Usable Security

Tobias Christen

CTO
DSwiss / DataInherit

OWASP-Italy Day IV
Milan
6th, November 2009

The OWASP Foundation
http://www.owasp.org

Content

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

Definition of Security

$$\frac{1}{\text{Risk of CIA(U) violation}}$$

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

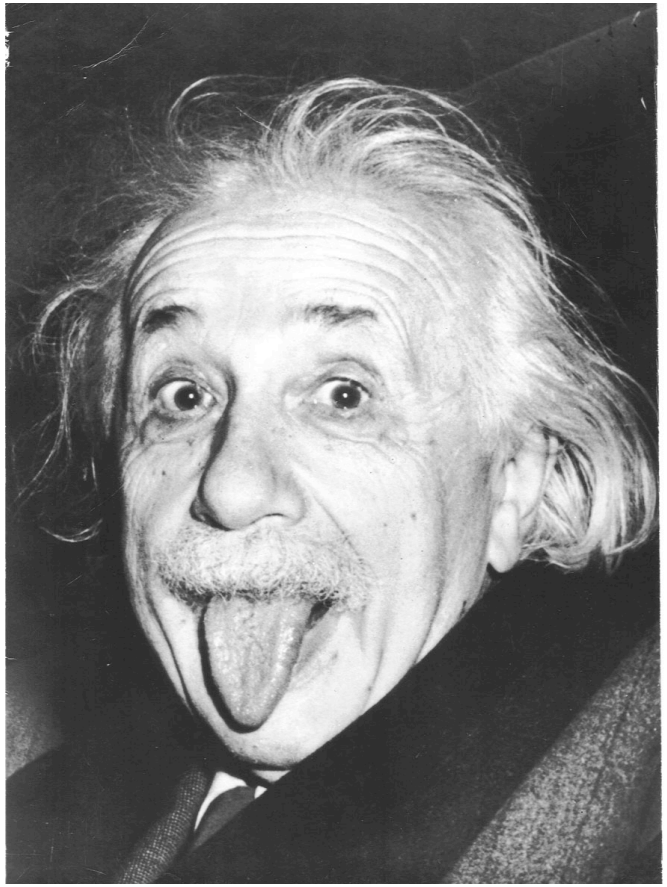
Simplicity

Simplicity

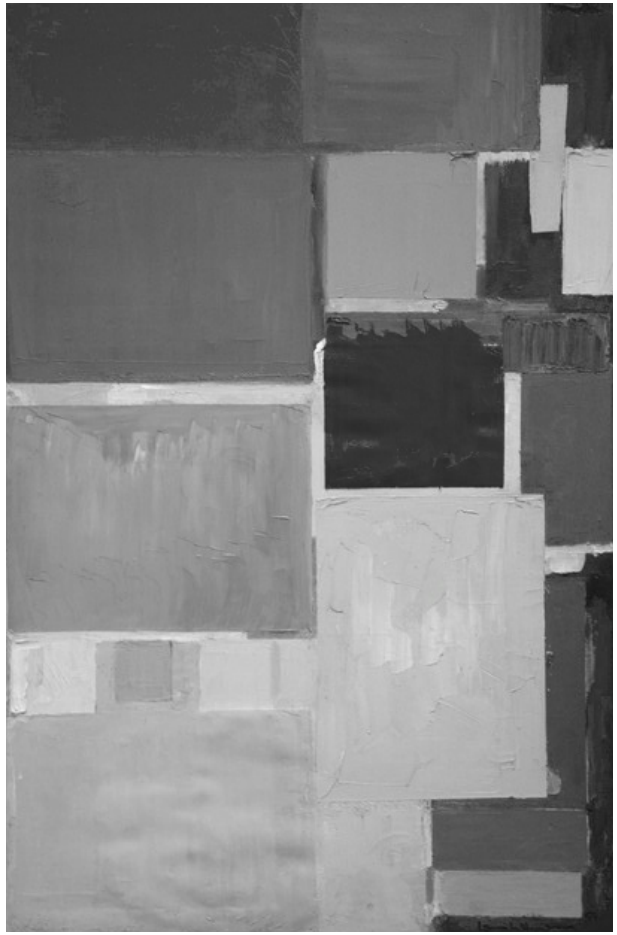
From
wisdom
to
action

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

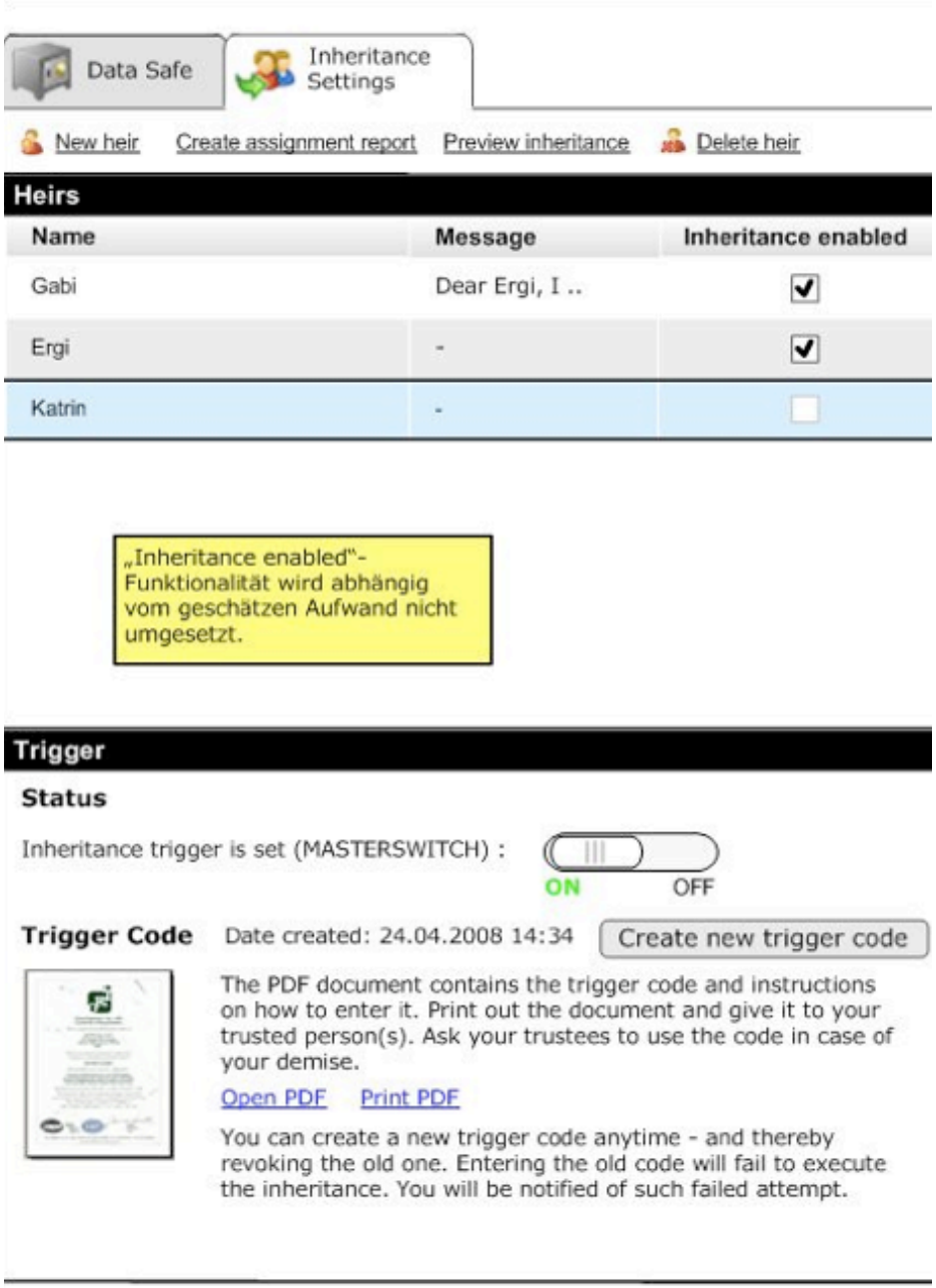
Kirsten MacDow
38 Jahre, Universitätsabschluss, wohnhaft in London
Job: Arbeitet seit 7 Jahren als Kundenberaterin (Consiglieri) im Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec ac nibh lectus. In bibendum ipsum vel orci pulvinar et dictum risus consequat. Mauris viverra elementum pretium. 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

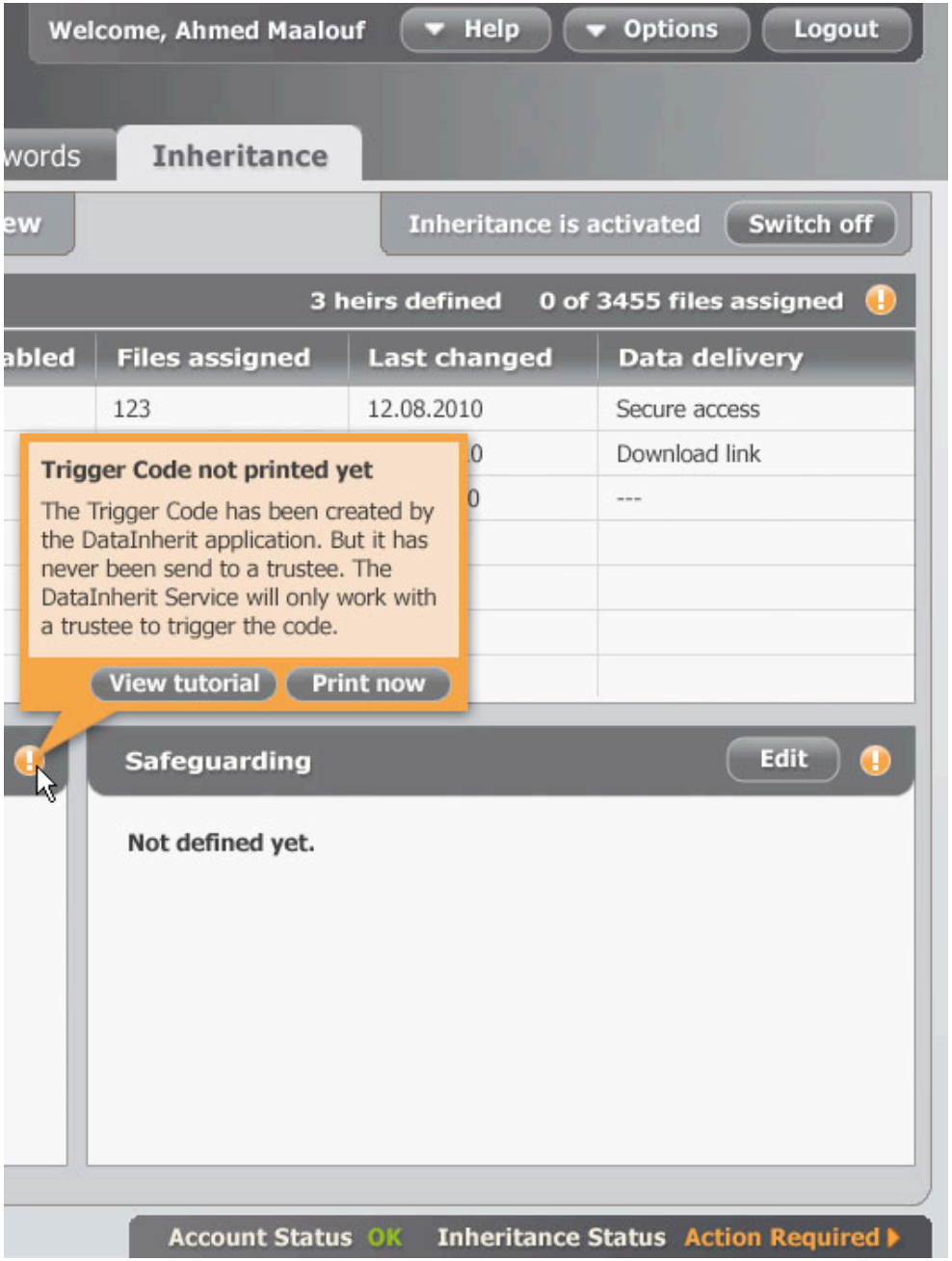
ORGANIZE



Graphical Design

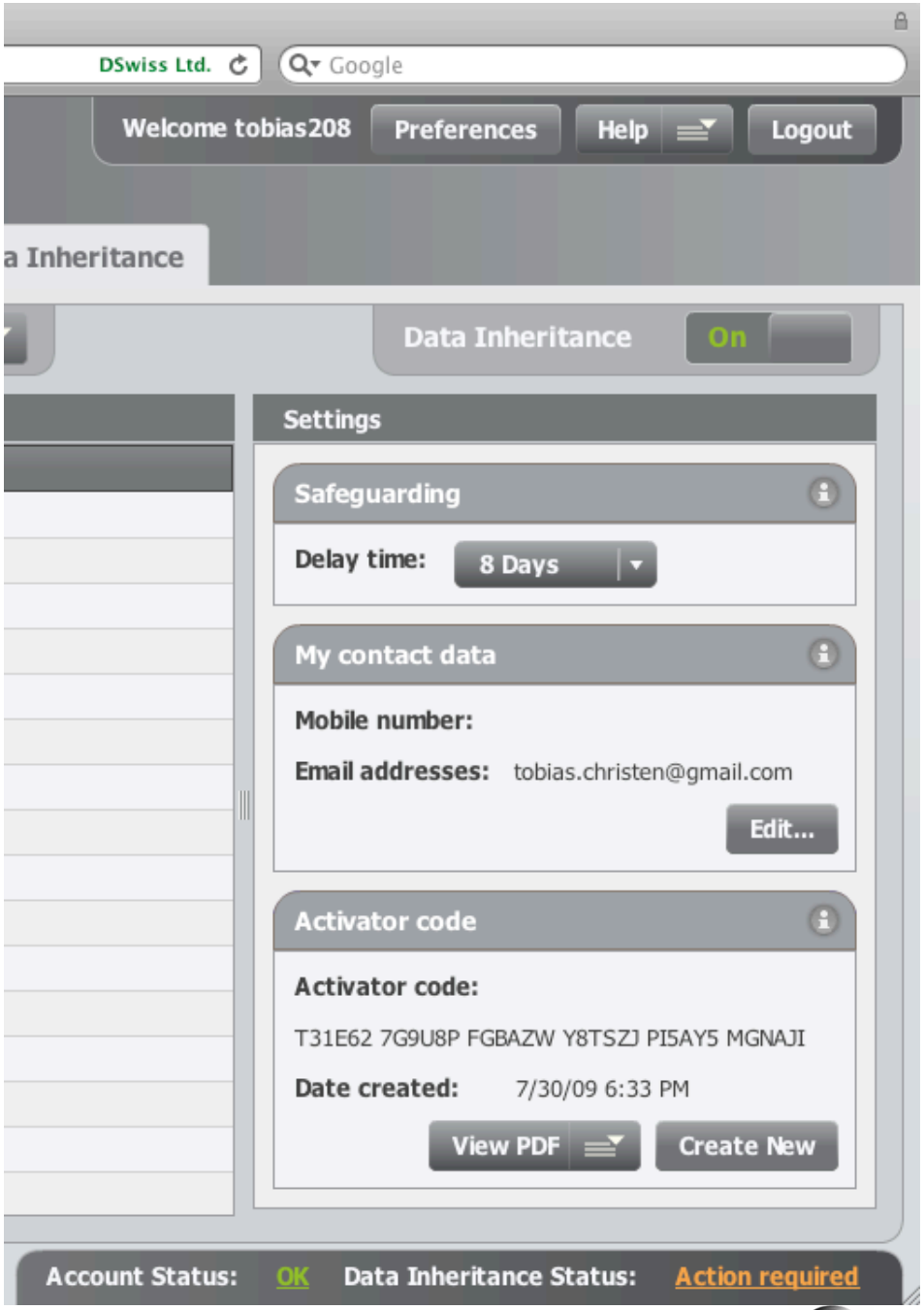
Guidelines
Re-Usable Panels
Consistency Checks

LEARN

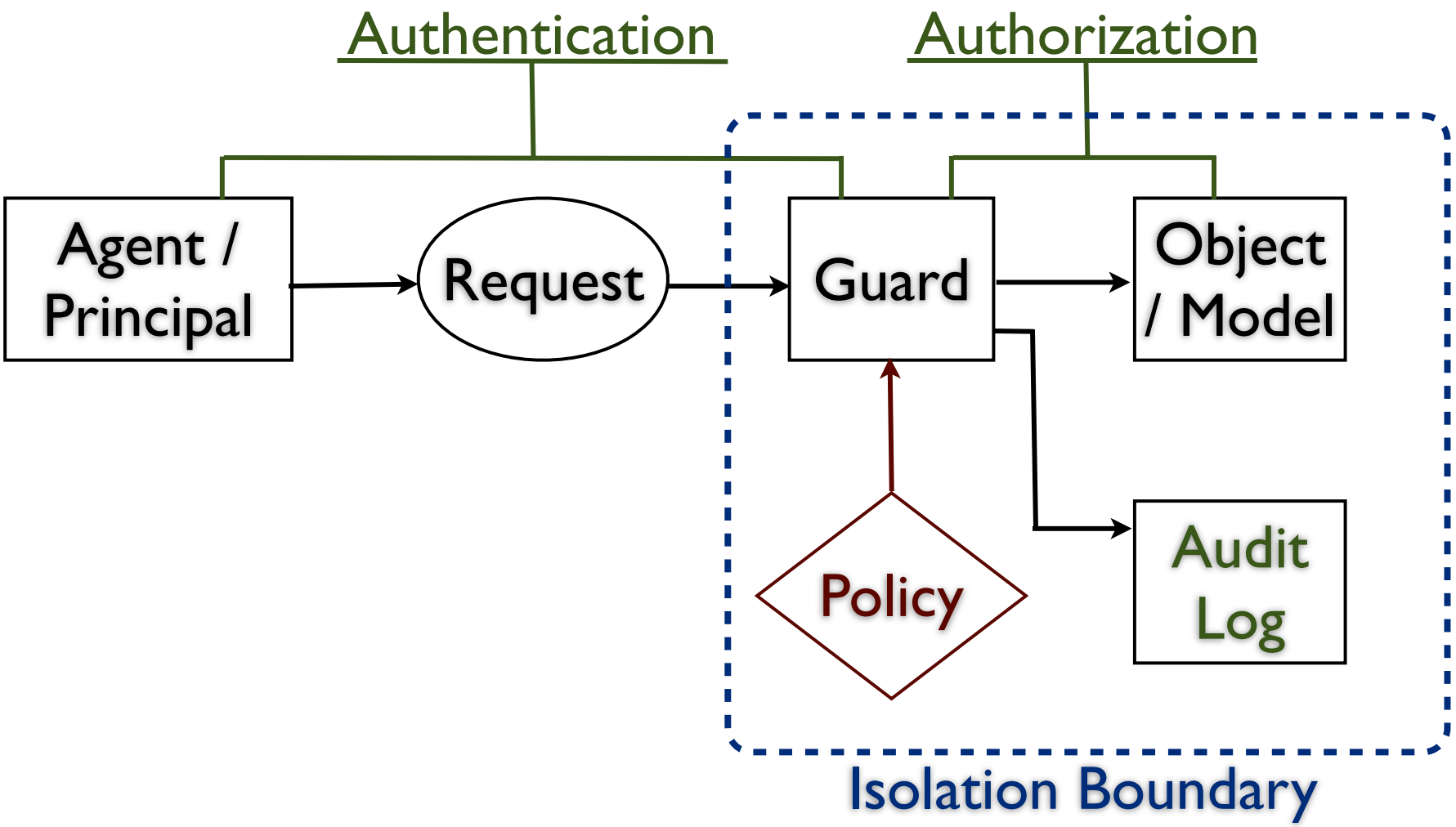


Feedback Driven Small Improvements

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 understanc

Usable Security Controls for Internet Apps

Authentication
Password helpers
Audit trails
Privacy Protection

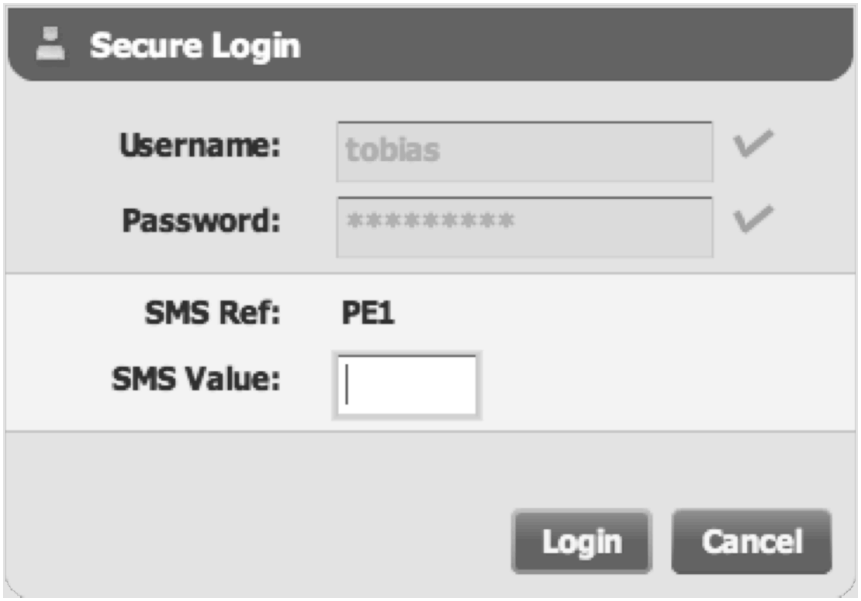
End-User

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

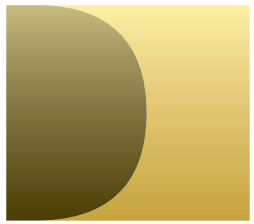
Create memorizable passwords
Rate passwords
Auto-fill forms
Store passwords encrypted
Store in DataSafe

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

- 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