"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
   - No/T: Multiple choice – Top 10% were invited to participate in the study
   - NVs: Think-aloud protocol – Audiotapes/VR images
   - NoNVs: Open-ended questions – Demographics, previous experience
   - NVs: Expert interviews
      - NoC: Tasks – structured scenarios
      - Ecological validity

   Different parts of the study

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

3. Post-Study Questionnaire

4. Expert Interviews

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

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.
