Participatory Design for Security-Relevant User Interfaces

Susanne Weber, Marian Harbach

Usable Security and Privacy Lab
Gottfried Wilhelm Leibniz Universität Hannover, Germany

{weber,harbach}@usecap.uni-hannover.de

Matthew Smith

Usable Security and Privacy Lab
Rheinische Friedrich-Wilhelms-Universität Bonn, Germany

smith@cs.uni-bonn.de

Content

- Motivation
- Participatory Design
- Approach
- Results

Motivation

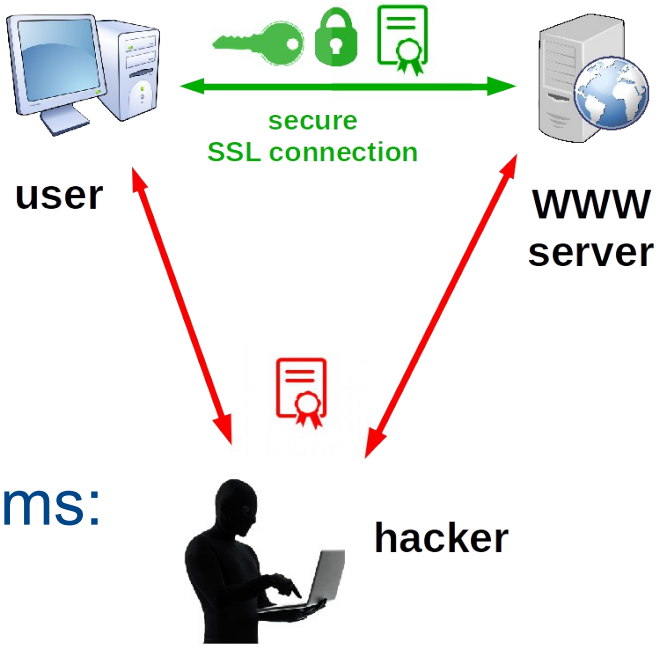
- Users are overwhelmed by warning messages
- Lacking comprehension → wrong decisions→ security issues
- Design does not focus on user's knowledge

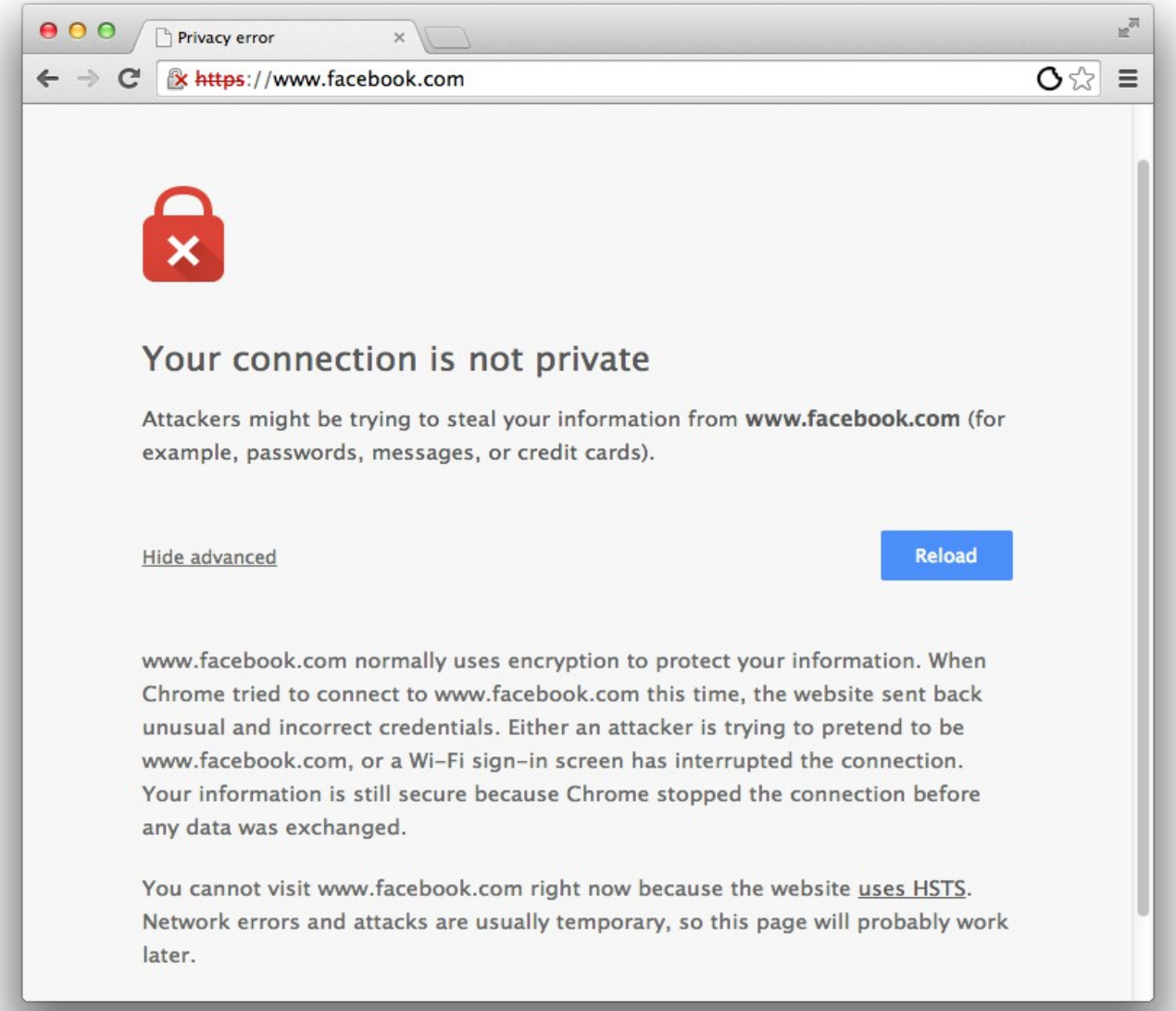
Plan

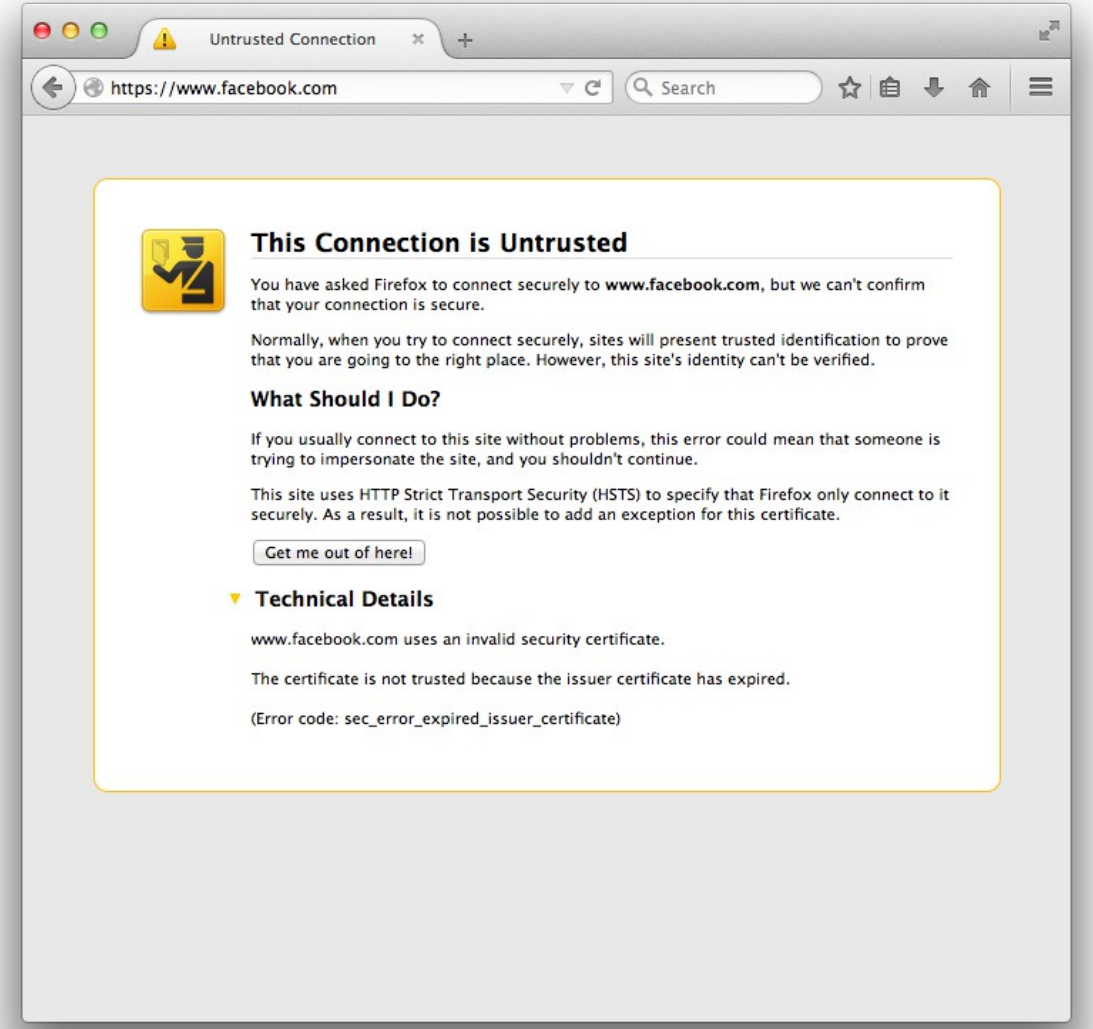
- Exploratory application of PD methods for security-relevant user interfaces
- Evaluate PD process, design and conduct first PD study
- In cooperation with users: Designing a new and **usable** warning message

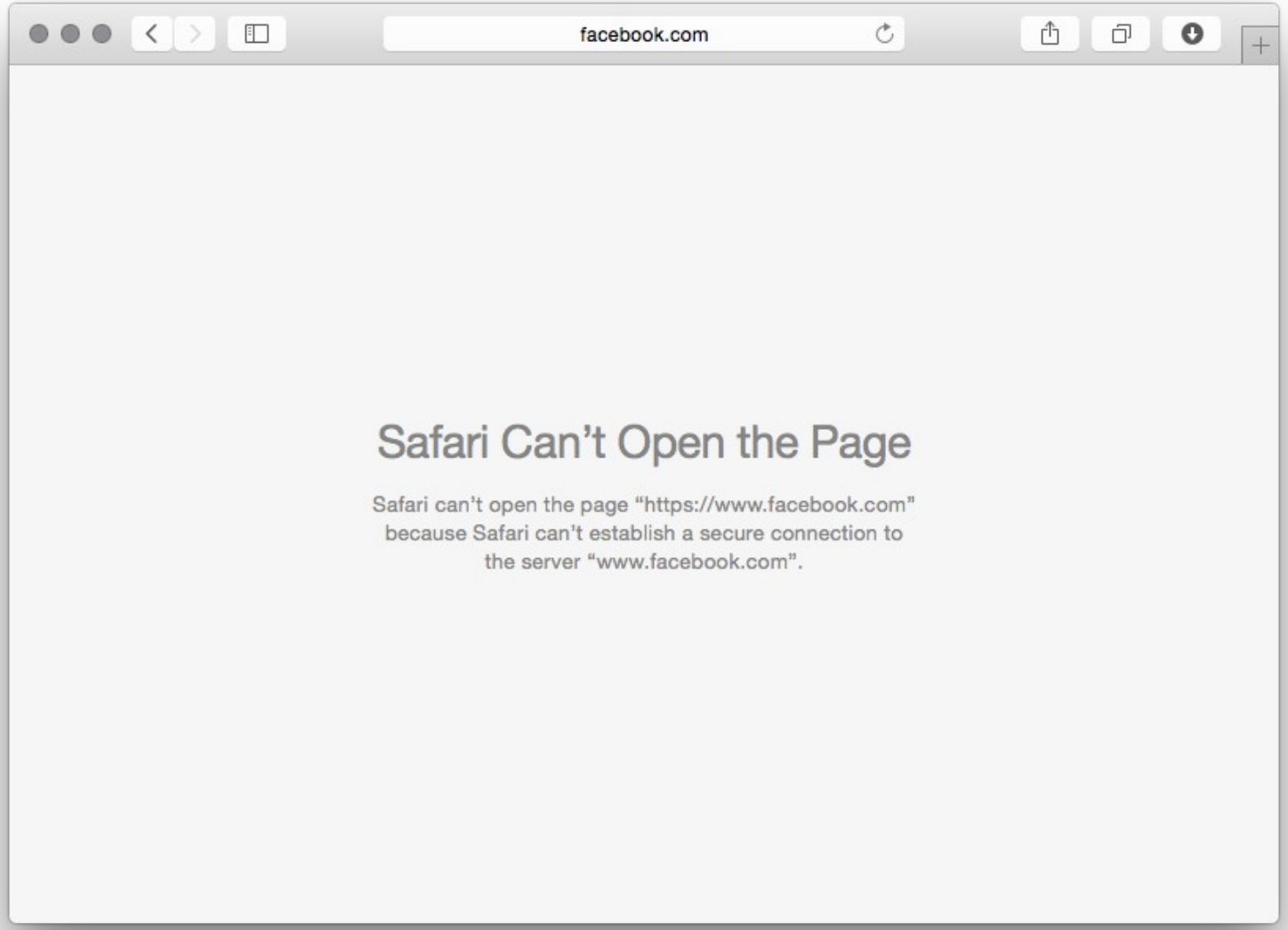
Use Case: SSL warnings

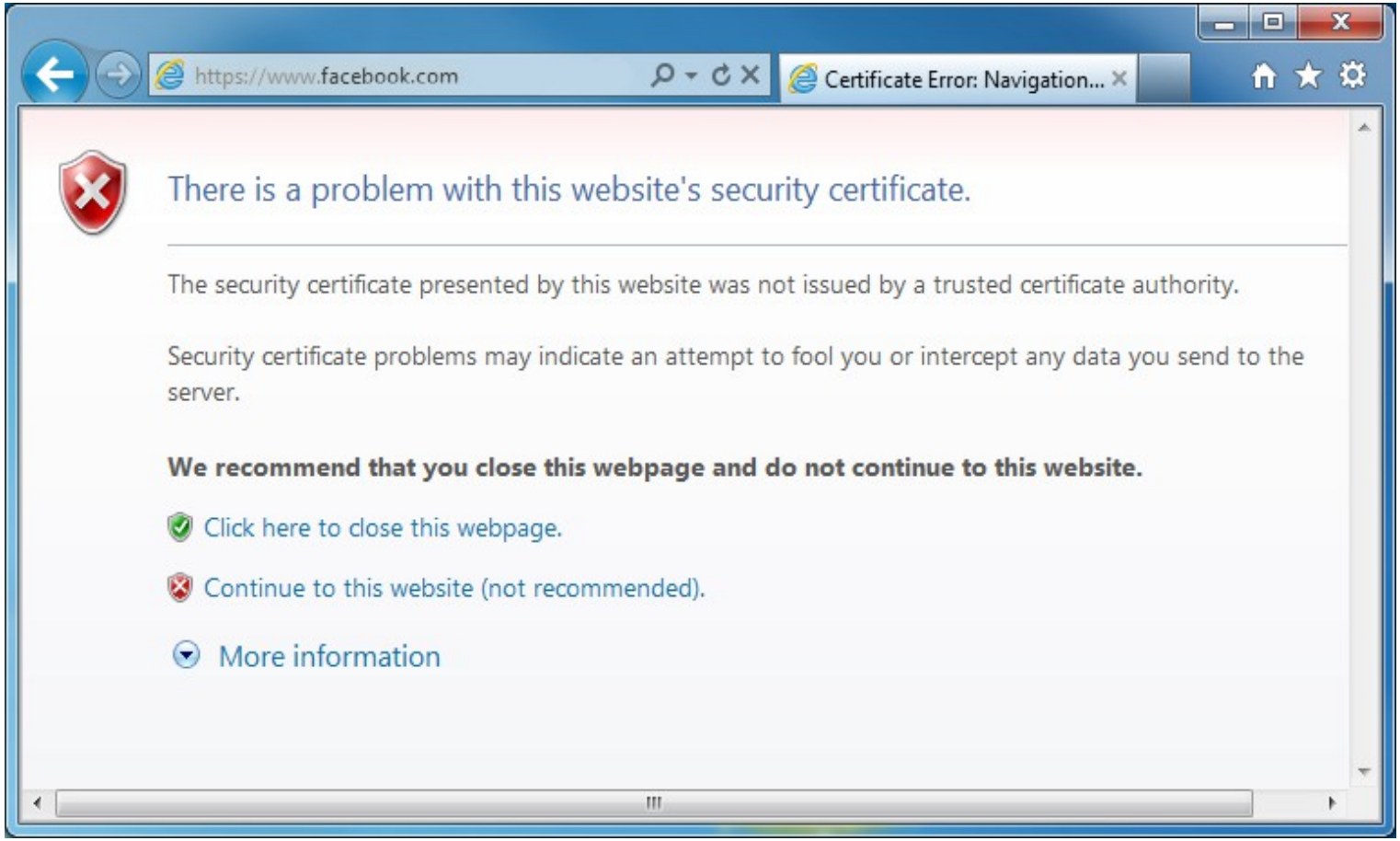
- SSL warnings confuse users
- SSL: secure connection between user and WWW server
- Possible attack: Man In The Middle
- Certificates to identify websites
- Users are not familiar with mechanisms:
  - Optical browser features
  - Certificate warnings

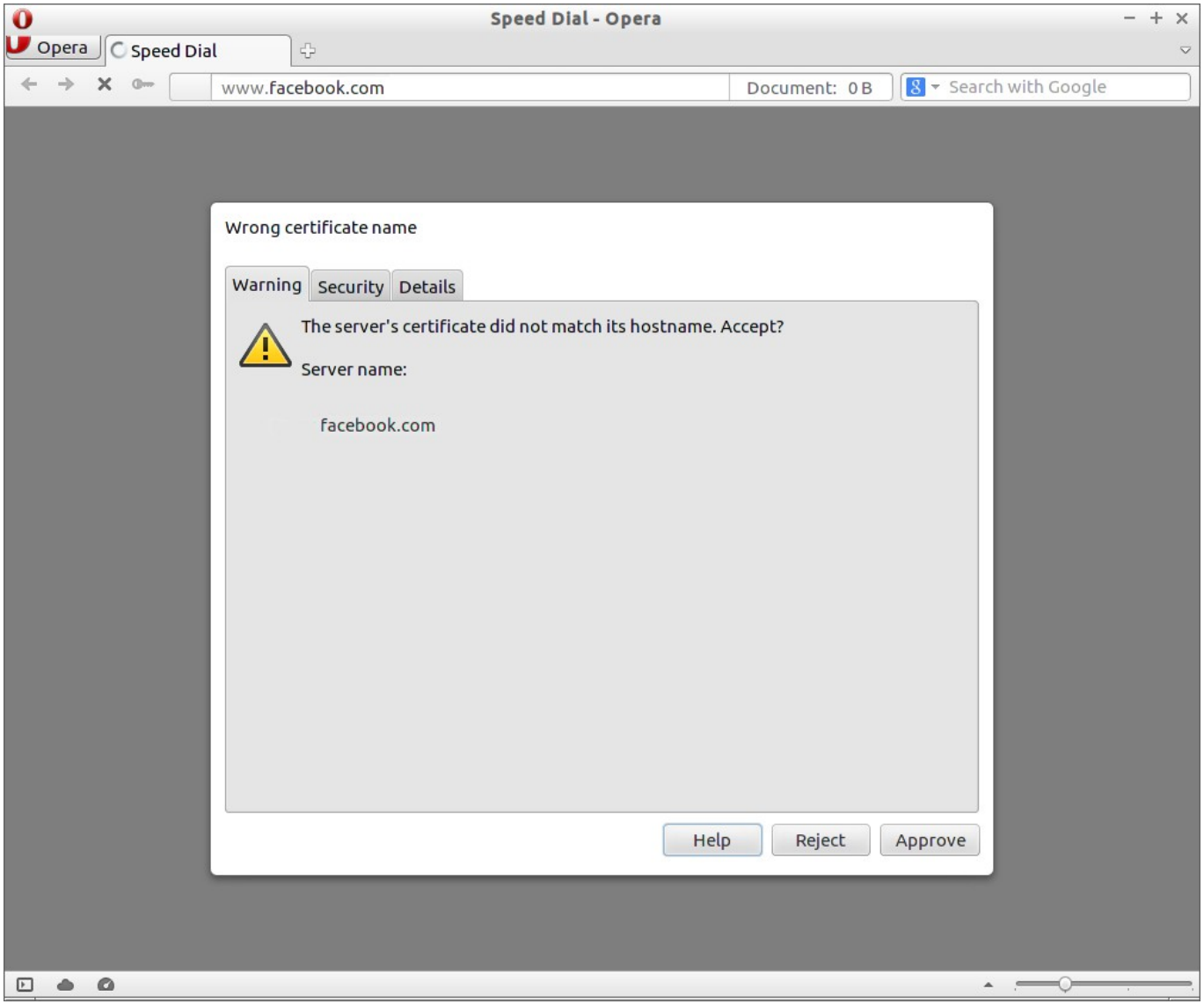



Privacy error
https://www.facebook.com
Your connection is not private
Attackers might be trying to steal your information from www.facebook.com (for example, passwords, messages, or credit cards).
Hide advanced
Reload
www.facebook.com normally uses encryption to protect your information. When Chrome tried to connect to www.facebook.com this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be www.facebook.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.
You cannot visit www.facebook.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.


Untrusted Connection
https://www.facebook.com
Search
This Connection is Untrusted
You have asked Firefox to connect securely to www.facebook.com, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox only connect to it securely. As a result, it is not possible to add an exception for this certificate.
Get me out of here!
Technical Details
www.facebook.com uses an invalid security certificate.
The certificate is not trusted because the issuer certificate has expired.
(Error code: sec_error_expired_issuer_certificate)

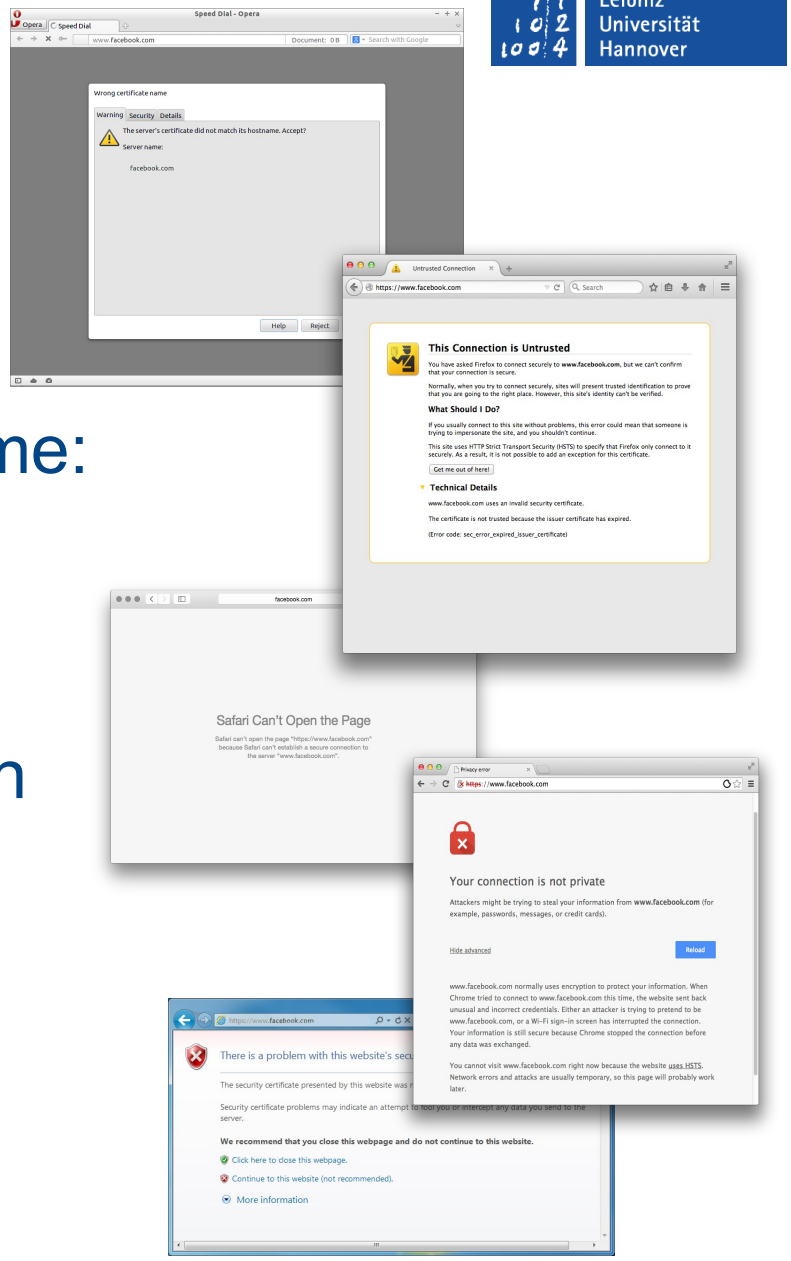

facebook.com
Safari Can't Open the Page
Safari can't open the page "https://www.facebook.com" because Safari can't establish a secure connection to the server "www.facebook.com".


https://www.facebook.com
Certificate Error: Navigation...
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information


Speed Dial - Opera
Opera
Speed Dial
www.facebook.com
Document: 0 B
Search with Google
Wrong certificate name
Warning
Security
Details
The server's certificate did not match its hostname. Accept?
Server name:
facebook.com
Help
Reject
Approve

SSL Warnings

- Akhawe et al.
  SSL warning in Google Chrome:
  70.2% click-through rate
- Potential for improvements
- Experts have been working on this for over a decade



Participatory Design (PD)

- Enhanced user-centered design
- Users are involved **actively** throughout the **whole** design process
- Focusing on users' experiences, ideas, and opinions
- User and designer working as a team: *Shared Language*
- Various possible application scenarios
  → workflows, layouts, contents, …
- Flexible techniques
  → workshops, interviews, studies, surveys, ...

Workshops

- Small groups: Analyzing existing SSL warnings and problems to find alternative representation
- 15 participants (aged 22-35, 8 female) in five workshops
  → IT m (pilot), IT f, IT mixed, lawyers, others
- Designer as neutral supporter
  - 1. Explanation on technical background (Shared Language) and Brainstorming
  - 2. Creating new designs (Mock-Ups)
  - 3. Ending (Feedback)

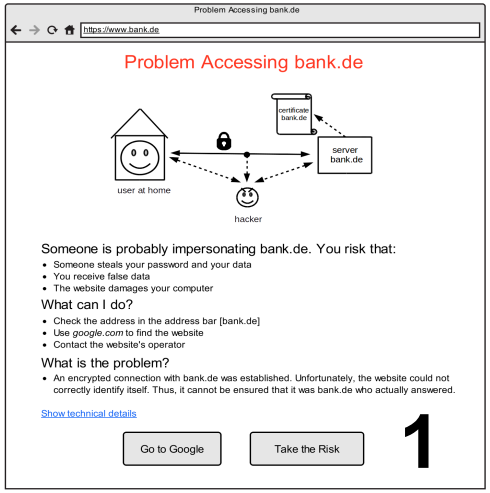
Results

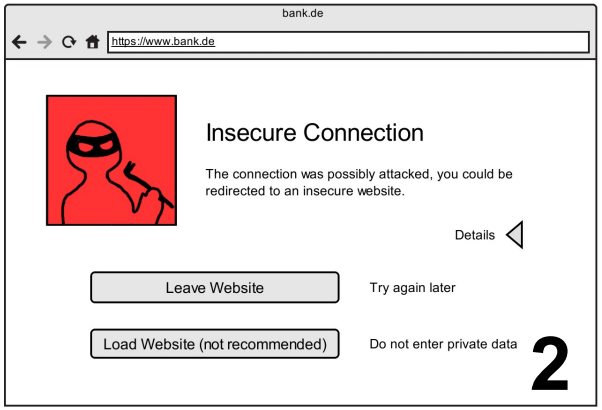
- All groups mentioned quite similar usability aspects:
  - Text too long and unclear
  - Technical details unnecessary for non-experts
  - Use of colors for recommendations and graphics for explanations helpful
  - Capability to decide action should be provided
- Many ideas for improvements already suggested during brainstorming phase

Quotes

- „This is censorship!“ – Users do not want to be patronized and decide on their own instead
- „I feel like a slave“ – Security measures mostly help the device instead of the user
- Group composition influences results
  → Target group specific messages

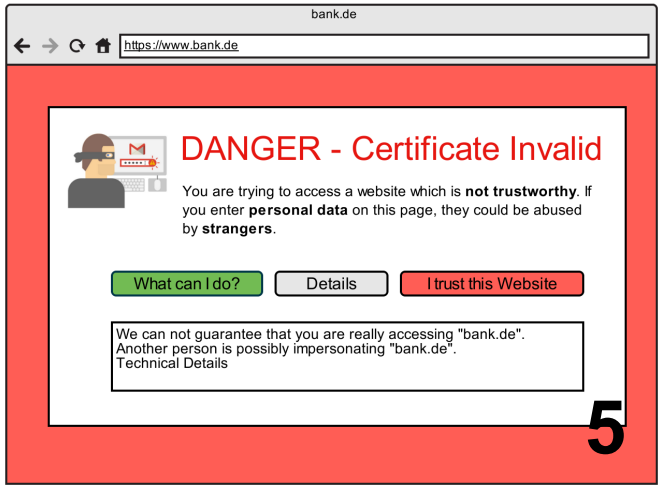
Results


Problem Accessing bank.de
https://www.bank.de
Problem Accessing bank.de
certificate bank.de
server bank.de
user at home
hacker
Someone is probably impersonating bank.de. You risk that:
Someone steals your password and your data
You receive false data
The website damages your computer
What can I do?
Check the address in the address bar [bank.de]
Use google.com to find the website
Contact the website's operator
What is the problem?
An encrypted connection with bank.de was established. Unfortunately, the website could not correctly identify itself. Thus, it cannot be ensured that it was bank.de who actually answered.
Show technical details
Go to Google
Take the Risk
1


bank.de
https://www.bank.de
Insecure Connection
The connection was possibly attacked, you could be redirected to an insecure website.
Details
Leave Website
Try again later
Load Website (not recommended)
Do not enter private data
2


bank.de
https://www.bank.de
STOP
Security Problem
The Internet address you entered was unable to sufficiently identify itself and thus guarantee a secure connection.
A hacker is possibly eavesdropping on your personal data.
What should I do now?
Make sure that your wireless network is sufficiently secured!
If you were redirected to this page, check the address in the address bar.
If you would like to continue, do not enter commercially exploitable or security-relevant data (PIN, password, email address, bank account data, credit card data, etc.)!
Recommended: Cancel and try again later!
Continue
Cancel
Does this problem occur repeatedly?
3


facebook
bank.de
https://www.bank.de
Security Error
Starting now, your data (passwords, bank account data, ...) can be eavesdropped on.
Back to Homepage
(3, 2, 1, ...) Load anyway
What happened?
4


bank.de
https://www.bank.de
DANGER - Certificate Invalid
You are trying to access a website which is not trustworthy. If you enter personal data on this page, they could be abused by strangers.
What can I do?
Details
I trust this Website
We can not guarantee that you are really accessing "bank.de".
Another person is possibly impersonating "bank.de".
Technical Details
5

Results

- Warnings differ although groups criticized similar aspects of existing warnings
- Three warnings very short with only few text
- All hide technical details
- All use signal colors (red, green) and graphics or symbols
- All recommend clearly to stop, but provide a possibility to continue
- Concrete visualization of a hacker
- Various design ideas realized in a very short amount of time

Meta-Results

- PD as educational method
  → Introducing unknown topics: Metaphors helpful
- „Guys, look, we are actually doing what we criticized before!“

Meta-Results

- Users approach „new“ problems with an open mind
  → Included elements from other contexts
- Feedback: Participants were satisfied with results and workshop procedure
- Participants perceived designer as a welcome support and she was treated as an equal during the experiment

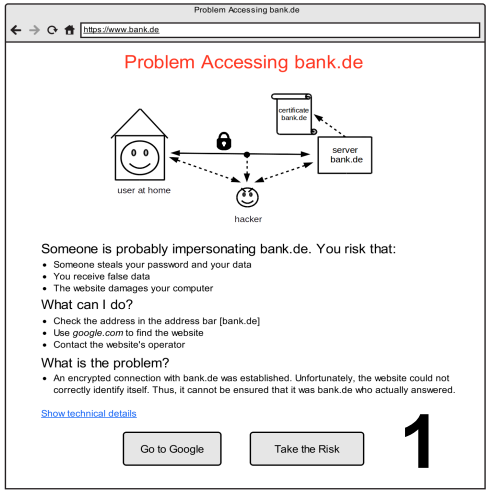
Limitations

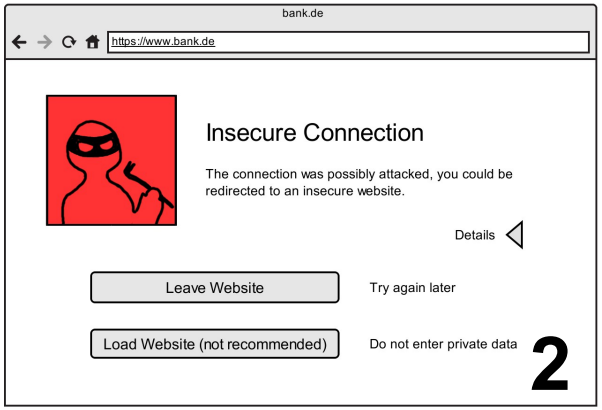
- Small convenience sample
- Current SSL warning shown and dicussed
- No professional designers in team
-
- Our first contact with PD

Next steps

- Refine warnings
  - Each warning for itself
  - Combine warnings in another PD design workshop
- Implementation of a prototype
- Study: Evaluation with users
  - Test the effectivness of warning created by group
    - For own group
    - And for other groups

Questions?


Problem Accessing bank.de
https://www.bank.de
Problem Accessing bank.de
certificate bank.de
server bank.de
user at home
hacker
Someone is probably impersonating bank.de. You risk that:
Someone steals your password and your data
You receive false data
The website damages your computer
What can I do?
Check the address in the address bar [bank.de]
Use google.com to find the website
Contact the website's operator
What is the problem?
An encrypted connection with bank.de was established. Unfortunately, the website could not correctly identify itself. Thus, it cannot be ensured that it was bank.de who actually answered.
Show technical details
Go to Google
Take the Risk
1


bank.de
https://www.bank.de
Insecure Connection
The connection was possibly attacked, you could be redirected to an insecure website.
Details
Leave Website
Try again later
Load Website (not recommended)
Do not enter private data
2


bank.de
https://www.bank.de
STOP
Security Problem
The Internet address you entered was unable to sufficiently identify itself and thus guarantee a secure connection.
A hacker is possibly eavesdropping on your personal data.
What should I do now?
Make sure that your wireless network is sufficiently secured!
If you were redirected to this page, check the address in the address bar.
If you would like to continue, do not enter commercially exploitable or security-relevant data (PIN, password, email address, bank account data, credit card data, etc.)!
Recommended: Cancel and try again later!
Continue
Cancel
Does this problem occur repeatedly?
3


facebook
bank.de
https://www.bank.de
Security Error
Starting now, your data (passwords, bank account data, ...) can be eavesdropped on.
Back to Homepage
(3, 2, 1, ...) Load anyway
What happened?
4


bank.de
https://www.bank.de
DANGER - Certificate Invalid
You are trying to access a website which is not trustworthy. If you enter personal data on this page, they could be abused by strangers.
What can I do?
Details
I trust this Website
We can not guarantee that you are really accessing "bank.de".
Another person is possibly impersonating "bank.de".
Technical Details
5