“I HAVE NO IDEA WHAT I’M DOING” – ON THE USABILITY OF DEPLOYING HTTPS

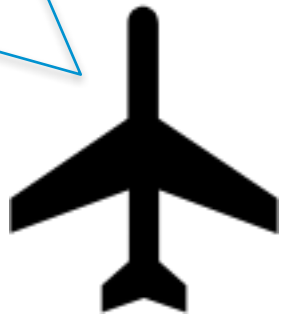
Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, Edgar Weippl

SBA Research

“I HAVE NO IDEA WHAT I’M DOING”

SBA Research

“I HAVE NO IDEA WHAT I’M DOING”



SBA Research

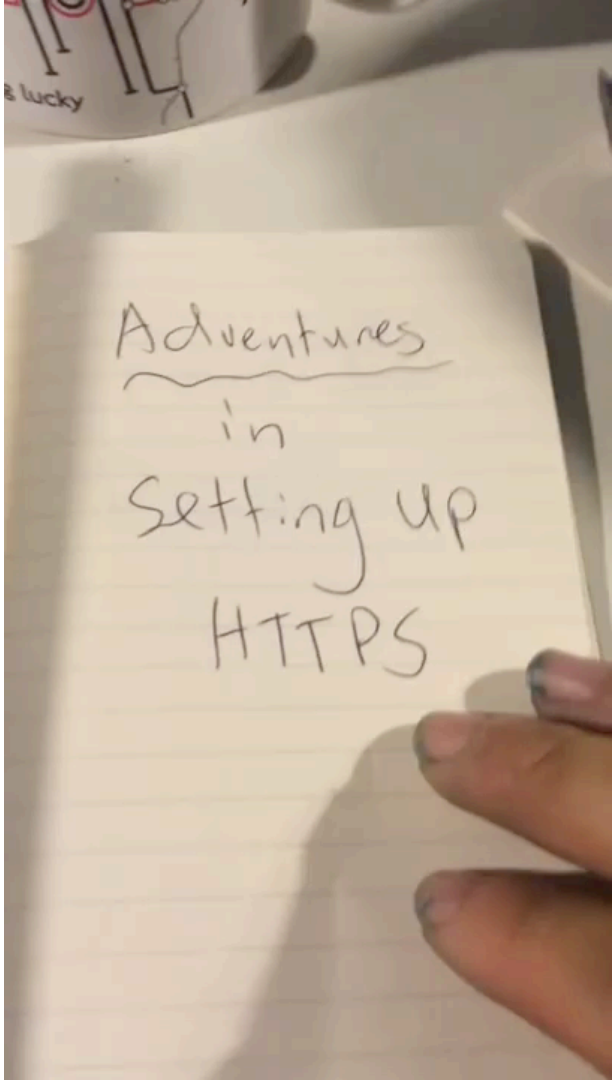
“I HAVE NO IDEA WHAT I’M DOING”

SBA Research

Motivation and Goals

- Explore reasons for TLS misconfigurations – usability from the administrator‘s perspective
- Study Task: Configure HTTPS on Apache
  - HTTP -> HTTPS
  - get a certificate
  - integration, hardening
  - testing
  - done!

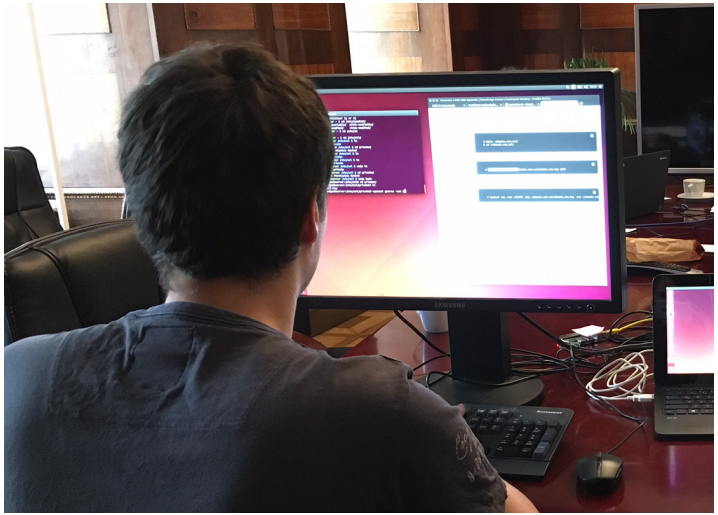
SBA Research

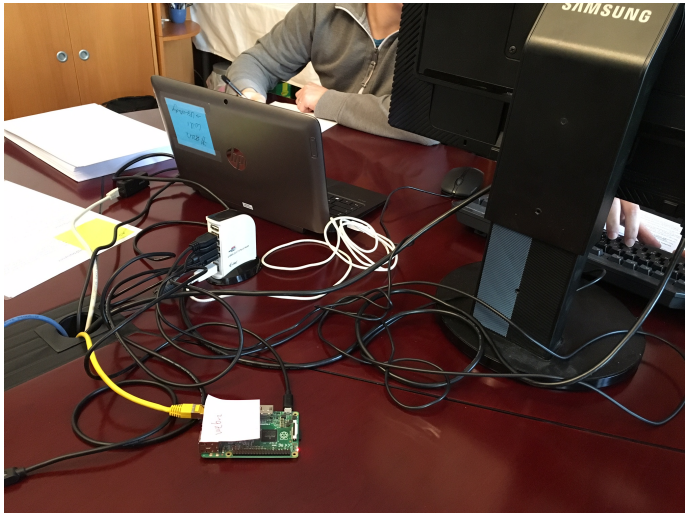


source: **(mis)adventures in setting up HTTPS** by Yan Zhu https://www.youtube.com/watch?v=Q0VdlLG7t1w

User Study – The Expert's Perspective

- Lab study with 28 knowledgeable participants
- Expert interviews with 7 security auditors





SBA Research

Let’s Encrypt

- Eases the interaction with the CA
- Hardening and integration still needs to be done at least once
- Our study focuses on **integration** and **hardening**

Methodology - Data Collection

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

SBA Research

Lab Study - Participants

- N=28
- Gender: 2 female, 26 male
- Experienced admins: 17
- configured TLS before: 17

SBA Research

Data Analysis

- Observation protocols:
  Qualitative analysis with open/axial/selective coding

- Bash/browser history, Apache log files:
  - Quantitative analysis
  - Metrics based on Qualy's SSL Test (grades A-F)

- Statistical significance

Security Evaluation

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	●	○	○	○	●	●	●	○	○	●	●	○

SBA Research

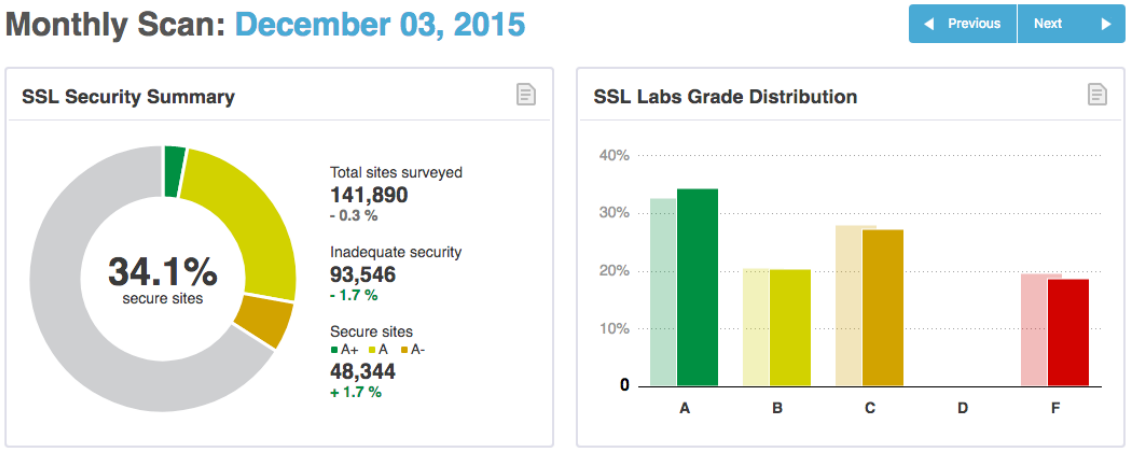
Security Evaluation

- Only 4 participants deployed an A grade configuration (25%)
- 15 deployed a B grade configuration (67%)
- 4 participants did not manage to deploy any valid configuration

SBA Research

Security Evaluation

- Only 4 participants deployed an A grade configuration (25%)
- 15 deployed a B grade configuration (67%)
- 4 participants did not manage to deploy any valid configuration



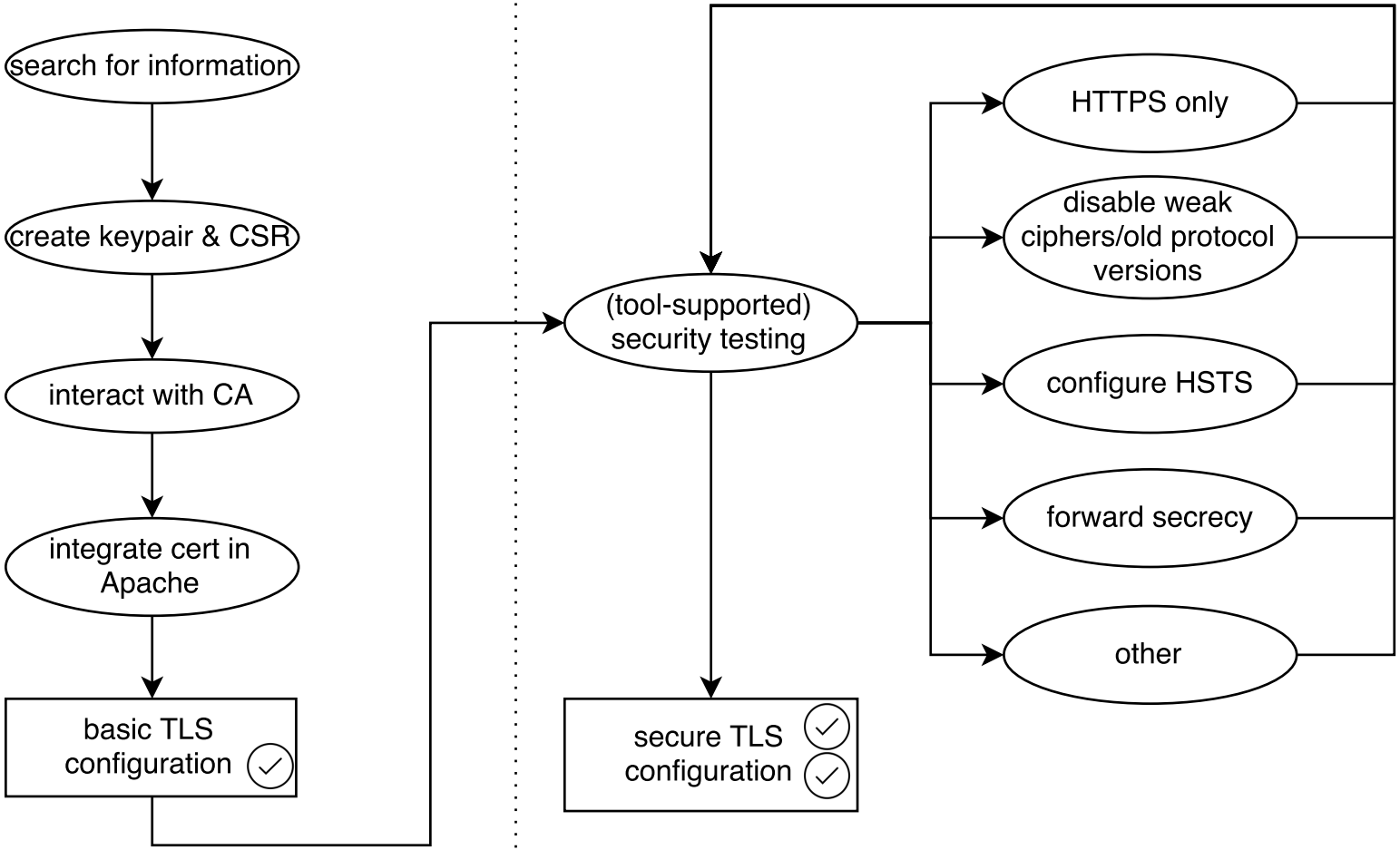
Security Evaluation

- 2 participants used self-signed certificates
- No participant chose a key size smaller than 2048 for their RSA key
- forward secrecy: 14
- HSTS headers: 11
- HPKP: 2

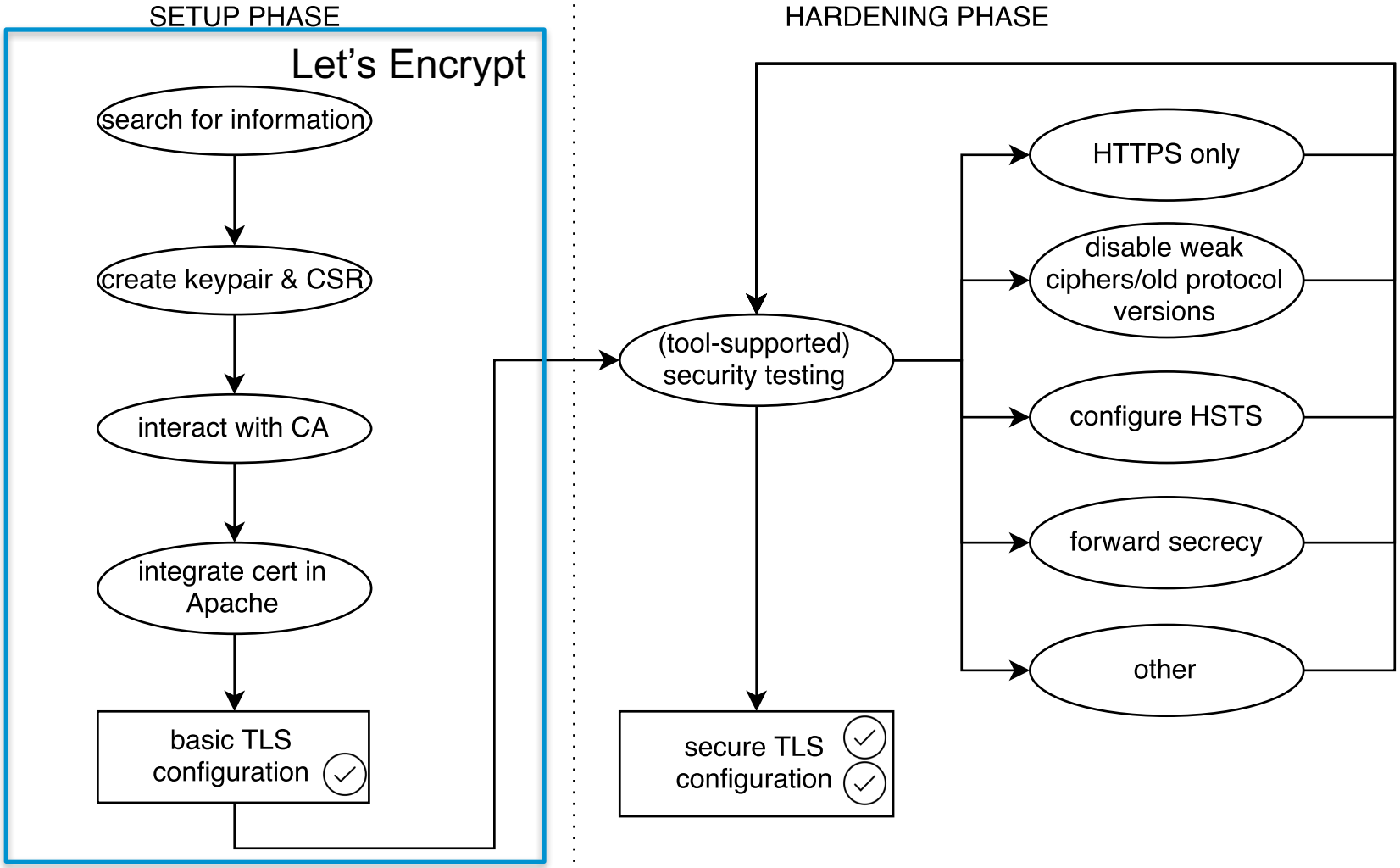
SBA Research

SETUP PHASE

HARDENING PHASE



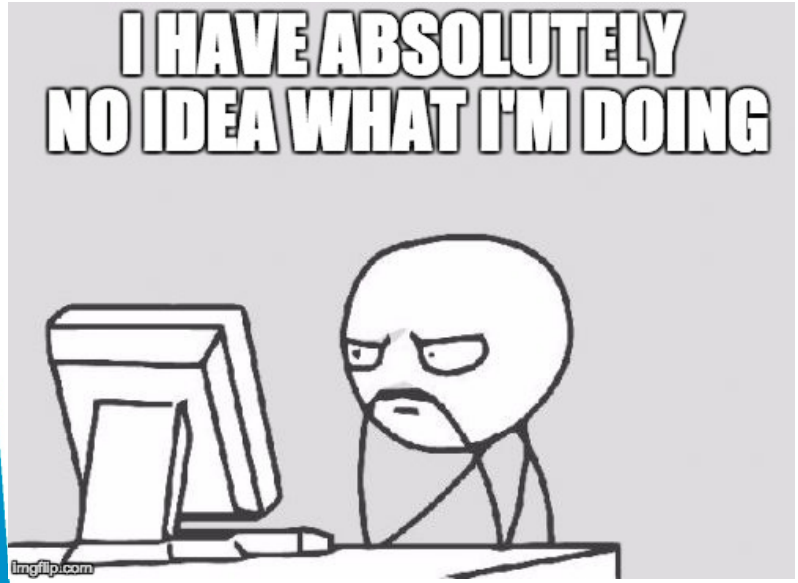
SBA Research

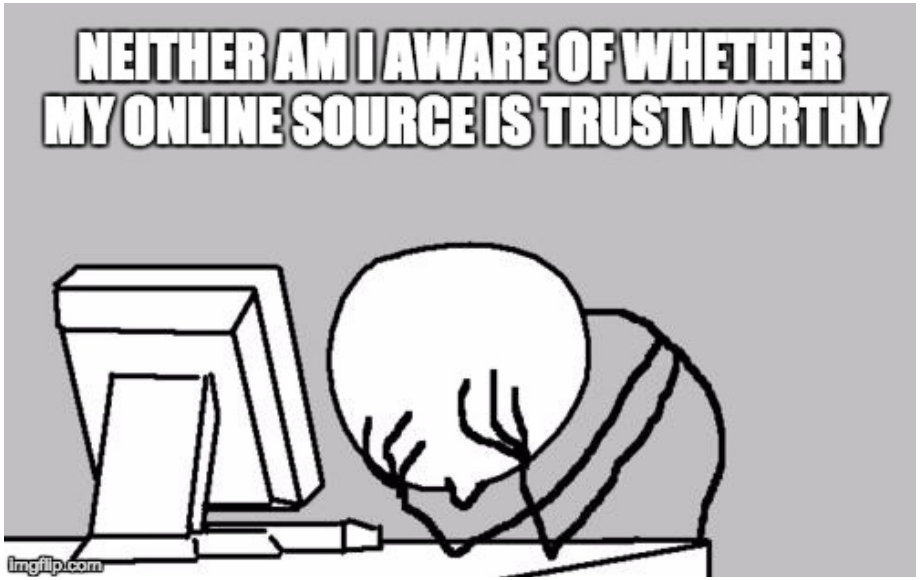

SETUP PHASE
HARDENING PHASE
Let's Encrypt
search for information
create keypair & CSR
interact with CA
integrate cert in Apache
basic TLS configuration
(tool-supported) security testing
HTTPS only
disable weak ciphers/old protocol versions
configure HSTS
forward secrecy
other
secure TLS configuration

Perceptions of Usability

- Finding the best-practice workflow is hard (19)
- Misleading terminology (15)
- Weak default configuration (12)

Online Sources





(P23)

Online Sources

„The configuration process is fiddly and one has to google tons of pages to get it right. Even then one cannot be sure to have a good configuration because vulnerabilities are discovered almost on a regular basis.“ (P9)

SBA Research

Online Sources

- Average number of visited websites: 60
- Number of visited websites had **no impact on the quality** of the resulting configuration

SBA Research

Online Sources

- Decision-making process is **mostly based on online sources**
- No in-depth understanding of underlying fundamentals
  - e.g. choosing cipher suites

SBA Research

Impact of prior experience

- There is an association between prior experience and quality of the resulting configuration
- No evidence that previous employment impacts configuration quality

SBA Research

Confusing File Structure and Terminology

- Configuring virtual host and port is time consuming
- Apache configuration files are perceived as confusing and as a distraction from the main task
- Multiple configuration files and options

More Usability Challenges

- High effort for hardening
- Confusion: Is the site still reachable via HTTP?
- Finding the right balance between security and compatibility

Interviews with Security Auditors

- Goal: **confirm the ecological validity** of our results
- Participants: 7 security auditors
  - from well-respected security consulting firms
  - with experience as security auditor > 2 years

SBA Research

Interviews with Security Auditors

- Auditing TLS connections
  - Activated versions?
  - Activated cipher suites?
  - Cert recognized by web browsers?
  - HSTS, key pinning etc.
- Tools:
  - Qualy's SSL Test
  - NMap
  - Nessus modules
  - OpenVAS

Configurations in the Wild

- poor ciphers
- no hardening
- self-signed certificates
- Two auditors had never seen HTTPS public key pinning during an audit

Configurations in the Wild

- Administrators who are “afraid of using crypto”
- TLS deployment was not sufficiently streamlined in companies
  - Multiple servers – updated separately
  - Varying configurations

Compatibility

”In most cases backward compatibility is the show-stopper regarding proper TLS configurations” (E3)

- .. Sometimes just a mock argument
- But finding the best fit is hard, even for experts

SBA Research

Suggested improvements

- Let’s Encrypt
- Security by default (Caddy web server)
- Compatibility flags
- Guidelines: deploy everything that doesn’t impact compatibility: e.g. HSTS
- HTTPS should fully replace HTTP
- Concept of having CAs is flawed

Conclusions

- Configuring TLS on Apache is a challenging task, even for experienced users **and we should take this serious!**
- Administrators struggle with important security decisions
- Concerns are mainly driven by compatibility
- Hard to find reliable information sources

SBA Research

Questions?

Thank you!

Google

SBA Research