User Interface vs. Security

Tom Vogt <tom@lemuria.org>
What’s the weakest link in security?
UI vs. Security

The dumb user

- clicks on anything
- chooses weak passwords
- installs insecure software
- falls for phishing, etc.
- uses IE, Outlook, etc.
UI vs. Security

Wrong!

• The user isn’t the problem
• He’ll do whatever seems best in context (NLP!)
• We control the context
• We don’t control the user
User Interface Design for Security
User Interface
Design for Security
The Trouble with Passwords

Password for all admin accounts

Enter a password of at least 16 characters. Use special characters and numbers. Do not use names or words from a dictionary. Do not use dates, sizes, room numbers or other meaningful numbers.

Make your password difficult to guess, but choose something you can remember. Choose a password you can type quickly, without looking at the keyboard.

Never write your password down.
Do not choose a password you are using for something else already.

Enter password: ********

Re-enter password to verify: ********
Passwords

Users choose weak passwords because passwords are a weak system

- Conflict of human memory and machine requirements
- Enforcing requirements weakens security
- Inhuman requirements lead to (unconscious) sabotage
The Trouble with Confirmation Dialogs
Confirmation dialogs are the wrong answer.

- Interrupt workflow
- Condition the wrong response if used in excess
- Shift responsibility
- are often confusing
More Bad Examples

- Error: Are you sure?
- Revert: Do you want to discard all unsaved changes to the file?
- Ok to not save game?
The Trouble with Phishing and Trojans

1. Questionable Sender’s Address
2. Sense of Urgency
3. Non-US Dating Format
4. Threat!
5. Link & URL in Status Bar Doesn’t Match
Phishing and Trojans

Phishing works because the user interface sucks

• Human perception works the exact opposite
  • bigger == more important
  • colours == important
  • center == important
• Info needed to spot a phishing attack often hidden in status/URL bar
  - if visible at all!
Phishing and Trojans

Good News
• recognized as a problem
• countermeasures are being tested and deployed
• many solutions target the proper level: The UI

Bad News
• most solutions still in experimental stage
• many available solutions too specific (ebay/paypal toolbar)
• phishing is big business not likely to just pack up and go away
The Trouble with Metaphors

Select key

To protect your images (encrypt) you need an encryption key.

- Create a short key: A short key is quick to work with and gives moderate protection.
- Create a long key: A long key is safer but encryption and decryption takes more time.
- Load existing key: Use a previously created key.
Metaphors

- very useful shortcuts to understanding
- but often used carelessly
- transporting wrong or unintended meaning
Metaphors

one especially bad example:

• taken too far, we see applications as documents
• ... opened with - themselves
• blurring the line between data and code:

<table>
<thead>
<tr>
<th>“document”</th>
<th>data</th>
<th>code</th>
</tr>
</thead>
<tbody>
<tr>
<td>information for me</td>
<td>information for me</td>
<td>instructions for machine</td>
</tr>
<tr>
<td>safe to handle</td>
<td>safe to handle</td>
<td>unsafe at any speed</td>
</tr>
<tr>
<td>(except for papercuts)</td>
<td>(except for overflows)</td>
<td></td>
</tr>
</tbody>
</table>
example of doing it right:

Chameleon
Chameleon

- role-based execution environments for apps
- similar to sandboxing
- visible indication of each windows role

- coarse roles sufficient:
  - system
  - vault
  - default
  - testing
Chameleon

- good metaphor: Trust
  - people understand not to trust everyone
  - people understand roles - the wife gets the keys, but not the mailman
- feedback loop kept intact
  - visual feedback about trust levels apps operate under
Conclusion
UI vs. Security

The “dumb“ user

• clicks on anything ➡ has been taught that’s how you access stuff

• chooses weak passwords ➡ hard passwords are not for humans

• installs insecure software ➡ system allows untrusted apps more than user expects

• falls for phishing, etc. ➡ tests show security experts don’t score much better...

• uses IE, Outlook, etc. ➡ ok, got me on that one, that is a user problem 😊
Conclusion

• Users are not the problem, the user interface is.

• Good user interface design:
  • put responsibility where it belongs
  • be unobtrusive
  • speak the language of the recipient
  • do not expect non-human behaviour from humans
UI and Security

- Considering human factors will improve security
  - higher acceptance
  - less errors

- Respecting user and his needs will gain cooperation
  - people like to be treated with respect
Principles

I. user profiling: know your user, speak his language
II. metaphor: borrow behaviours from contexts familiar to users
III. exposure: let the user clearly see his options
IV. coherence: behaviour should be consistent
V. context and workflow: adapt to the modus the user is currently in
VI. user testing: recruit help to spot inevitable defects
Some References

- Security and Usability
  ISBN 0596008279

- The Paradox of Choice
  ISBN 0060005696

- Language, Thought and Reality
  ISBN 0262730065