Making systems secure and usable – what can software developers do?

M. Angela Sasse
Professor of Human-Centred Technology
Director, Academic Centre of Excellence for Cyber Security
Research & Research Institute for Science of Cyber Security
University College London, UK
www.ucl.cs.ac.uk/staff/A.Sasse
Background

Study on escalating cost of password resets at BT too high workload leads to shortcut security mechanisms users don’t understand threats and risks

Also 1999: Whitten & Tygar “Why Johnny Can’t Encrypt”
Progress since then?

ACM SOUPS (Symposium on Usable Security and Privacy) since 2004
SHB (Security & Human Behaviour) since 2008
Papers in CHI, CCS, Usenix, NSPW …
Books: Cranor & Garfinkel, Shostack, Lacey
University courses on usable security
US National Academy of Sciences Workshop on *Usable Security and Privacy* 2009
And – has it made security more usable? Consider authentication

Nielsen (2000) said that biometrics are highly usable and would replace passwords. Schneier (2000) and Gates (2004) predicted that passwords would become obsolete. Hasn’t happened – why not? Research on usable security has produced many “better” authentication mechanisms – but we see little change in practice …
More ‘usable’ authentication ...

Authentication via Rorschach inkblot tests
Singing your password
Thinking your password (free EEG thrown in)
Schneier: fMRI would be cool
More biometrics (ear, nose, butt recognition)
Additional layers of knowledge-based credentials
Ringing up your friends in the middle of the night to provide you with previously entrusted re-set codes
Make people watch ads & authenticate by recognising 4 frames
Passive phishing indicators do not work (Djamija et al., Wu et al.)
‘stop-look-listen’ for every web page?
Active anti-phishing tool: SOLID
SOLID Anti-phishing tool

Safe Website Green
Experimental design

- real-world risk in the experimental setup to produce ecologically valid results
- provide same incentives to users they see in real world

<table>
<thead>
<tr>
<th>Website</th>
<th>Price</th>
<th>Potential reward</th>
<th>Condition</th>
<th>Actual reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigantic</td>
<td>£50</td>
<td>£10</td>
<td>Real – Green</td>
<td>£10</td>
</tr>
<tr>
<td>HMV Tickets</td>
<td>£50</td>
<td>£10</td>
<td>Real – Green</td>
<td>£10</td>
</tr>
<tr>
<td>See</td>
<td>£25</td>
<td>£35</td>
<td>Fake – Red</td>
<td>£0</td>
</tr>
<tr>
<td>Skiddle</td>
<td>£20</td>
<td>£40</td>
<td>Real – Gray</td>
<td>£40</td>
</tr>
<tr>
<td>Sold-out ticket market</td>
<td>£40</td>
<td>£20</td>
<td>Fake – Gray</td>
<td>£0</td>
</tr>
<tr>
<td>View London</td>
<td>£20</td>
<td>£40</td>
<td>Fake - Yellow</td>
<td>£0</td>
</tr>
</tbody>
</table>
Did they look at the warning?

All participants looked at the tool window before making decision.
Did they understand warning?

All participants said they understood what the different indicators signified:

Interview data confirmed:

- Green = safe
- Red = unsafe
- Yellow = “something went wrong during authentication”
- Grey = unknown website.
Improvement in decision-making - BUT

significant difference in the participants’ decisions when the tool was used compared to the control condition.

But: 8 in experimental condition still bought from grey & yellow sites …

<table>
<thead>
<tr>
<th>Potential Payoff</th>
<th>Number of participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>£10</td>
<td>Control: 5</td>
</tr>
<tr>
<td></td>
<td>SOLID: 10 (green)</td>
</tr>
<tr>
<td>£35-40</td>
<td>Control: 12</td>
</tr>
<tr>
<td></td>
<td>SOLID: 8 (grey/yellow)</td>
</tr>
<tr>
<td>£20</td>
<td>Control: 1</td>
</tr>
<tr>
<td></td>
<td>SOLID: 0 (red)</td>
</tr>
</tbody>
</table>
Why do users ignore the tool?

Motivation: better price
Believe their own ability to judge a website is adequate to protect them against scams
  - Past experience with high false-positive security tools creates a negative attitude

Cormac Herley *(So Long, And No Thanks for All The Externalities)*: users ignore security mechanism because they have high cost and little benefit
“Trust indicators” mentioned by participants

1. Previous experience with website
2. Logos and certifications
3. Advertisements
4. Social networking references
5. Inclusion of charity names
6. Amount of information provided
7. Website layout
8. Company information
Study 2 – Focus on one of the factors

- Previous experience with website
- Logos and certifications
- Advertisements
- Social networking references
- Inclusion of charity names
- Amount of information provided
- Website layout
- Company information

Iacovos Kirlappos, M. Angela Sasse, "Security education against phishing: A modest proposal for a major re-think", VeriSign Secured
Methodology

- 60 participants
- Six websites
- Two conditions
  1) Original websites
  2) Trust seals reversed (removed from sites that had one, added to those that didn’t)
Wireless

These are the dates we have for Wireless

**Dates and tickets for Wireless**

**The Black Eyed Peas**
plus special guests Plan B, Tinie Tempah, Bruno Mars, Example, Wretch 32, Far East Movement,
Labrinth, Yasmin & David Guetta live at Wireless

Hyde Park
London
Friday 01 Jul 2011
Gates at 14:30, show starts 16:00

**The Chemical Brothers**
plus special guests Chase & Status, The Streets,
ApheX Twin, Chromeo, Katy B, Janelle Monae,
Battles, Devlin, Digitalism, The Whip, Justin Robertson & Nero live at Wireless

Hyde Park
London
Saturday 02 Jul 2011
Gates at 12:00, show starts 14:00

**Pulp**
plus special guests Grace Jones, TV On The Radio, Foals, The Horrors & Metronomy live at Wireless

Hyde Park
London
Sunday 03 Jul 2011
Gates at 12:00, show starts 13:45

**NEVER MISS ANOTHER GIG!**

Subscribe to Gigantic’s free weekly email and we’ll let you know about new events as tickets go on sale. Click here for more details...

**BOOKMARK THIS...**

- Facebook
- MySpace
- Bebo
- Yahoo!
- Delicious
- Digg
- Reddit
- StumbleUpon
- Twitter

**View (110%)**
Wireless

Dates and tickets for Wireless

- The Black Eyed Peas
- Timberlake
- Bruno Mars
- Example, Wretch 32
- Far East Movement
- Labrinth, Yasiin & David Guetta live at Wireless

Hyde Park
London
Gates at
Friday 01 Jul 2011
14:30, show starts 16:00

- The Chemical Brothers
- Chase & Status, The Streets
- Aphex Twin, Chromeo, Katy B, Janelle Monae
- Battles, Devlin, Digitalism, The Whip, Justin Robertson & Nero live at Wireless

Hyde Park
London
Gates at
Saturday 02 Jul 2011
12:40, show starts 14:00

- Pulp
- plus special guests Grace Jones, TV On The Radio, Foals, The Horrors & Metronomy

Hyde Park
London
Gates at
Sunday 03 Jul 2011
12:30, show starts 13:15

NEVER MISS ANOTHER GIGI!

Subscribe to Gigantic’s free weekly email and we’ll let you know about new events as tickets go on sale. Click here for more details.

BOOKMARK THIS...

VERISIGN SECURED

TERMS & CONDITIONS | FAQS | PRIVACY POLICY | ADVANCED SEARCH | GOOD CAUSE STUFF
Were trust seals effective?

Eye-tracking data analysis results:
Only 12/60 participants noticed all three trust seals

23/60 did not notice any of them

<table>
<thead>
<tr>
<th>No of seals noticed</th>
<th>No of participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
</tr>
</tbody>
</table>
When noticed, trust seals influence ratings

<table>
<thead>
<tr>
<th>Website</th>
<th>Number of participants noticed</th>
<th>Rating when noticed</th>
<th>Rating when not noticed/not present</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventim.co.uk</td>
<td>18</td>
<td>0.94</td>
<td>0.00</td>
</tr>
<tr>
<td>getmein.com</td>
<td>15</td>
<td>0.73</td>
<td>-0.04</td>
</tr>
<tr>
<td>gigantic.com</td>
<td>14</td>
<td>0.64</td>
<td>-0.11</td>
</tr>
<tr>
<td>hmvtickets.com</td>
<td>8</td>
<td>1.25</td>
<td>1.04</td>
</tr>
<tr>
<td>seetickets.com</td>
<td>11</td>
<td>0.27</td>
<td>0.37</td>
</tr>
<tr>
<td>skiddle.com</td>
<td>5</td>
<td>0.40</td>
<td>-0.40</td>
</tr>
</tbody>
</table>

- Statistically significant increase in ratings
  $t(5) = 3.3786, p = 0.0099$
But: is this influence a good thing?

participants made lots of assumptions
  Website is verified by the payment method company (e.g. VISA, MasterCard)
  Provides confirmation that website is genuine (could not explain why)
Conclusions - Trust seals don’t work

Not reliably noticed
When noticed, they influence user perceptions towards trust,
BUT people
don’t verify them
don’t understand what they mean
attribute far too much protection
Makes most users more vulnerable!

*Kirlappos, Sasse & Havey: Why Trust Seals Don’t Work. Procs TRUST2012*
Study 3: pdf warnings

The experiment

Two conditions: between-subjects design

Participant task: reading two articles and evaluating their summaries

Choosing the first article: no warning

Choosing the second article: a warning with each article the participants tried
General results

120 participants (64 female, mean age 25.7)

<table>
<thead>
<tr>
<th>Warning type</th>
<th>Downloaded</th>
<th>Refused</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic</td>
<td>52</td>
<td>8</td>
</tr>
<tr>
<td>Specific</td>
<td>46</td>
<td>14</td>
</tr>
<tr>
<td>Σ</td>
<td>98</td>
<td>22</td>
</tr>
</tbody>
</table>

χ² = 1.391    p = 0.238    df = 1
Gender differences

Women were more cautious and less likely to download an article with a warning.

<table>
<thead>
<tr>
<th></th>
<th>Download</th>
<th>Refusal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>50</td>
<td>6</td>
</tr>
<tr>
<td>Female</td>
<td>48</td>
<td>16</td>
</tr>
</tbody>
</table>

χ² = 4.071, p = 0.044, df = 1
Eye-tracking data

Fixation time in seconds
By warning type

- 6.13 for generic warnings
- 6.33 for specific warnings

By subsequent reaction

- 6.94 for those who subsequently refused to download
- 5.63 for those who subsequently downloaded the article

No significant difference between the length of fixation – all participants noticed the warning
Hypothetical vs. observed behaviour

**Generic warning**

<table>
<thead>
<tr>
<th></th>
<th>Download</th>
<th>Refusal to download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothetical</td>
<td>52</td>
<td>8</td>
</tr>
<tr>
<td>Actual</td>
<td>41</td>
<td>19</td>
</tr>
</tbody>
</table>

\[ \chi^2 = 6.039, \ p = 0.014 \]

**Specific warning**

<table>
<thead>
<tr>
<th></th>
<th>Download</th>
<th>Refusal to download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothetical</td>
<td>46</td>
<td>14</td>
</tr>
<tr>
<td>Actual</td>
<td>13</td>
<td>47</td>
</tr>
</tbody>
</table>

\[ \chi^2 = 36.31, \ p < 0.0001 \]
Conclusions: What can be done?

1. Kill all security tools with false positive rate higher than 1%.
2. Understand how much time and effort you are asking for.
3. Security should not be an afterthought: Integrate security into task, eliminate choice, automatically direct users to safe option.
4. Challenge dangerous misconceptions users have.
Better security education - Verisign ‘Phish or NoPhish’
Often, phishing sites will look just like the real thing. However, if you look closely, you may spot misspellings and other typos that indicate the site is fraudulent. Misspellings may also appear in the preliminary email, too.
Obstacle security = bad security
Encourages workarounds …
Security that supports user goals

Give an Allowance with Amazon PayPhrase

What is Amazon PayPhrase?
PayPhrase is an easy-to-remember shortcut to the payment and shipping information in your Amazon.com account. Each PayPhrase can be configured with simple controls, including monthly spending limits and e-mail alerts, so you can share your account with family members without sharing your credit card number or account password.

PayPhrase allowance controls include:
- Monthly spending limits
- Unspent allowance roll-over settings
- Order approval by e-mail or text message

Create your PayPhrase
Integrate requirements into specs

AEGIS – Integration of security and usability into requirements process, UML (Fléchais, Sasse & Mascolo, 2007)
IRIS – meta-model, based on KAOS (Faily & Fléchais, 2010)
Integration of personas (Faily & Fléchais, 2010)
CAIRIS – software tool to support process (Faily & Flechais 2011)
Personas for attackers

- Victor
  - Description: Victor is a contractor and expert in the SCADA systems used in South East Wales, having helped develop them over 15 years ago. Due to the recent economic downturn, Victor has been forced to take a recent pay-cut.

- Gareth
  - Description: Gareth is 35 and is unemployed. Gareth has friends who work as building labourers as part of some capital project at Rick’s water treatment works. They tell him that computer hardware and surplus piping and copper can be found at the site.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Role</th>
<th>Motive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day</td>
<td>Vendor</td>
<td>Revenge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Capability</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Medium</td>
</tr>
<tr>
<td>Software</td>
<td>Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environment</th>
<th>Role</th>
<th>Motive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day</td>
<td>Petty Criminal</td>
<td>System resource theft</td>
</tr>
<tr>
<td>Night</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Capability</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources/Personnel and Time</td>
<td>High</td>
</tr>
</tbody>
</table>
Back to good old principles

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. **It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;**
4. The system ought to be compatible with telegraph communication;
5. **The system must be portable, and its use must not require more than one person;**
6. Finally, regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.