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

Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, Edgar Weippl
“I HAVE NO IDEA WHAT I’M DOING”
“I HAVE NO IDEA WHAT I’M DOING”
“I HAVE NO IDEA WHAT I’M DOING”
Motivation and Goals

• Explore reasons for TLS misconfigurations—usability from the administrator’s perspective
• Study Task: Configure HTTPS on Apache
  o HTTP -> HTTPS
  o get a certificate
  o integration, hardening
  o testing
  o done!
Adventures in Setting up HTTPS
User Study – The Expert’s Perspective

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• N=117</td>
<td>• N=28</td>
<td>• N=28</td>
<td>• N=7</td>
</tr>
<tr>
<td>• Multiple choice</td>
<td>• Think-aloud protocol</td>
<td>• Open/closed-ended questions</td>
<td>• Semi-structured interviews</td>
</tr>
<tr>
<td>• Top 30 candidates</td>
<td>• Bash/browser history</td>
<td>• Demographics, previous experience</td>
<td>• Ecological validity</td>
</tr>
<tr>
<td>were invited to participate</td>
<td>• VM images</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in the study</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lab Study - Participants

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

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

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

• Statistical significance
Security Evaluation
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

- 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

Monthly Scan: December 03, 2015
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
Perceptions of Usability

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

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 vulnerabilities are discovered almost on a regular basis.” (P9)
Online Sources

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

• Decision-making process is *mostly based on online sources*

• No in-depth understanding of underlying fundamentals
  - e.g. choosing cipher suites
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
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
  o from well-respected security consulting firms
  o with experience as security auditor > 2 years
Interviews with Security Auditors

• Auditing TLS connections
  o Activated versions?
  o Activated cipher suites?
  o Cert recognized by web browsers?
  o HSTS, key pinning etc.

• Tools:
  o Qualy’s SSL Test
  o NMap
  o Nessus modules
  o 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 showstopper regarding proper TLS configurations" (E3)

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

Thank you!