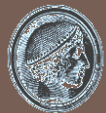


Security and privacy in the smartphone ecosystem: Final progress report

Alexios Mylonas



Athens University of Economics & Business



European Union
European Social Fund



Co- financed by Greece and the European Union



Overview

2

- Research Motivation
- Related work
- Objective
- Approach
 - ▣ Methodology
 - ▣ Threat model
 - ▣ Smartphone definition & data
- Contribution
 - ▣ Browser controls
 - ▣ User practices
 - ▣ Malware mitigation
 - ▣ Smartphone forensics
- Future work

Research Motivation

3

- Smartphone ecosystem facts:
 - Increase
 - Popularity of *devices*
 - Installations of *third-party apps*
 - *web browsing*
 - Great source of personal and business data



- Smartphones appealing target for attackers

Related work

4

- Android-centered & focused on malware mitigation
- Permission system
 - ▣ Policies, all-or-nothing
- Static analysis
 - ▣ e.g. static analysis on manifest
- Dynamic analysis
 - ▣ e.g. Taint analysis

Related work

4

- Android-centered & focused on malware mitigation
- Permission
 - Permission
- Static
 - m
- Dynamic analysis
 - Taint analysis
 - Instrumentation

Problem:

1. Require advanced technical skills!

Related work

4

- Android-centered & focused on malware mitigation
- Permission-based
 - Policy-based
- Static analysis
 - machine learning
- Dynamic analysis
 - Taint analysis
 - Instrumentation

Problem:
1. Require advanced technical skills!



Related work

4

- Android-centered & focused on malware mitigation
- Permission

 - ▣ Po

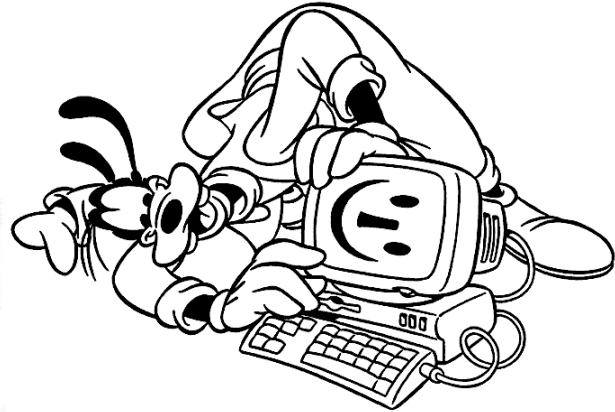
- Static

 - ▣ m

- Dynamic

 - ▣ Te
 - ▣ In

Problem:
1. Require advanced technical skills!



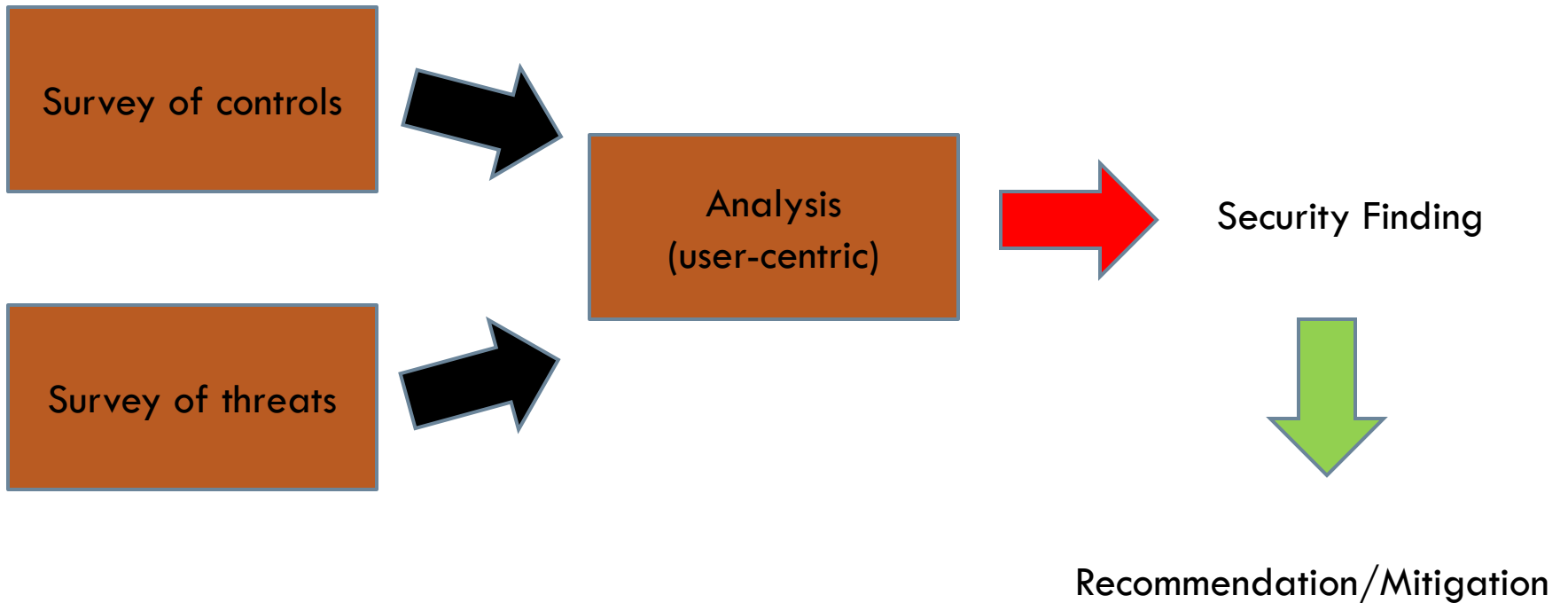
Objectives

5

- Study user practices
 - ▣ adoption of security controls
- User-centric protection
 - ▣ Include user input in our approach
 - Users value their data types differently
- Case study: Smartphone forensics

Methodology

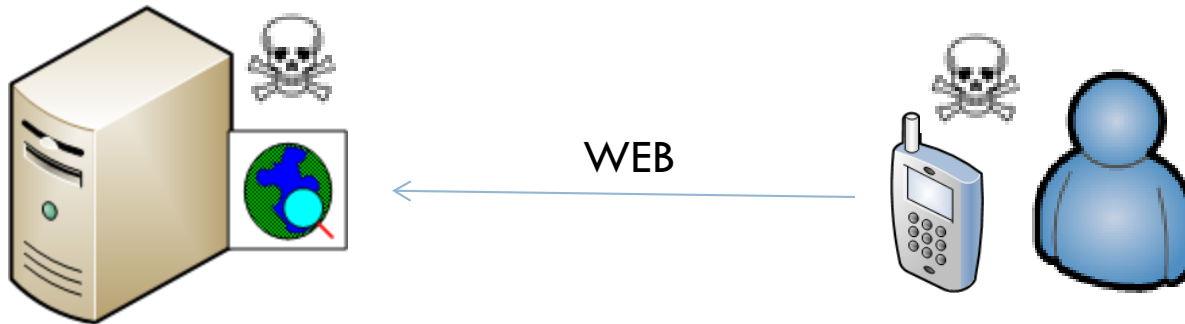
6



Threat model

7

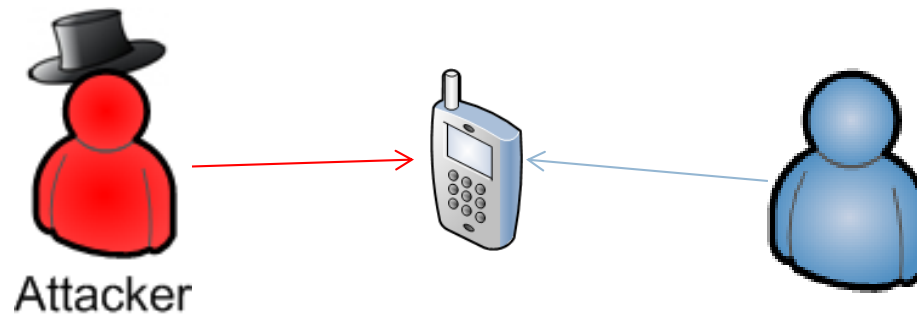
T1. Malicious web (servers)



Threat model

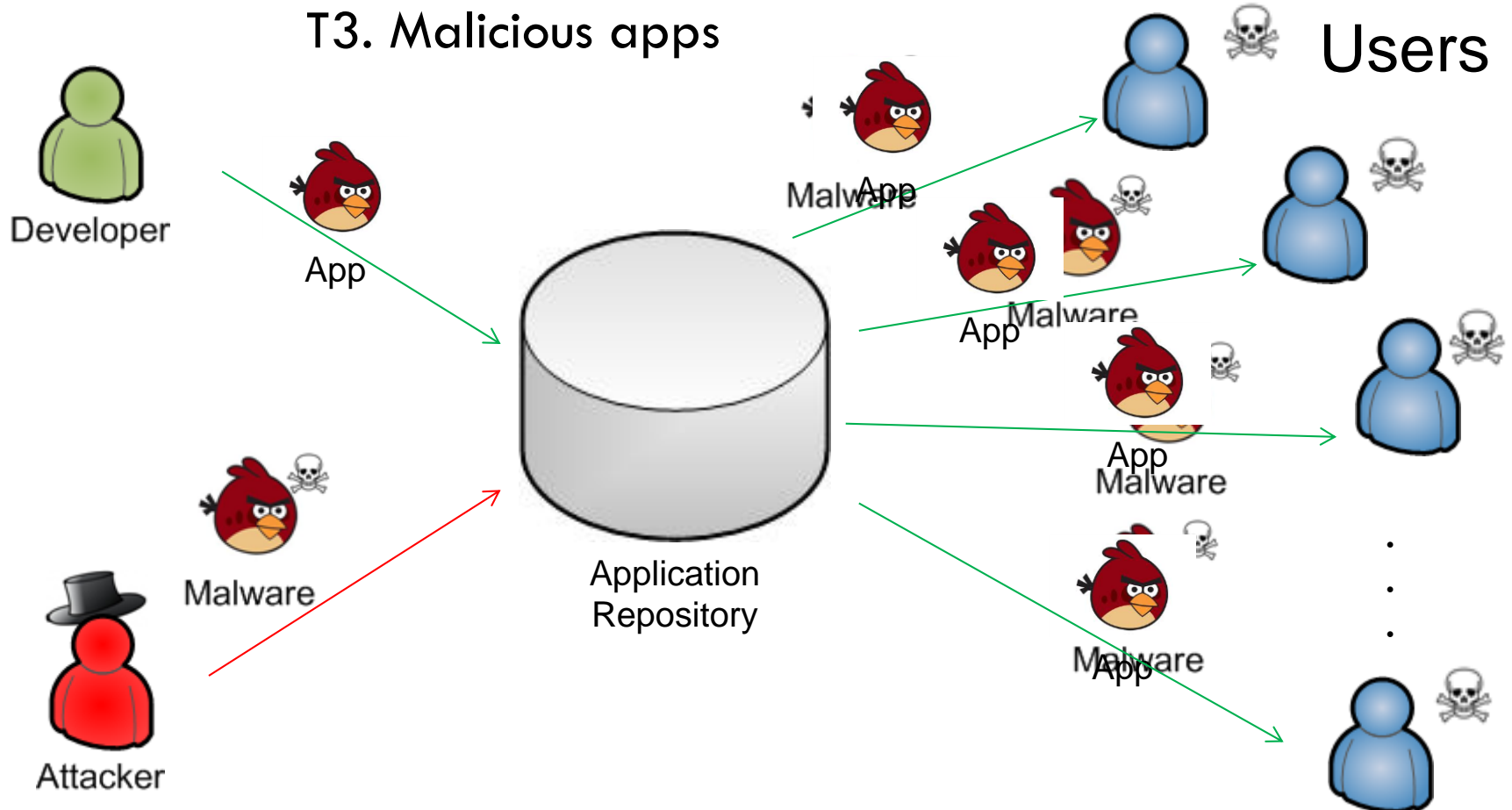
7

T2. Physical access



Threat model

7



A smartphone?

8

Cell\feature phone

- used to access mobile network carrier services
- contains a smartcard

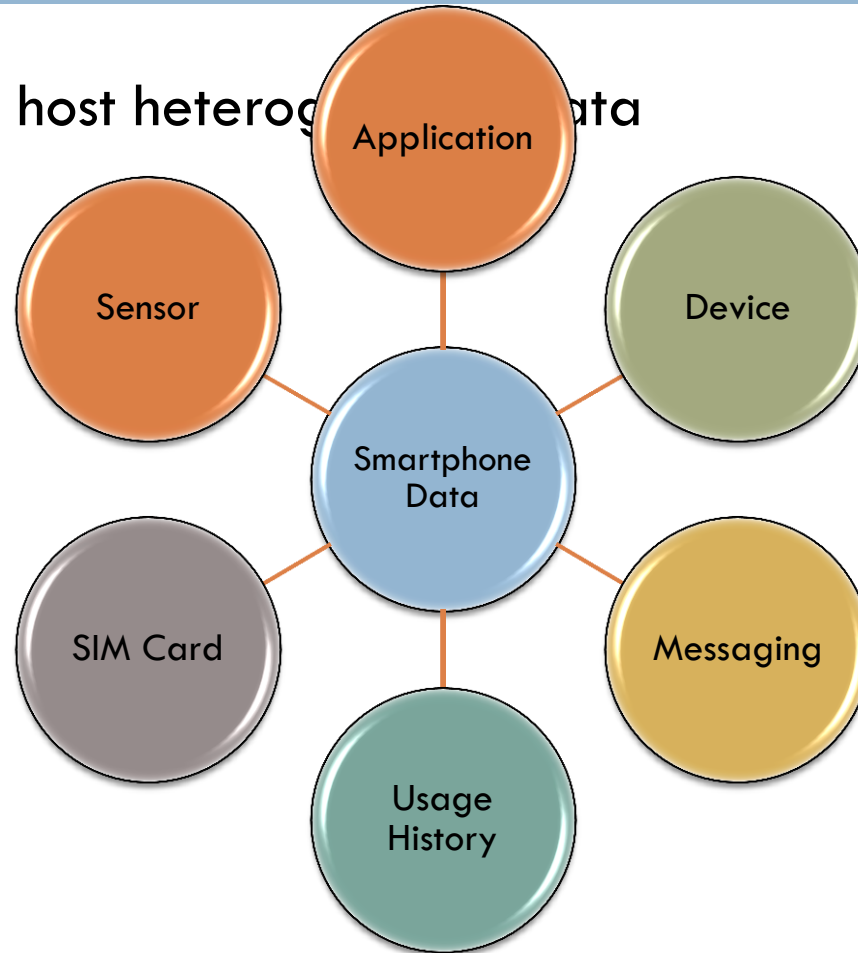
Smartphone

- a *cell phone*
- advanced hardware capabilities
- an identifiable OS
- supports 3rd-party apps
- apps from app repository

Smartphone Data

8

- Smartphones host heterogeneous data



C4. Mylonas A, Meletiadis V, Tsoumas B, Mitrou L, Gritzalis D. Smartphone forensics: A proactive investigation scheme for evidence acquisition. In: 27th IFIP International Information Security and Privacy Conference. Springer; AICT-376; 2012. p. 249–260.

Browser controls

9

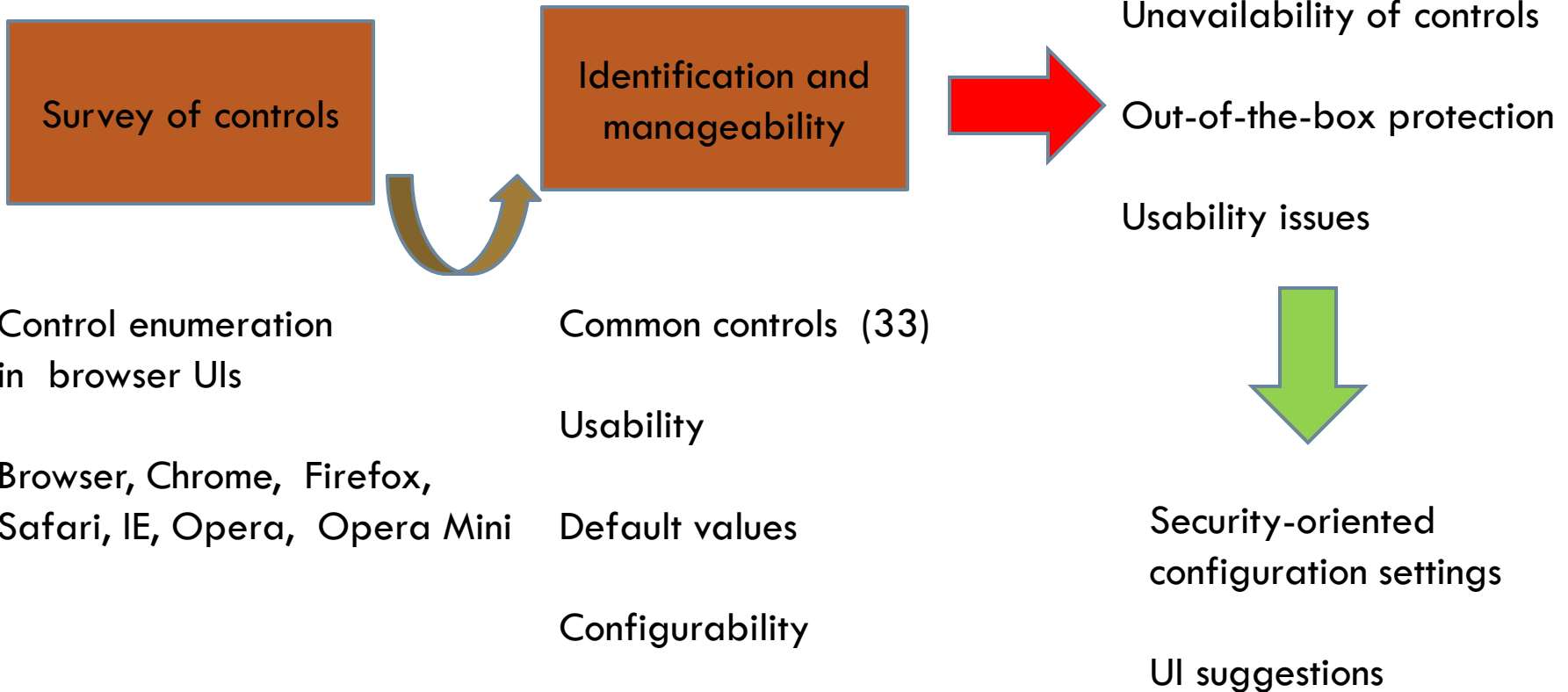
- Manageability of browser security controls
 - ▣ PC, smartphones
- Out-of-the box protection offered

C7. Mylonas A, Tsalis N, Gritzalis D. Evaluating the manageability of web browsers controls. In: Proc. of the 9th International Workshop on Security and Trust Management (STM-2013), Springer; LNCS-8203; 2013; p 82-98.

Browser Controls

9

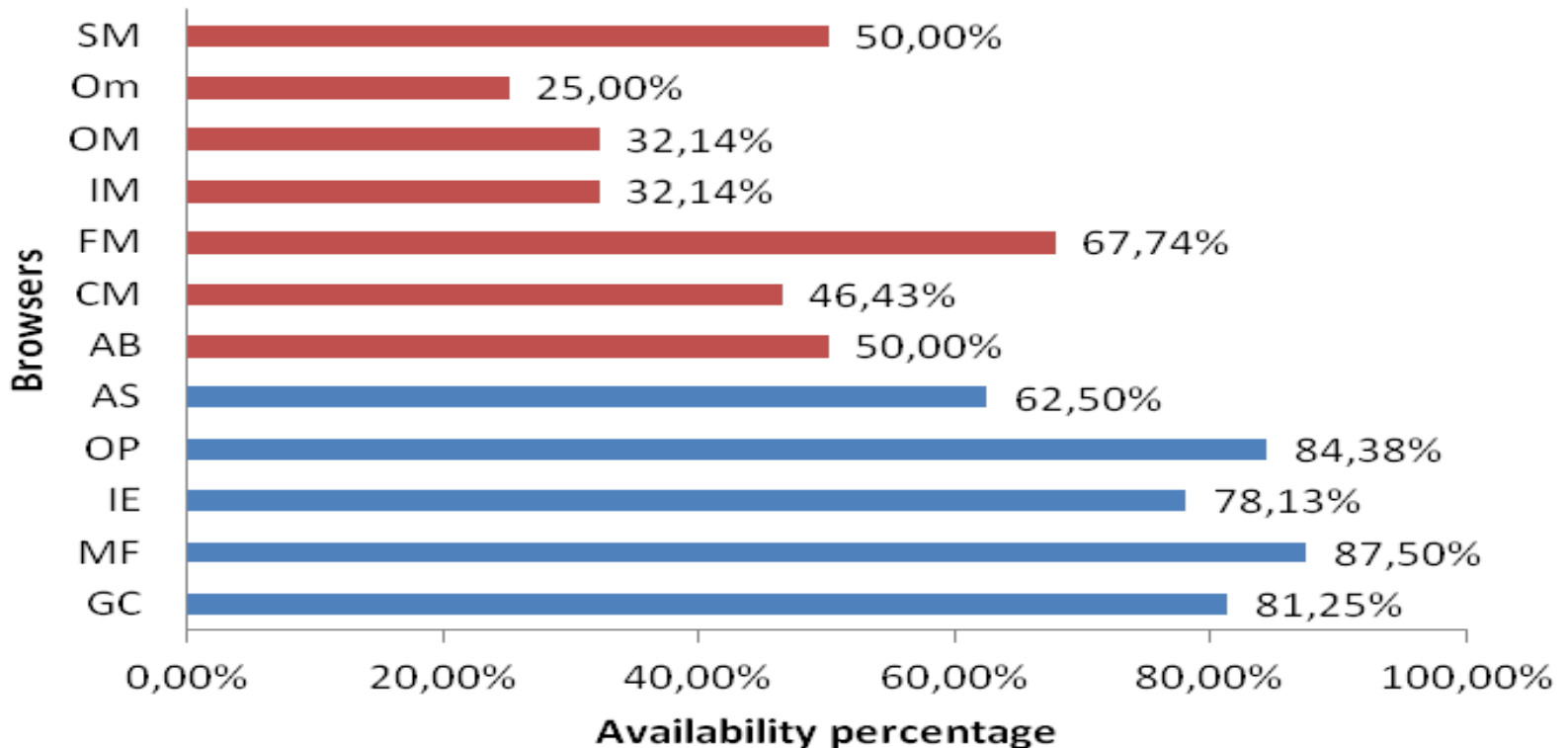
□ Web threats



Browser controls

10

- Availability of controls
 - ▣ PC vs. smartphone
 - ▣ Smartphones browsers offer less controls



Browser controls

10

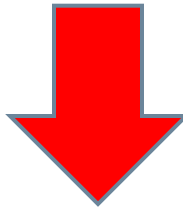
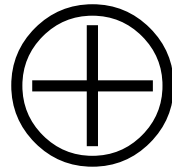
- Availability of controls
 - ▣ PC vs. smartphone
 - ▣ Smartphones browsers offer less controls
- Blame the sandbox?
 - ▣ Counterexamples
 - ▣ Android and iOS (10)
 - e.g. block location data, block third-party cookies, enable DNT, certificate warning, private browsing, ... (c.f. C.7)
 - ▣ Android (5)
 - i.e. block referrer, disable plugin, malware protection, master password, search engine manager

Mitigation of web threats

11

- identified controls (32)
 - ▣ enabled by-default
 - ▣ editable

- Web threats
 - ▣ ICT web threats
 - ▣ Smartphone threats

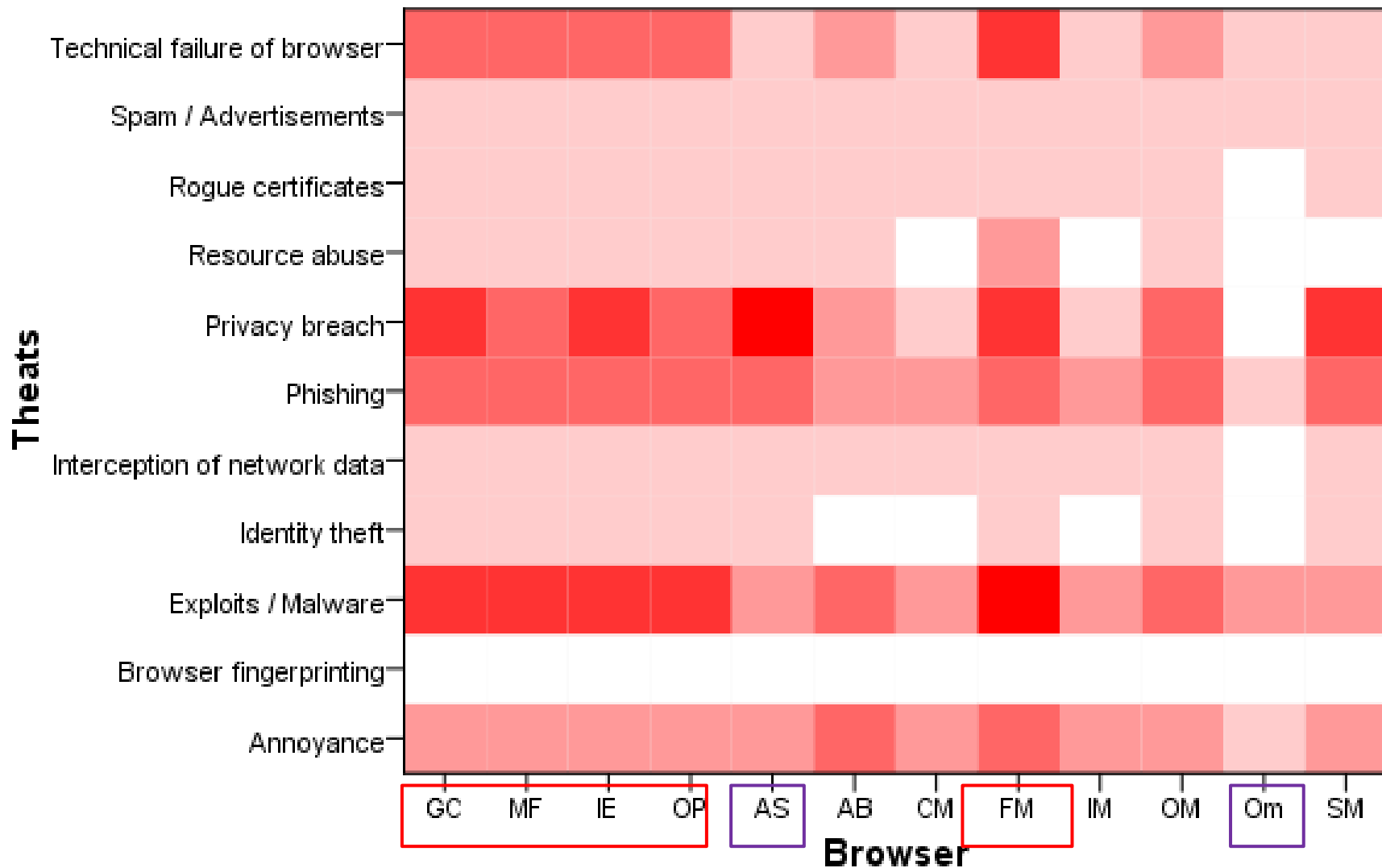


a) default protection/threat

b) control manageability/threat

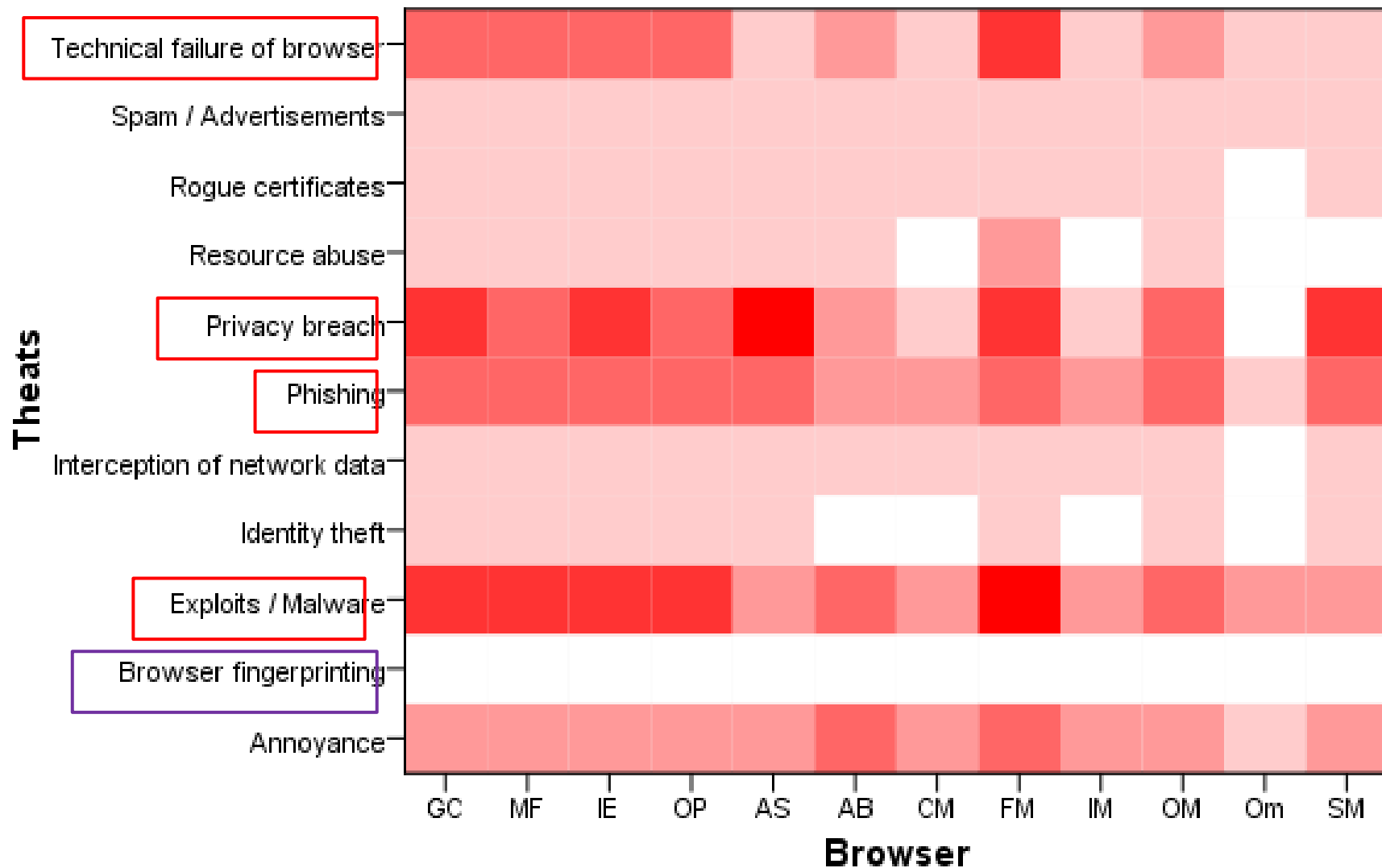
Default protection / threat

12



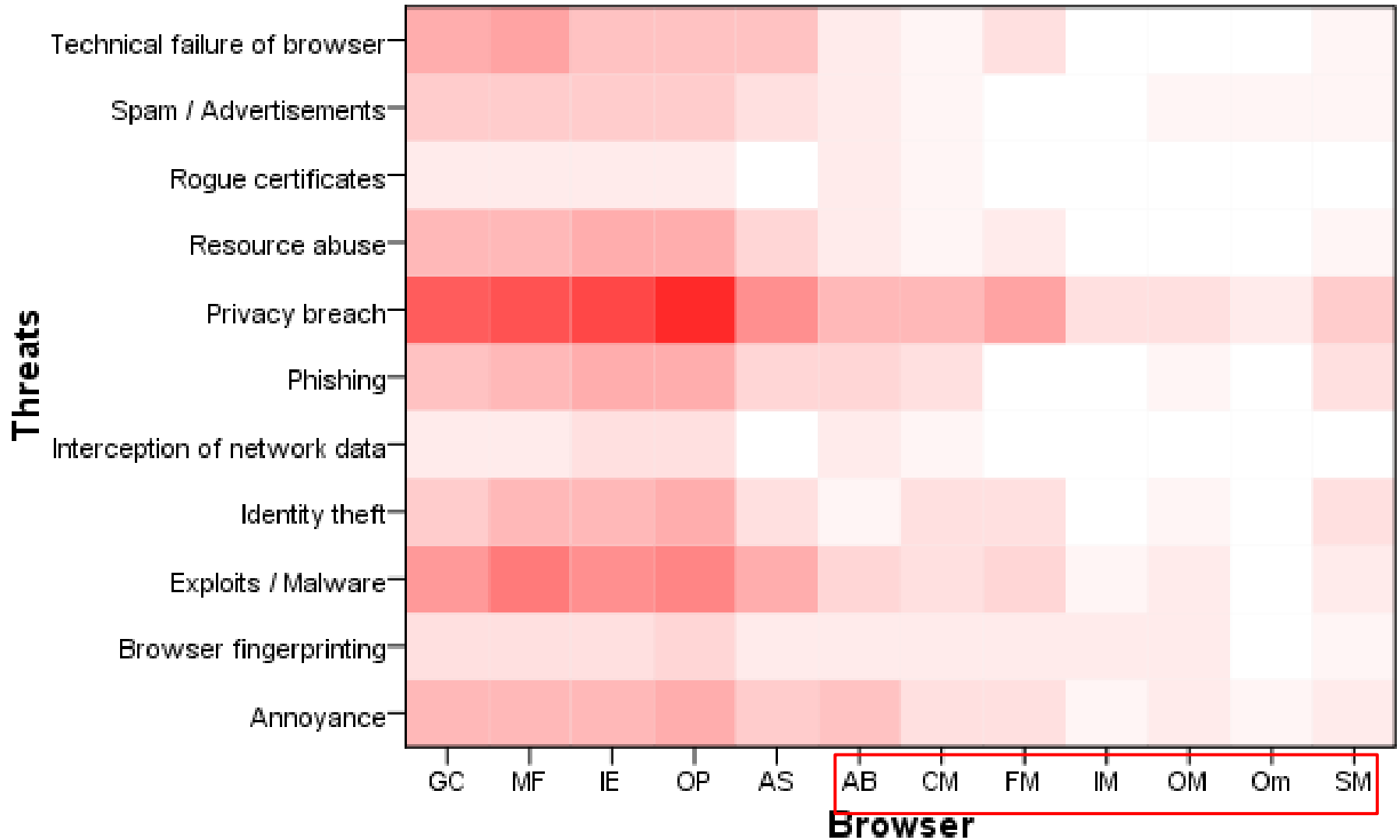
Default protection / threat

12



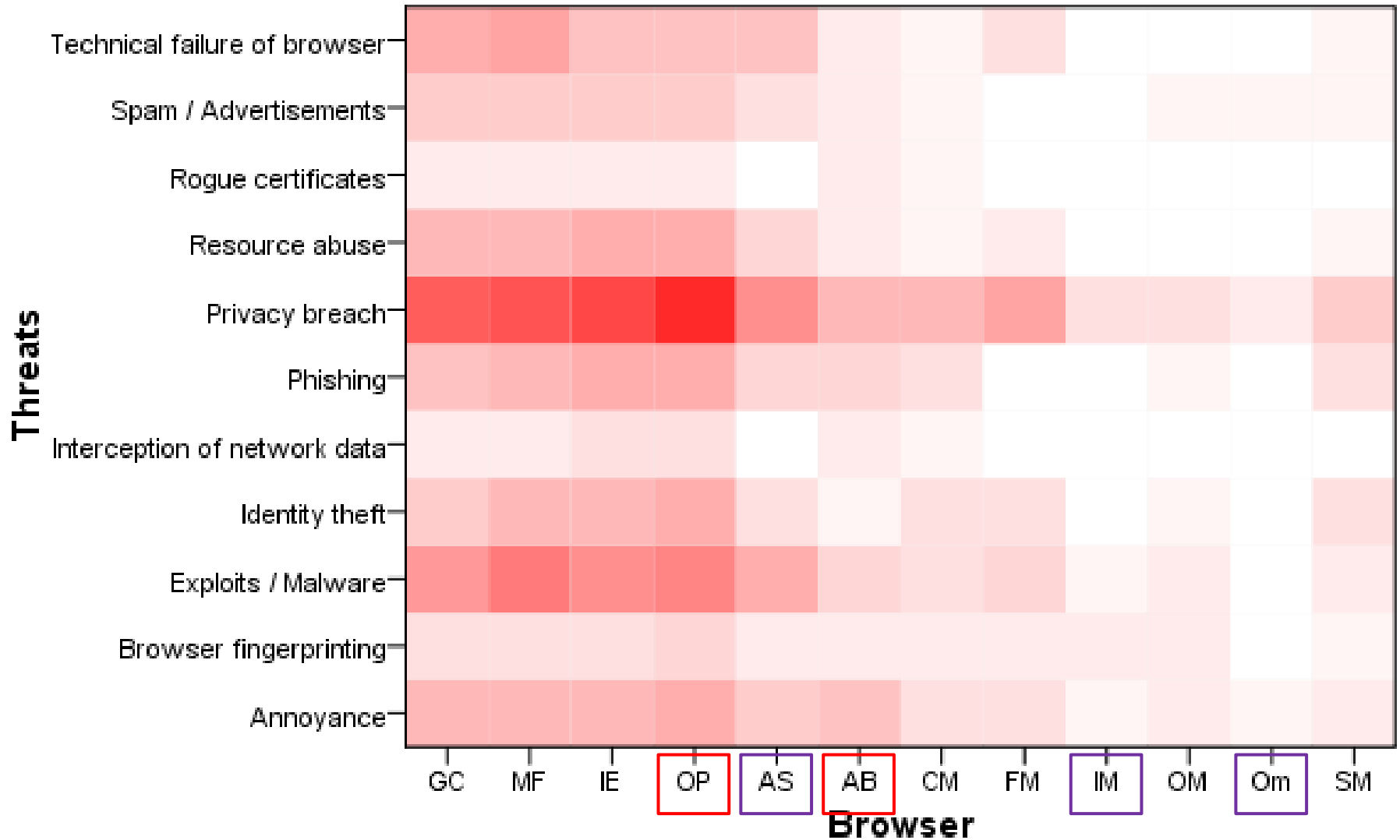
Manageability of controls / threat

13



Manageability of controls / threat

13



Recommendations

14

Vendor Settings & UI

- Functionality-oriented
- Users can disable controls without confirmation
- Security settings mixed with other settings

Proposed Settings & UI

- Security-oriented
 - all controls configurable & enabled
 - discourage changes
 - certificate warning, malware/phishing protection
 - confirmation for update settings
 - ask default value
 - block cookies, block location data, block 3rd party cookies, enable DNT, and master password

Recommendations

14

- Proposed settings restrictive
 - ▣ Security vs. user experience
 - ▣ Local blacklist
 - Per-site configuration of controls
- User awareness
 - ▣ Users trained to use control(s) correctly
 - ▣ Users aware of web threats

User practices

15

- Adoption of controls
 - ▣ Physical attacks
 - ▣ Malicious apps
- Statistical analysis (n=458, Athens, Fall 2011)

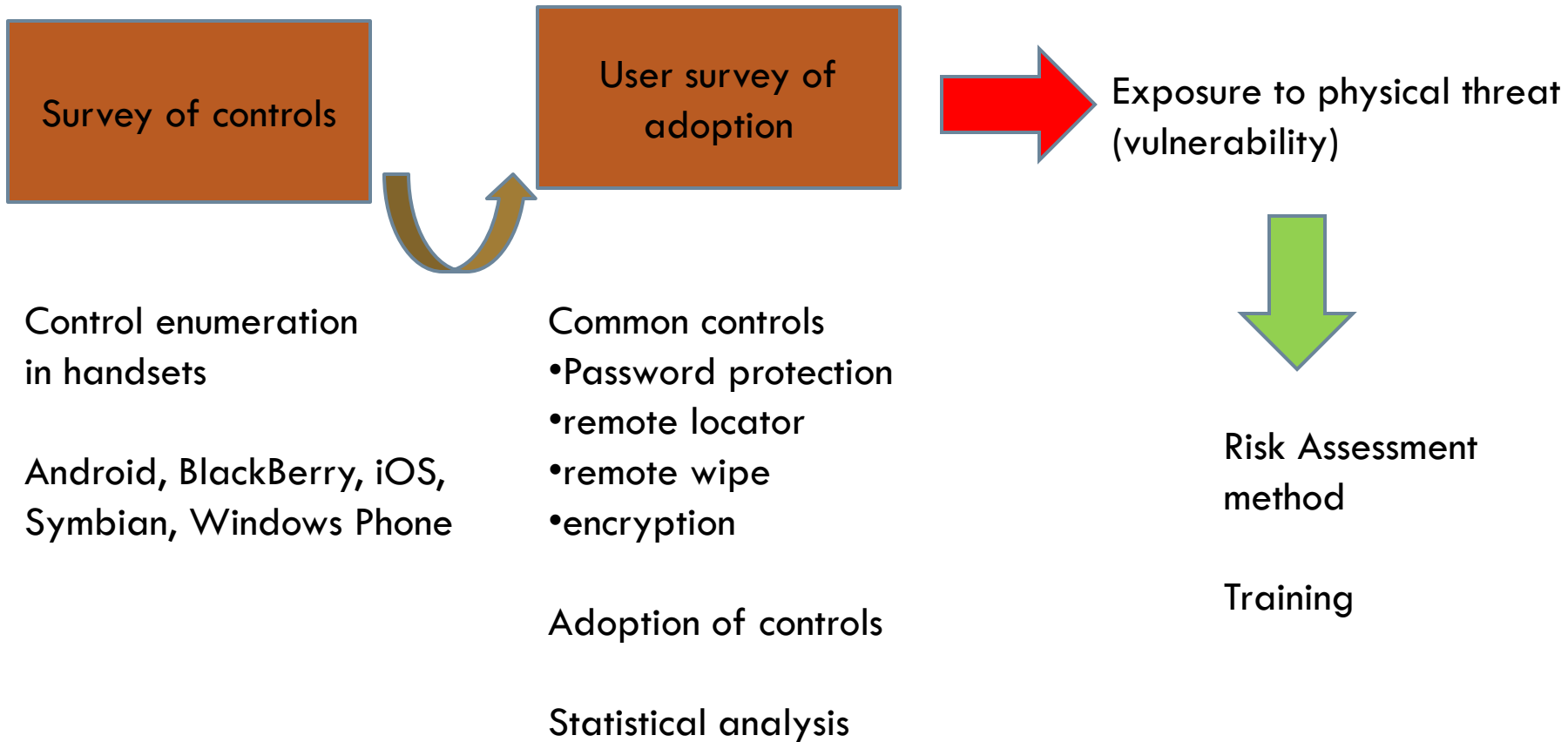
C6. Mylonas A, Gritzalis D, Tsoumas B, Apostolopoulos T. A qualitative metrics vector for the awareness of smartphone security users. In: 10th International Conference on Trust, Privacy & Security in Digital Business. 2013.p. 173–84.

J1. Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security 2013;34(0):47–66.

User practices against physical access

10

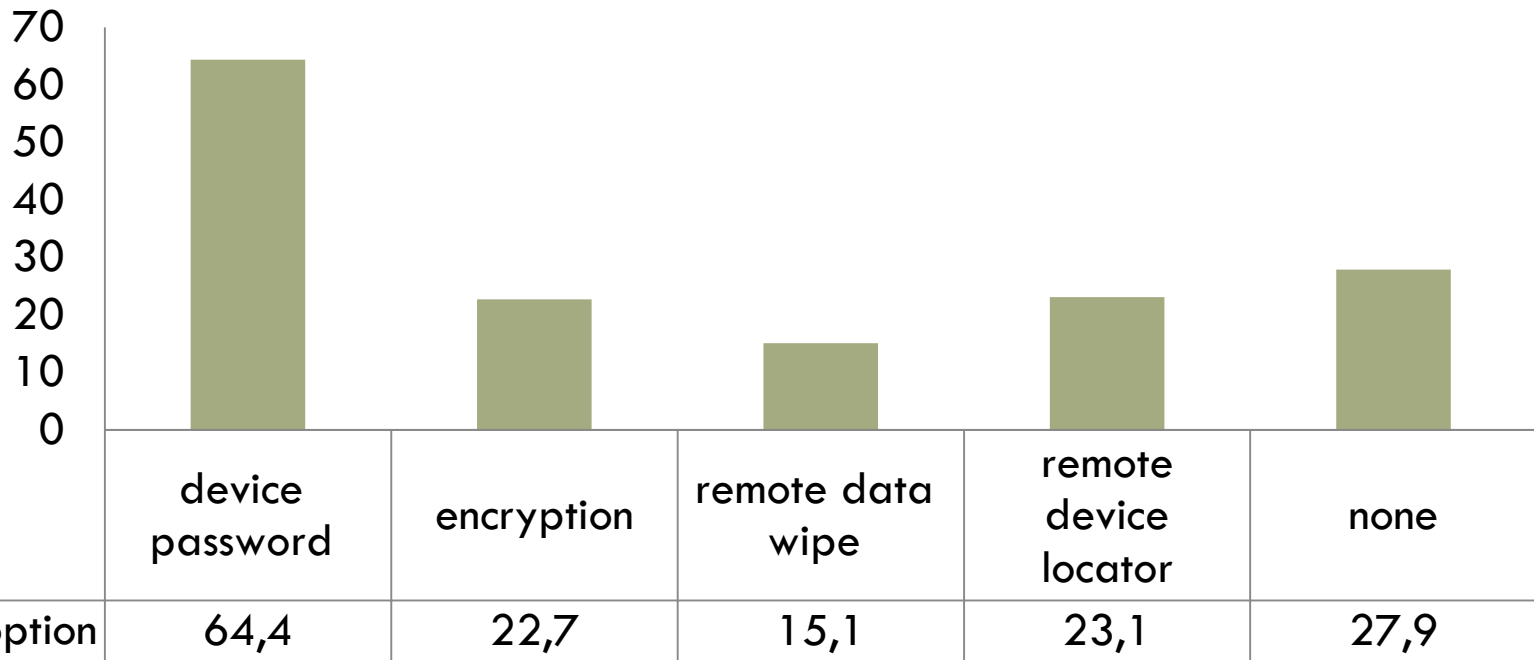
□ Physical threat



User practices against physical access

16

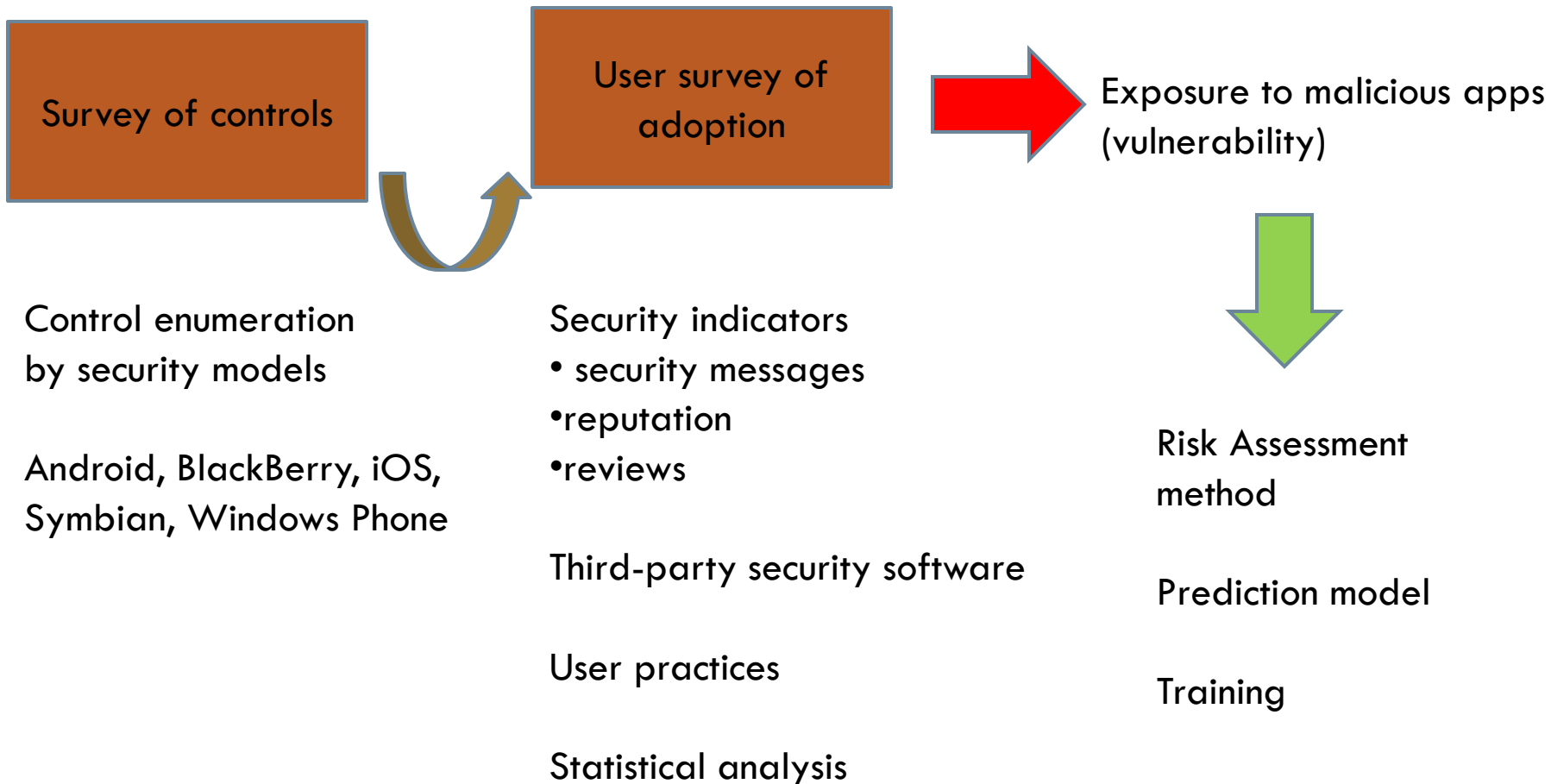
- Poor adoption of physical access controls



User practices against malware

10

□ Threat of malicious apps



User practices against malware

17

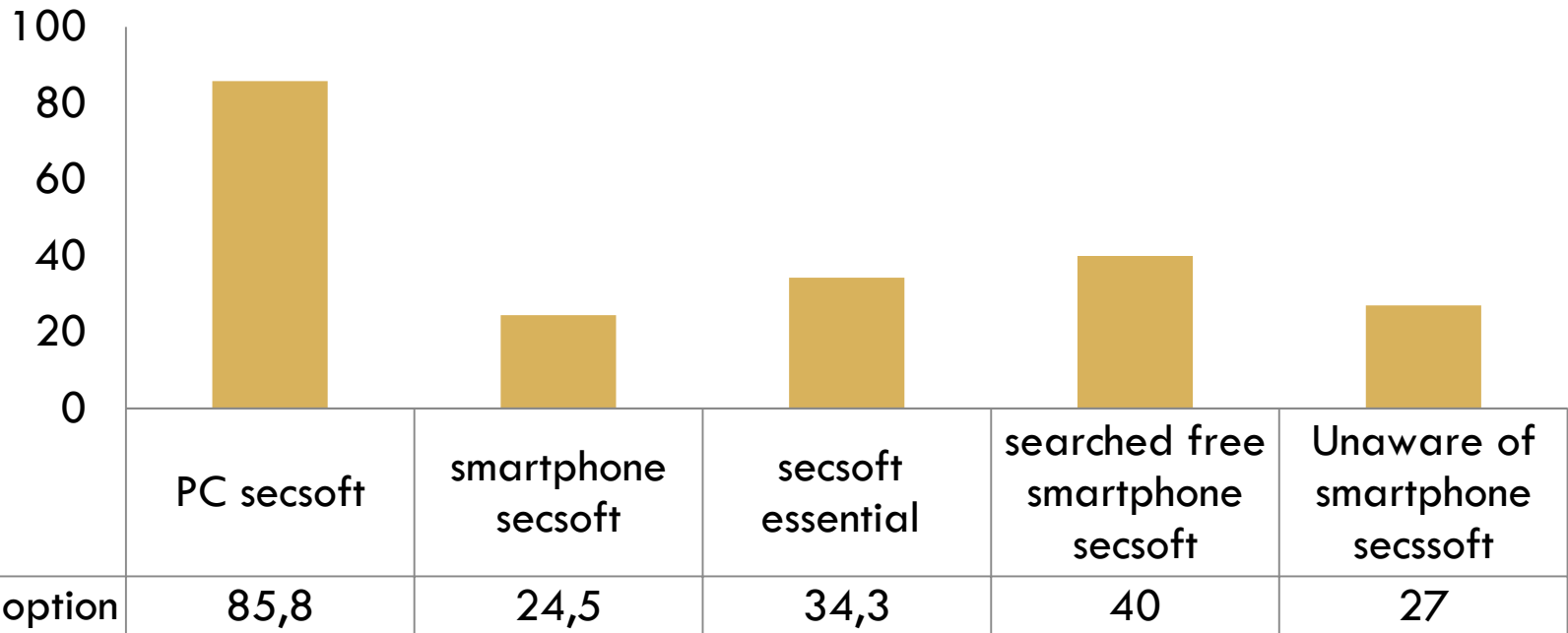
- User practises when installing apps from the app repository



User practices against malware

17

- Poor use of smartphone security software



User practices against malware

17

- Users believe that installing apps from the repository is secure (~3/4 users)
- These users are exposed to malware
 - ▣ *Unaware users of smartphone malware* more likely trust the app repository
 - ▣ Users who trust the repository tend to be *unaware* about *smartphone secsoft*
 - ▣ Users who trust app repository are *less likely* to *scrutinize security* msgs

Malware Mitigation

19

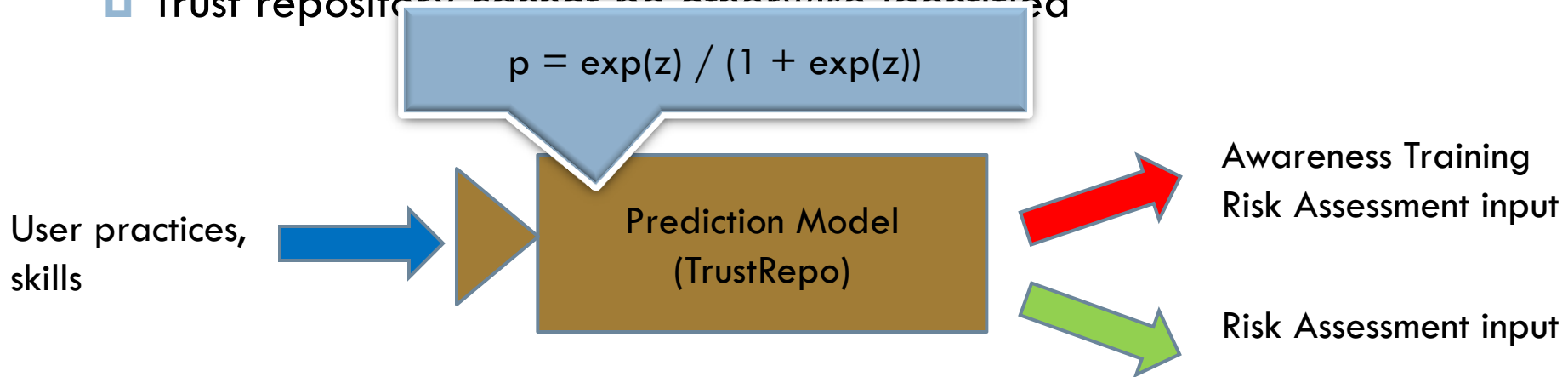
- Prediction model
 - Trust repository cannot be otherwise identified



Malware Mitigation

19

- Prediction model
 - Trust repository cannot be otherwise identified



Malware Mitigation

19

□ Prediction model

$$z = 1.351*x_1 + 1.092*x_2 - 1.688 *x_3 + 1.523*x_4 + 1.314*x_5 - 0.475*x_6 - 0.741*x_7$$

User practices,
skills



Prediction Model
(TrustRepo)



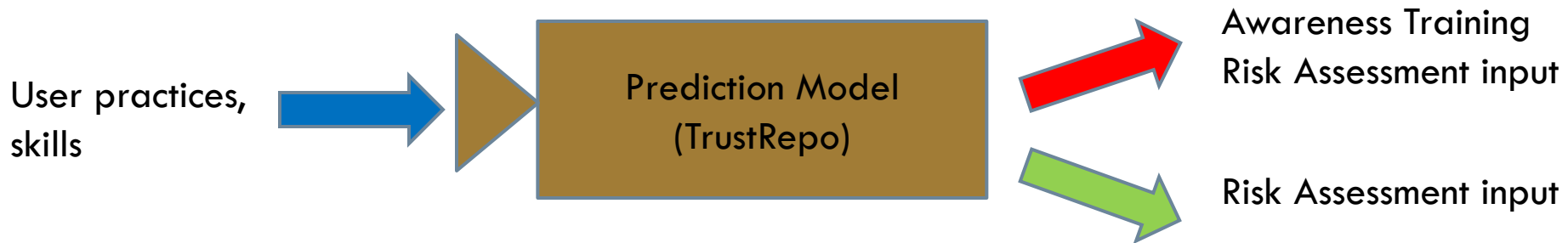
Awareness Training
Risk Assessment input

Risk Assessment input

Malware Mitigation

19

- Prediction model
 - Trust repository cannot be otherwise identified

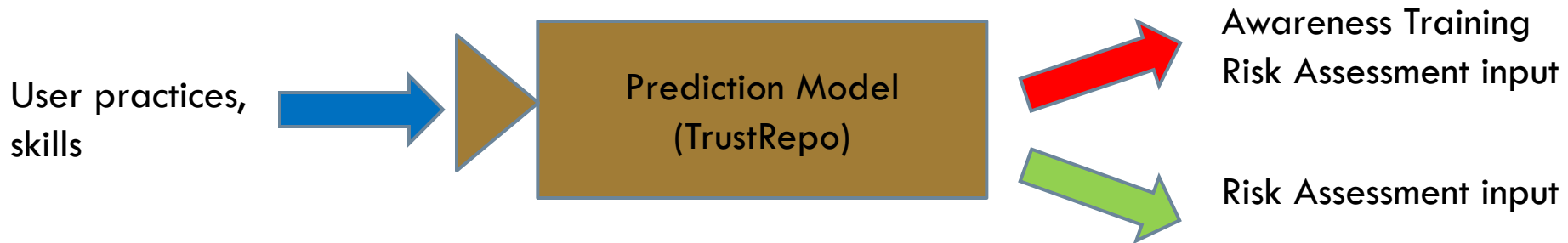


Score\Sample	Greek (n=458)	UK (n=102)
Effectiveness	79.0%	78.4%
Type I	74.5%	68.2
Type II	4.0%	8.7%

Malware Mitigation

19

- Prediction model
 - Trust repository cannot be otherwise identified



J1. Mylonas A, Kastania A, Gritzalis D. Delegate the smartphone user? Security awareness in smart-phone platforms. *Computers & Security* 2013;34(0):47–66.

Malware Mitigation

19

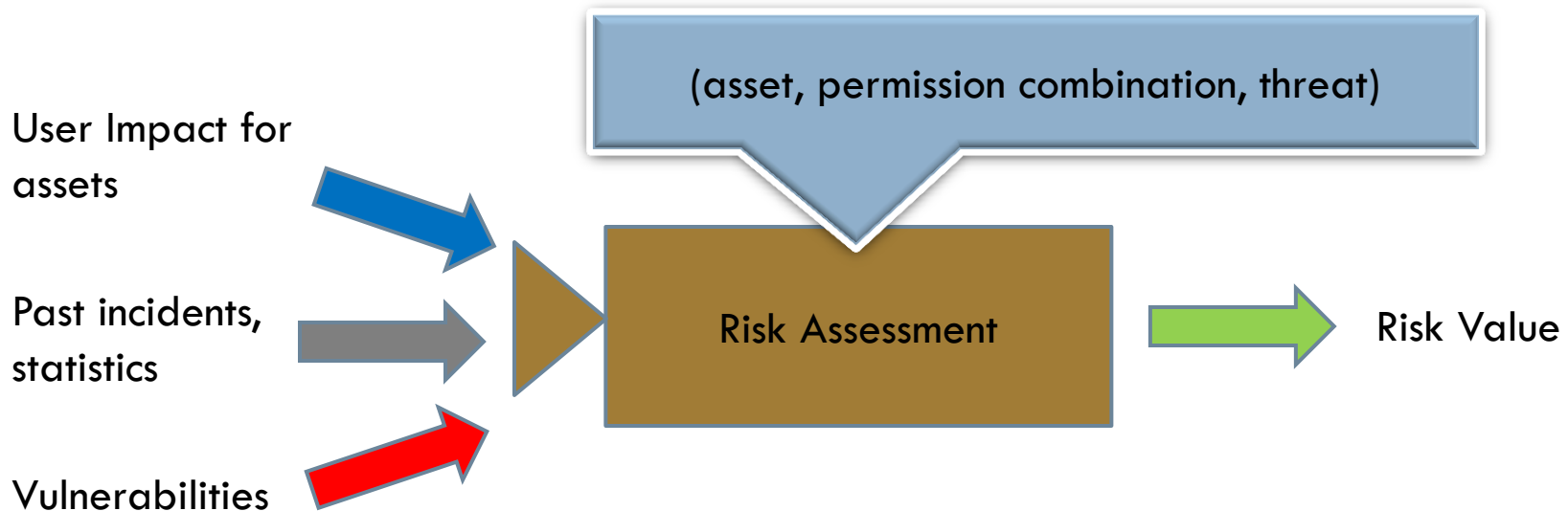
- Risk Assessment for smartphones
 - ▣ Treats the device's subassets and not as a whole
 - ▣ Treats permission granting as a vulnerability



Malware Mitigation

19

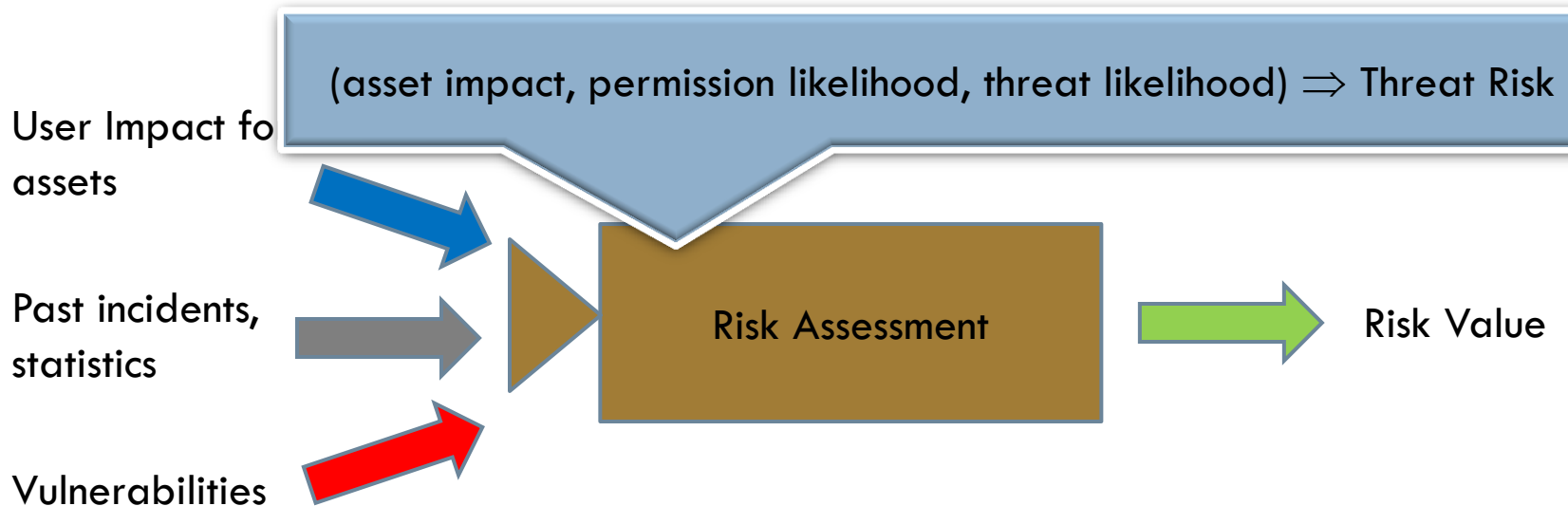
- Risk Assessment for smartphones
 - ▣ Treats the device's subassets and not as a whole
 - ▣ Treats permission granting as a vulnerability



Malware Mitigation

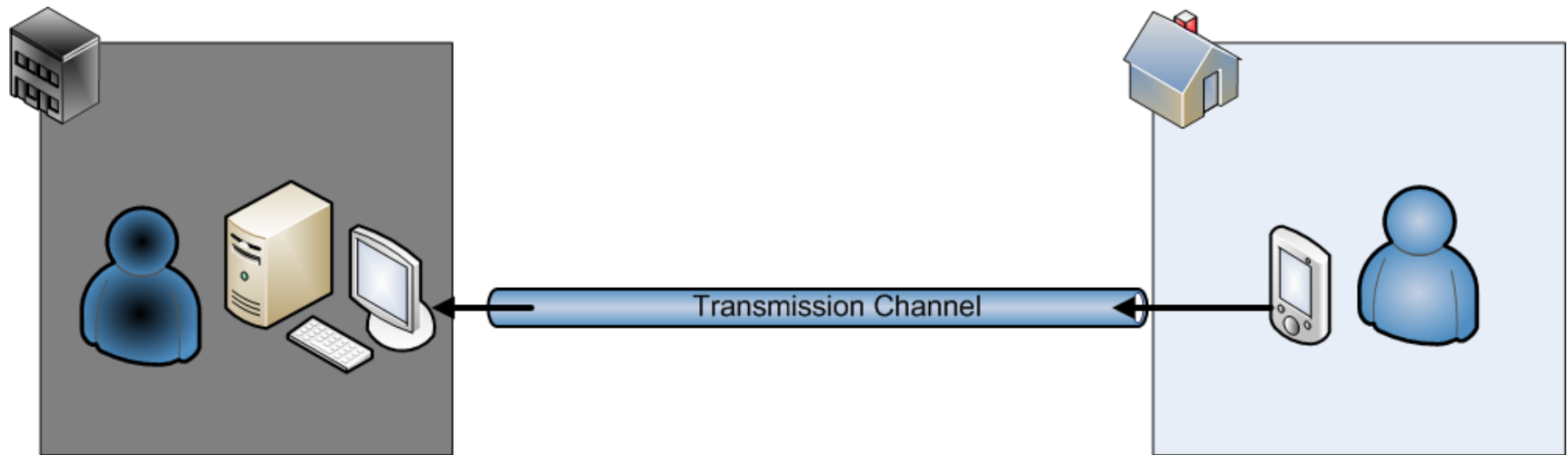
19

- Risk Assessment for smartphones
 - ▣ Treats the device's subassets and not as a whole
 - ▣ Treats permission granting as a vulnerability



Smartphone Forensics

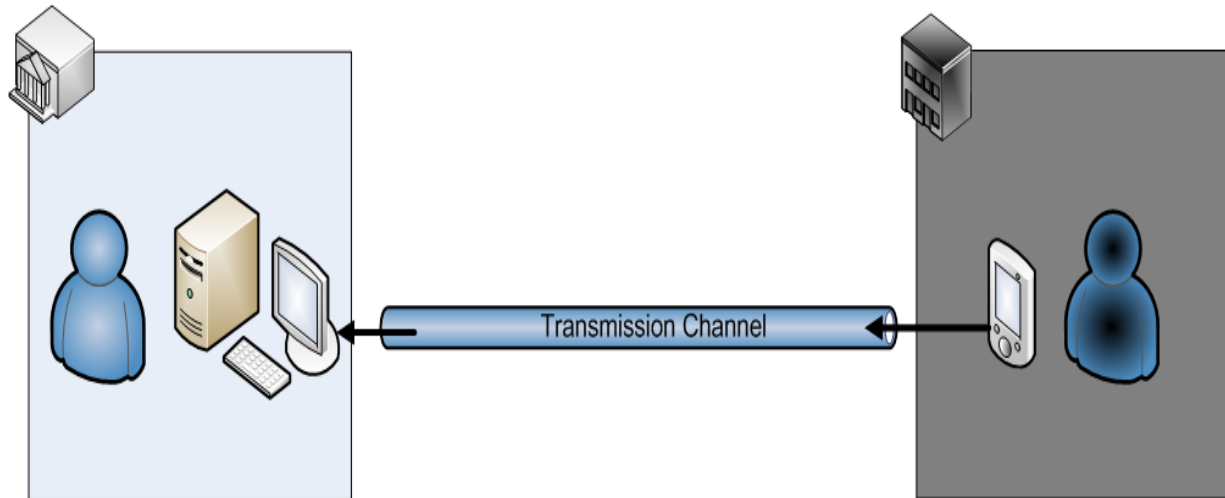
20



Smartphone Forensics

20

- What if the 'good' guys collect the data?

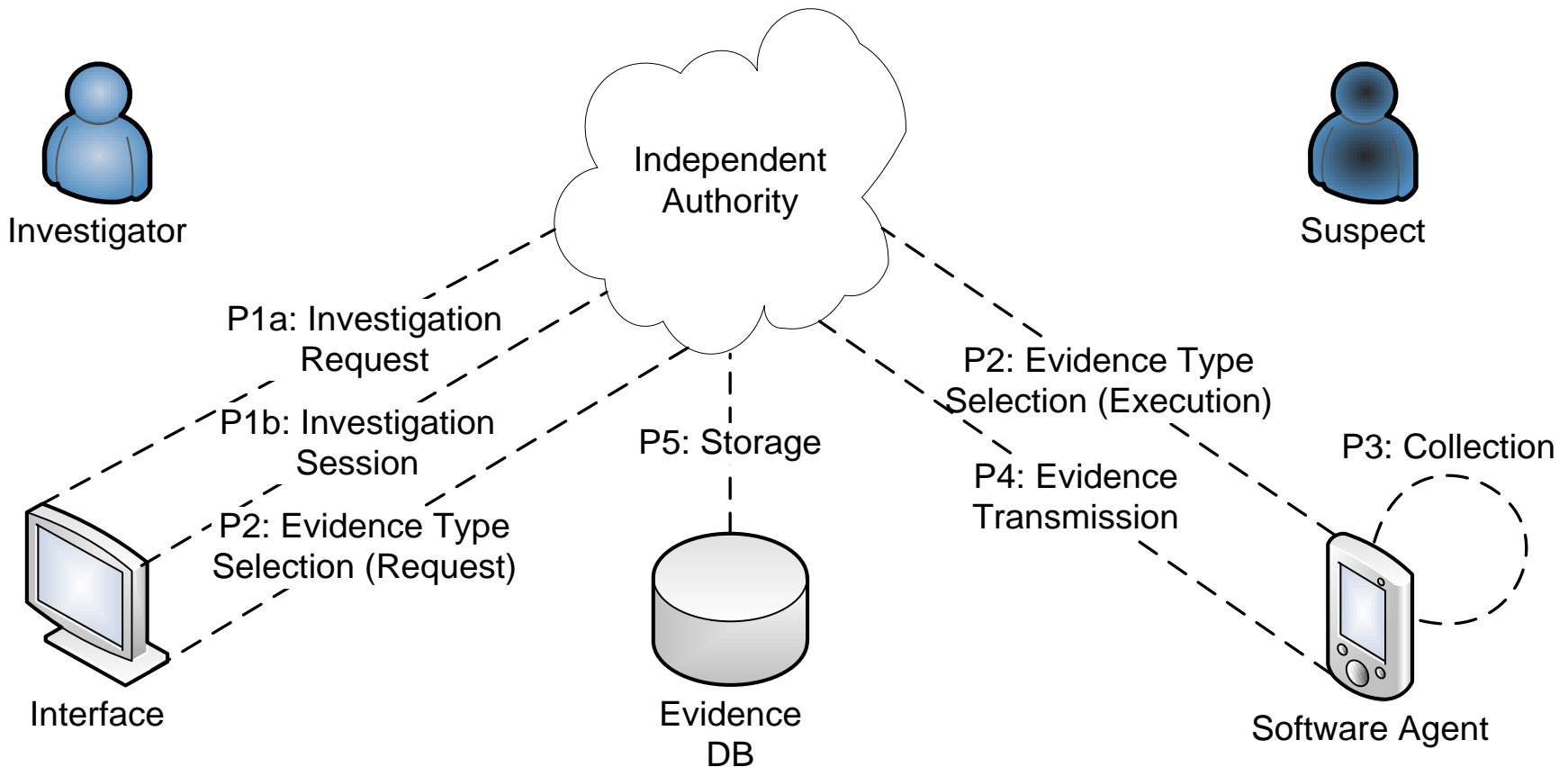


- Can we control its abuse?

Smartphone Forensics Scheme

20

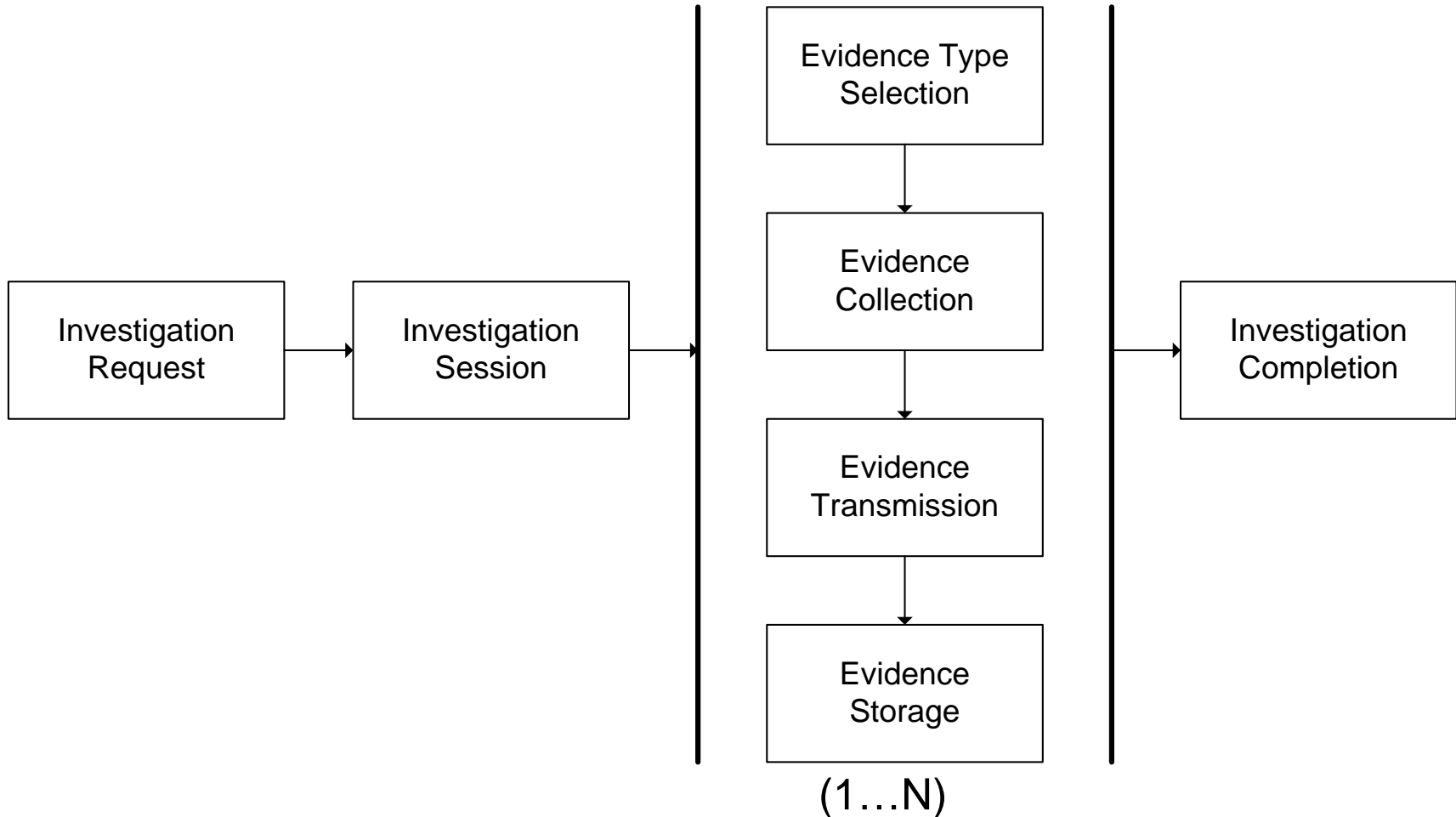
- A scheme to avoid *intelligence gathering*



Smartphone Forensics Scheme

21

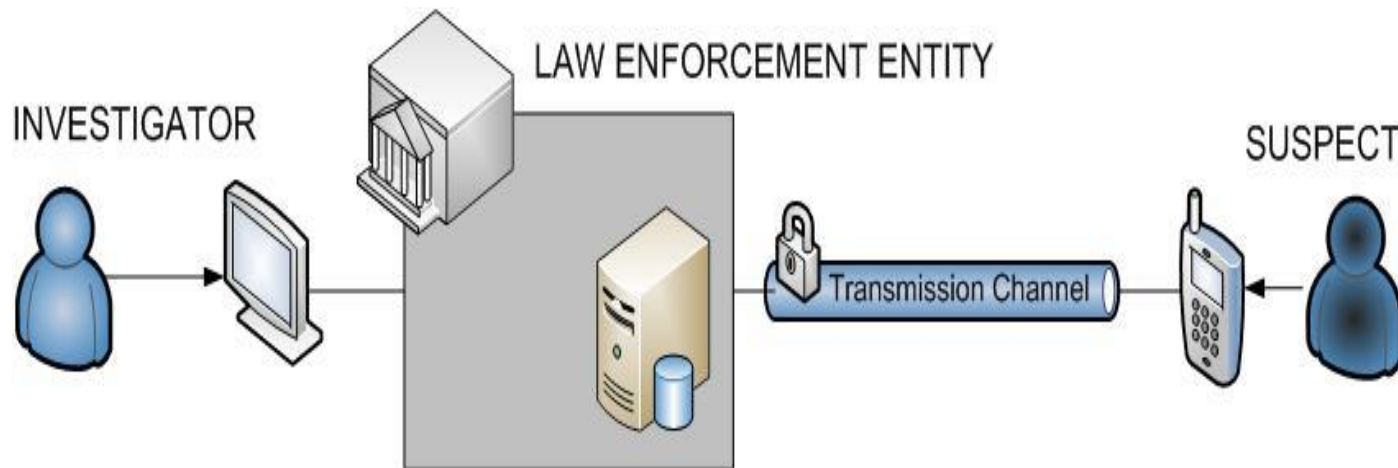
□ Scheme's processes



Smartphone Forensics

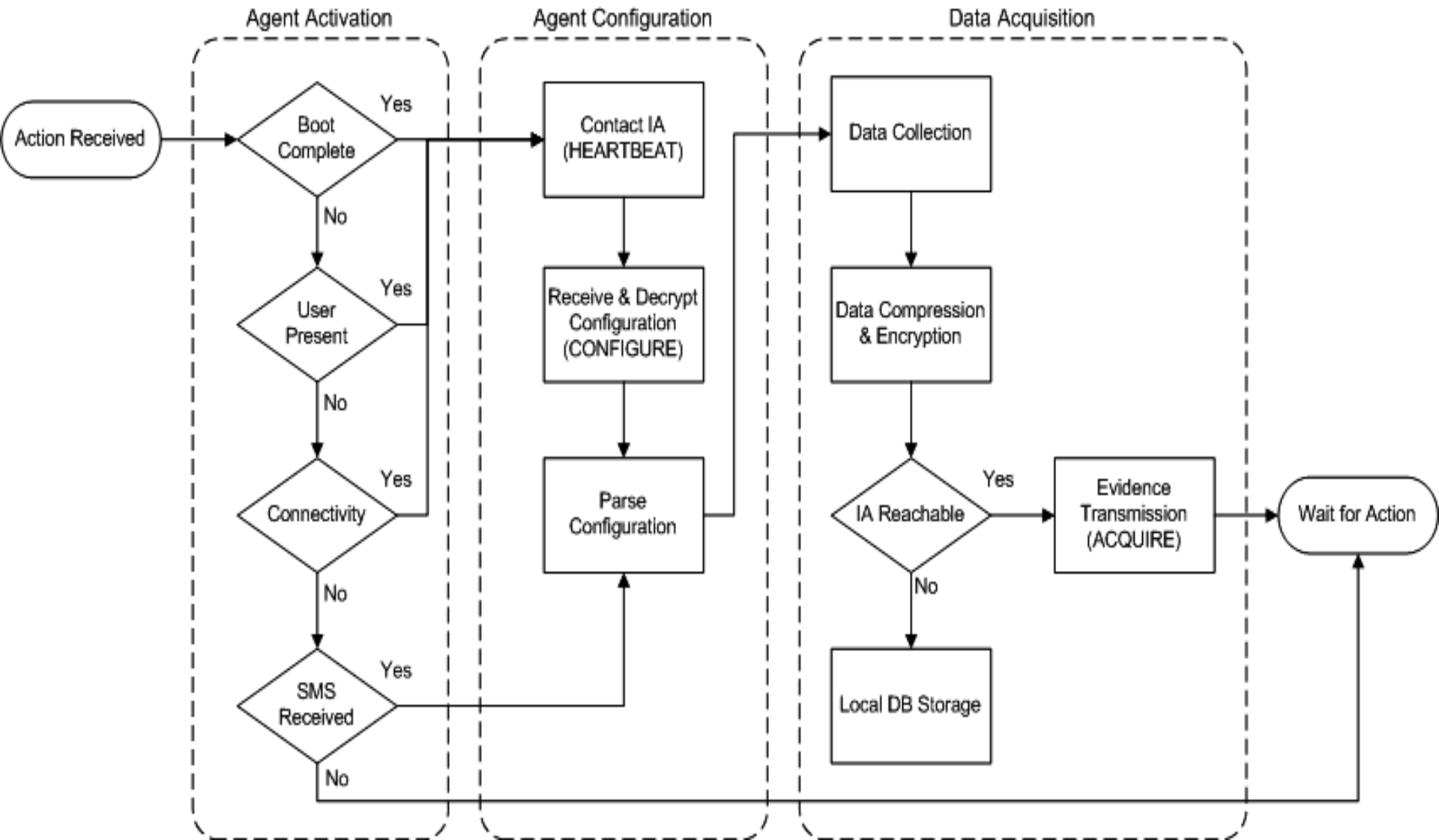
22

- Android implementation
 - ▣ Mechanisms typically used by attackers
 - Spyware, botnets, social engineering



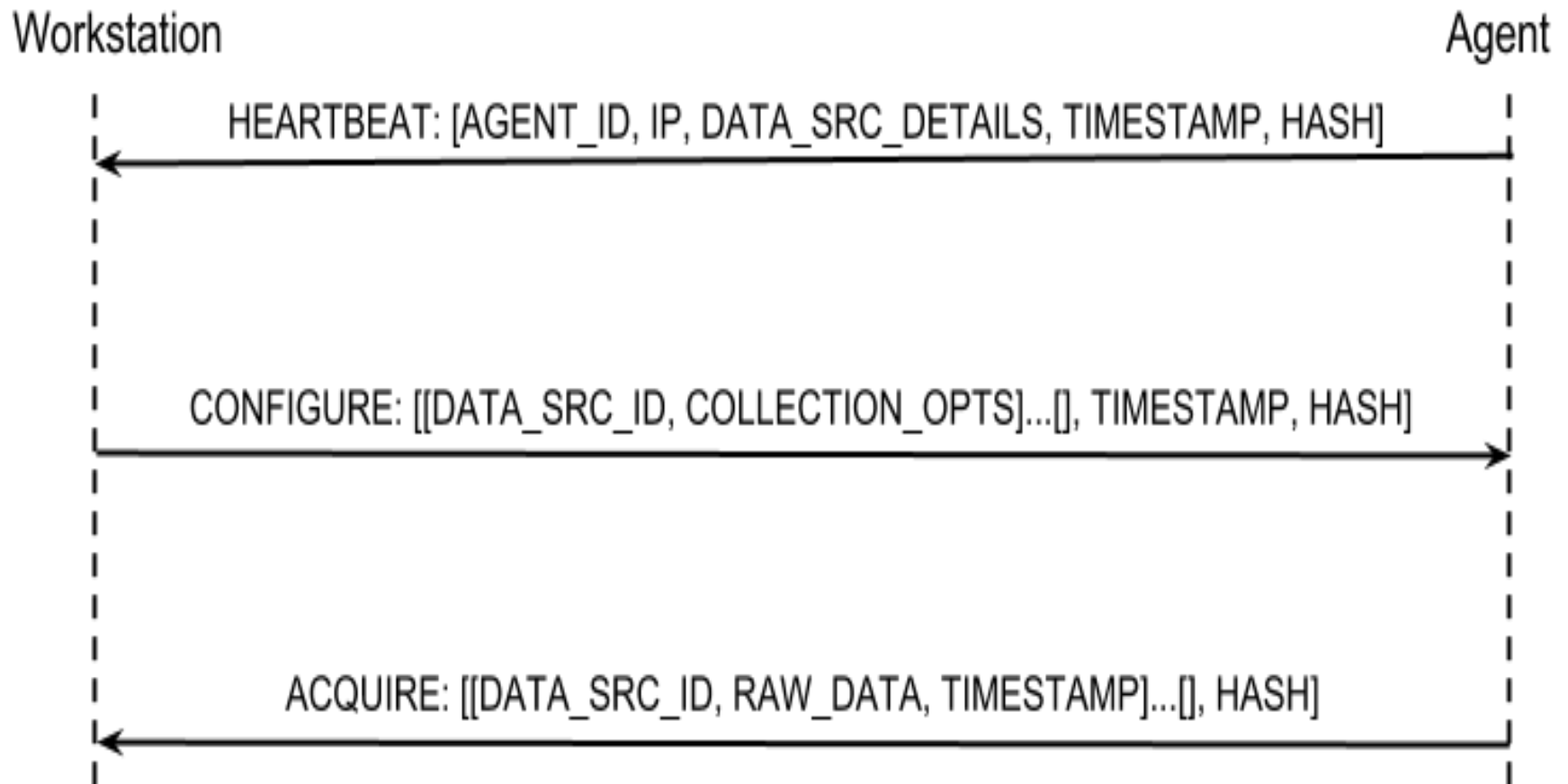
Smartphone Forensics

22



Smartphone Forensics

22



Future work

24

- New user study of the adoption of security controls
- User study on the usability of web browser controls
- Design and implement standardized interface for web browsers
- Study the security models of new platforms
- Examination of alternative misuse mechanisms for proactive forensics

References

1. Mylonas, A., Kastania, A., Gritzalis, D., “Delegate the smartphone user? Security awareness in smartphone platforms”, *Computers & Security*, Vol. 34, pp. 47-66, 2013.
2. Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D., “Smartphone sensor data as digital evidence”, *Computers & Security (Special Issue: Cybercrime in the Digital Economy)*, Vol. 38, pp. 51-75, 2013.
3. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., “Smartphone security evaluation: The malware attack case”, in *Proc. of the International Conference on Security and Cryptography*, SciTePress; p. 25-36, Spain 2011.
4. Mylonas, A., Tsoumas, B., Dritsas, S., Gritzalis, D., “A secure smartphone applications roll-out scheme”, in *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, Springer, LNCS-6863, p. 49-61, 2011.
5. Kandias, M., Mylonas, A., Theoharidou, M., Gritzalis, D., “Exploitation of auctions for outsourcing security-critical projects”, in *Proc. of the 16th IEEE Symposium on Computers and Communications*, p. 646–51, Greece, 2011.
6. Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., Gritzalis, D., “Smartphone forensics: A proactive investigation scheme for evidence acquisition”, in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, Springer, AICT-376, p. 249–260, Greece, 2012.
7. Theoharidou, M., Mylonas, A., Gritzalis, D., “A risk assessment method for smartphones”, in *Proc. of the 27th IFIP Information Security and Privacy Conference*, Springer, AICT-376, p. 443-456, Greece, 2012.
8. Mylonas, A., Gritzalis, D., Tsoumas, B., Apostolopoulos, T., “A qualitative metrics vector for the awareness of smartphone security users”, in *Proc. of the 10th International Conference on Trust, Privacy & Security in Digital Business*, p. 173–84, Czech Republic, 2013.
9. Mylonas, A., Tsalis, N., Gritzalis, D., “Evaluating the manageability of web browsers controls”, in *Proc. of the 9th International Workshop on Security and Trust Management*, Springer, LNCS-8203, p. 82-98, United Kingdom, 2013.
10. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., “On the feasibility of malware attacks in smartphone platforms”, in *Security and Cryptography*, Springer, p. 217-232, 2012.