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.

Content

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

Definition of Security

$$\frac{1}{\text{Risk of CIA violation}}$$

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

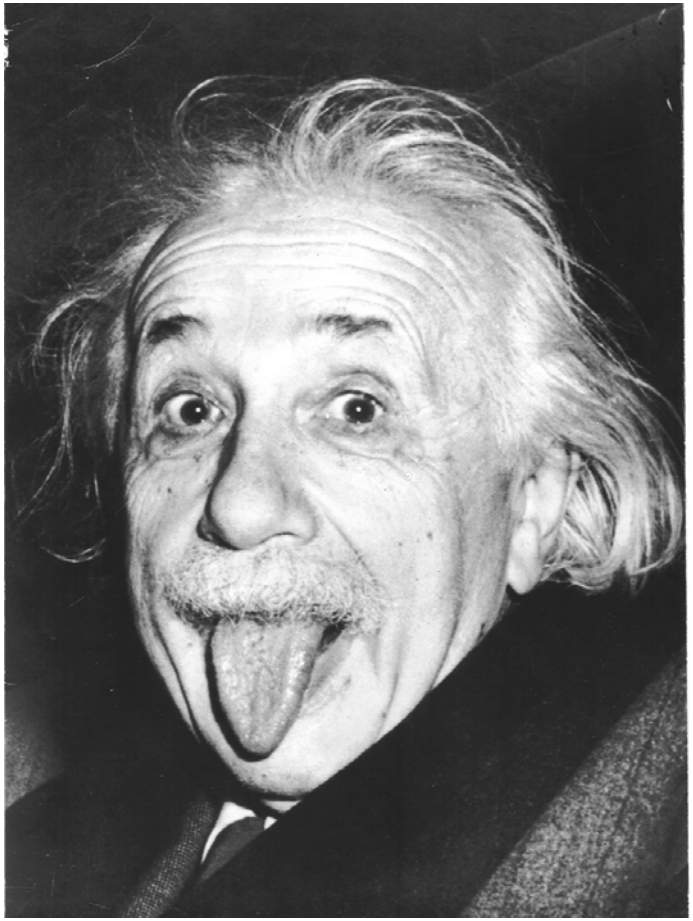
Simplicity

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

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".

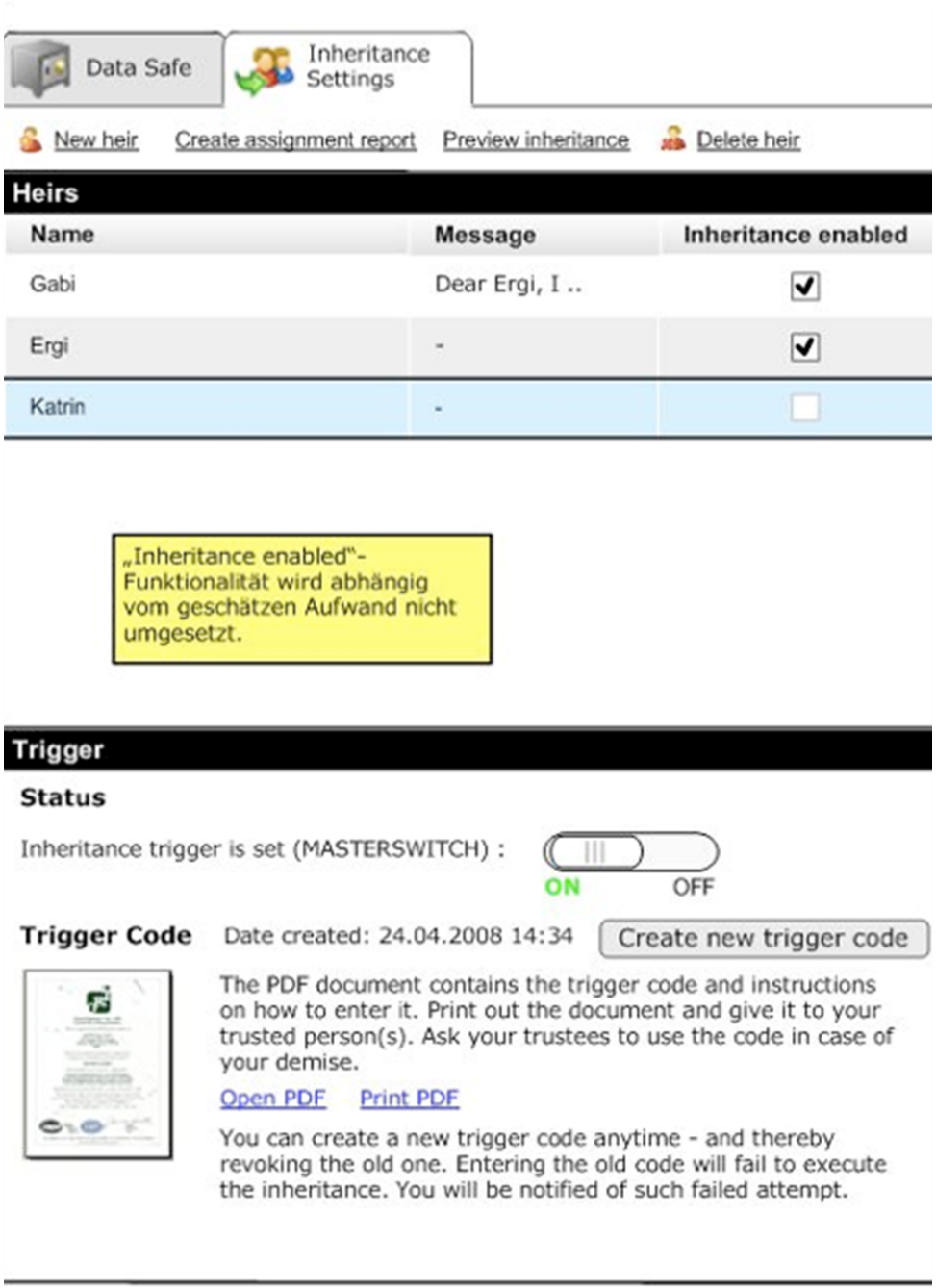
Private Situation und Einstellung: Ahmed zählt zur libanesischen Elite, welche von den Auswirkungen des Krieges 2006 weitgehend verschont geblieben ist. Geschäft- und Privatleben sind für Ahmed untrennbar miteinander verbunden. Die Grundlage für sein Unternehmen sowie auch sein Sozialleben bildet ein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



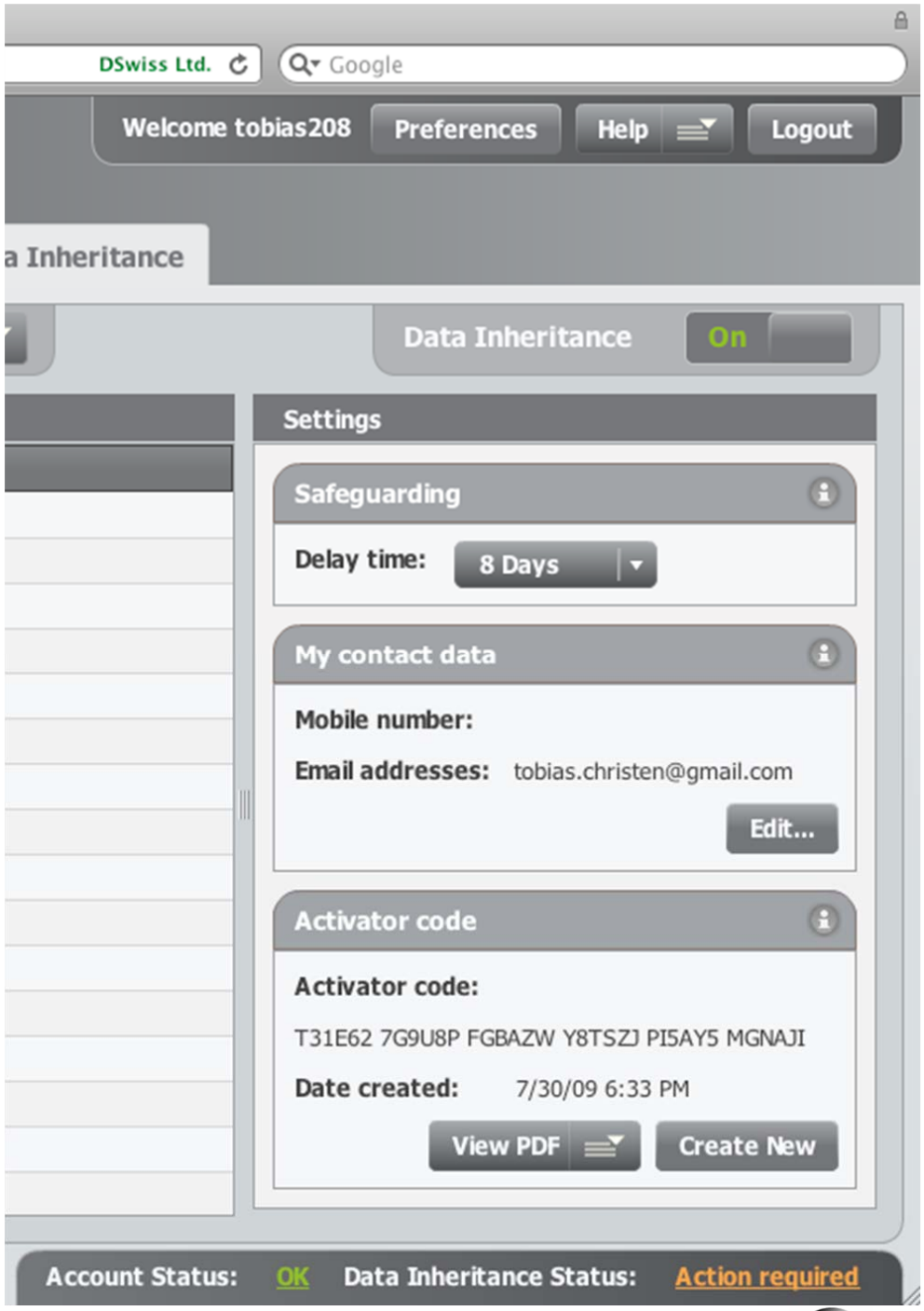
Graphical Design

Guidelines
Re-Usable Panels
Consistency Checks

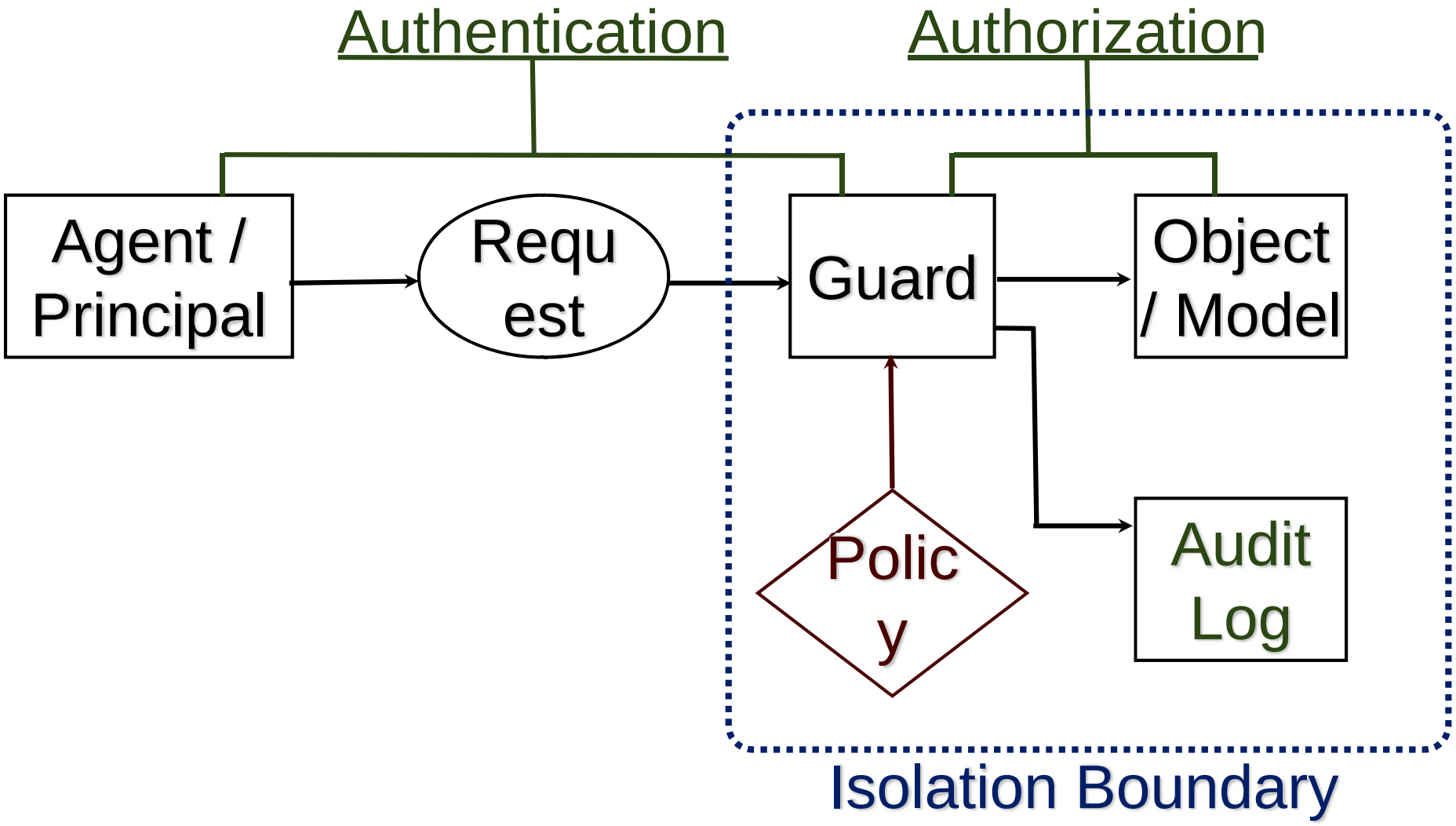
LEARN

Feedback Driven Small Improvements

SAVE TIME



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

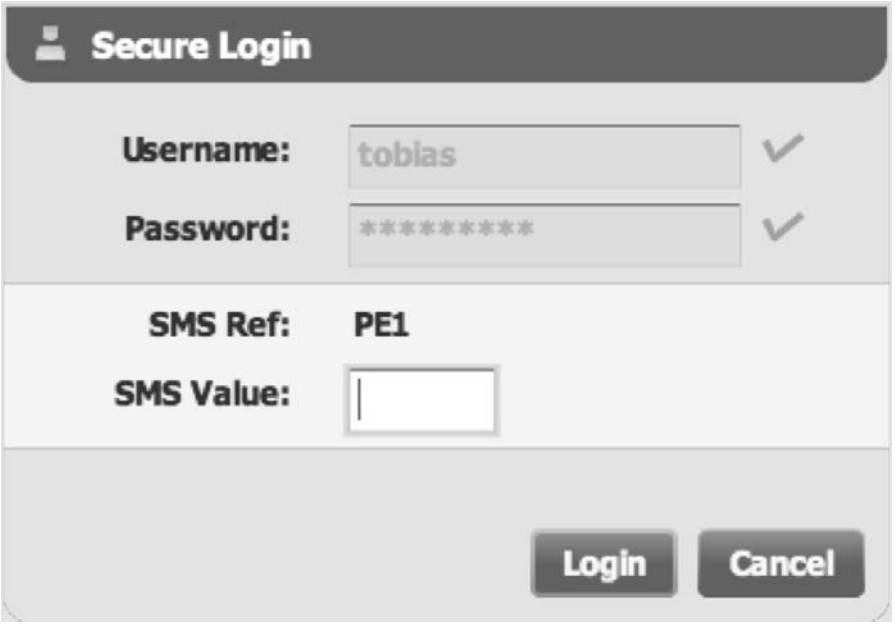
Security Operations

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



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