CISPA
HELMHOLTZ-ZENTRUM i. G.

A User-Centric Approach to Securing the HTTPS Ecosystem

Who should we blame for security misconfigurations and vulnerable code?

Usability of Configuring HTTPS

“I have no idea what I’m doing“ - On the Usability of Deploying HTTPS, Krombholz et al., Usenix Security’17

Mental Models of HTTPS

“If HTTPS were secure, I wouldn’t need 2FA“ - End User and Administrator Mental Models of HTTPS, Krombholz et al., IEEE S&P’19

Security Misconfigurations in Companies

Operators’ Perspective on Security Misconfigurations, Dietrich et al., CCS‘19

HTTPS

- Encrypted version of HTTP using Transport Layer Security (TLS)
- Protocol to secure information in transit
- Ensures privacy and data integrity between communication parties
- Certificates/Extended Validation (EV) certificates

The Internet ecosystem 2014

Monthly Scan: April 05, 2014

Previous Next

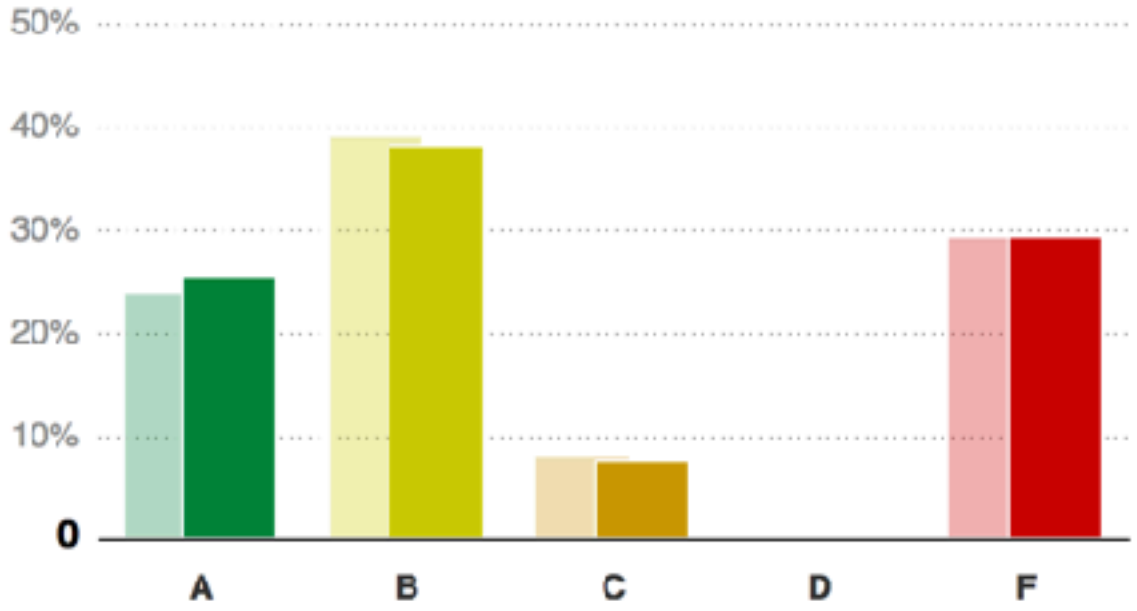
SSL Security Summary

Total sites surveyed
157,281
- 0.6 %

Inadequate security
117,483
- 1.4 %

Secure sites
A+ A A-
39,798
+ 1.4 %

SSL Labs Grade Distribution



source: Qualy's SSL Labs ssllabs.com

The Internet ecosystem 2014

The Internet ecosystem 2019

Monthly Scan: June 03, 2019

Previous Next

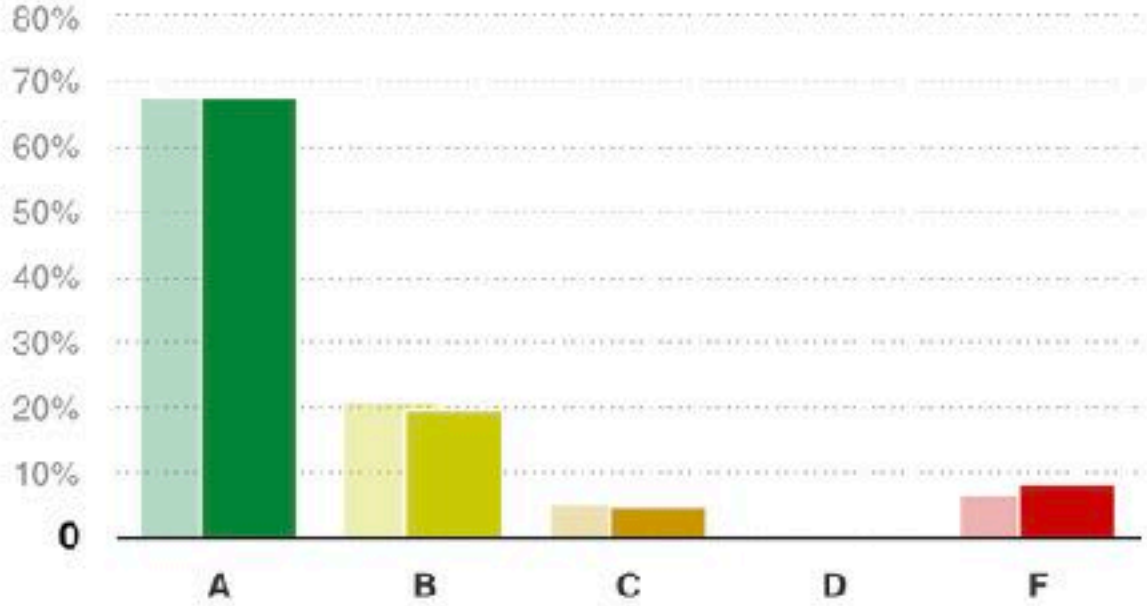
SSL Security Summary

Total sites surveyed
139,659
- 0.2 %

Inadequate security
45,746
+ 0.2 %

Secure sites
A+ A A-
93,913
- 0.2 %

SSL Labs Grade Distribution



source: Qualy's SSL Labs ssllabs.com

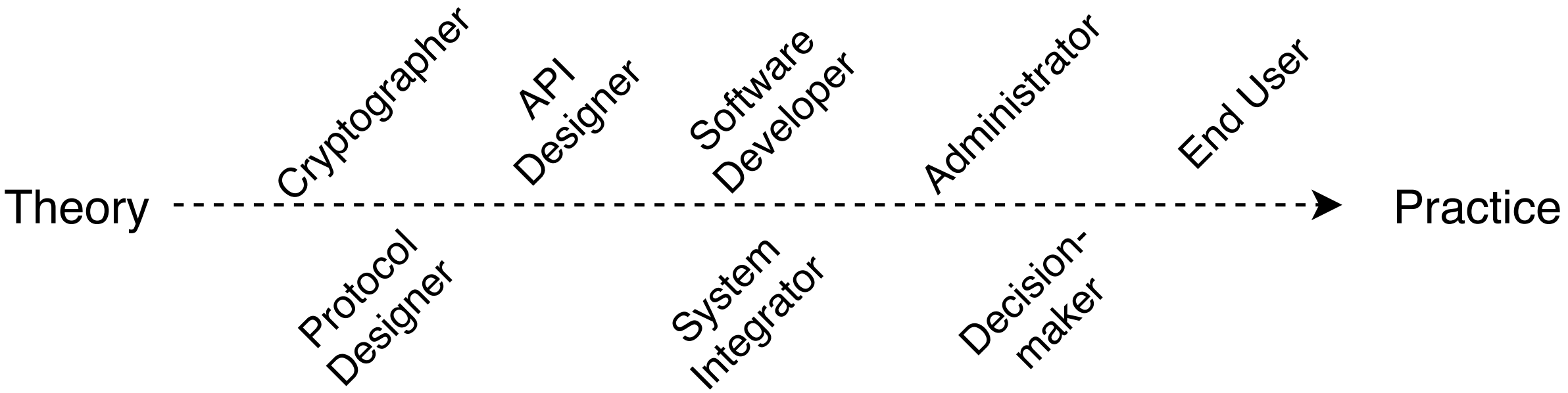
What happened since 2014?

The Google Chrome Team worked on Improving Security Indicators

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	https://www	https://mixe	https://wro	www.examp	Symantec Co	https://dow
Edge 20 Win	example.	https://mix	wrong.host.bads	example.com	Symantec Co	Unsafe website
Firefox 44 Win	https://www.e	https://mixed	https://expire	www.example	Symantec Corpo	https://spacet
Safari 9 Mac	example.com	mixed.badssl.c	*URL hidden*	example.com	Symantec Corp	downloadgam
Chrome 48 And	https://w	https://mixe	https://w	www.examp	https://w	https://spac
Opera Mini 14 And	www.examp	mixed.badssl.c	wrong.host.ba	www.example	www.syma	*Unavailable*
UC Mini 10 And	Example D	mixed.bads	*Blocked*	Example D	Endpoint, C	*Blocked*
UC Browser 2 iOS	Example Do.	mixed.bads..	wrong.host..	Example Do.	Endpoint, C.	*Unavailable*
Safari 9 iOS	example.c	mixed.badss	wrong.host	example.com	Symantec	*Unavailable*

Porter Felt et al. (2016): Rethinking Connection Security Indicators

Usable security should consider all users



Usability of Configuring HTTPS

“I have no idea what I’m doing“ - On the Usability of Deploying HTTPS, Krombholz et al., Usenix Security’17

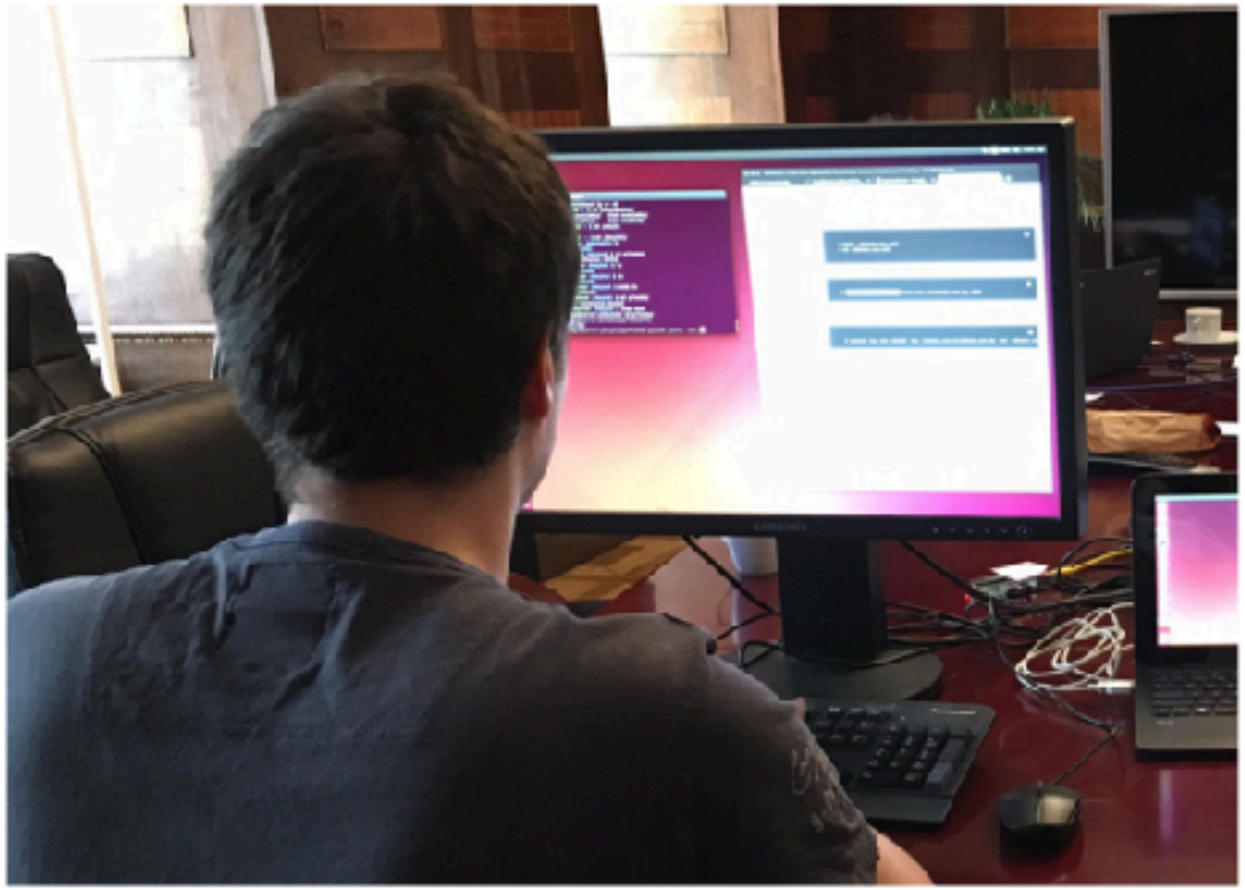
Mental Models of HTTPS

“If HTTPS were secure, I wouldn’t need 2FA“ - End User and Administrator Mental Models of HTTPS, Krombholz et al., IEEE S&P’19

Security Misconfigurations in Companies

Operators’ Perspective on Security Misconfigurations, Dietrich et al., CCS‘19

Usability from the Administrators' Perspective



Measuring HTTPS usability from the administrators' perspective

CISPA HELMHOLTZ-ZENTRUM i. G.

1. Recruitment Questionnaire

- N=117
- Multiple choice
- Top 30 candidates were invited to participate in the study

2. Lab Study

- N=28
- Think-aloud protocol
- Bash/browser history
- VM images

3. Post-Study Questionnaire

- N=28
- Open/closed-ended questions
- Demographics, previous experience

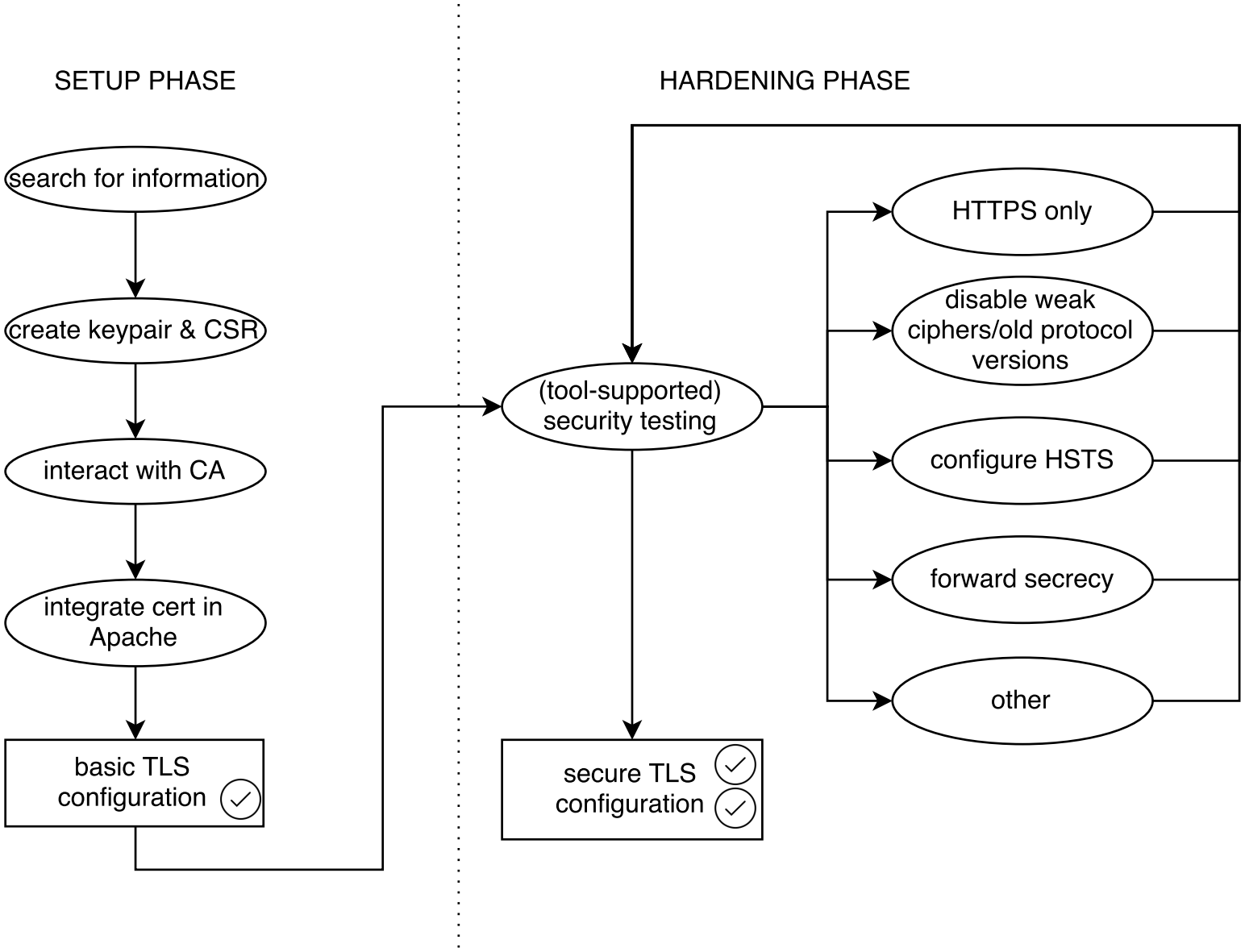
4. Expert Interviews

- N=7
- Semi-structured interviews
- Ecological validity

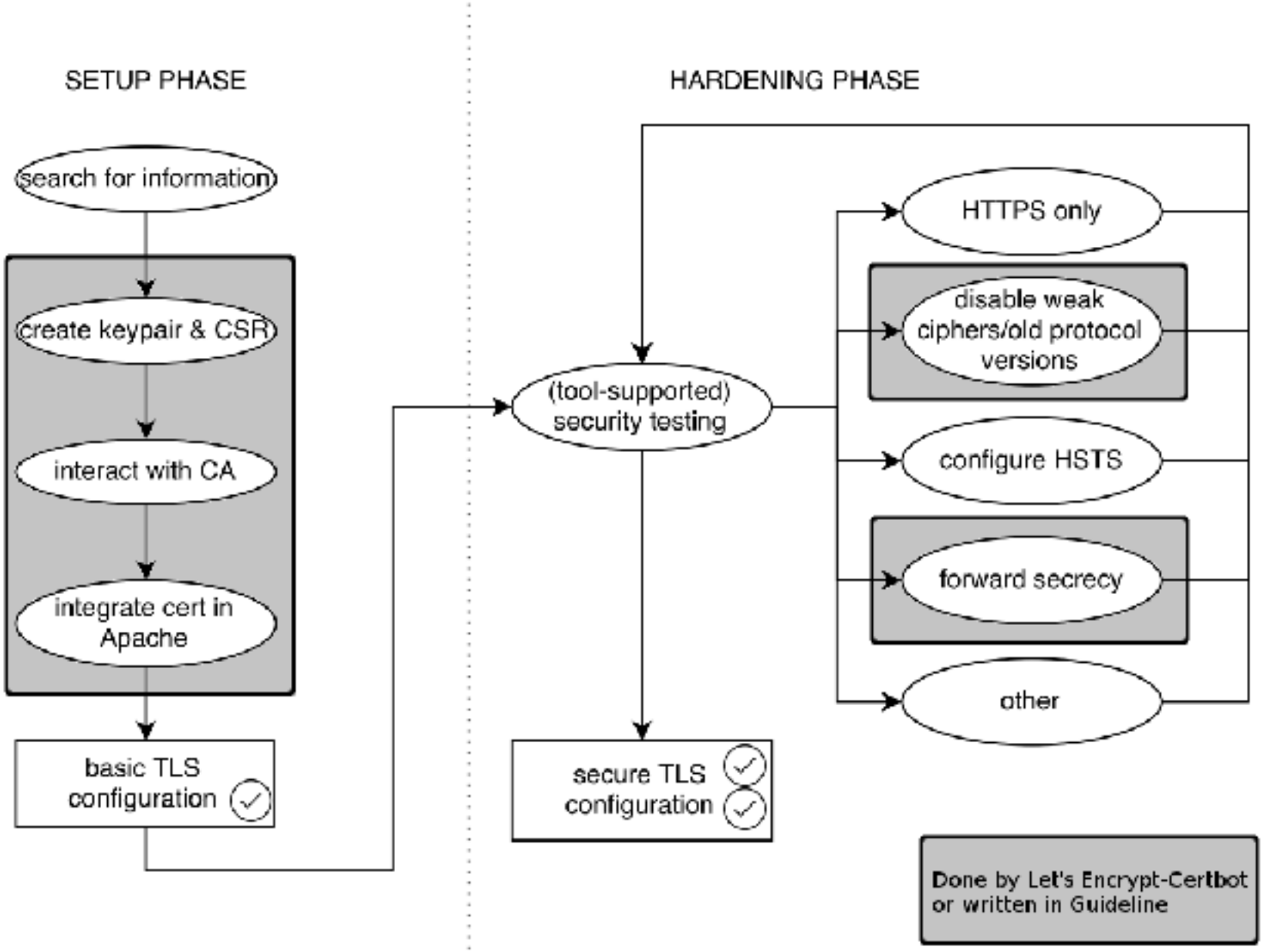
User Research - Qualitative vs. Quantitative Data

- Qualitative research
  - answer questions like “*why?*“, “*how?*“
  - smaller sample size
  - go deep
  - exploratory
- Quantitative research
  - answer questions like “*how many?*“
  - larger sample size (depending on statistical assumptions and models)
  - go broad
  - quantify phenomena

The standard deployment process is complicated



The standard deployment process vs. let's encrypt



Usability Was Considered From The Administrators' Perspective

ID	Grade	Errors / Warnings / Highlights	Cipher Strength Score	Key Exchange Score	Protocol Support Score	Common Name	Key Size	Certificate Chain Length	Used Provided CA to Sign	Encrypted Private Key	SSL 2	SSL 3	TLS 1.0	TLS 1.1	TLS 1.2	RC4 Support	Vulnerable to POODLE (SSL 3)	Forward Secrecy	HSTS	HPKP
P1	A	2	90	90	95	web.local	4096	3	●	○	○	○	●	●	●	○	○	●	●	○
P2	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	○	○
P3	B	2,3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	●	○
P4	A		90	90	95	web.local	2048	3	●	○	○	○	●	●	●	○	○	●	○	○
P5	B		90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	○
P6	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	○	○
P7	Not valid																			
P8	C	3-6,8	90	90	50	web.local	2048	1	●	○	○	●	●	○	○	●	●	◐	○	○
P9	B	1-3	100	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	●
P10	B	1-3	90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	●	●	●
P11	B	3,4	90	90	95	web.local	2048	1	●	●	○	○	●	●	●	○	○	◐	○	○
P12	B	2,3	90	90	95	web.local	4096	1	●	○	○	○	●	○	●	○	○	●	●	○
P13	B	3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P14	A-	4	90	90	100	raspberrypi	2048	1	○	○	○	○	○	○	●	○	○	◐	○	○
P15	C	4,7	50	90	95	-	2048	1	○	○	○	○	●	●	●	●	○	◐	○	○
P16	A-	4	90	90	95	web.local	2048	3	●	○	○	○	●	●	●	○	○	◐	○	○
P17	B	2,3	90	90	95	web.local	3096	1	●	○	○	○	●	●	●	○	○	●	●	○
P18	Not valid																			
P19	B	2,3	90	90	95	web.local	2048	1	●	●	○	○	●	●	●	○	○	●	●	○
P20	B	2,3	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	●	●	○
P21	B	3,4	90	90	95	Test	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P22	B	3,4	90	90	95	web.local	2048	1	●	○	○	○	●	●	●	○	○	◐	○	○
P23	Not valid																			
P24	A	2	90	90	97	web.local	2048	3	●	○	○	○	○	●	●	○	○	●	●	○
P25	B	3	90	90	95	SME	4096	1	●	○	○	○	●	●	●	○	○	◐	○	○
P26	Not valid																			
P27	B	3,4	90	90	95	web.local	4096	1	●	○	○	○	●	●	●	○	○	◐	○	○
P28	A	2	90	90	95	web.local	4096	3	●	○	○	○	●	●	●	○	○	●	●	○

Summary of findings

- ssllabs score does not reflect administrators' mental models
- high effort for hardening
- misconceptions of cipher suites
- compatibility vs. security
- administrators heavily rely on online sources
- misconceptions of terminology and file structures

- consultants report that administrators are "afraid of using crypto"

Usability of Configuring HTTPS

“I have no idea what I’m doing“ - On the Usability of Deploying HTTPS, Krombholz et al., Usenix Security’17

Mental Models of HTTPS

“If HTTPS were secure, I wouldn’t need 2FA“ - End User and Administrator Mental Models of HTTPS, Krombholz et al., IEEE S&P’19

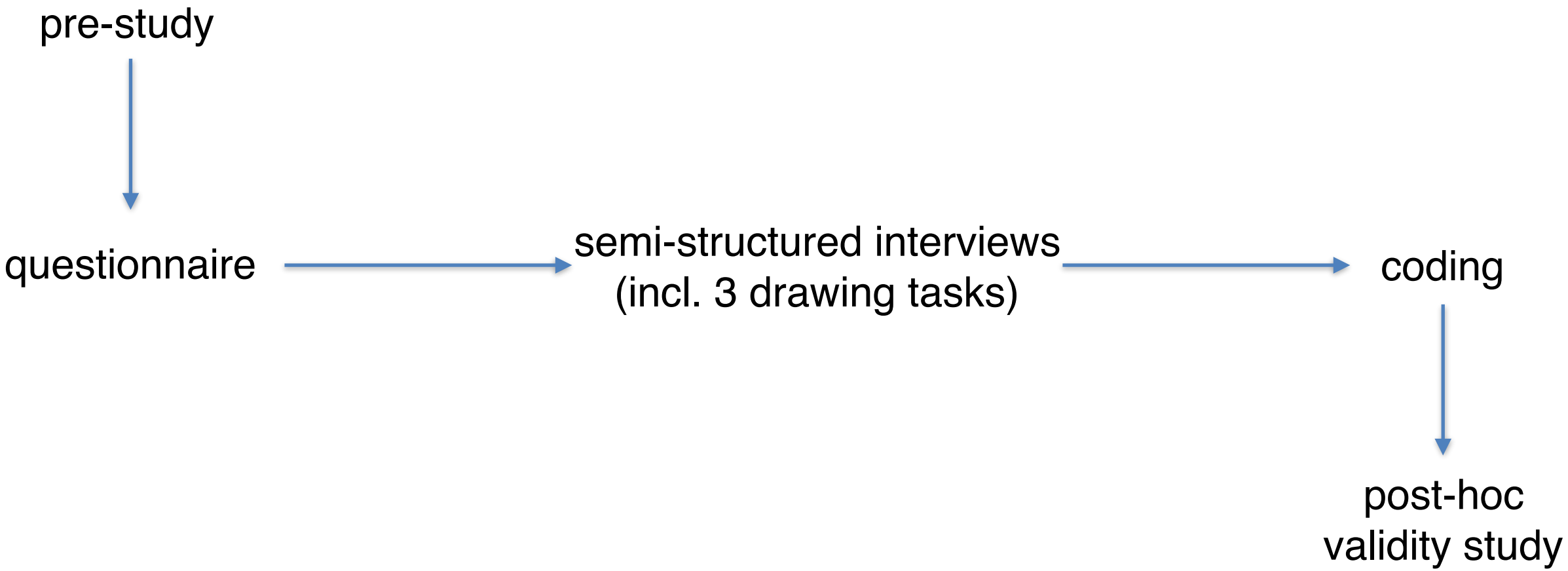
Security Misconfigurations in Companies

Operators’ Perspective on Security Misconfigurations, Dietrich et al., CCS‘19

Mental Models of HTTPS

- mental representation of the surrounding world or technology, the relationships between its various parts and a person's intuitive perception

Study methodology

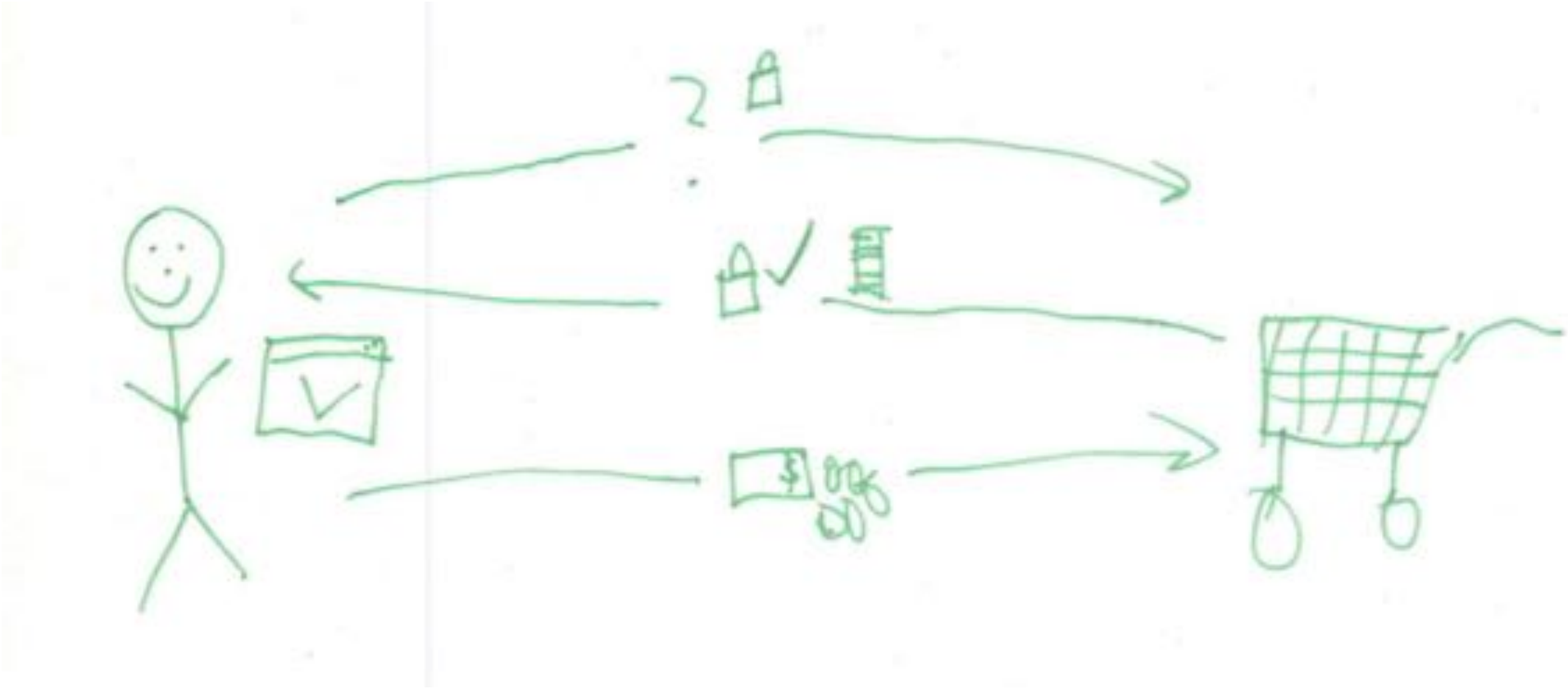


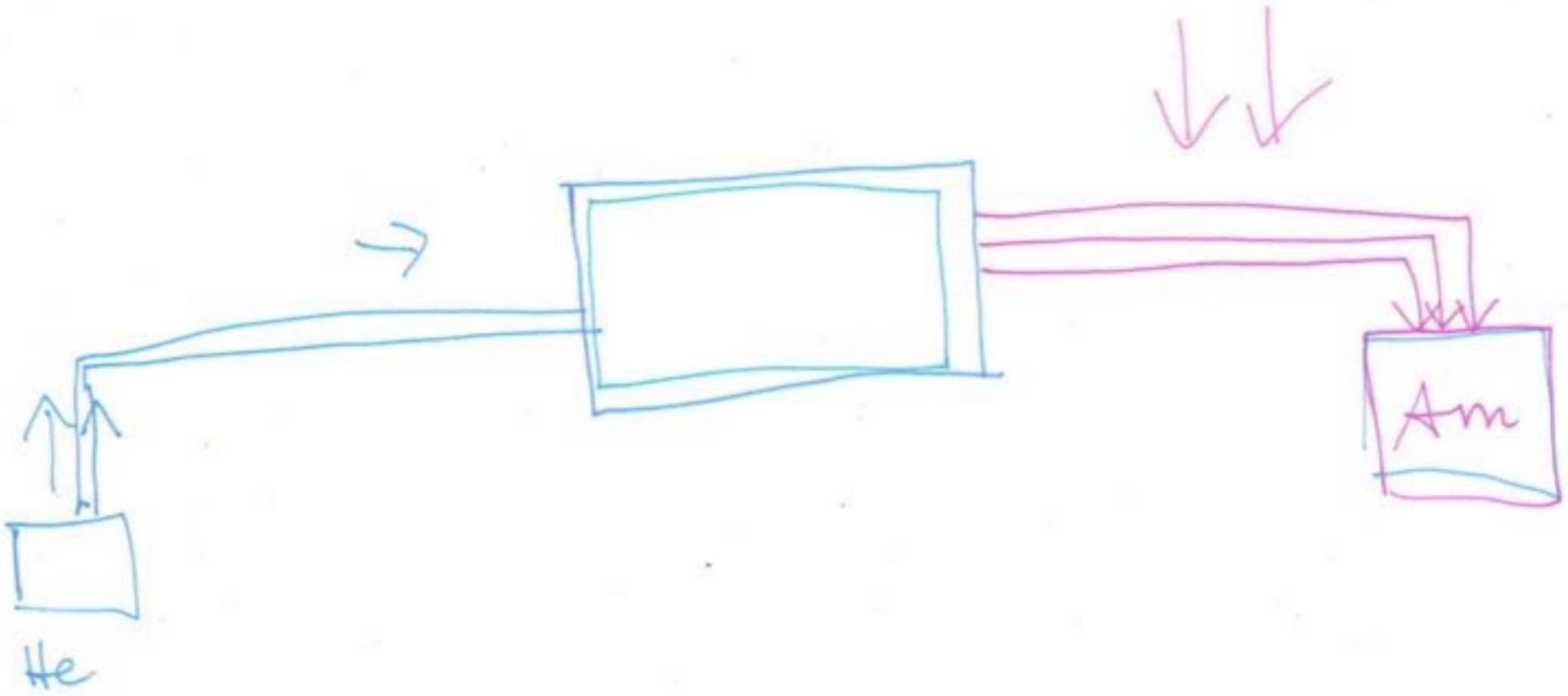
Study methodology - interview guideline

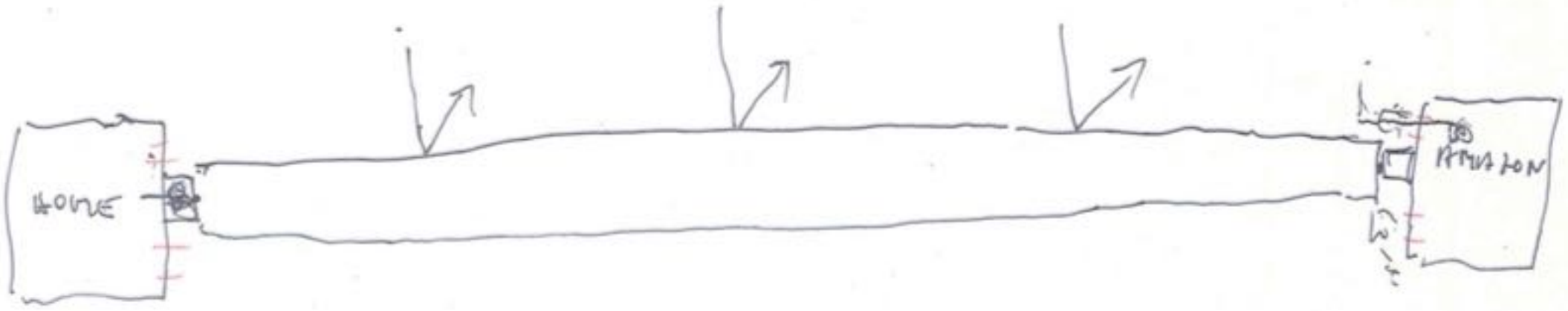
- Interviews
  - general questions about security expectation, behavior
  - drawing tasks
    1. encryption in general
    2. online shopping with HTTPS
    3. online banking with HTTPS
  - attacker models

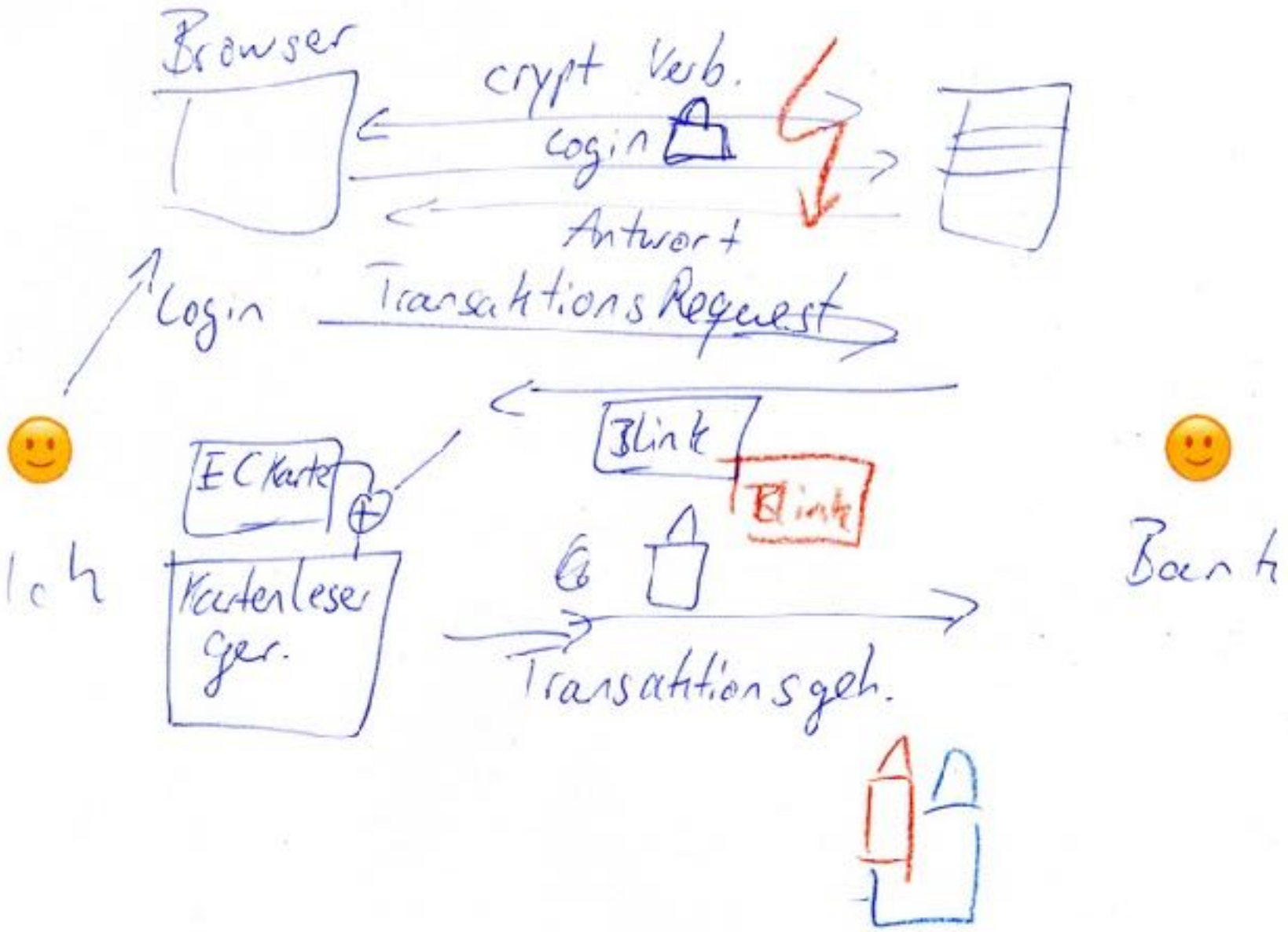
Study methodology - data analysis

- dataset
  - 30 participants (18 end users,12 administrators)
  - quantitative and qualitative data
    - questionnaire
    - drawings
    - hand-written notes
    - audio transcripts
- coding
  - two rounds of open coding (3 independent coders)
  - descriptive axial coding (Strauss & Corbin)
  - selective coding

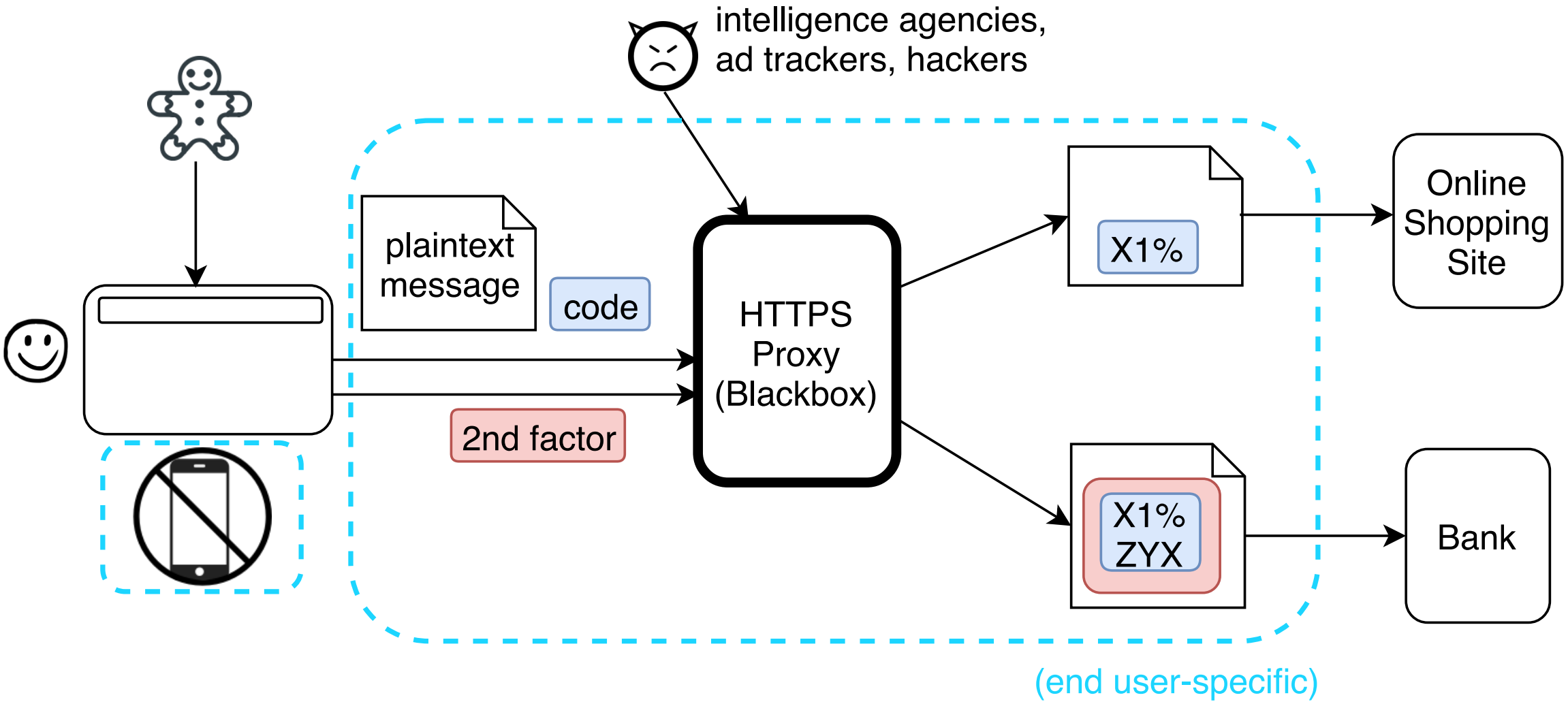



He
Am

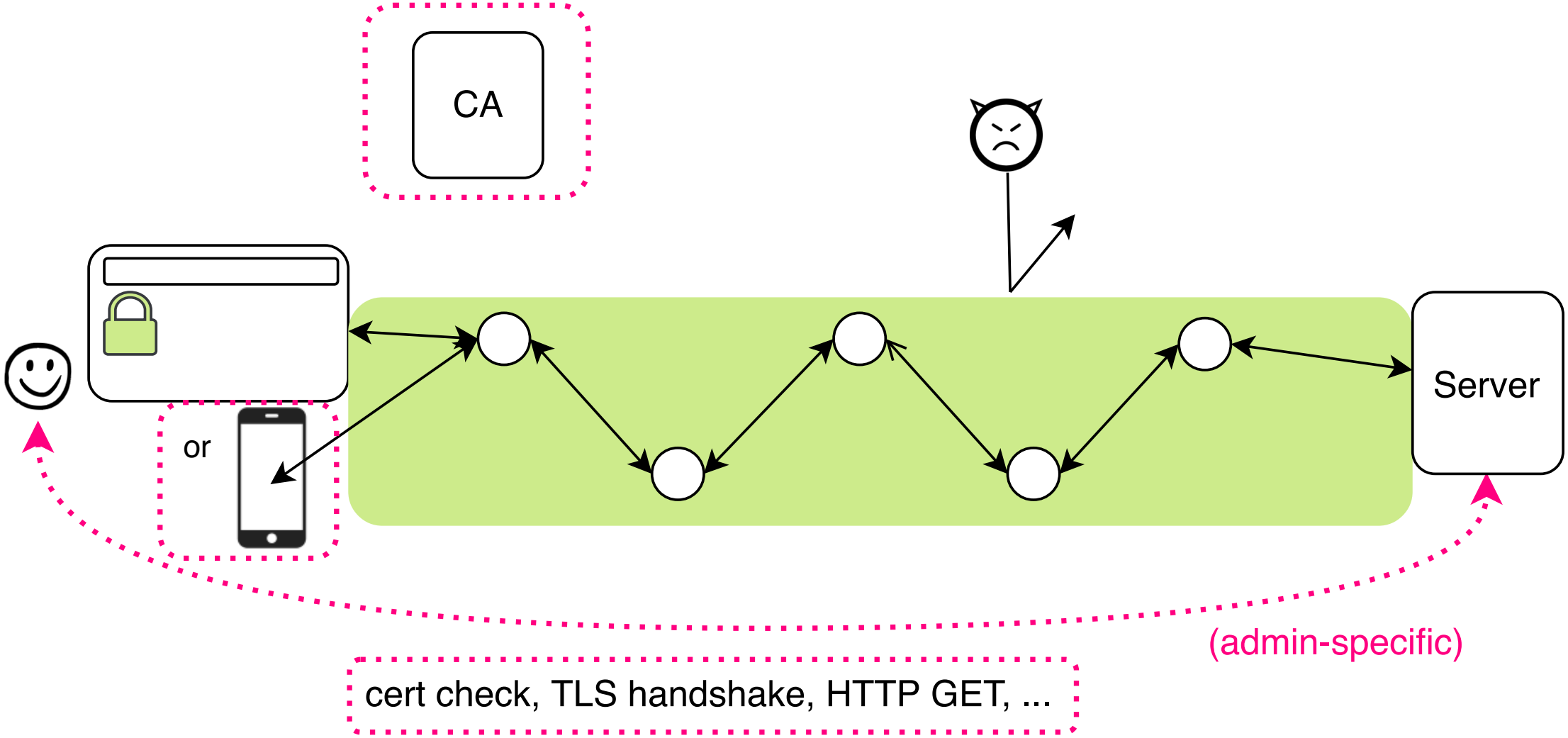

HOME


Browser
crypt Verb.
Login
Antwort
Login
Transaktions Request
Blink
Blink
EC Karte
Kartenleser ger.
Ich
Bank
Transaktionsgeh.

The Worst-Case Model



The Best-Case Model



Summary of findings

- our findings reveal **misconceptions** about security benefits and threat models from both groups.
- we identify **protocol components that interfere with secure configurations and usage behavior**.
- our results suggest that end user mental models are more **conceptual** while administrator mental models are more **protocol-based**.
- end users often **confuse encryption with authentication**
- users **distrust security indicators**.
- administrators often do not understand the **interplay of protocol components**.

Usability of Configuring HTTPS

“I have no idea what I’m doing“ - On the Usability of Deploying HTTPS, Krombholz et al., Usenix Security’17

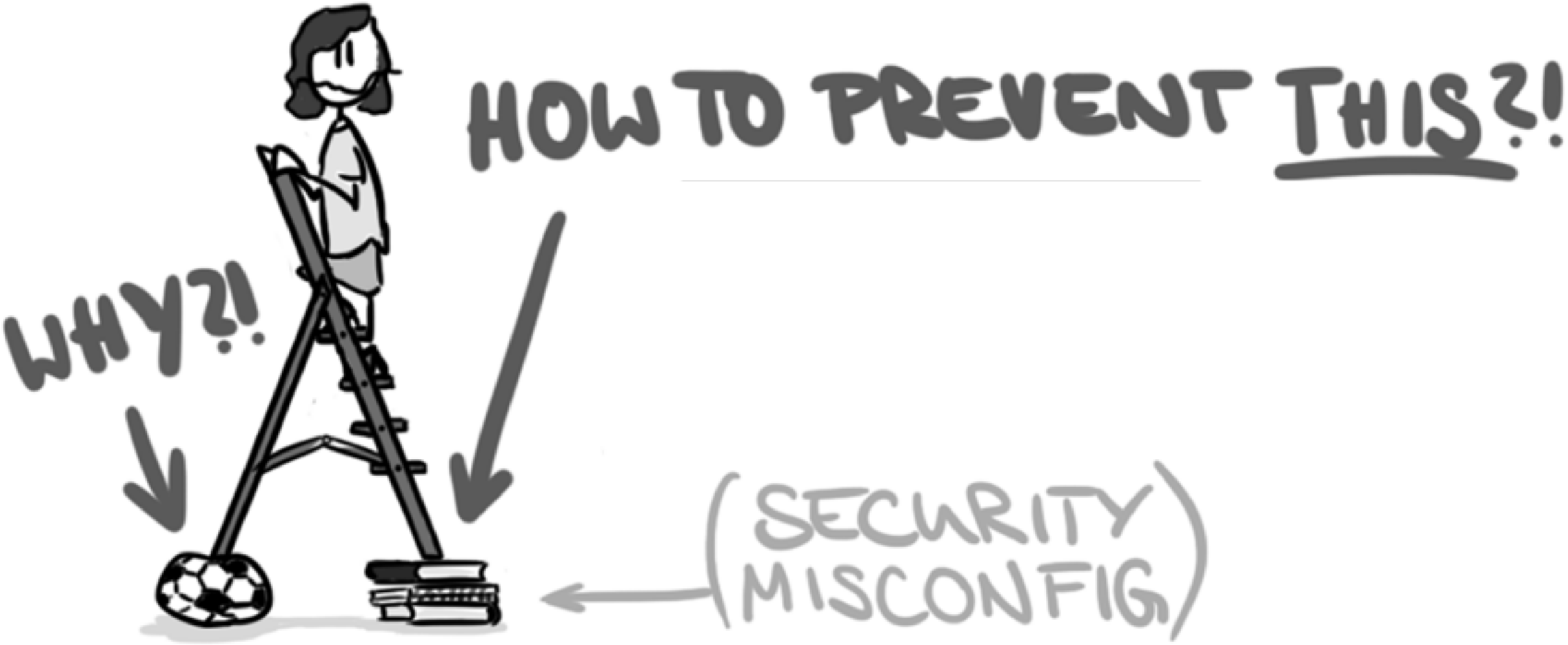
Mental Models of HTTPS

“If HTTPS were secure, I wouldn’t need 2FA“ - End User and Administrator Mental Models of HTTPS, Krombholz et al., IEEE S&P’19

Security Misconfigurations in Companies

Operators’ Perspective on Security Misconfigurations, Dietrich et al., CCS‘19

What are organizations doing to prevent security misconfigurations?



Organizations struggle with post-mortems and configuration errors

CISPA HELMHOLTZ-ZENTRUM i. G.

Investigating System Operators' Perspective on Security Misconfigurations

Constanze Dietrich — Berliner Hochschule für Technik* — constanze.die@gmail.com

Katharina Krombholz — CISPA Helmholtz Center (i.G.)† — krombholz@cispa.saarland

Kevin Borgolte — Princeton University‡ — kevin@iseclab.org

Tobias Fiebig — TU Delft§ — t.fiebig@tudelft.nl

ABSTRACT

Nowadays, security incidents have become a familiar "nuisance," and they regularly lead to the exposure of private and sensitive data. The root causes for such incidents are rarely complex attacks. Instead, they are enabled by simple misconfigurations, such as authentication not being required, or security updates not being installed. For example, the leak of over 140 million Americans' private data from Equifax's systems is among most severe misconfigurations in recent history: The underlying vulnerability was long known, and a security patch had been available for months, but was never applied. Ultimately, Equifax blamed an employee for forgetting to update the affected system, highlighting his *personal* responsibility.

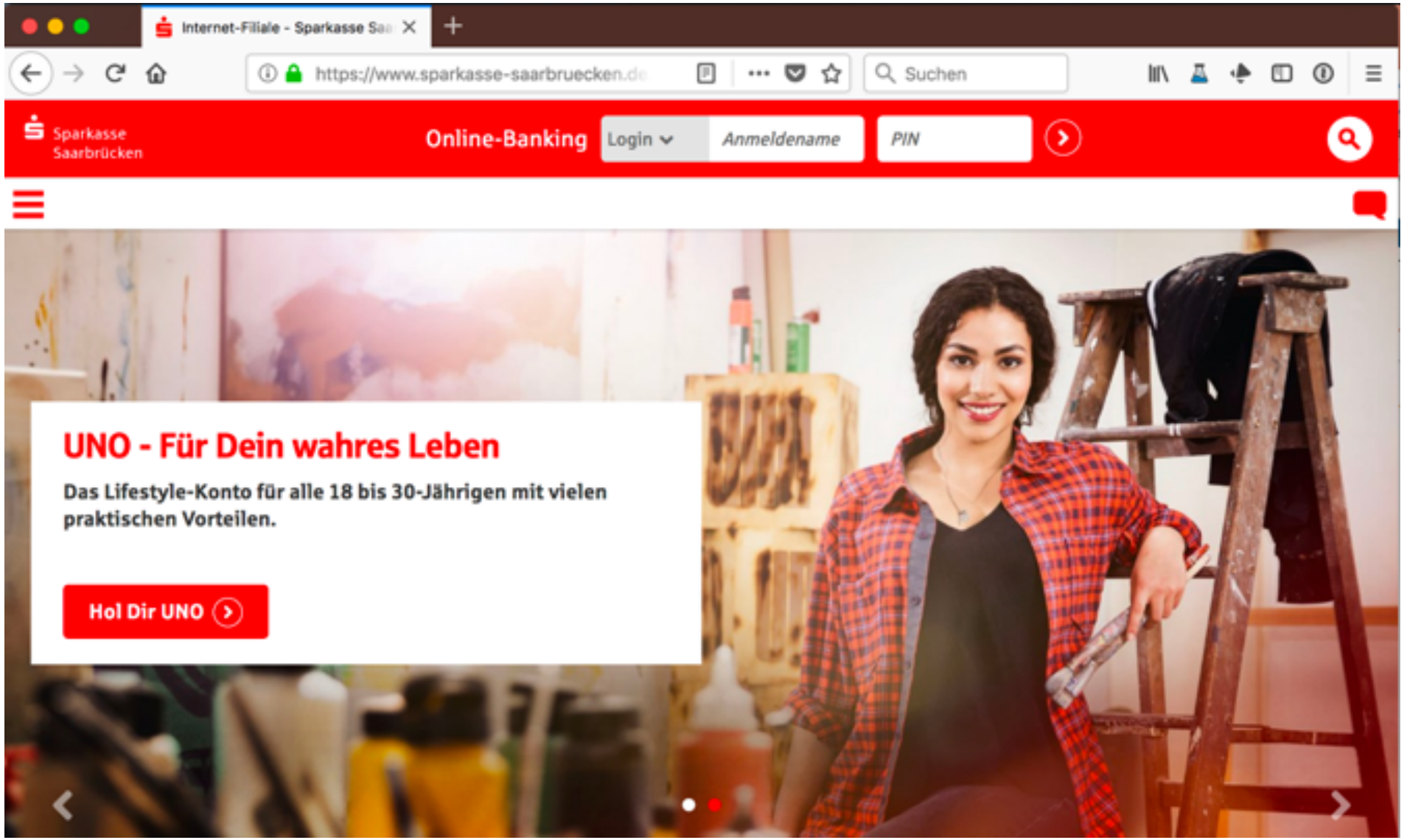
In this paper, we investigate the operators' perspective on security misconfigurations to approach the human component of this class of security issues. We focus our analysis on system operators, who have not received significant attention by prior research. Hence, we investigate their perspective with an inductive approach and apply a multi-step empirical methodology: *(i)* a *qualitative* study to

1 INTRODUCTION

Security incidents and vulnerabilities in today's Internet are often believed to be caused by programming errors, such as faulty input validation, race conditions, or buffer overflows, that are exploited to disrupt services without the vulnerability being publicly known and before a patch is available (0 days). However, when investigating recent security incidents, such as those of Equifax [2,3], we find a different picture. The vulnerability exploited in the primary Equifax incident, in which personally identifiable information of 143 million customers were inadvertently disclosed and which sparked a congressional inquiry, was clearly a programming mistake. However, while a patch to address the bug was released months prior, it was simply not yet deployed to the production environment.

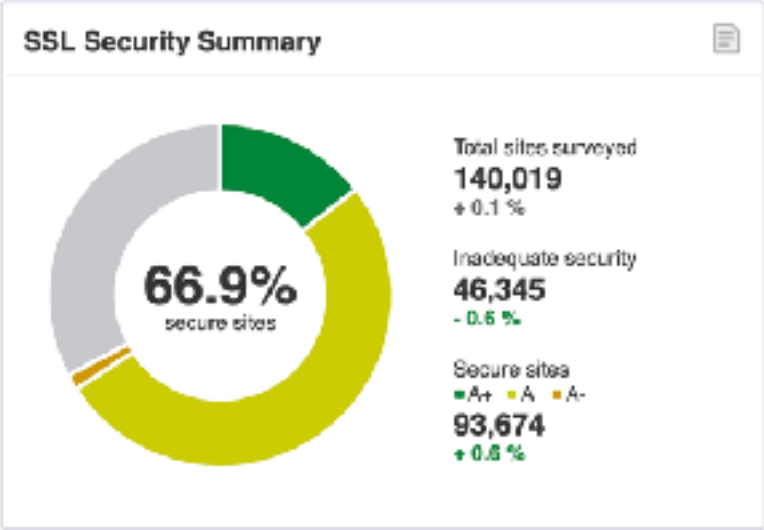
Of course, not applying (security) patches can have its cause in countless reasons, such as technical debt accumulated over time, or availability and functionality requirements. Yet, when investigating the Equifax incident, such complex reasons are not the breach's cause. In the end, Equifax blamed the entire incident on a single

Would you log into this site?



Remaining challenges - what now?

- we need to *again* re-think connection security indicators
- phishing sites have HTTPS - false sense of security
- organizations need blameless post-mortems, more automation, shared responsibilities
- still ~35% of sites are vulnerable (especially the long tail)
- user-centric design approaches!



Remaining challenges - designing security tools

Designing security tools

- design of security APIs, protocols, tools has an impact on user mental models
- how can technology design help to construct meaningful mental models?

  Metaphors

Who should we blame for security misconfigurations and vulnerable code?

https://arstechnica.com/information-technology/2017/09/in-spectacular-fail-adobe-security-team-posts-private-pgp-key-on-blog/

ars TECHNICA

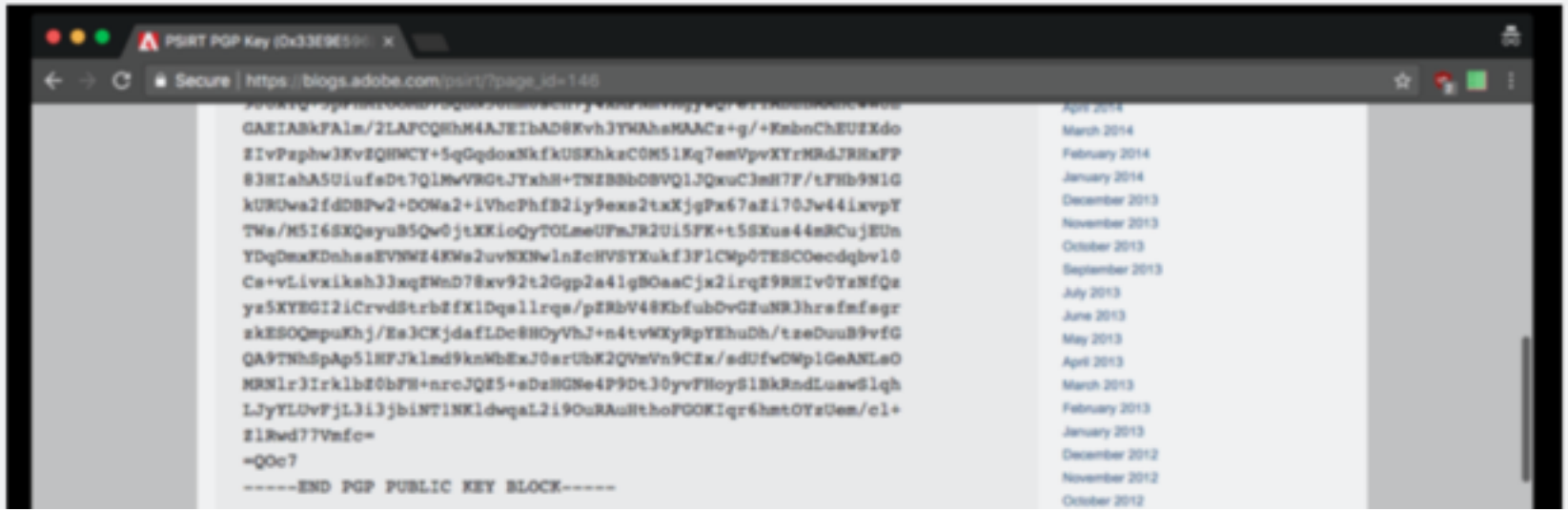
BIZ & IT | TECH | SCIENCE | POLICY | CARS | GAMING & CULTURE | FORUMS

YOU HAD ONE JOB —

In spectacular fail, Adobe security team posts private PGP key on blog

Since deleted, post gave public *and* private key for Adobe incident response team.

SEAN GALLAGHER - 9/22/2017, 10:37 PM



https://techcrunch.com/2017/10/03/former-equifax-ceo-says-breach-boiled-down-to-one-person-not-doing-their-job/?guccounter=1

Former Equifax CEO says breach boiled down to one person not doing their job

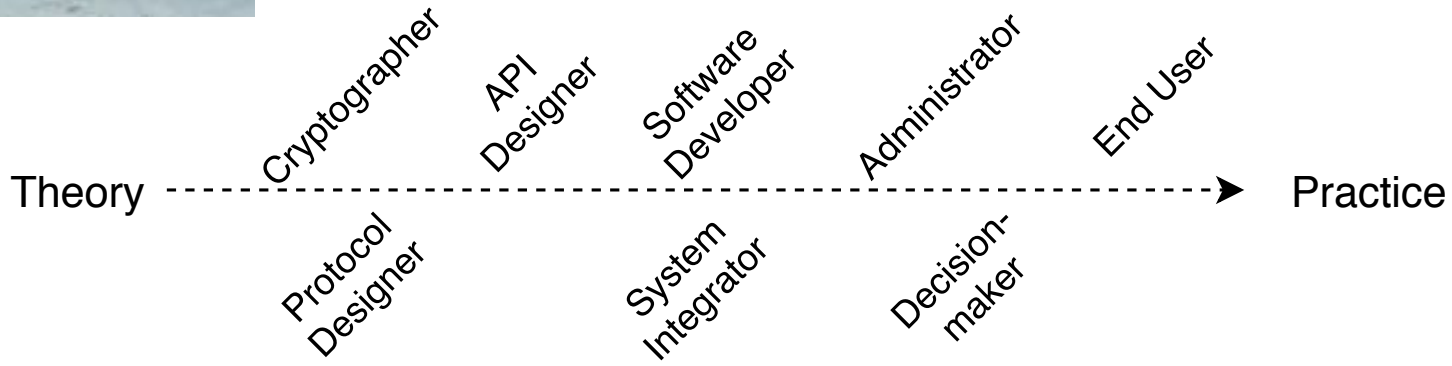
Sarah Buhr @sarahbuhr / 1 year ago

Comment

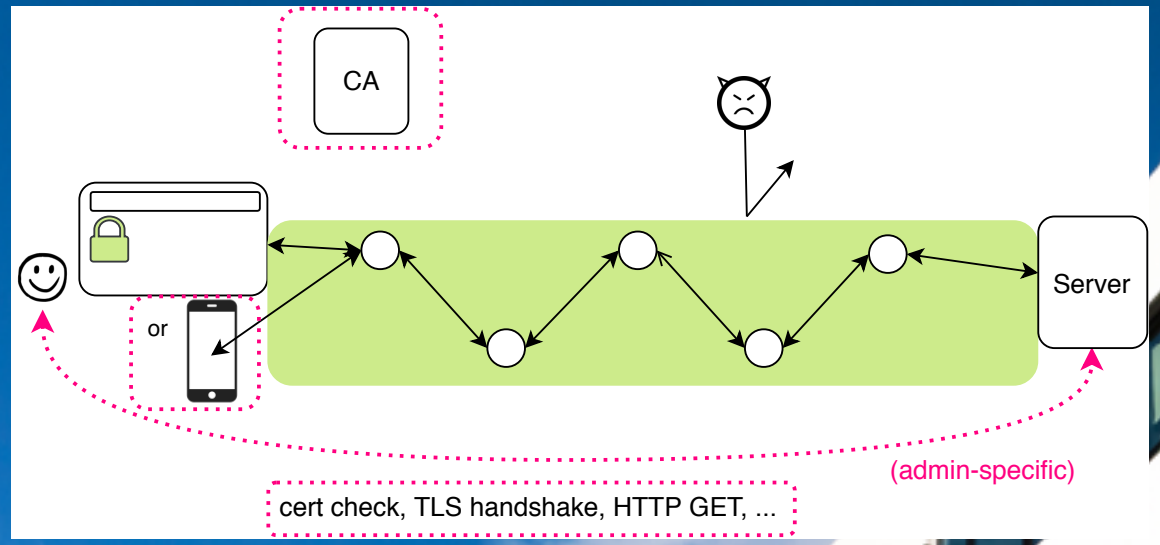
e

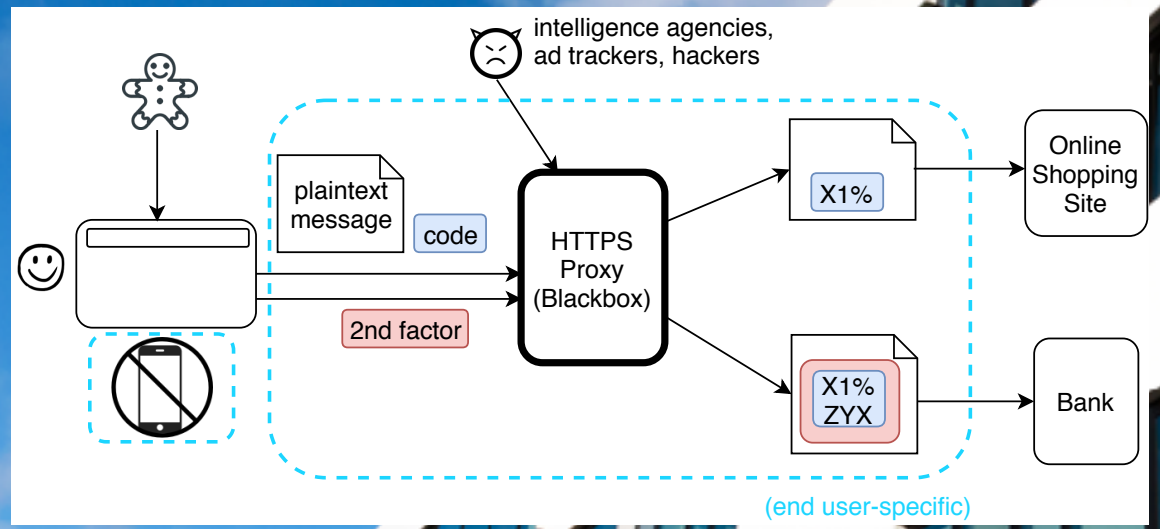
R/VR 2018

“Umbrella conservation“



Summary and Questions





- we have shown that **configuring HTTPS is hard** even for experts, admins heavily **rely on online resources**
- end user mental models are more **conceptual** while administrator mental models are more **protocol-based**.
- users often **confuse encryption with authentication**
- users **distrust security indicators**.
- administrators often do not understand the **interplay of protocol components**.