



Usable Security

Tobias Christen

CTO

DSwiss / DataInherit

OWASP-Italy Day IV
Milan
6th, November 2009

Copyright © 2008 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

The OWASP Foundation

<http://www.owasp.org>

Content

- Definitions and Assumptions
- Simplicity
- Usable Security in the SDLC
- What others said
- Examples



Definition of Security

1

Risk of CIA violation



Definition of Usable (Security)

Security controls are:

- accepted
- learnable
- cost effective



Accountability will not work for B2C Apps



Nr 1 Risk in IT (Security)

Complexity



Nr 1 Goal in Usable Security

Simplicity





Simplicity

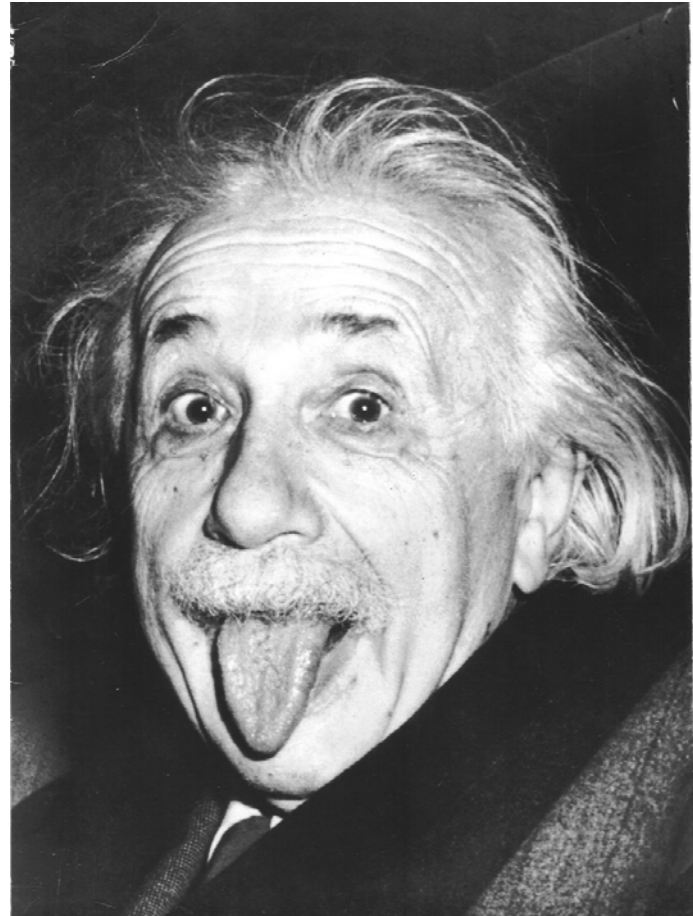
From
wisdom
to
action



Simplicity is
the ultimate
sophistication



Make it as
simple as
possible but
not simpler



to eliminate
the
unnecessary
so that the
necessary
may speak.



REDUCE
ORGANIZE
SAVE TIME
LEARN
EMOTION

10 Laws of Simplicity

by John Maeda





Usable Security in the SDLC





Performance

Security

Usability

One Architect for Everything?



Personas

Align Thinking
Focus Design
Recruit Testers

EMOTION

M1 CONFIDENTIAL

1 Primäre Persona

1.1 Ahmed Maalouf

53 Jahre, verheiratet, MBA des Imperial College in London UK, wohnhaft in Beirut (Republik Libanon). Arbeitet als selbstständiger Geschäftsmann im Import / Export. Zwei seiner Söhne sind ebenfalls in der Firma beschäftigt. Politisch engagiert sich Ahmed persönlich und finanziell in einer Bewegung „Freies Libanon“.




Private Situation und Einstellung: Ahmed zählt zur libanesischen Elite, welche von den Auswirkungen des Krieges 2006 weitgehend verschont geblieben ist. Geschäft- und Privatleben sind für Ahmed untrennbar miteinander verbunden. Die Grundlage für sein Unternehmen sowie auch sein Sozialleben bildet ein Netzwerk aus nationalen und internationalen Kontakten.


Drei von Ahmeds 5 Kindern haben im europäischen Ausland studiert. Trotz der eigenen Auslandserfahrung und der unsicheren Situation im Libanon, kommt es für Ahmed und seine Familie nicht in Frage, Beirut zu verlassen.

Wireframes

Compare Alternatives
Organize Elements
Reduce Navigation

ORGANIZE

 Data Safe

 Inheritance Settings


[New heir](#) [Create assignment report](#) [Preview inheritance](#) [Delete heir](#)

Heirs		
Name	Message	Inheritance enabled
Gabi	Dear Ergi, I ..	<input checked="" type="checkbox"/>
Ergi	-	<input checked="" type="checkbox"/>
Katrin	-	<input type="checkbox"/>

"Inheritance enabled"-
Funktionalität wird abhängig
vom geschätzten Aufwand nicht
umgesetzt.


Trigger

Status

Inheritance trigger is set (MASTERSWITCH) :  ON OFF

Trigger Code

Date created: 24.04.2008 14:34 [Create new trigger code](#)



The PDF document contains the trigger code and instructions on how to enter it. Print out the document and give it to your trusted person(s). Ask your trustees to use the code in case of your demise.

[Open PDF](#) [Print PDF](#)

You can create a new trigger code anytime - and thereby revoking the old one. Entering the old code will fail to execute the inheritance. You will be notified of such failed attempt.

Graphical Design

Guidelines
Re-Usable Panels
Consistency Checks

LEARN

The screenshot shows a web application interface for 'Inheritance' management. At the top, a user is logged in as 'Ahmed Maalouf' with links for 'Help', 'Options', and 'Logout'. The main section is titled 'Inheritance' and shows 'Inheritance is activated' with a 'Switch off' button. Below this, a summary bar indicates '3 heirs defined' and '0 of 3455 files assigned'. A table lists inheritance details with columns: 'abled', 'Files assigned', 'Last changed', and 'Data delivery'. The first row shows '123' files assigned, last changed on '12.08.2010', and 'Secure access'. A tooltip is displayed over the table, titled 'Trigger Code not printed yet', explaining that the code has been created but not sent to a trustee. It includes buttons for 'View tutorial' and 'Print now'. Below the table, a 'Safeguarding' section is visible, currently 'Not defined yet', with an 'Edit' button. At the bottom, a status bar shows 'Account Status OK' and 'Inheritance Status Action Required'.

Welcome, Ahmed Maalouf Help Options Logout

words **Inheritance**

ew Inheritance is activated Switch off

3 heirs defined 0 of 3455 files assigned

abled	Files assigned	Last changed	Data delivery
	123	12.08.2010	Secure access
			Download link

Trigger Code not printed yet
The Trigger Code has been created by the DataInherit application. But it has never been send to a trustee. The DataInherit Service will only work with a trustee to trigger the code.

View tutorial Print now

Safeguarding Edit

Not defined yet.

Account Status **OK** Inheritance Status **Action Required**



Feedback Driven Small Improvements

SAVE TIME

The screenshot shows a web application interface for DSwiss Ltd. The browser address bar displays "DSwiss Ltd." and a Google search bar. The user is logged in as "tobias208". The interface includes a "Data Inheritance" section with a toggle switch set to "On". Below this, there are three main settings panels: "Safeguarding" with a "Delay time" dropdown set to "8 Days"; "My contact data" with fields for "Mobile number:" and "Email addresses:" (showing "tobias.christen@gmail.com") and an "Edit..." button; and "Activator code" with an "Activator code:" field displaying "T31E62 7G9U8P FGBAZW Y8TSZJ PI5AY5 MGNAJI", a "Date created:" field showing "7/30/09 6:33 PM", and buttons for "View PDF" and "Create New". At the bottom, the "Account Status:" is "OK" and the "Data Inheritance Status:" is "Action required".

DSwiss Ltd. Google

Welcome tobias208 Preferences Help Logout

Data Inheritance **On**

Settings

Safeguarding

Delay time: 8 Days

My contact data

Mobile number:

Email addresses: tobias.christen@gmail.com

Edit...

Activator code

Activator code:

T31E62 7G9U8P FGBAZW Y8TSZJ PI5AY5 MGNAJI

Date created: 7/30/09 6:33 PM

View PDF Create New

Account Status: OK Data Inheritance Status: Action required



What others said



Exploit differences between users and bad guys

Bruce Tognazzini



Exploit differences in physical location

Bruce Tognazzini



Make security understandable

- Reduce configurability
- Visible security states
- Intuitive user interfaces
- Metaphors that users can understand



Usable Security Controls for Internet Apps

Authentication
Password helpers
Audit trails
Privacy Protection

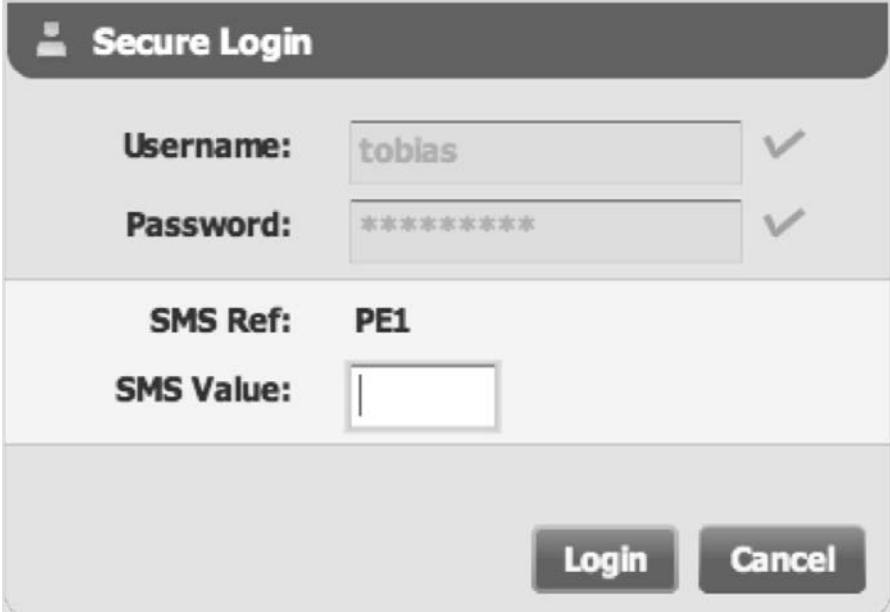


Secure Remote Password Protocol

Nothing new to learn from a user's perspective

Mitigates several pw related threats

Provides a symmetric shared secret as a side-effect

A screenshot of a 'Secure Login' dialog box. The dialog has a title bar with a user icon and the text 'Secure Login'. It contains three input fields: 'Username:' with the value 'tobias', 'Password:' with masked characters '*****', and 'SMS Ref:' with the value 'PE1'. Below these is an 'SMS Value:' field which is empty. To the right of the 'Username:' and 'Password:' fields are checkmark icons. At the bottom right are 'Login' and 'Cancel' buttons.

Secure Login

Username: ✓

Password: ✓

SMS Ref:

SMS Value:

Login **Cancel**

Password helpers

Create memorizable passwords

Rate passwords

Auto-fill forms

Store passwords encrypted

Store in DataSafe



Discussion

Where did you see the lack of usability in security?



Literature

- <http://simson.net/ref/2009/2009-10-29-HCI-SEC.pdf>
- <http://cacm.acm.org/magazines/2009/11/48419-usable-security-how-to-get-it/fulltext>
- <http://oreilly.com/catalog/9780596008277>





DataInherit
Preserve what matters.

Questions?

tobias.christen@dswiss.com

