



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





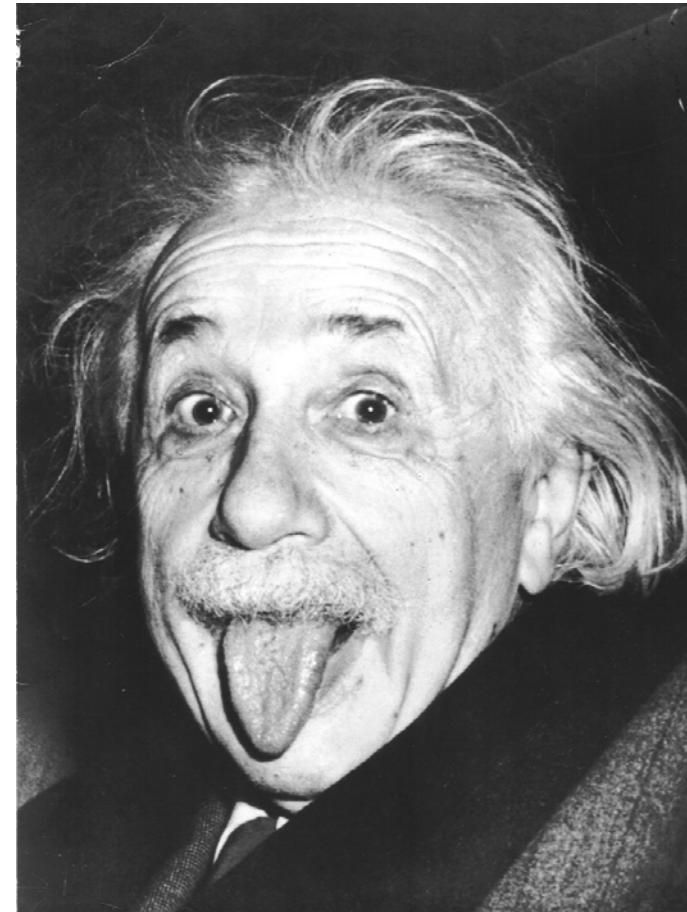
Simplicity

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

| 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) :

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-based application interface for managing inheritance. At the top, there's a navigation bar with 'Welcome, Ahmed Maalouf', 'Help', 'Options', and 'Logout'. Below the navigation is a header with tabs like 'words' and 'Inheritance'. A status message 'Inheritance is activated' with a 'Switch off' button is displayed. The main area shows a summary: '3 heirs defined' and '0 of 3455 files assigned'. A table lists inheritance details:

| Enabled | Files assigned | Last changed | Data delivery |
|---------|----------------|--------------|---------------|
| Enabled | 123 | 12.08.2010 | Secure access |
| Enabled | 0 | 0 | Download link |
| Enabled | 0 | 0 | --- |

A tooltip box is overlaid on the first row, containing the message: '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.' It includes 'View tutorial' and 'Print now' buttons.

Below the table, a panel titled 'Safeguarding' contains the message 'Not defined yet.' There are 'Edit' and a warning icon buttons at the bottom right of this panel.

At the very bottom, a footer bar displays 'Account Status OK', 'Inheritance Status Action Required ▶', and a small circular logo.



Feedback Driven Small Improvements

SAVE TIME

The screenshot shows a software application window titled "DSwiss Ltd." with a "Welcome tobias208" message. The top navigation bar includes "Preferences", "Help", and "Logout". A sidebar on the left lists "a Inheritance" and "Data Inheritance" (which is turned "On"). The main content area is titled "Settings" and contains the following sections:

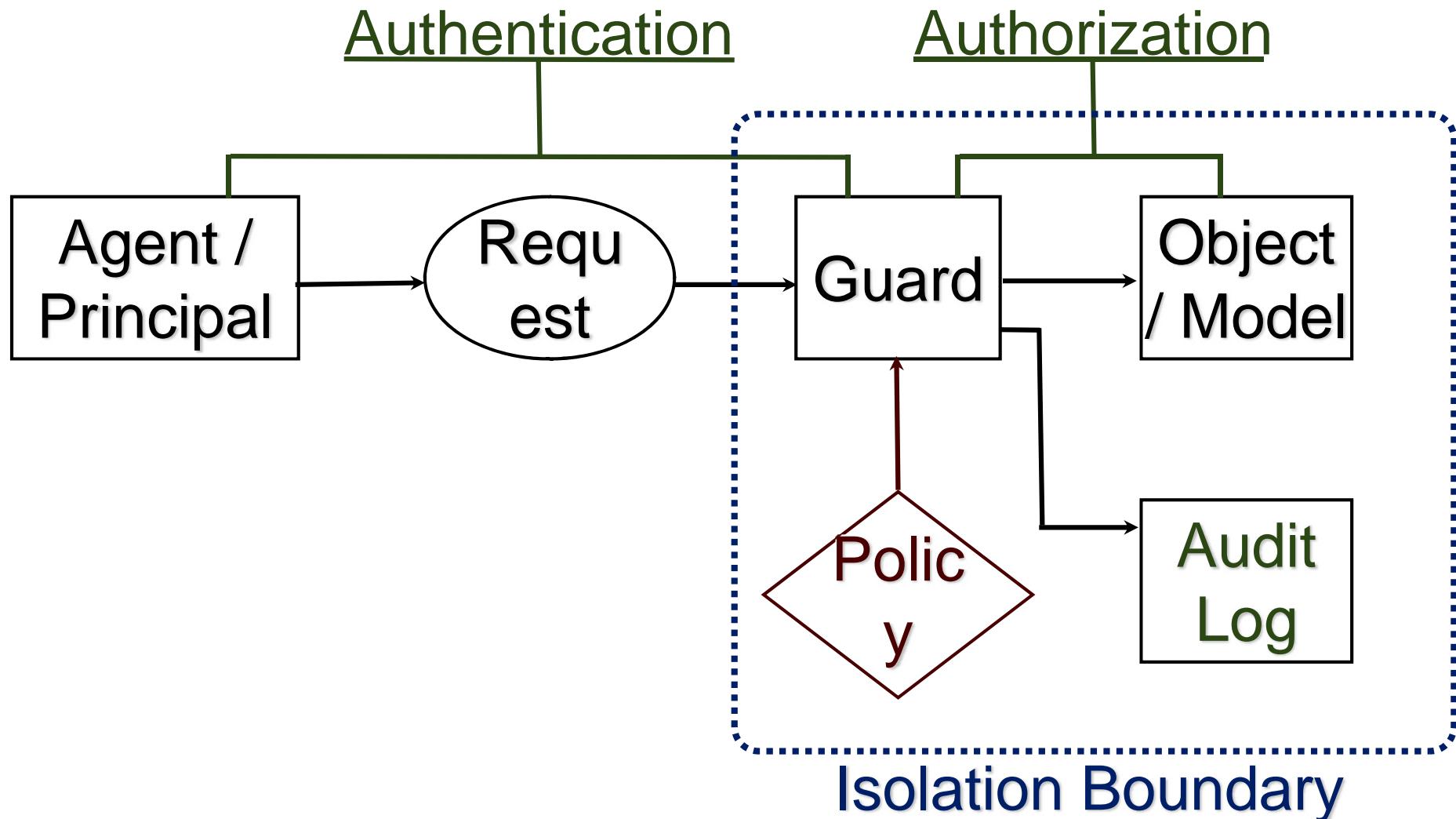
- Safeguarding**: Delay time: 8 Days
- My contact data**: Mobile number: (empty), Email addresses: tobias.christen@gmail.com, Edit...
- Activator code**: Activator code: T31E62 7G9U8P FGBAZW Y8TSZJ PI5AY5 MGNAJI, Date created: 7/30/09 6:33 PM, View PDF, Create New

At the bottom, the "Account Status" is "OK" and the "Data Inheritance Status" is "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



End-User



Sys-Admin



Security
Operations



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

The image shows a 'Secure Login' interface. The form fields are as follows:

- Username:** tobias
- Password:** *****
- SMS Ref:** PE1
- SMS Value:** (empty)

At the bottom right are two buttons: 'Login' and '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

