EVALUATING THE MANAGEABILITY OF WEB BROWSERS CONTROLS

Alexios Mylonas, Nikolaos Tsalis, and Dimitris Gritzalis
Information Security and Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics & Business (AUEB)

12/09/2013

Security & Trust management (STM) 2013

Outline

- Introduction
  - Motivation
  - Methodology
- Results
  - Manageability of controls
  - Availability of controls
  - Mitigation of web threats
- Conclusions and Future Work

Motivation

- Web browsing on smartphones more **ubiquitous**
  - Limited security options
- Proliferation of browser exploits
  - EaaS, PPI
  - Found in benign sites (e.g. in social media)
- Users expected to adjust security settings
  - Personalized level of privacy & security

Motivation

- Web browsing on smartphones more ubiquitous
- Research Questions:
  - *Availability* & *manageability* of security controls in browsers
    - PC, smartphones
  - *Out-of-the box protection* offered
- Users expected to adjust security settings
  - Personalized level of privacy & security

Methodology

- Browsers in scope
  - Windows
    - Chrome (v. 27), Firefox (v. 21), Internet Explorer 10, Opera (v. 12.15), and Safari (v. 5.1.7)
  - Smartphones
    - Browser, Chrome Mobile, Firefox Mobile, IE Mobile, Opera Mobile, Opera Mini, Safari Mobile
    - Different availability of browsers

Methodology

Platform	Version	Device	Chrome Mobile (v. 26)	Firefox Mobile (v.21)	Opera Mobile (v. 14)	Opera Mini (v. 10)	Stock Browser†
Android	2.3.5	HTC Explorer			X		X
	2.3.6	LG-E400			X		X
	4.0.3	LG - P700	X	X	X		X
	4.0.4	Sony Xperia	X	X	X	X	X
	4.1.2	Samsung Galaxy S3	X	X	X		X
		Samsung Nexus S	X	X	X		X
iOS	5.1.1	iPhone 4	X			X	X
	6.1.2	iPhone 4S	X			X	X
Windows Phone	7.5	HTC Trophy7					X

† Browser for Android, Safari for iOS, and IE Mobile for Windows Phone.

Methodology

- Browsers in scope
  - Windows
    - Chrome (v. 27), Firefox (v. 21), Internet Explorer 10, Opera (v. 12.15), and Safari (v. 5.1.7)
  - Smartphones
    - Browser, Chrome Mobile, Firefox Mobile, IE Mobile, Opera Mobile, Opera Mini, Safari Mobile
    - Different availability of browsers
- Collected widgets for security settings in the browsers' GUIs
  - Collected default values
  - Marked usability problems

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) content controls, (b) privacy controls, (c) browser manageability, (d) third-party software controls, and (e) web browsing controls.
- Used the following notation for their presentation
  - ☒ control *is not supported*
  - ☐ control *is supported but not configurable*
  - ▣ control *is supported but is not easily configurable*
  - ■ control *is supported and easily configurable*
  - ○ control default disabled control
  - ● control default enabled control

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) content controls, (b) privacy controls, (c) browser

Controls	GC	MF	IE	OP	AS	AB	CM	FM	IM	OM	Om	SM
Browser update	■●	■●	■●	■●	☒	□●	▣●	■●	□●	▣●	▣●	□●
Certificate manager	■	■	■	■	□	□/■[2]	■/□[2]	□	□	■	☒	□
Master Password	☒	■○	☒	■○	☒	☒	☒	■○	☒	☒	☒	☒
Proxy server	■	■	■	■	■	▣[1]	▣[1]	▣[1]	▣[1]	☒	▣[1]	▣[1]
Search engine manager	■	■	■	■	□[1]	□[1]	□[1]	☒	☒	☒	□[1]	□[1]
SSL/TLS version selection	☒	☒	■	■	☒	☒	☒	☒	☒	☒	☒	☒
Task manager	■	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) content controls, (b) privacy controls, (c) browser manageability, (d) third-party software controls, and (e) web browsing controls.
- Used the following notation for their presentation
  - ☒ control *is not supported*
  - ☐ control *is supported but not configurable*
  - ▣ control *is supported but is not easily configurable*
  - ■ control *is supported and easily configurable*
  - ○ control default disabled control
  - ● control default enabled control

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) c… rowser man… rols, and (e) web brow…
- Used t… sentation
  - ☒ control *is not supported*
  - ☐ control *is supported but not contig…ble*
  - ▣ control *is supported but is not easily configurable*
  - ■ control *is supported and easily configurable*
  - ○ control default disabled control
  - ● control default enabled control

'not easily configurable'
- configured from a hidden menu
- configuration has usability problem

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) content controls, (b) privacy controls, (c) browser

Controls	GC	MF	IE	OP	AS	AB	CM	FM	IM	OM	Om	SM
Browser update	■●	■●	■●	■●	☒	□●	◙●	■●	□●	◙●	◙●	□●
Certificate manager	■	■	■	■	□	□/■[2]	■/□[2]	□	□	■	☒	□
Master Password	☒	■○	☒	■○	☒	☒	☒	■○	☒	☒	☒	☒
Proxy server	■	■	■	■	■	◙[1]	◙[1]	◙[1]	◙[1]	☒	◙[1]	◙[1]
Search engine manager	■	■	■	■	□[1]	□[1]	□[1]	☒	☒	☒	□[1]	□[1]
SSL/TLS version selection	☒	☒	■	■	☒	☒	☒	☒	☒	☒	☒	☒
Task manager	■	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Manageability of controls

- Identified 32 common security controls in web browsers
-

home button-> device's options button -> settings-> wifi->on->hold network id* -> modify network-> scroll down-> check show advanced options-> scroll down-> proxy setting -> manual -> scroll down-> fill in proxy details -> tap save

*unless the user holds the network id for a few seconds the hidden menu will not appear

Controls												SM
Browser												
Certificat												
Master Password												
Proxy server	■	■	■	■	■	[1]	[1]	[1]	[1]	☒	[1]	[1]
Search engine manager	■	■	■	■	☐[1]	☐[1]	☐[1]	☒	☒	☒	☐[1]	☐[1]
SSL/TLS version selection	☒	☒	■	■	☒	☒	☒	☒	☒	☒	☒	☒
Task manager	■	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories
  - (a) content controls, (b) privacy controls, (c) browser manageability, (d) third-party software controls, and (e) web browsing controls.
- Used the following notation for their presentation
  - ☒ control *is not supported*
  - ☐ control *is supported but not configurable*
  - ▣ control *is supported but is not easily configurable*
  - ■ control *is supported and easily configurable*
  - ○ control default disabled control
  - ● control default enabled control

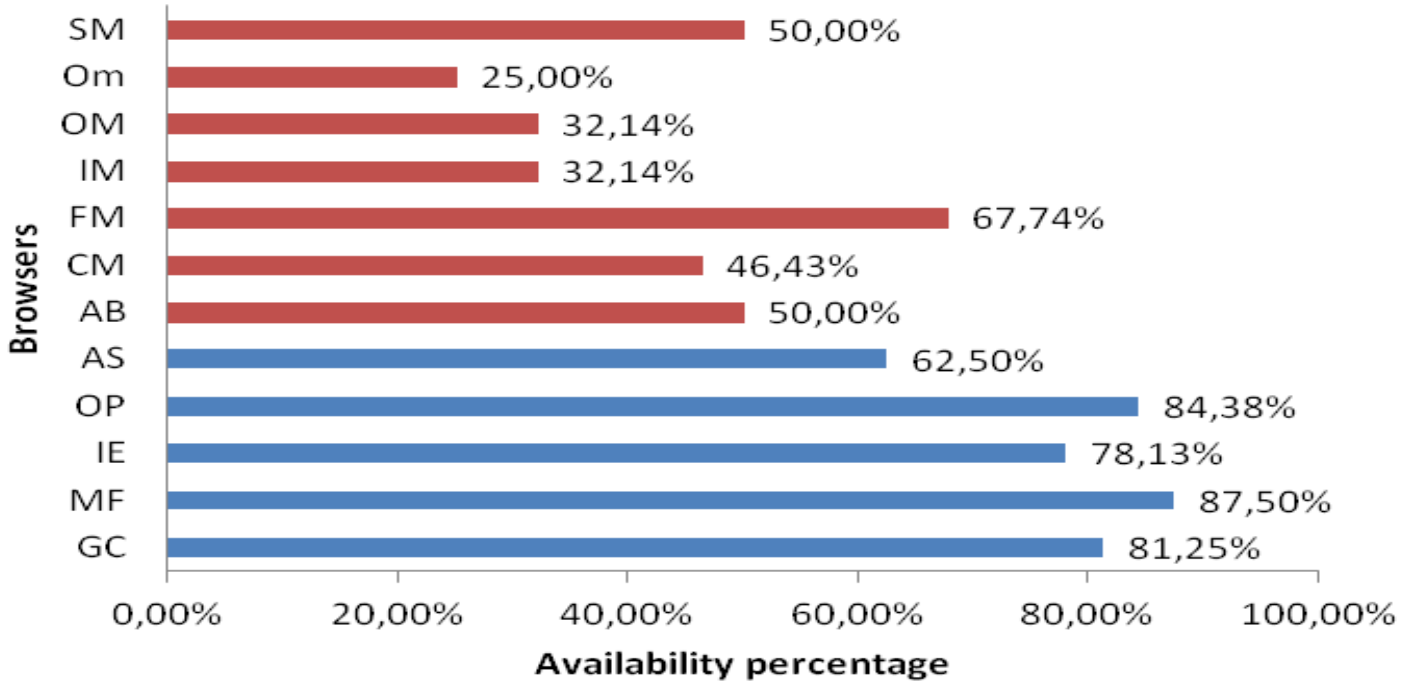
Manageability of controls

- Identified 32 common security controls in web browsers
- Grouped findings into 5 categories

Controls	GC	MF	IE	OP	AS	AB	CM	FM	IM	OM	Om	SM
Certificate Warning	◻●	◻●	◻●	◻●	◻●	■●	◻●	◻●	◻●	◻●	☒	◻●
Local blacklist	■	■	■	■	☒	☒	☒	☒	☒	☒	☒	☒
Malware protection	■●	■●	■●	■●	■●	☒	☒	◻●	☒	◻●	☒	☒
Modify user-agent	▣	▣	▣	■	▣	■	■	■	■	■	☒	☒
Phishing protection	■●	■●	■●	■●	■●	☒	☒	◻●	☒	◻●	☒	■●
Report rogue Website	☒	■	■	■	☒	☒	☒	☒	☒	☒	☒	☒
Website checking	☒	☒	■	■	☒	☒	☒	☒	☒	☒	☒	☒

Availability of controls (1/2)

- PC vs. smartphone
  - Browsers in smartphones offer less controls



Availability of controls (2/2)

- PC vs. smartphone
  - Browsers in smartphones offer less controls
  - Shall we blame the *sandbox*?
  - *Counterexamples*?

Availability of controls (2/2)

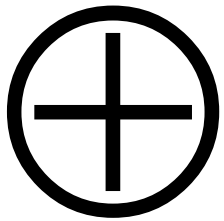
Controls	GC	MF	IE	OP	AS	AB	CM	FM	IM	OM	Om	SM
Block images	■○	■○	■○	■○	■○	■○	☒	▣○	☒	☒	■○	☒
Block location data	■●	▣○	■○	■○	■●	■○	☒|■○	▣○	■○	☒	☒	▣●
Block referrer	▣○	▣○	☒	■○	☒	☒	☒	▣○	☒	☒	☒	☒
Block third- party cookies	■○	■○	■○	■○	■●	☒	☒	■○	☒	☒	☒	■●
Certificate manager	■	■	■	■	□	□/■	■/□	□	□	■	☒	□
Certificate Warning	□●	□●	□●	□●	□●	■●	□●	□●	□●	□●	☒	□●
Disable JavaScript	■○	■○	■○	■○	■○	■○	□|■○	▣○	☒	☒	☒	■○
Disable plugin	■○	■○	■○	■○	☒	■○|●	☒	■●	☒	☒	☒	☒
Enable DNT	■○	■○	■●	■○	▣○	☒	■○	■○	☒	☒	☒	☒|▣○
Malware protection	■●	■●	■●	■●	■●	☒	☒	□●	☒	□●	☒	☒
Master Password	☒	■○	☒	■○	☒	☒	☒	■○	☒	☒	☒	☒
Modify user-agent	▣	▣	▣	■	▣	■	■	■	■	■	☒	☒
Phishing protection	■●	■●	■●	■●	■●	☒	☒	□●	☒	□●	☒	■●
Private browsing	■	■	■	■	■	☒|▣	■	■	☒	☒	☒	■
Search engine manager	■	■	■	■	□	□	□	☒	☒	☒	□	□

Availability of controls (2/2)

- Browsers in smartphones offer less controls
- Can you blame the sandbox?
- Counterexamples?
- Android and iOS
  - Block images, Block location data, Block third-party cookies, Enable DNT, Certificate manager, Certificate Warning, Disable JavaScript, Modify user-agent, Phishing protection, Private browsing
- Android
  - Block referrer, Disable plugin, Malware protection, Master password, Search engine manager

Mitigation of web threats (1/2)

- 32 identified controls (C_i)
  - see web link for notation



- Web threats
  - ICT web threats
  - Smartphone threats

Mitigation of web threats (1/2)

- 22 identified controls
- Web threats

Threat (T_i)	Security Controls
Annoyance (T1)	C4, C6, C11, C12, C13, C14, C15, C19, C24
Browser fingerprinting (T2)	C14, C19, C24, C27
Exploits/Malware (T3)	C1, C2, C6, C9, C12, C13, C14, C15, C17, C19, C20, C21, C22, C24, C27, C28, C32
Identity theft (T4)	C14, C18, C19, C23, C25, C26, C28, C32
Data interception (T5)	C10, C11, C19, C30
Phishing (T6)	C6, C10, C11, C14, C19, C25, C27, C28, C32
Privacy breach (T7)	C3, C4, C5, C7, C8, C11, C12, C13, C14, C15, C16, C18, C19, C20, C23, C24, C25, C26, C27, C28, C29, C32
Resource abuse (T8)	C12, C13, C14, C15, C17, C19, C20, C28, C31, C32
Rogue certificates (T9)	C10, C11, C19
Spam advertisements (T10)	C4, C6, C19, C27, C29
Technical failure (T11)	C1, C2, C9, C12, C13, C14, C15, C17, C20, C21, C22, C31

Mitigation of web threats (1/2)

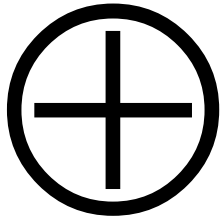
- 22 identified controls
- Web threats

Threat (T_i)	Security Controls
Annoyance (T1)	C4, C6, C11, C12, C13, C14, C15, C19, C24
Browser fingerprinting (T2)	C14, C19, C24, C27
Exploits/Malware (T3)	C1, C2, C6, C9, C12, C13, C14, C15, C17, C19, C20, C21, C22, C24, C27, C28, C32
Identity theft (T4)	C14, C18, C19, C23, C25, C26, C28, C32
Data interception (T5)	C10, C11, C19, C30
Phishing (T6)	C6, C10, C11, C14, C19, C25, C27, C28, C32
Privacy br	C18, C19, C20, C23, C24, C25,
Resource abuse (T8)	13, C14, C15, C17, C19, C20, C28, C31, C32
Rogue certificates (T9)	C10, C11, C19
Spam advertisements (T10)	C4, C6, C19, C27, C29
Technical failure (T11)	C1, C2, C9, C12, C13, C14, C15, C17, C20, C21, C22, C31

Certificate manager, Certificate Warning, Local blacklist

Mitigation of web threats (2/2)

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

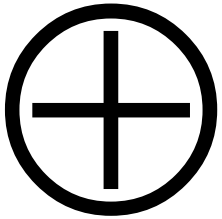


- Web threats
  - ICT web threats
  - Smartphone threats

Mitigation of web threats (2/2)

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

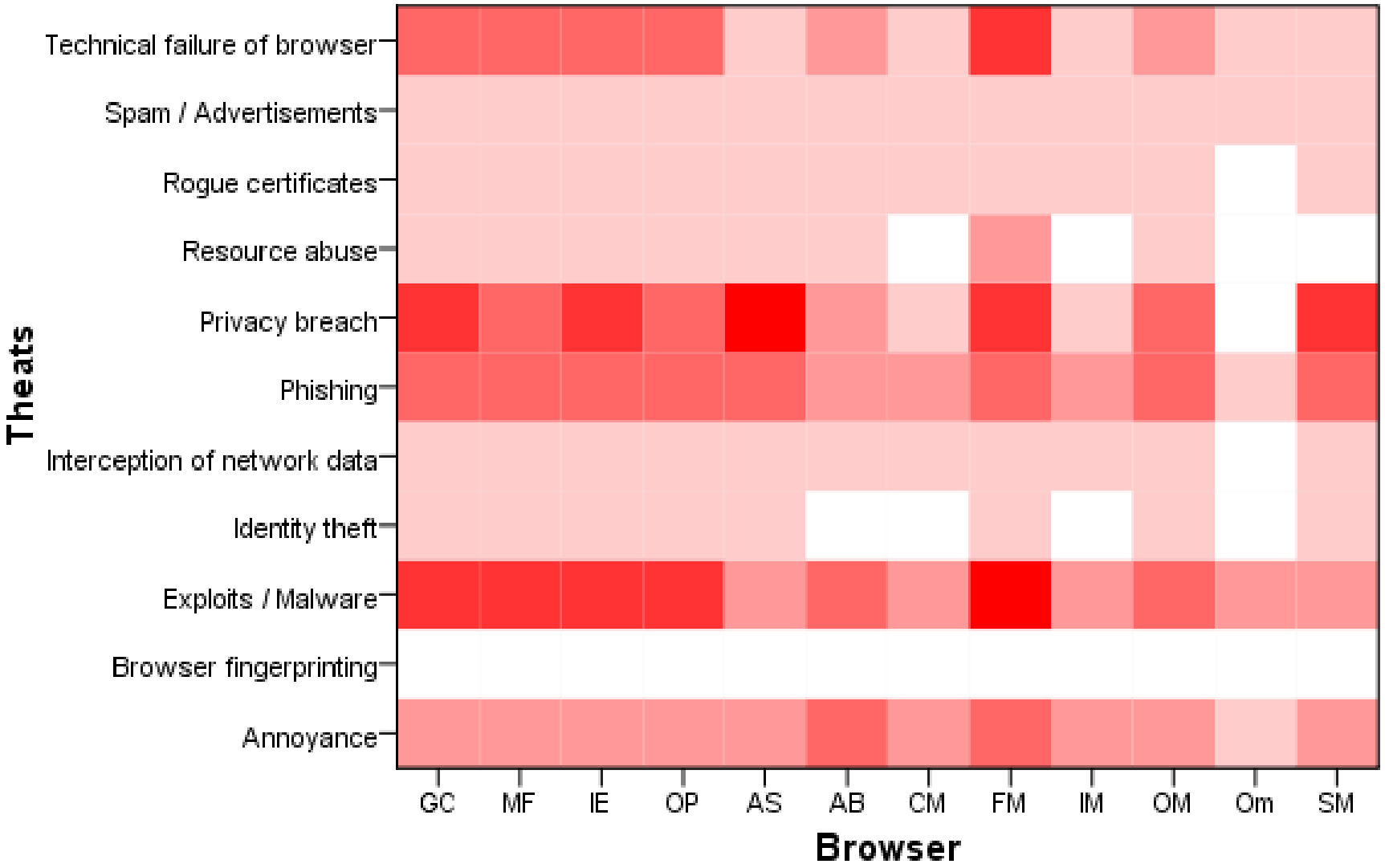
- Web threats
  - ICT web threats
  - Smartphone threats



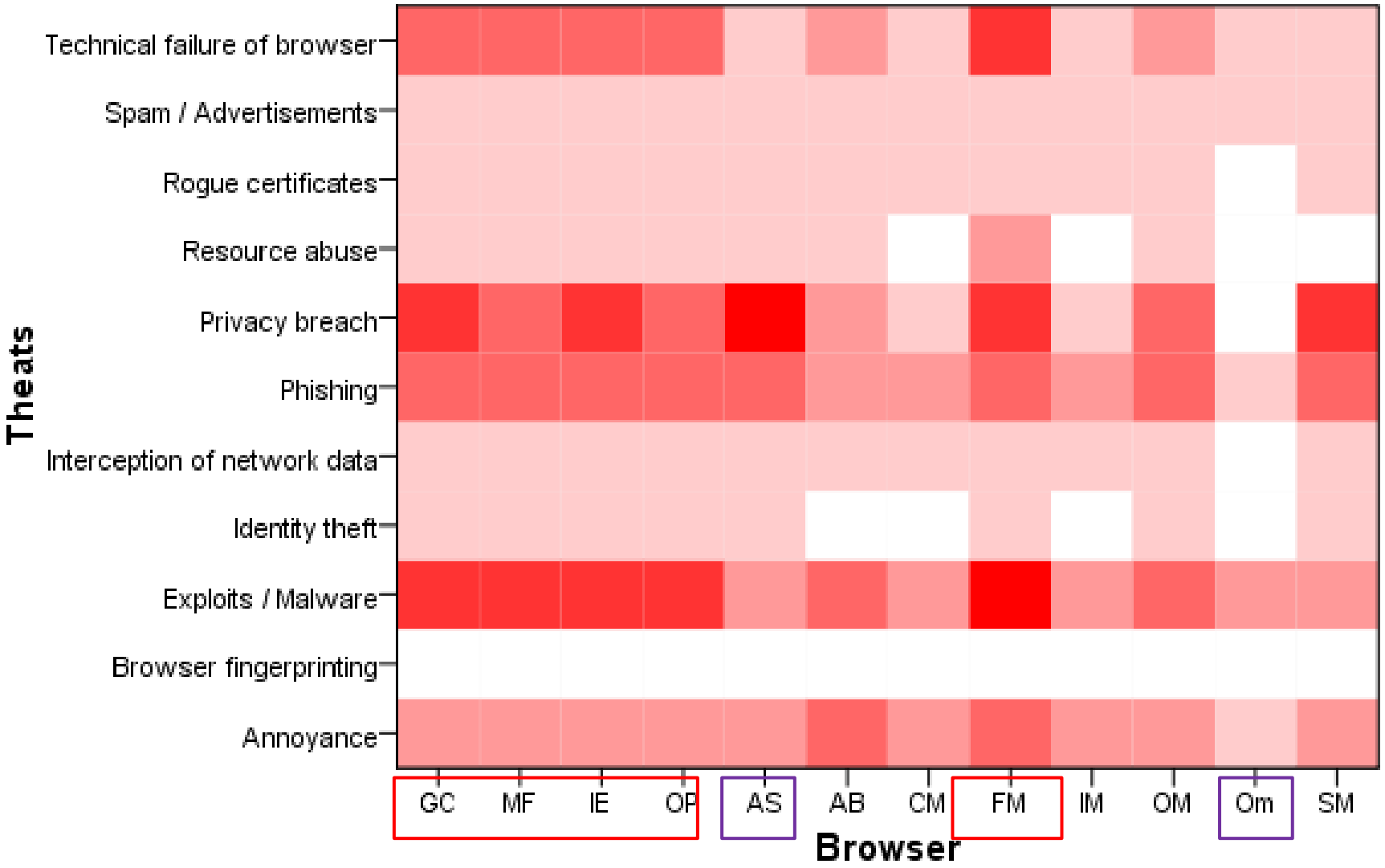
a) default protection per threat

b) manageability of controls per threat

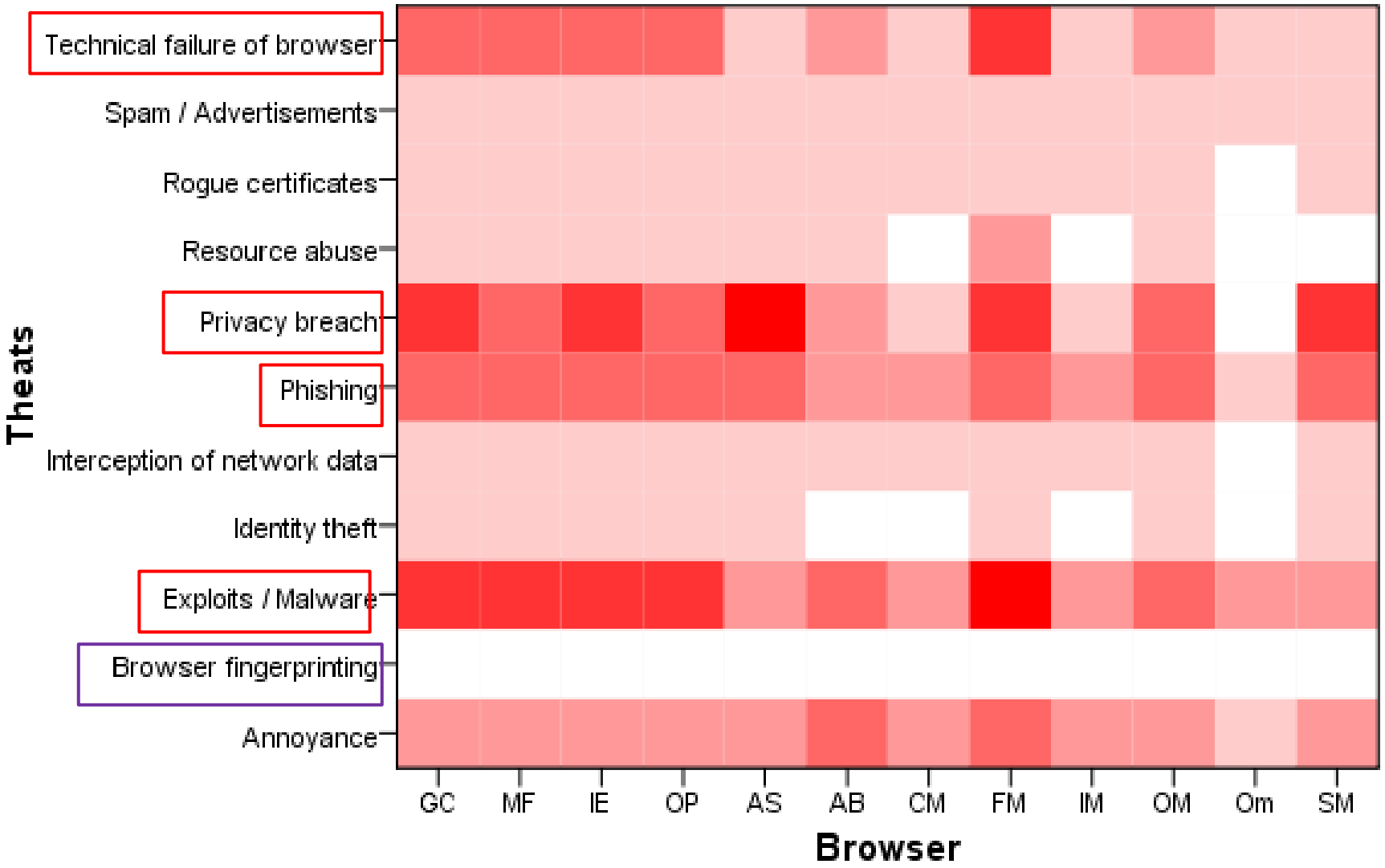
Default protection /threat



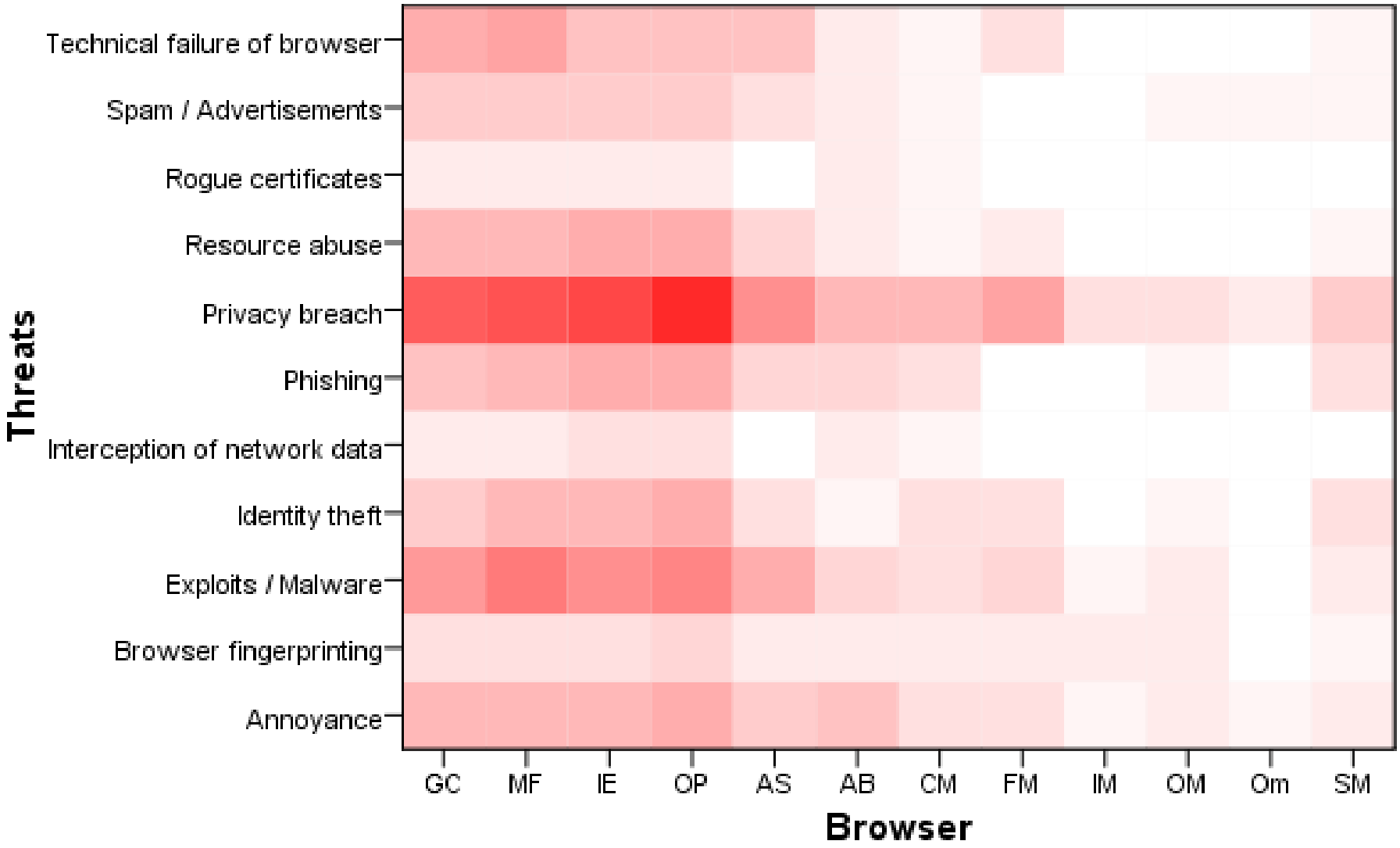
Default protection /threat



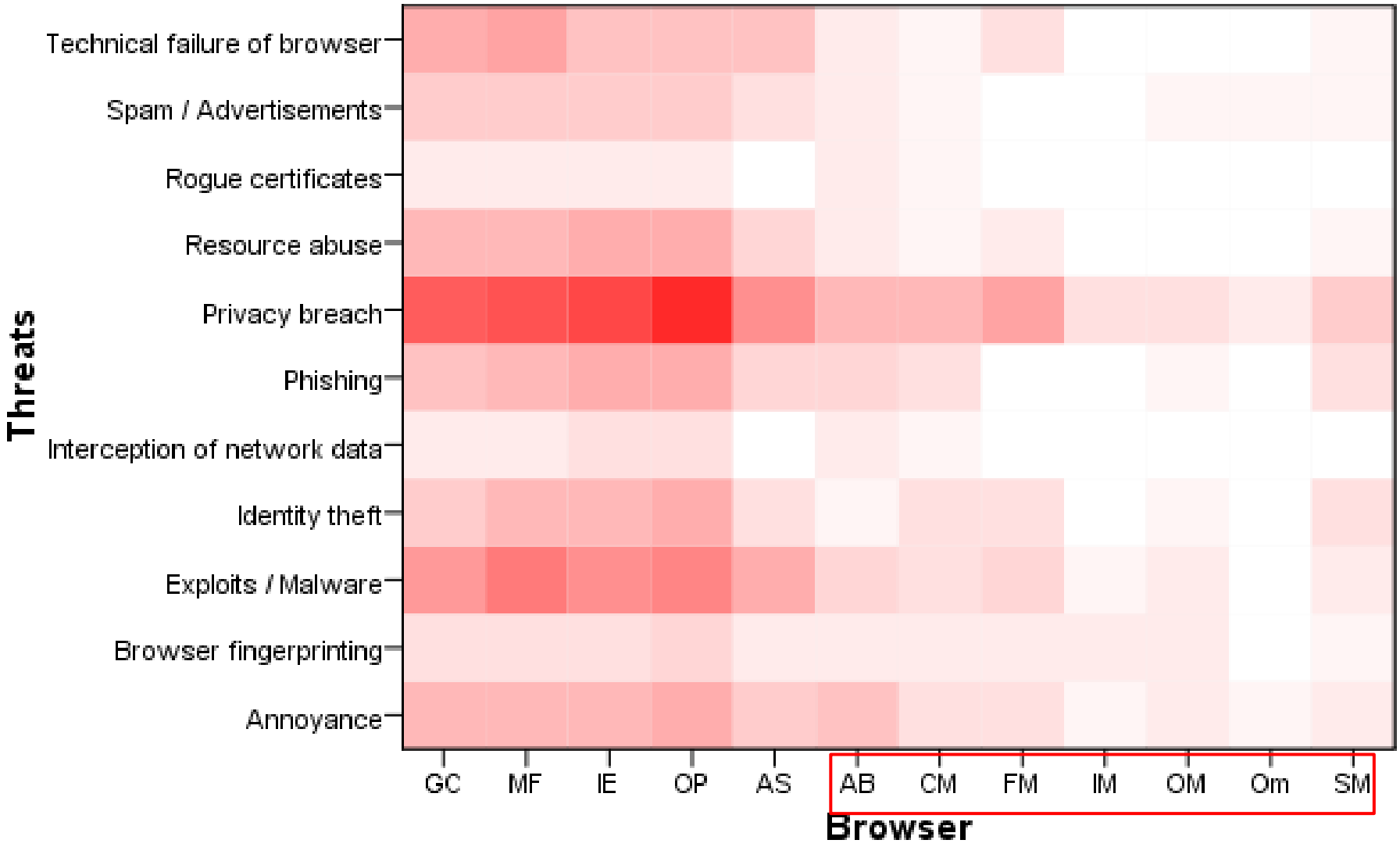
Default protection /threat



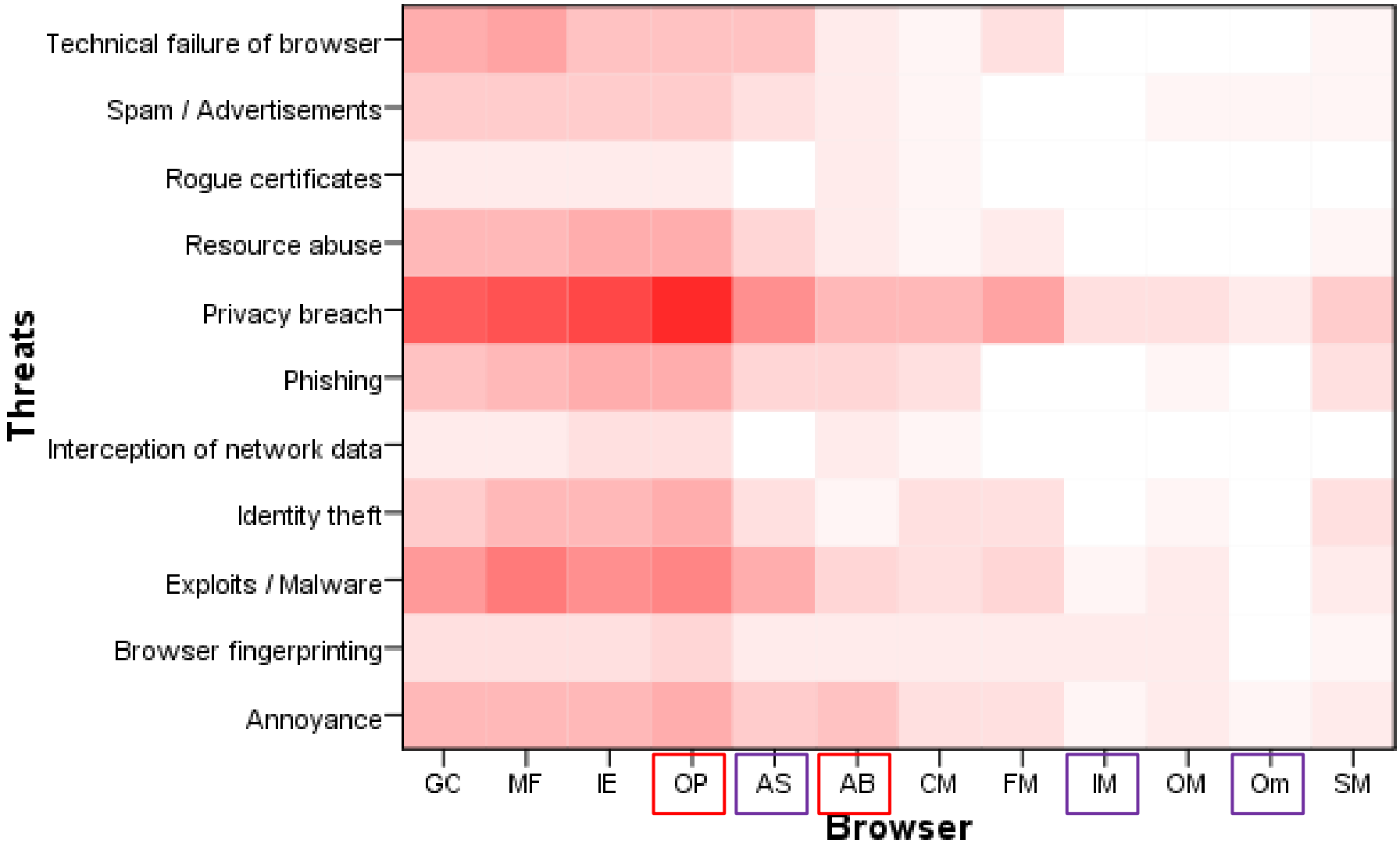
Manageability of controls /threat



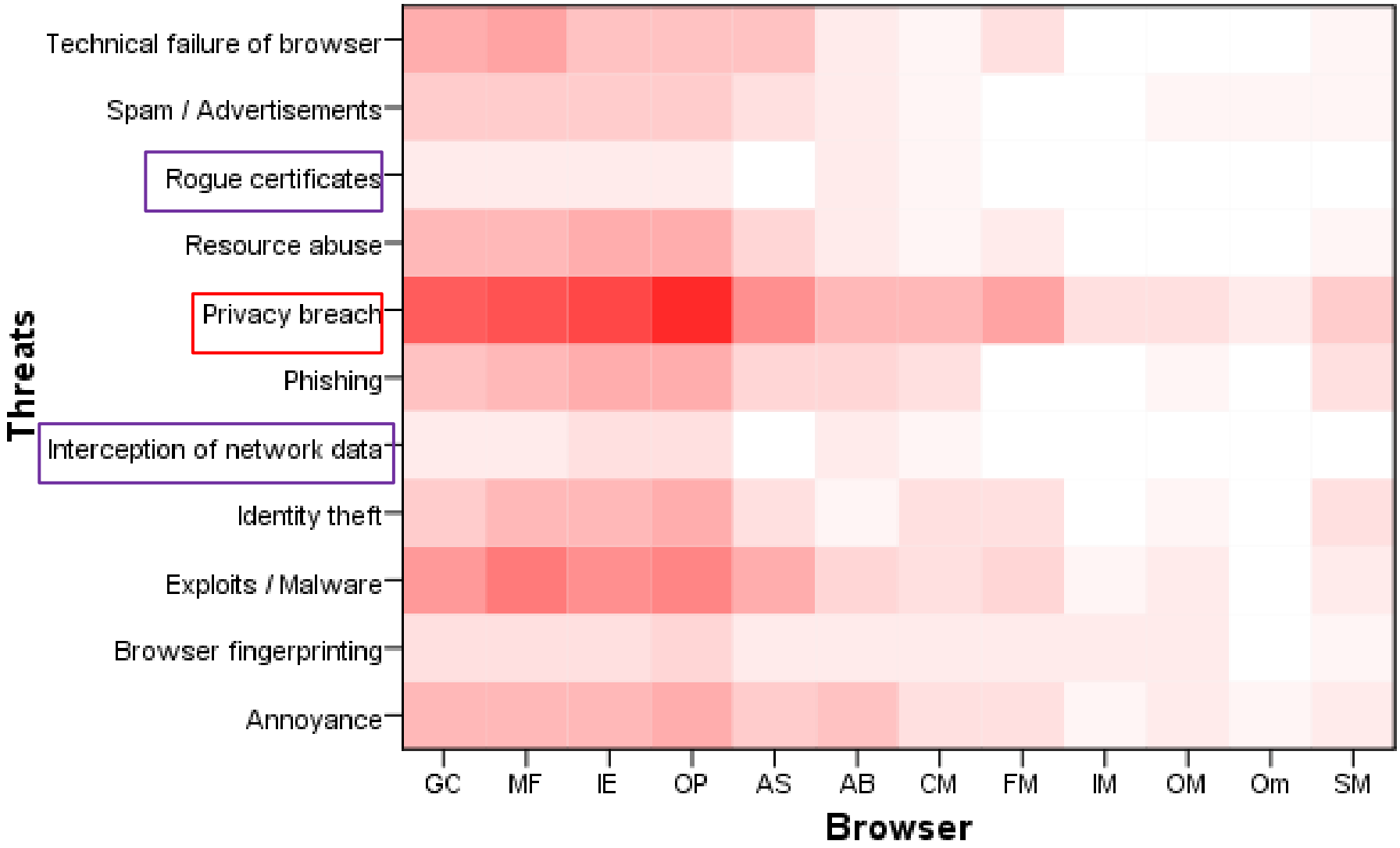
Manageability of controls /threat



Manageability of controls /threat



Manageability of controls /threat



Recommendations (1/2)

Vendor Settings & UI

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

Proposed Settings & UI

- Security-oriented
  - all controls configurable
    - except for certificate warning, malware/ phishing protection
      - users should be discouraged to change them

Recommendations (1/2)

Vendor Settings & UI

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

Proposed Settings & UI

- Security-oriented
  - all controls configurable
    - except for certificate warning, malware/ phishing protection
      - users should be discouraged to change them
    - confirmation should be asked for update settings

Recommendations (1/2)

Vendor Settings & UI

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

Proposed Settings & UI

- Security-oriented
  - all controls configurable
    - except for certificate warning, malware/ phishing protection
      - users should be discouraged to change them
    - confirmation should be asked for update settings
  - default enabled
    - but users asked for
      - Block cookies, Block location data, Block third-party cookies, Enable do-not-track, and Master password

Recommendations (2/2)

- 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

Conclusions and Future Work

- Comprehensive analysis of **availability** and **manageability** of security controls
  - **Out-of-the-box protection** against web threats
  - **Flexibility** to adjust the offered protection w.r.t. user's **risk appetite**
- Browser users
  - Select a browser
  - Adjust their settings
- Browser vendors
  - Cross compare their security
- Further research
  - Further comparison of protection against threats ?

Thank you!

- Now
- Later
  - amylonas@aueb.gr
  - amylwnas@gmail.com