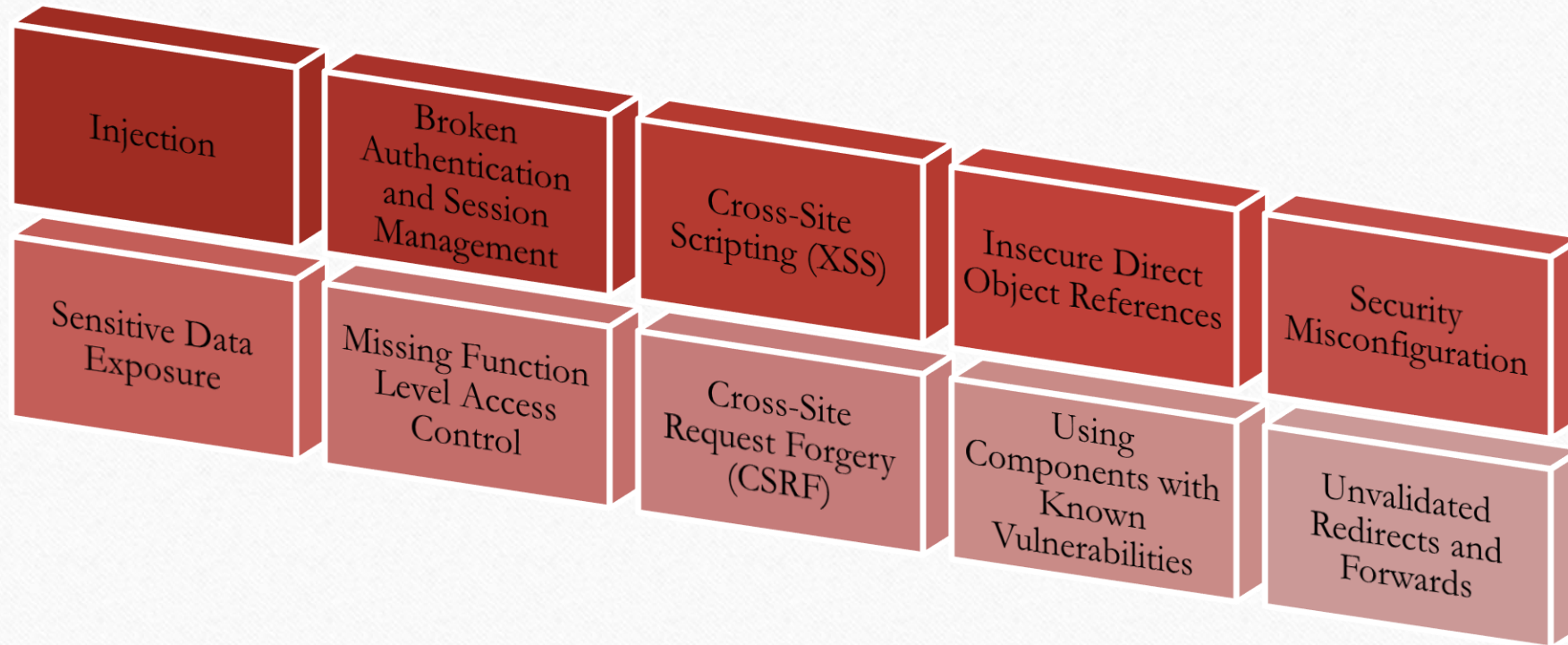
- **Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory**
 - Dept. of Informatics, Athens University of Economics & Business, Greece
- **Research topics**
 - Critical Information Systems Security
 - Web Security
 - Cloud Computing
 - Smartphone Forensics
 - Security and Privacy in Online Social Networks

Topics at a glance



1. **Introduction**
2. **Part 1 – Browser Controls**
 - Methodology
 - Proposed categorization
 - Results
3. **Part 2 – Security and privacy add-ons**
 - Methodology
 - Observations
 - Proposed categorization
 - Results
4. **Part 3 – Phishing and malware protection**
 - Methodology
 - Results
5. **Conclusions**

OWASP Top 10



What about the average user?

- Does she know **if** there are any **available** security mechanisms?
- Does she know **which** are they?
- Does she know **how to use** them properly?
- ...
- Are they **effective**?

Tested browsers



Windows 7

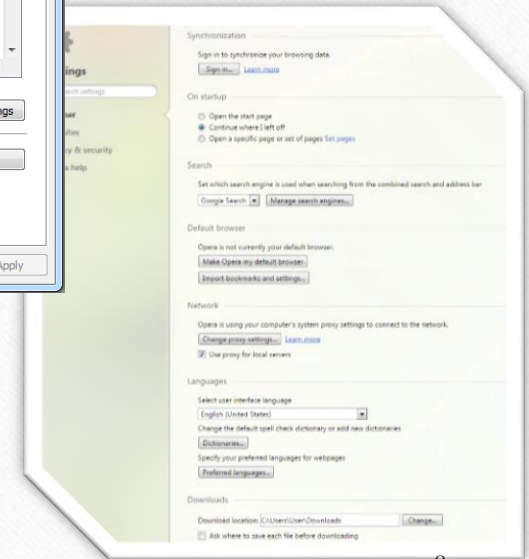
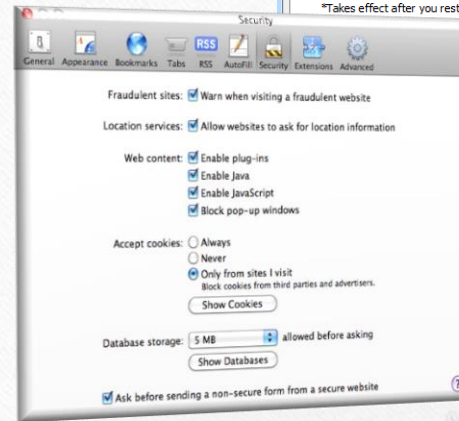
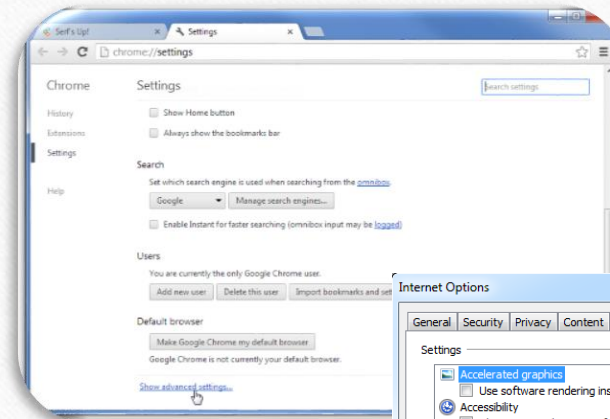
Part 1

Methodology

Browser controls (n=32)

Enumeration of browsers':

- graphical interfaces and
- available hidden menus – if any – e.g. *"about:config"* in Mozilla Firefox



Proposed categorization

Content controls

Block cookies

Block images

Block pop-ups

Privacy controls

Block location data

Block referrer

Block third-party cookies

Enable DNT

History manager

Private browsing

Browser management controls

Browser update

Certificate manager

Master password

Proxy server

Search engine manager

SSL/TLS version selection

Task manager

Third-party software controls

Auto update extensions

Auto update plugins

Disable extension

Disable Java

Disable JavaScript

Disable plugin

External plugin check

Manually update extensions

Manually update plugins

Web browsing controls

Certificate warning

Local blacklist

Malware protection

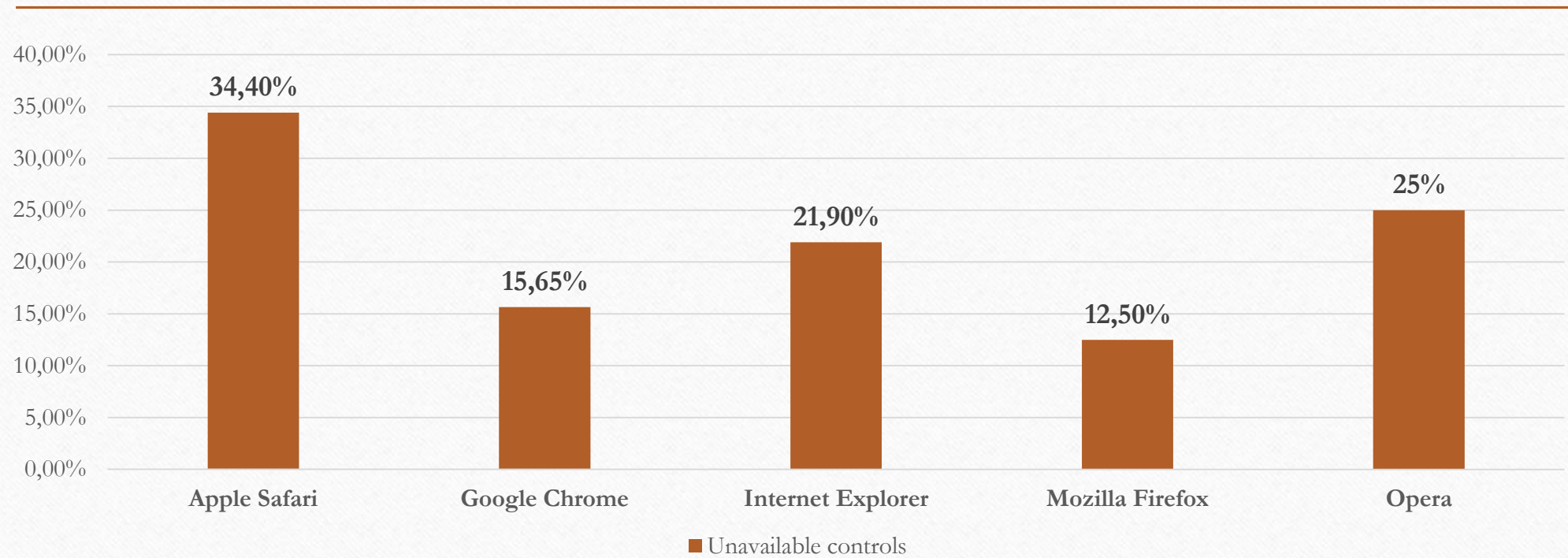
Modify user-agent

Phishing protection

Report rogue Website

Website checking

Results



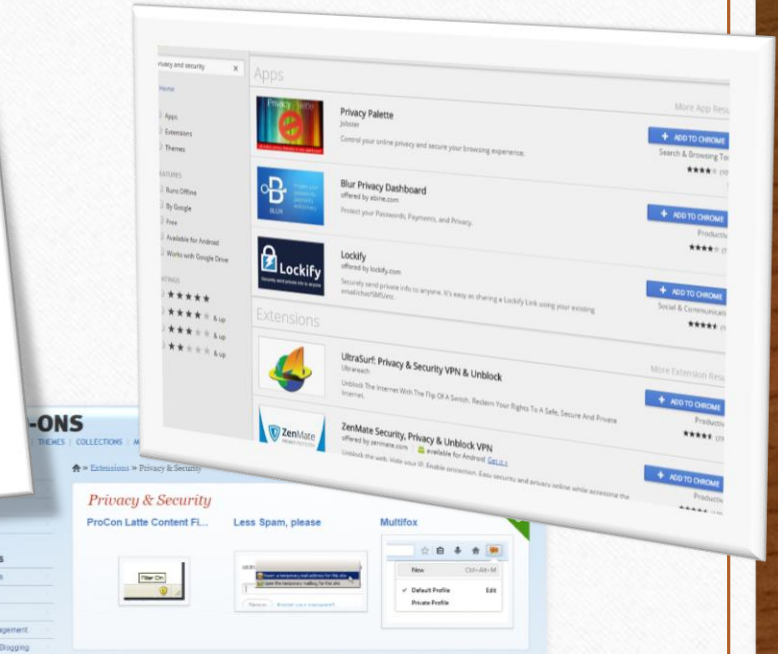
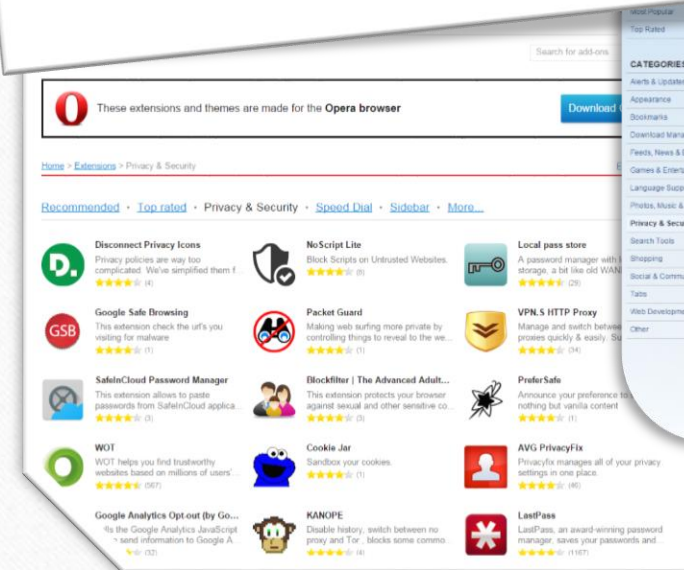
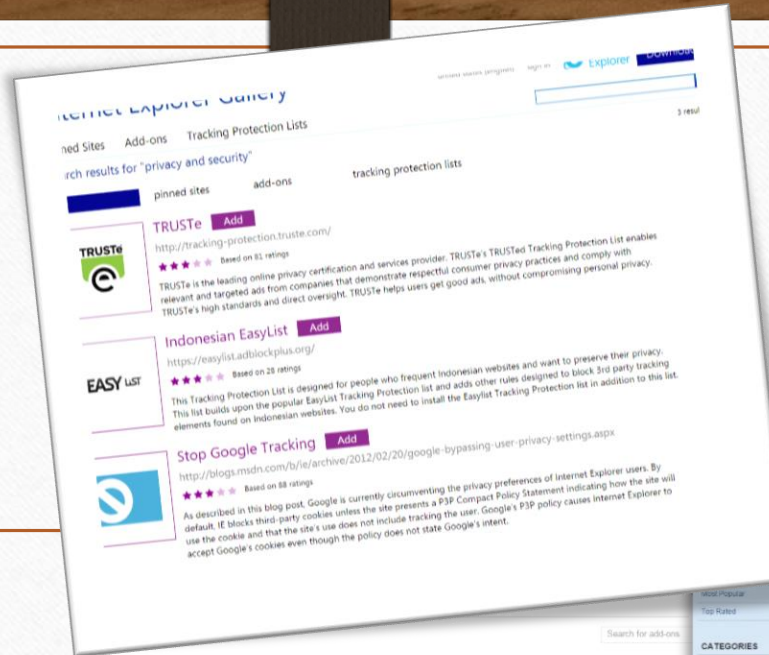
Part 2

Methodology

Browser add-ons (n=227)

Enumeration of browsers' security and privacy add-ons, that were available in each repository.

Browser	No
Safari	38
Chrome	N/A (65)
Internet Explorer	7
Firefox	1327 (65)
Opera	52



Observations

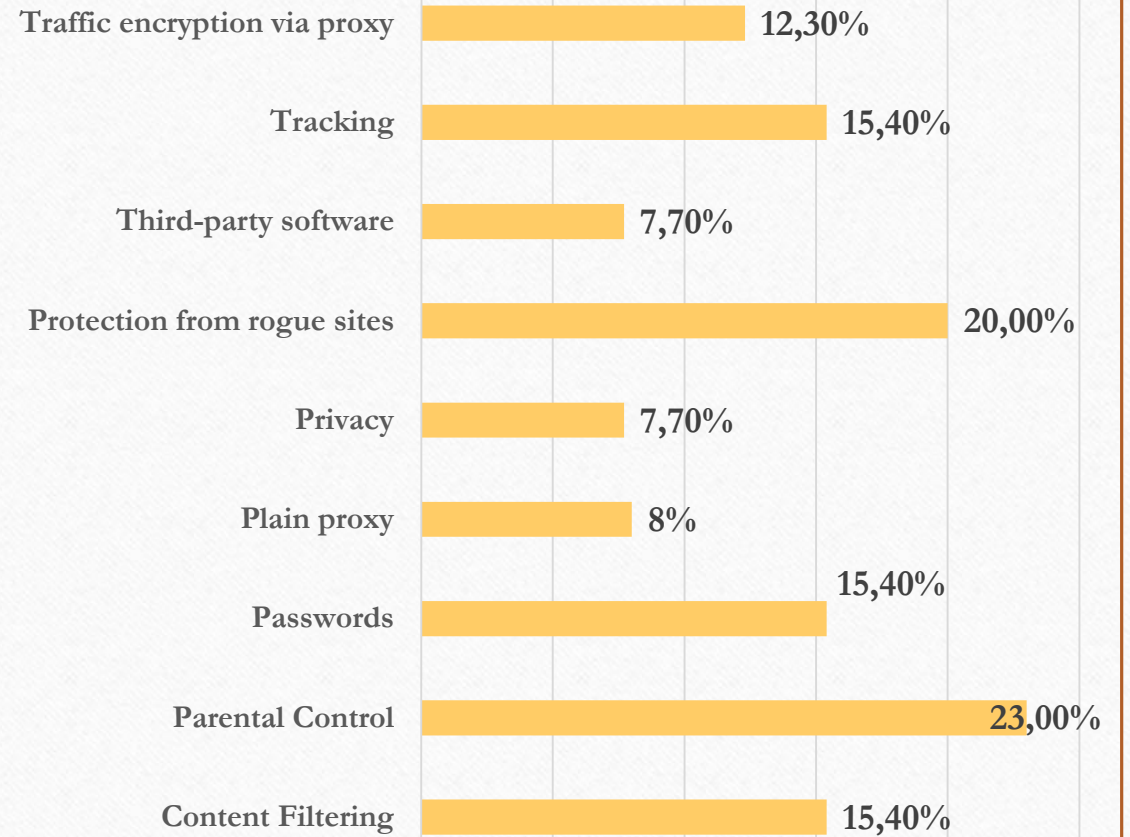
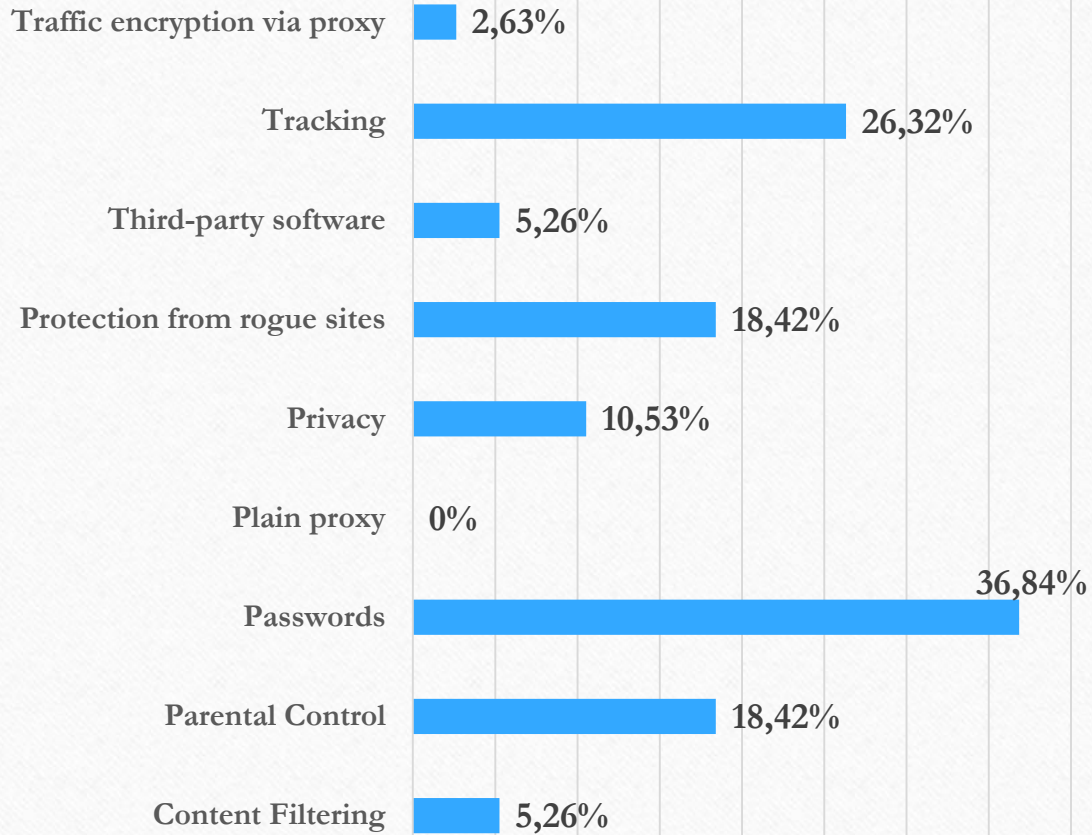
- **Variety** of available add-ons for each browser
- **Confusing grouping** of add-ons in repository

1 st level categorization	2 nd level categorization
Safari	None
Firefox	
Opera	

Proposed Categorization

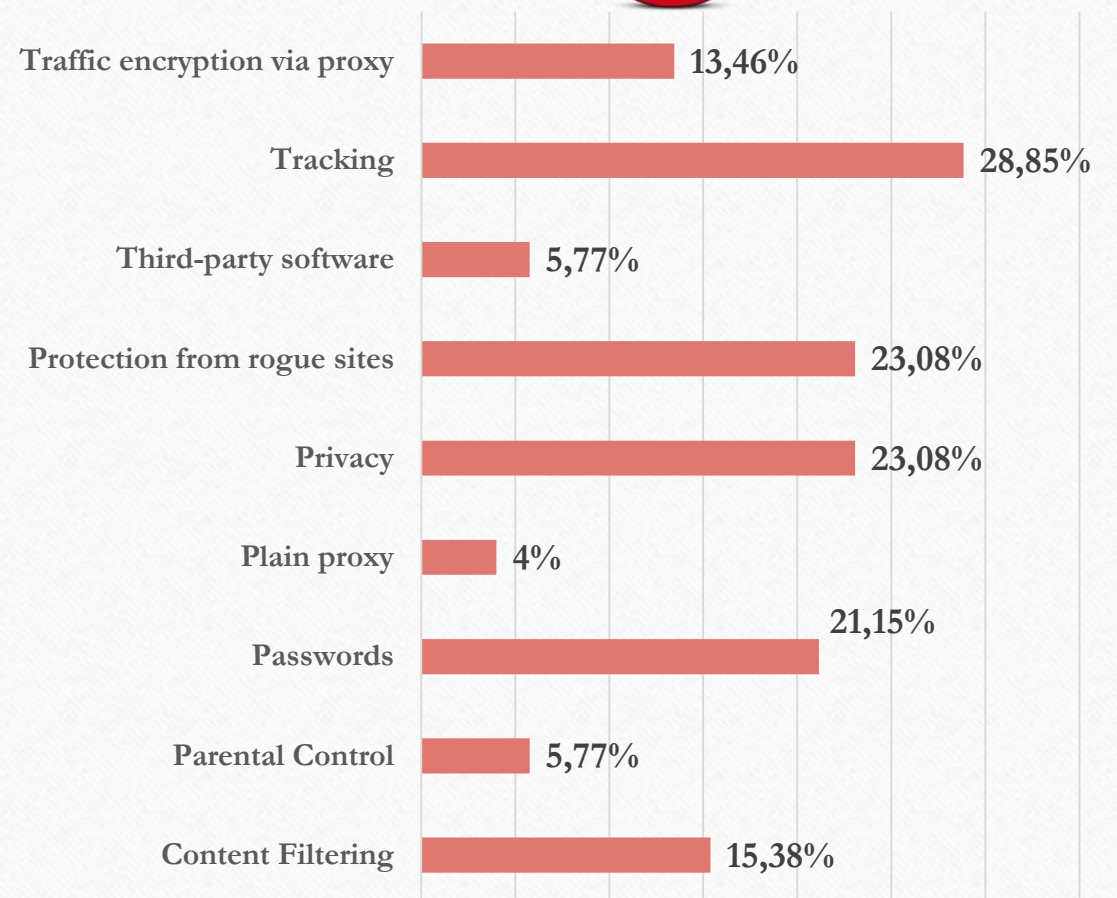
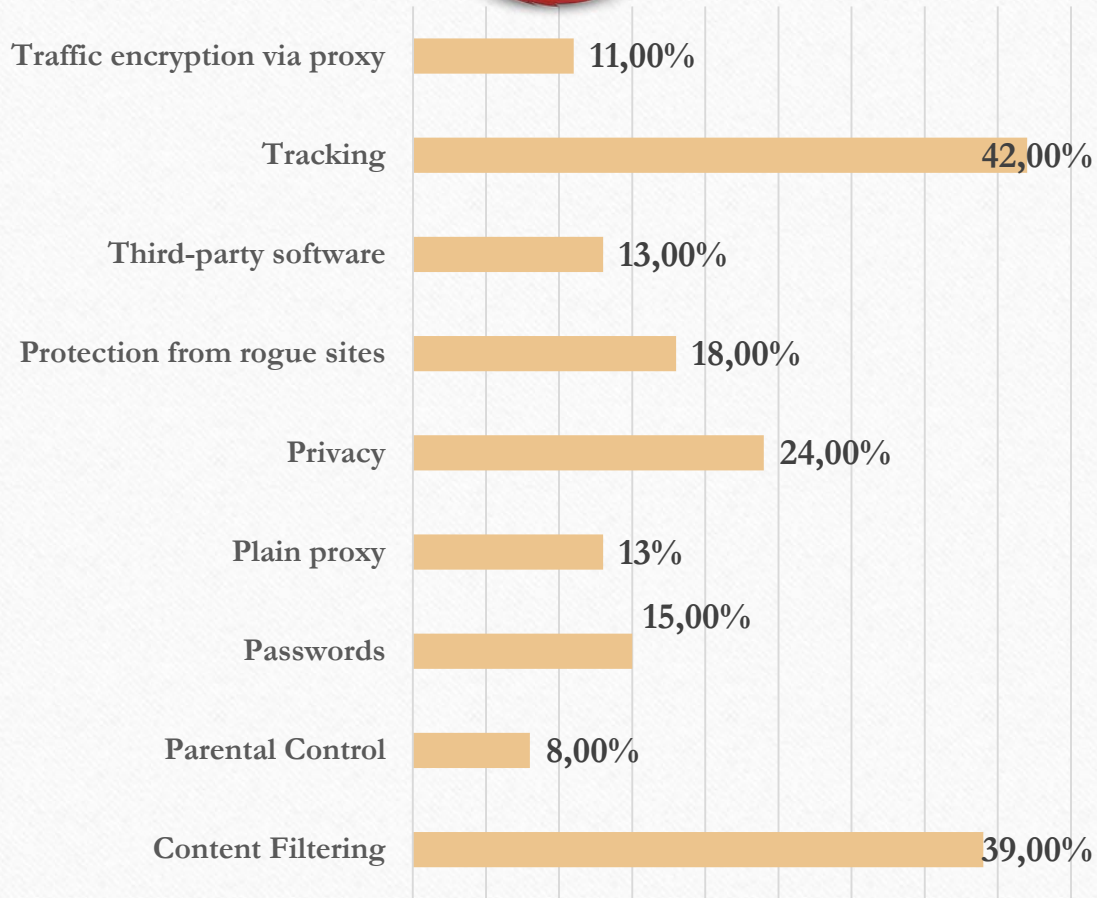
- 1. Content filtering:** Block content (advertisements, cookies, images, pop-ups, etc.)
- 2. Parental control:** Includes traffic filters to block websites containing inappropriate material
- 3. Passwords:**
 - Generators
 - Managers
- 4. Plain proxy:** Simple proxy without any encryption included
- 5. Privacy:** Privacy protection add-ons (e.g. privacy settings manager)
- 6. Protection from rogue websites:**
 - Antivirus blacklists
 - Malware blacklists
 - Phishing blacklists
 - Reputation blacklists
 - Sandbox
- 7. Third-party software management:** Blocking third-party software (e.g. Flash, Java, JavaScript, etc.)
- 8. Tracking:** Blocking website(s) that track user's online behavior
 - Social Media (SM) redirection
- 9. Traffic encryption via proxy:** Proxy that encrypts user's traffic

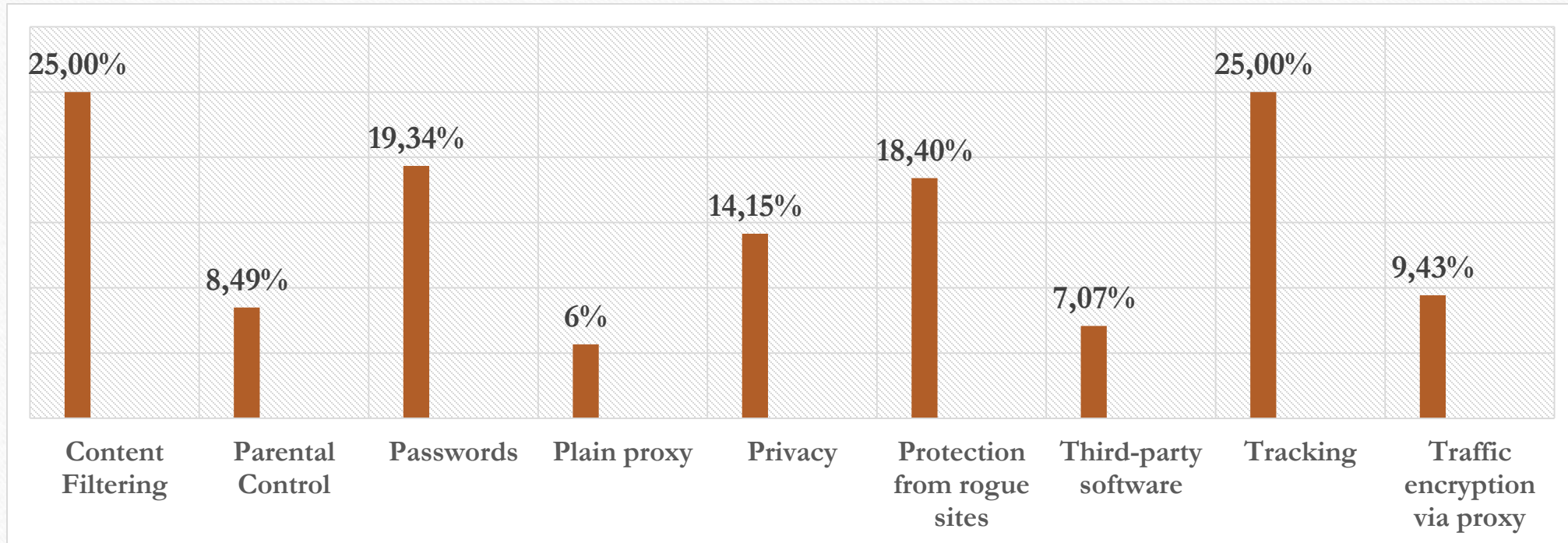
Results





Results





Part 3

Methodology

Phishing and malware protection

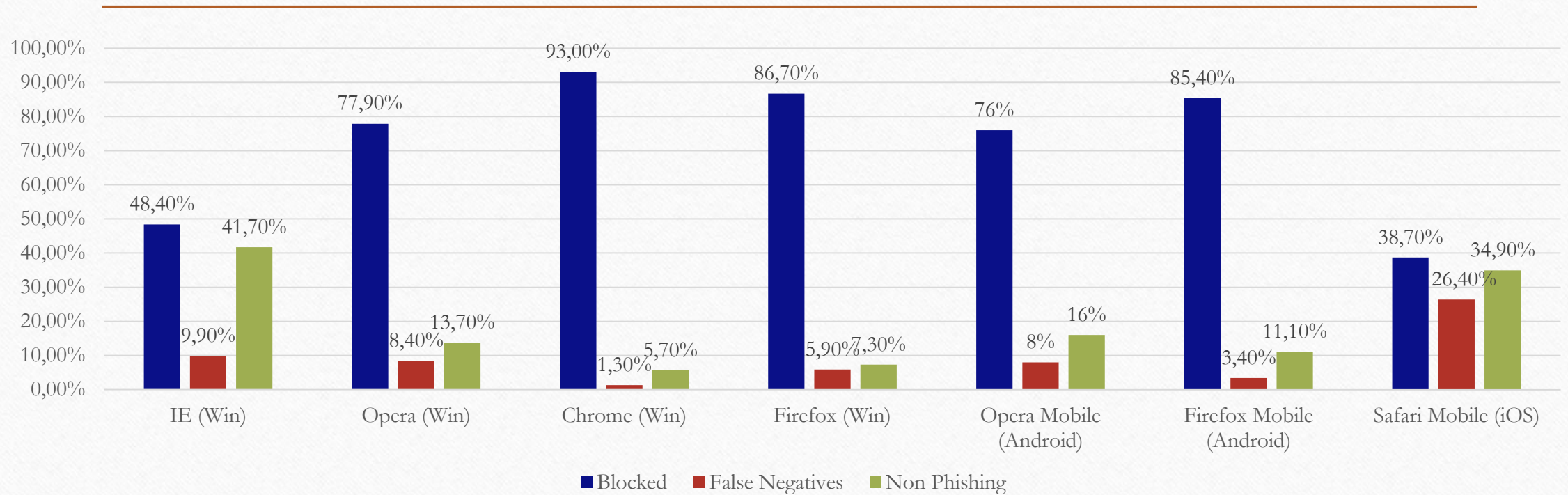
- To evaluate the protection against **phishing attacks**, we collected phishing URLs that were reported by PhishTank.
- To evaluate the protection against **malware attacks**, we used the open source “Collective Intelligence Framework” (CIF), which allows the collection and analysis of malicious threat information from a large number of trusted sources



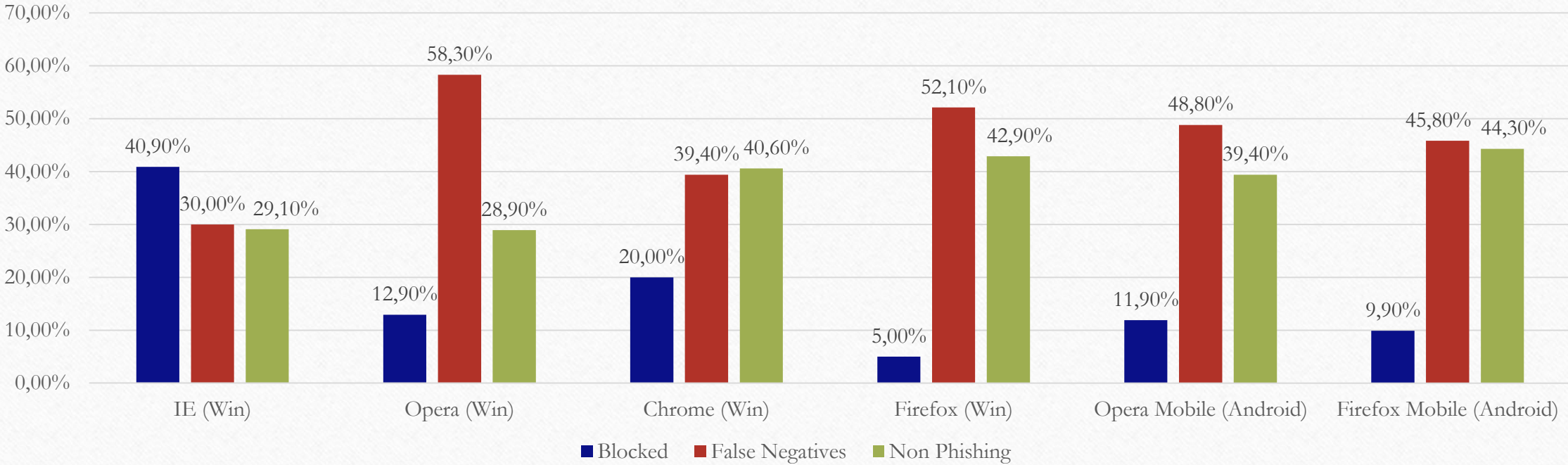
Browser	iOS 7.0.4	Android 4.0.4	Windows 7
Safari Mobile	X		
Chrome Mobile	X	X	
Opera Mini	X	X	
Browser [†]		X	
Firefox Mobile		X	
Opera Mobile		X	
Chrome			X
Firefox			X
Internet Explorer			X
Opera			X

[†] 'Browser' is the pre-installed browser in Android

Phishing URL Detection



Malicious URL Detection



Conclusions

- There is an **adequate amount** of controls available for the average user
- Although, it is still **unclear** if:
 - Alice knows **which** are they
 - **how to use** them and
- **If** these mechanisms **offer a proper level** of protection

All comes down to the user...

“

*I am regularly asked what average Internet users
can do to ensure their security.
My first answer is usually, “Nothing -- you're screwed.”*

”

Bruce Schneier

References

1. Theoharidou, M., Tsalis, N., Gritzalis, D., “In Cloud we trust: Risk-assessment-as-a-service”, in *Proc. of the 7th IFIP International Conference on Trust Management*, pp. 100-110, Springer (AICT 401), Spain, 2013.
2. Tsalis N., Mylonas A., Gritzalis D., “An intensive analysis of the availability of security and privacy browser add-ons”, in *Proc. of the 10th International Conference on Risks and Security of Internet and Systems (CRISIS-2015)*, Springer (LNCS), Greece, 2015.
3. Tsalis N., Virvilis N., Mylonas A., Apostolopoulos A., Gritzalis D., “Browser blacklists: A utopia of phishing protection”, in *Security and Cryptography*, M. Obaidad and A. Holzinger (Eds.), Lecture Notes (CCIS), Springer, 2015.
4. Tsalis, N., Theoharidou, M., Gritzalis, D., “Return on security investment for Cloud platforms”, in *Proc. of the Economics of Security in the Cloud Workshop*, pp.132-137, IEEE Press, United Kingdom, 2013.
5. Virvilis N., Mylonas A., Tsalis N., Gritzalis D., "Security busters: Web browser security vs. rogue sites", *Computers & Security*, Vol. 52. pp. 90-105, July 2015.
6. Virvilis, N., Tsalis, N., Mylonas, A., Gritzalis, D., "Mobile devices: A phisher's paradise", in *Proc. of the 11th International Conference on Security and Cryptography (SECRYPT-2014)*, pp. 79-87, ScitePress, Austria, 2014.