Do we need to care about users when building security?

Marko Helenius, Eleni Berki, Linfeng Li, Sunil Chaudhary, Tiina Schafheitl-Tähtinen & Joona Kannisto
A stunning moment

Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[ This isn’t a web forgery ]
Methods we have used

• CAN BE USED ALSO IN COMPANIES
  – Heuristic usability evaluation
    • Focus groups
  – Usability evaluation
  – Misuse case design
  – User modelling
  – Interviews

• RESEARCH ORIENTED
  – Systematic literature review
Heuristic usability evaluation

- Jakob Nielsen’s heuristics
- Only 4-6 experts needed
  - Expertise on security and usability
- Fast and cost-efficient
- Not as reliable as usability evaluation
Usability evaluation

- Real users involved
  - Still limited number
- Requires resources and time
Usability evaluation of whitelist- and blacklist-based anti-phishing applications

Test setup:
- fraudulent DNS and web server
Usability evaluation of whitelist- and blacklist-based anti-phishing applications

- Current anti-phishing mechanisms of web browsers are not very effective. They lack considerable information regarding user security, and this alone can mislead users into visiting phishing web pages and/or providing personal information to phishers.
User modelling

• Limited, as not everything can be modelled
• However, gives systematic approach to verify that all basic stages have been taken in account
• Takes in account that users have different understanding of their security.
Specification

COMPOSING = (messageReceived->INFORMATION),
INFORMATION = (messageRead->PROCESSING),
PROCESSING= (learnFromMessage ->ACQUIRING
    | takeActionUponMessage -> DECISIONMAKING),
ACQUIRING = (understandMessage->COMPOSING
    | misunderstandMessage->COMPOSING),
KNOWLEDGE = (knowledgeMatchinformation.normalInfo->BELIEVE
    | knowledgeNotmatchinformation.detectedFraud->NOTBELIEVE
    | knowledgeNotmatchinformation.checkingMoreinfo->INFORMATION
    | knowledgeNotmatchinformation.misled->DECISIONMAKING), ...
# States of the FSM

<table>
<thead>
<tr>
<th>States</th>
<th>Explanation</th>
<th>States</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>q0</td>
<td>A message is composed</td>
<td>q5</td>
<td>Corresponding uninformed decision is made</td>
</tr>
<tr>
<td>q1</td>
<td>A message is received</td>
<td>q6</td>
<td>Not believing the given information</td>
</tr>
<tr>
<td>q2</td>
<td>Processing information</td>
<td>q7</td>
<td>Believing the given information</td>
</tr>
<tr>
<td>q3</td>
<td>Making decision</td>
<td>q8</td>
<td>Corresponding informed decision is made</td>
</tr>
<tr>
<td>q4</td>
<td>Acquiring information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The state transition and the inputs of the FSM

<table>
<thead>
<tr>
<th>States transitions</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>-&gt;q0</td>
<td>A message is composed</td>
</tr>
<tr>
<td>q0-&gt;q1</td>
<td>ReceivedMessage</td>
</tr>
<tr>
<td>q1-&gt;q2</td>
<td>messageRead</td>
</tr>
<tr>
<td>q2-&gt;q3</td>
<td>takeActionUponMessage</td>
</tr>
<tr>
<td>q2-&gt;q4</td>
<td>learnFromMessage</td>
</tr>
<tr>
<td>q3-&gt;q4</td>
<td>nothingDecided</td>
</tr>
<tr>
<td>q3-&gt;q5</td>
<td>uninformedDecision</td>
</tr>
<tr>
<td>q3-&gt;q8</td>
<td>informedDecision</td>
</tr>
<tr>
<td>q4-&gt;q0</td>
<td>understandMessage, misunderstandMessage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>States transitions</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>q8-&gt;q3</td>
<td>knowledgeNotmatchinformation.misled</td>
</tr>
<tr>
<td>q5-&gt;q6</td>
<td>misknowledgeNotmatchinformation.obstinacy</td>
</tr>
<tr>
<td>q5-&gt;q7</td>
<td>misknowledgeMatchinformation.undetectedFraud</td>
</tr>
<tr>
<td>q6-&gt;q0</td>
<td>decisionMade</td>
</tr>
<tr>
<td>q7-&gt;q0</td>
<td>decisionMade</td>
</tr>
<tr>
<td>q8-&gt;q7</td>
<td>knowledgeMatchinformation.normalInfo</td>
</tr>
<tr>
<td>q8-&gt;q6</td>
<td>knowledgeNotmatchinformation.detectedFraud</td>
</tr>
<tr>
<td>q8-&gt;q1</td>
<td>knowledgeNotmatchinformation.checkingMoreinfo</td>
</tr>
<tr>
<td>q5-&gt;q3</td>
<td>misknowledgeNotmatchinformation.misknowledgeCorrected</td>
</tr>
</tbody>
</table>
Misuse case

- Design the use cases of the system
- Personate a misuser
- Design the misuse for a specific use case
- Find a countermeasure for a misuse case
- The countermeasure is vulnerable?
- Yes
- Any other misuse cases?
- Yes
- No
- End
- No
Example
Example

• Use case: to notify the user who does not use the account for a certain time.

• Misuse case 1: to sniff the message from the client side.

• Countermeasure 1: to encrypt every message.

• Is it enough?
<table>
<thead>
<tr>
<th>Name: Sending the email to confirm the use of one account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case ID: MC-1</td>
</tr>
<tr>
<td>Summary: A cracker can obtain the account name and password by sniffing plain messages.</td>
</tr>
<tr>
<td>Author: ******</td>
</tr>
<tr>
<td>Date: 2007-3-10</td>
</tr>
<tr>
<td>Basic path: 1. A cracker can obtain the account name and password from sniffing the communication of the server.</td>
</tr>
<tr>
<td>Alternative paths: 1. A cracker can harvest account name and password from a forged website. 2. Man-in-the-middle attack can be used for obtaining this information 3. Compromising the server</td>
</tr>
<tr>
<td>Capture points: 1. Password is changed 2. Forged site has been detected by the toolbar</td>
</tr>
<tr>
<td>Extension points: 1. Keep sniffing communication</td>
</tr>
<tr>
<td>Trigger: This can happen at any time.</td>
</tr>
<tr>
<td>Assumptions: 1. The communication is not encrypted. 2. The MusicBox server security capacity is not sufficient. 3. A number of customers created their own accounts</td>
</tr>
<tr>
<td>Preconditions: 1. The server and forged website are ready.</td>
</tr>
<tr>
<td>Worst case threat: 1. Launch another social phishing attack 2. The music can be downloaded freely.</td>
</tr>
<tr>
<td>Prevention guarantee: 1. SSL or TSL is used to protect secure communication 2. Login history offered to check the account history 3. Frequently change password</td>
</tr>
<tr>
<td>Detection guarantee: Check login history</td>
</tr>
<tr>
<td>Related business rules: 1. The purchased music product is listed in the account profile 2. The purchased music product can be downloaded for several times. 3. Users can access the account with the account name and password.</td>
</tr>
<tr>
<td>Potential misuser Profile: 1. Sufficient computer skills</td>
</tr>
<tr>
<td>Stakeholders and Threats: MusicBox: users complain that the system is not secure to be used. Customers: they lose their money.</td>
</tr>
<tr>
<td>Scope: Entire business</td>
</tr>
<tr>
<td>Abstraction level: Misuser goal</td>
</tr>
</tbody>
</table>
Systematic literature review

• Why to research something that has already been done?
• The value comes from putting research together in a new context.
• Requires time and efforts
Usability, security, and trust in password managers

- Systematic literature review of peer-reviewed articles studying usability and security of password managers.
- Though password managers are designed to help users in password management, users often encounter difficulties to perform even such basic actions as safe login while using the password manager.
- Properties and features which can elevate the usability and security of password managers were suggested.
- The goal was to provide practical, simple and useful guidelines for implementing a usable password manager.
Mental model & Understanding

- How this password manager works?
- Why should I consider this PM useful to me?
- Will this PM also function as my firewall/protect me from viruses/protect me from any other information security trouble I encounter?
- Can I stop worrying about security if I use this PM?
- Are the benefits of this PM bigger than the trouble for me?
- What disasters can happen if I do something wrong with this PM?
- How this password manager works?
Learnability

- Do I need to remember how to perform tasks with this PM?
- What I need to remember when I use this PM?
- Does this PM provide me help if I’m stuck?
- How easily I learn to use this PM?
- Do I still need to remember passwords?
Compatibility

Can I use this PM with all my laptops/tablets/phones?

I use web-site requiring both password and phone for login, can I use this PM with it?

Can I use my passwords from computers I don’t own?

Can I use this PM with all browsers or operating systems?

Can I share my password for a group?
User Interface & Performance

1. How easy it is for me to start using this PM?
2. Does it take forever to store all my existing passwords into this PM?
3. How easy it is to create a new password?
4. Will this PM slow down my logins?
5. Do I need to pay more attention when I login?
6. Will this PM fill my credentials for me?
7. How easy it is to manage all my passwords?
8. Does it take forever to store all my existing passwords into this PM?
Controlling Data & Passwords

- Can I see/change/delete my data/password/master password?
- Can I decide who has access to my data and passwords?
- Does this PM help me to create (good) passwords?
- Can I decide where my data/password/master password is stored?
- Will this PM suggest passwords for me?
- Can I reuse passwords?
- What if I accidentally delete/change my data/password/master password?
Security

- How is my data/password/master password protected?
- Are those protections correct, strong, and state of the art?
- Who has access to my data/password/master password?
- What if my master password is accidentally disclosed?
- Is this PM vulnerable to some kinds of attacks?
- Can I do an error with this PM that compromises my passwords?
- In what kind of situations my passwords can be compromised?
Trust

Can I choose what I disclose and to whom?

Who do I need to trust if I use this PM?

Why should I trust this PM or PM vendor?

Who has access to my data/passwords/master password?

Will I feel more secure if I use this PM?

Who is responsible if my data/passwords are compromised?
Summary

Enable trust in design
- Inform users how their data is stored and used
- Inform users how their data is protected
- Convince users of your trustworthiness as a PM vendor

Foster user perspective
- Use simple and clear design
- Support learnability in design
- Give users an experience of control over their data and passwords
- Give users alternatives for storing their data
- Ensure compatibility with web-site policies
- Ensure transportability

Ensure security
- Protect the master password
- Implement security mechanisms correctly
- Use third party services with caution
- Give users an understandable experience of security
- Balance security features with usability
Interview

• Suitable for finding deep insights
• Limited as well, because number of respondents is restricted
• Requires efforts, but parts can be externalized, especially littering
Respondent demographics

- The interview participants were collected with snowball recruiting starting from parents association
- Nuclear families with both parents working
- Parent ages were from 30 to 45, with children primarily between 9-12
Messages and Social Media

From an interview of parents

- The phones are totally open in our house.
- We have looked at the messages together.
- Sometimes we check sent and received messages.
- Text based messaging goes totally into a private area.
Monitoring and Restrictions

Information about exact sites can be too much. Yet, nothing that we do now doesn't violate her privacy as she is only 12.

One part of it is watching, but mostly I am interested in what they are doing.

I don't use a lot of time for it. I do things around the house and I watch them in between.
Parents Online Worries

- Nobody mentioned bullying as a concern affecting their own children
  - Related events seen in Facebook by couple
  - Facebook mostly forbidden, online communication limited overall
- Predators were mentioned as a threat (media)
- Overall, accidental exposure to harmful content was seen as a bigger threat than misbehavior
- Overuse was a concern especially for games
What the parents don’t need to know

• “I don’t need to know exactly what games they play” (on a gaming site)
• “We have not looked at their email”
• “Information about exact sites can be too much. Yet, nothing that we do now doesn’t violate child’s privacy as she is only 12.”
• “There is nothing that is too specific or private”
Summary

- Privacy was not an issue within family, for families with children ages 9-12
- Trust and conversation valued more than monitoring
- Location information OK to be shared at least approximately
- Mobile devices mentioned as hard to control