

"I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS

Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, Edgar Weippl

Problem & Motivation

- Explore reasons for TLS misconfigurations
- Usability from the administrator's perspective

- **Configure HTTPS on Apache**
 - ▷ Start with HTTP-configured Apache
 - ▷ Finish with secure HTTPS configuration

Methodology

1. Recruitment Questionnaire	2. Lab Study	3. Post-Study Questionnaire	4. Expert Interviews
<ul style="list-style-type: none"> • N=117 • Multiple choice • Top 30 candidates were invited to participate in the study 	<ul style="list-style-type: none"> • N=28 • Think-aloud protocol • Bash/browser history • VM images 	<ul style="list-style-type: none"> • N=28 • Open-/closed-ended questions • Demographics, previous experience 	<ul style="list-style-type: none"> • N=7 • Semi-structured interviews • Ecological validity

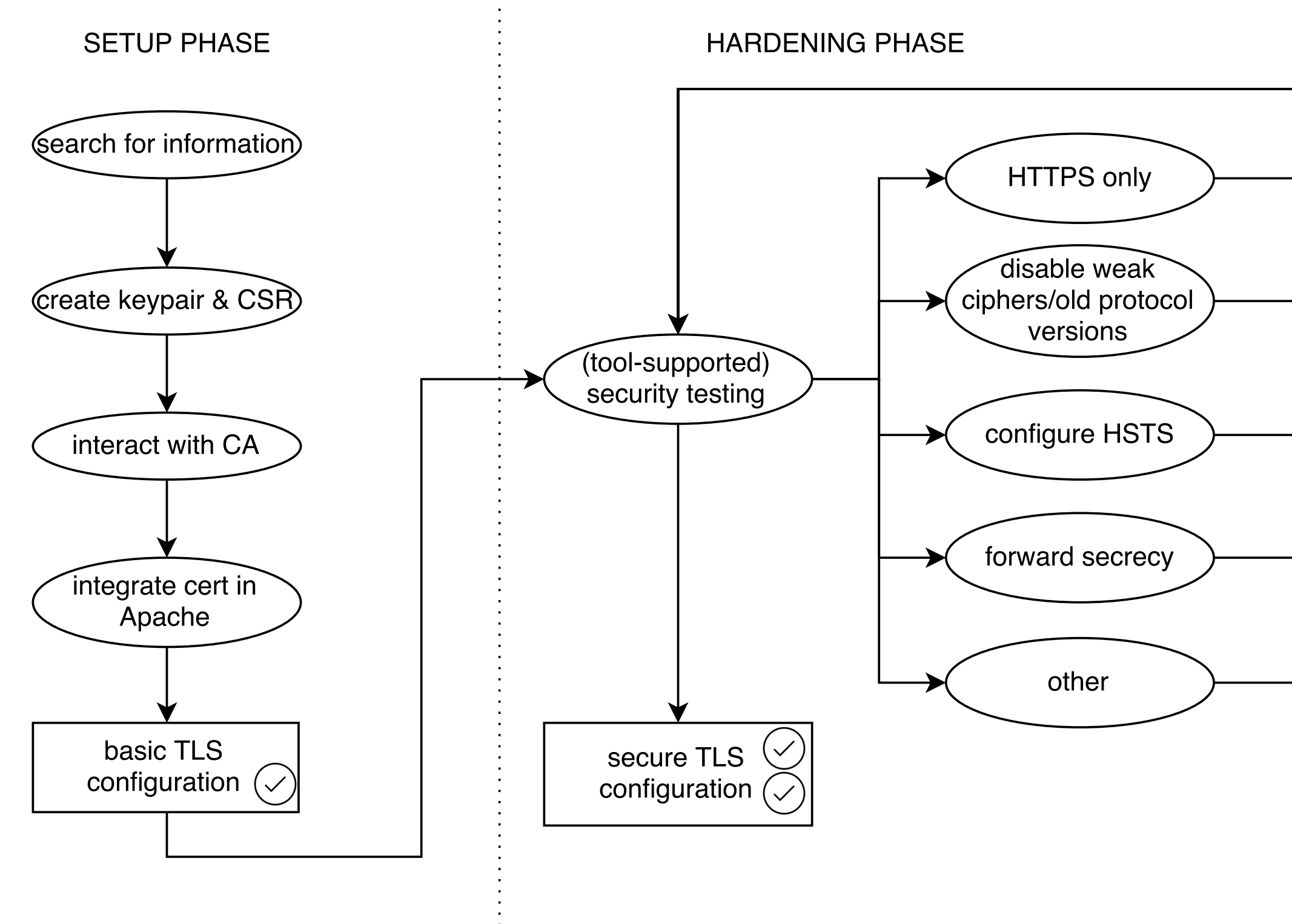
Different parts of the study

- **Lab Study**
 - ▷ Get a certificate – Interact with CA
 - ▷ Change correct parameters – Harden configuration
 - ▷ Testing

Statements

- "It seems that there is already a certificate called snakeoil, why can't I use this one?" (P7)
- "I have absolutely no idea what I'm doing. Neither am I aware of whether my online source is trustworthy." (P23)
- "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 SSL vulnerabilities are discovered almost on a regular basis." (P9)

Identified Workflow



Schematic representation of a successful workflow

Analyzed Results

ID	Grade	Errors / Warnings / Highlights	Cipher Strength Score	Key Exchange Score	Protocol Support Score	Common Name	Key Size	Certificate Chain Length	Used Provided C.A. to Sign	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	95	web.local	2048	3	●	○	○	○	○	○	○	○	○	○	○	
P5	B	90	90	95	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	●	○	○	○	○	○	○	○	○	○	○	

Analyzed Apache configurations

Usability Challenges in TLS Deployment

- Searching for information and finding the right workflow
- Creating a Certificate Signing Request (CSR)
- Choosing the appropriate cipher suites
- Strict HTTPS
- Multiple configuration files
- Finding the right balance between security and compatibility

Conclusion

- 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.
- It is hard to find reliable information sources.