



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

I

Risk of CIA(U) 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

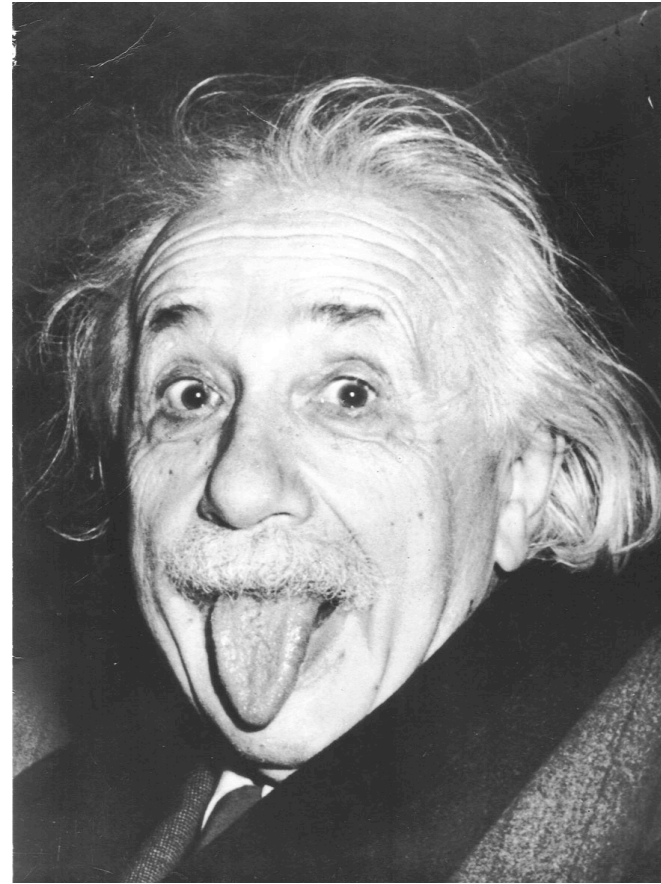
From
wisdom
to
action



Simplicity is the ultimate
sophistication



Make it as simple as possible
but not simpler



The ability to simplify means
to eliminate the unnecessary
so that the necessary may
speak.



REDUCE
ORGANIZE
SAVE TIME
LEARN
EMOTION



10 Laws of Simplicity

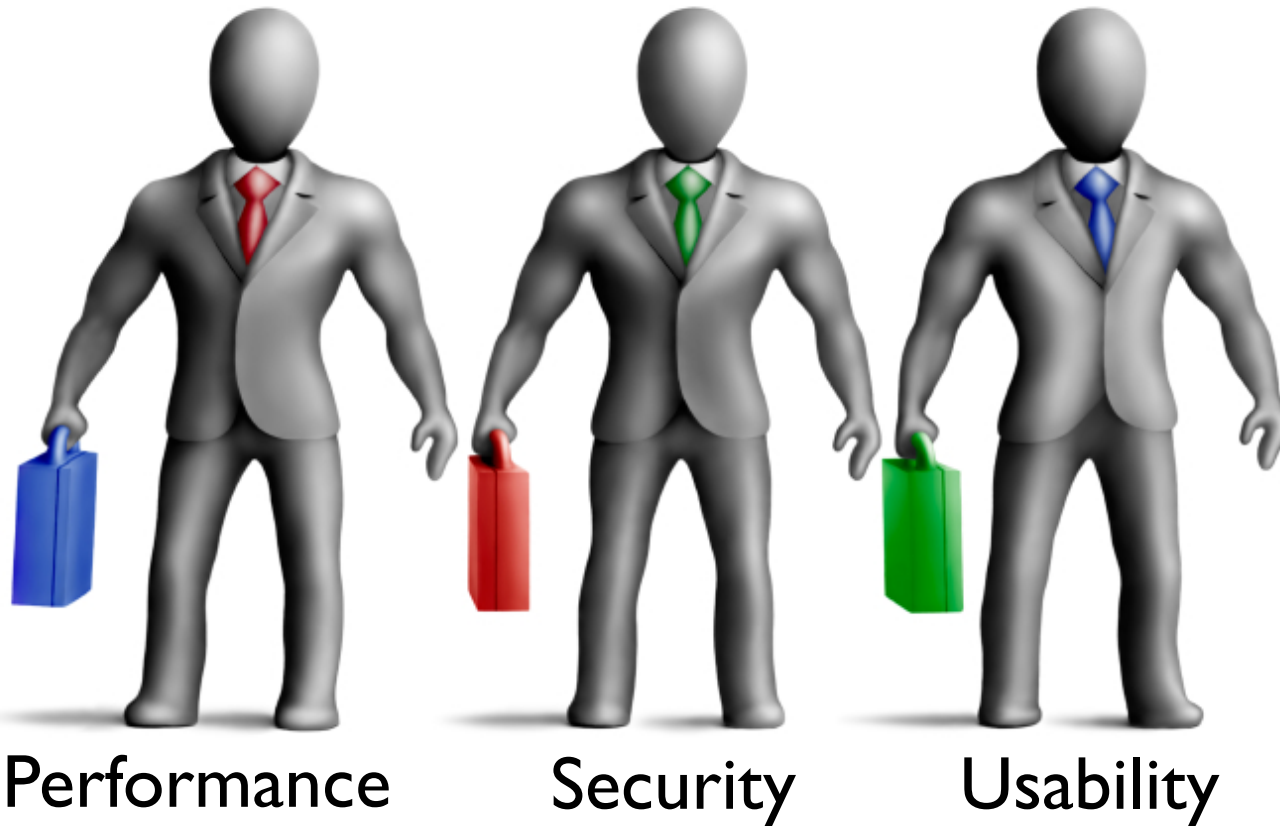
by John Maeda





Usable Security in the SDLC





One Architect for Everything?



Personas

Align Thinking
Focus Design
Recruit Testers

EMOTION

Primäre Persona



Kirsten MacDow

38 Jahre, Universitätsabschluss, wohnhaft in London

Job: Arbeitet seit 7 Jahren als Kundenberaterin (Consigliere) im Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec ac nibh lectus. In bibendum ipsum vel orci pulvinar et dictum risus consequat. Mauris viverra elementum pretium. Nunc iaculis volutpat magna, imperdiet posuere sapien consequat eu. Duis ac lacus enim. Integer rhoncus feugiat massa sit amet tempus. Nam vitae libero ac mauris dignissim faucibus. Nullam purus odio, lobortis vitae vestibulum a, lobortis at risus. Donec nec enim eget purus pretium molestie vitae id ipsum. Proin ullamcorper nulla a nunc rutrum tempus.

Computerkenntnisse: Gute bis sehr gute Anwenderkenntnisse von Microsoft Office Produkten, sowie Email und Internet. Zusätzlich verwendet sie Spezialsoftware ihres Arbeitgebers zur Verwaltung von Kundenaccounts.



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

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
	0		Download link
	0		---

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.' with a Google search bar. The user is logged in as 'tobias208'. The main navigation bar includes 'Welcome tobias208', 'Preferences', 'Help', and 'Logout'. The 'Data Inheritance' section is active, showing a toggle switch set to 'On'. The 'Settings' panel is open, displaying three sections: 'Safeguarding' with a 'Delay time' of '8 Days'; 'My contact data' with 'Mobile number:' and 'Email addresses: tobias.christen@gmail.com', and an 'Edit...' button; and 'Activator code' with 'Activator code: T31E62 7G9U8P FGBAZW Y8TSZJ PISAY5 MGNAJI', 'Date created: 7/30/09 6:33 PM', and buttons for 'View PDF' and 'Create New'. The footer shows 'Account Status: OK' and 'Data Inheritance Status: Action required'.

DSwiss Ltd. Google

Welcome tobias208 Preferences Help Logout

a Inheritance

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 PISAY5 MGNAJI

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

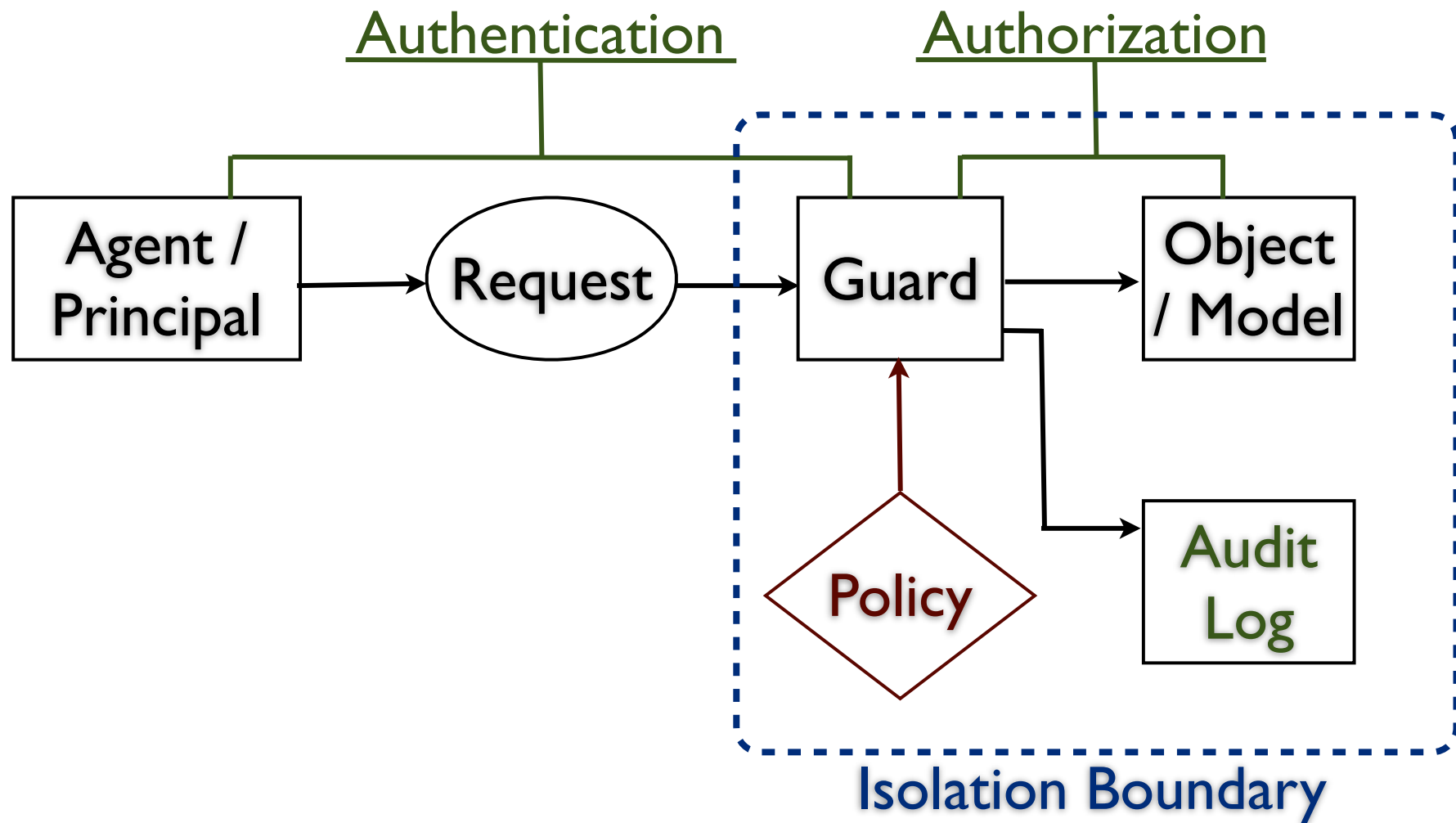
View PDF Create New

Account Status: **OK** Data Inheritance Status: **Action required**



What others said





The missing model ?

Burt Lampson



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

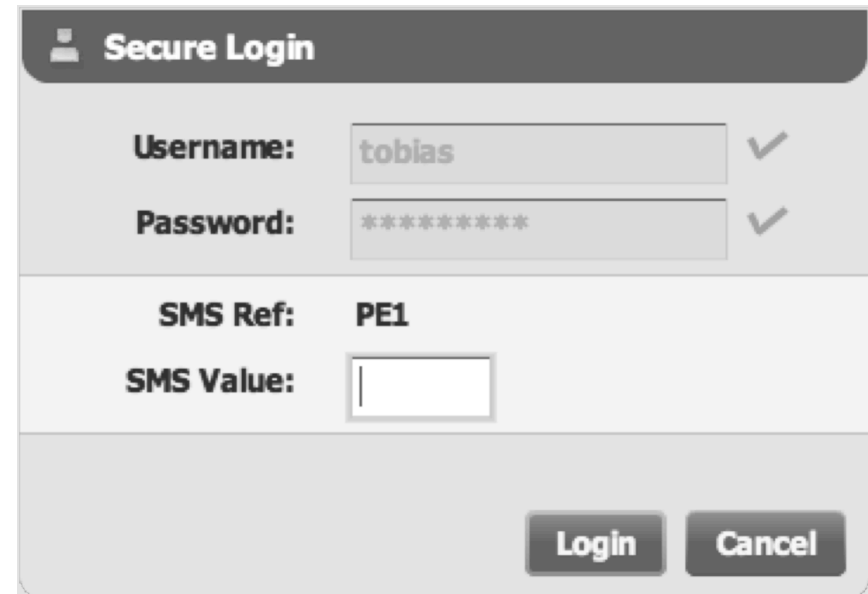


Secure Remote Password Protocol

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'. There are checkmarks to the right of the first two fields. Below these is an 'SMS Value:' field which is empty. At the bottom right are 'Login' and 'Cancel' buttons.

Secure Login	
Username:	tobias ✓
Password:	***** ✓
SMS Ref:	PE1
SMS Value:	
Login Cancel	



Password helpers

Create memorable 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>





Questions?

tobias.christen@dswiss.com



- Threat universe --> intentional vs non-intentional vs neglectance
- Misuse cases versus abuse cases
- SDLC from the user's perspective
- Fraud detection SW
- Transaction PINs must be combined with fraud detection software

