



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

Risk of CIA(U) violation



Definition of Usable (Security)

Security controls are:

- accepted
- learnable
- cost effective



Accountability will not work for B2C Apps



Nr I Risk in IT (Security)

Complexity



Nr 1 Goal in Usable Security

Simplicity





Simplicity

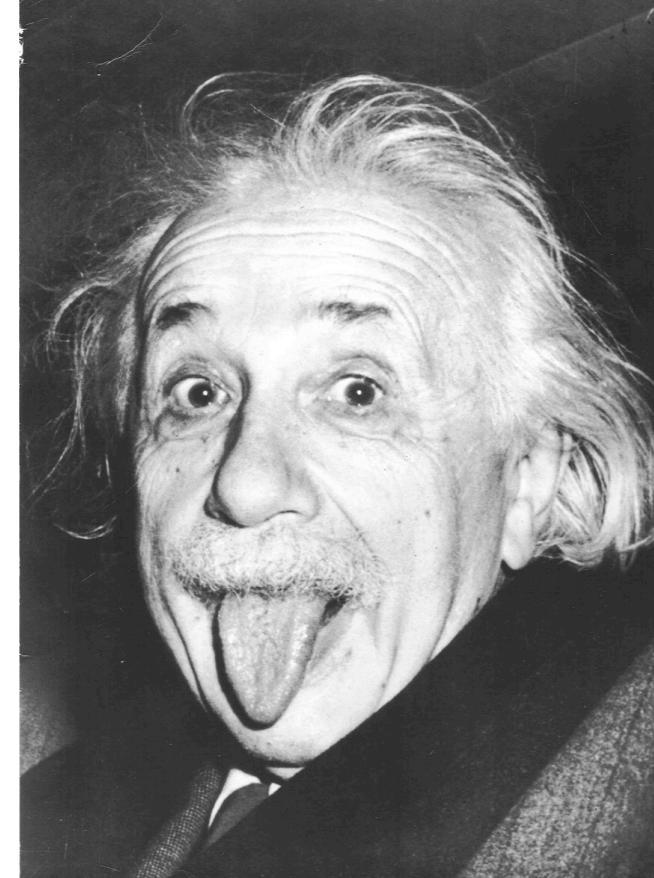
From
wisdom
to
action



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



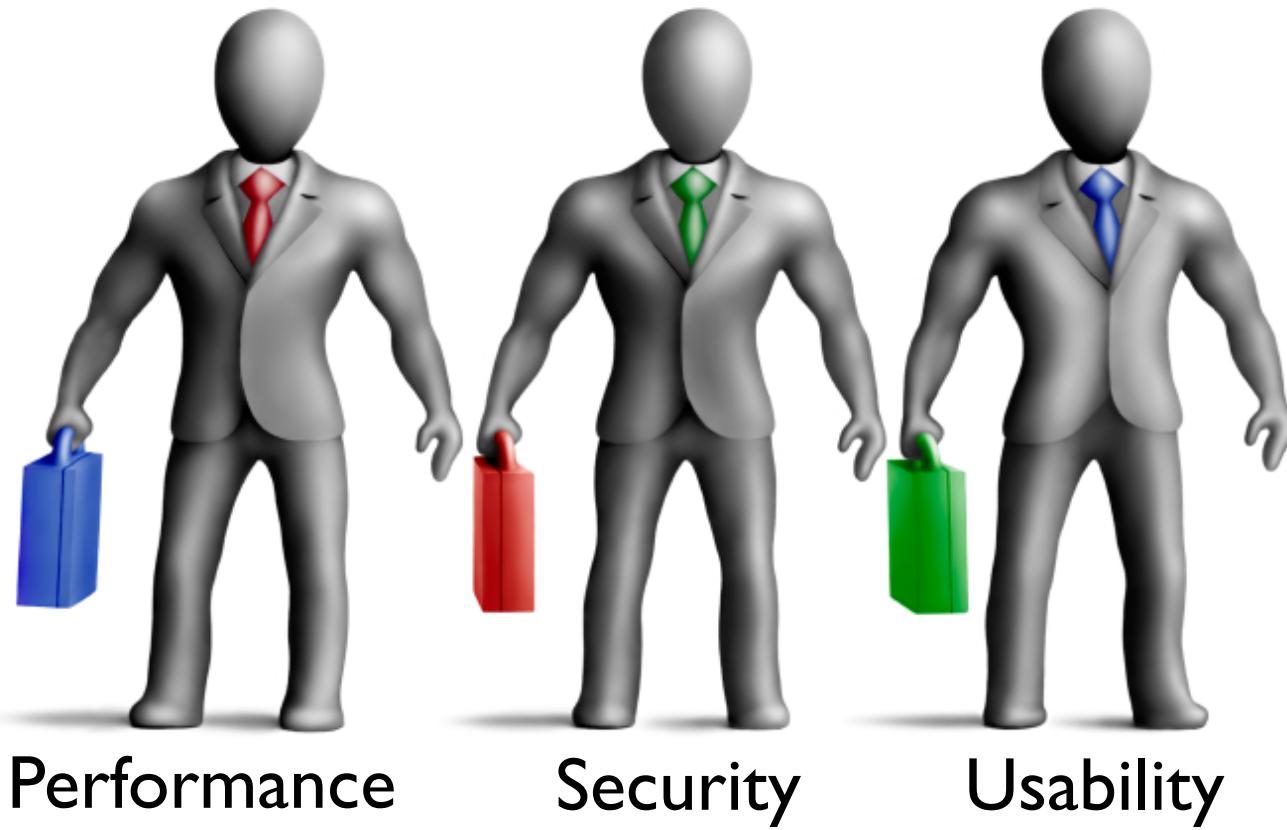
10 Laws of Simplicity
by John Maeda





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

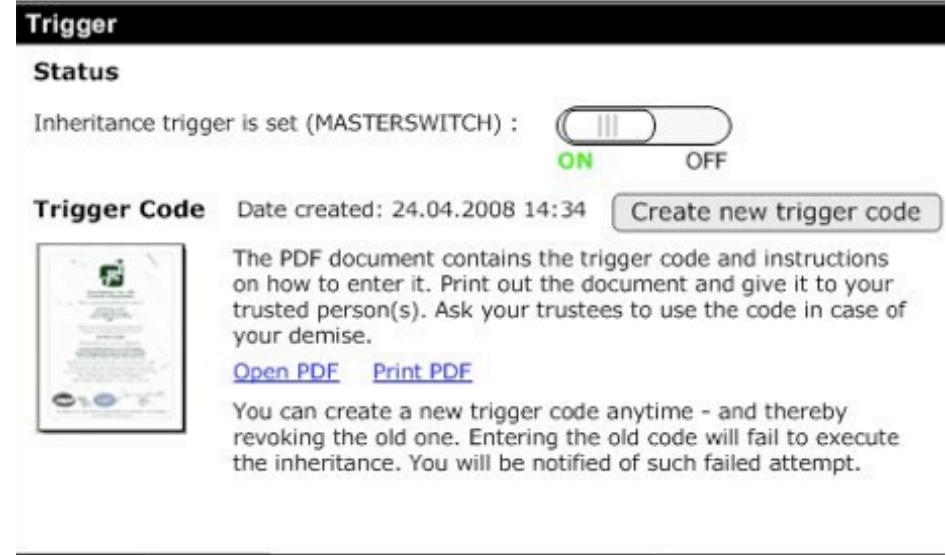
Compare Alternatives
Organize Elements
Reduce Navigation

ORGANIZE



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](#)

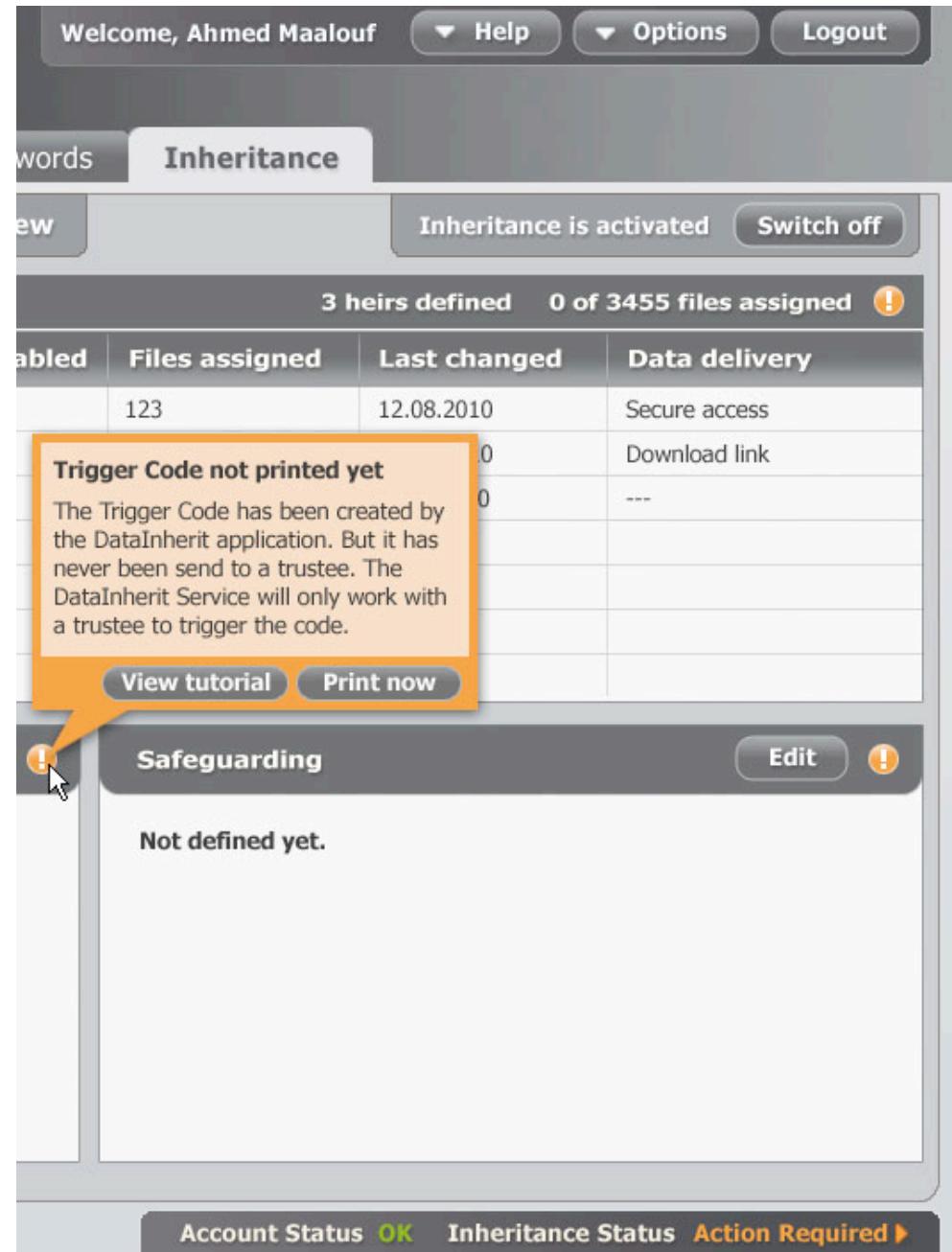
You can create a new trigger code anytime - and thereby revoking the old one. Entering the old code will fail to execute the inheritance. You will be notified of such failed attempt.



Graphical Design

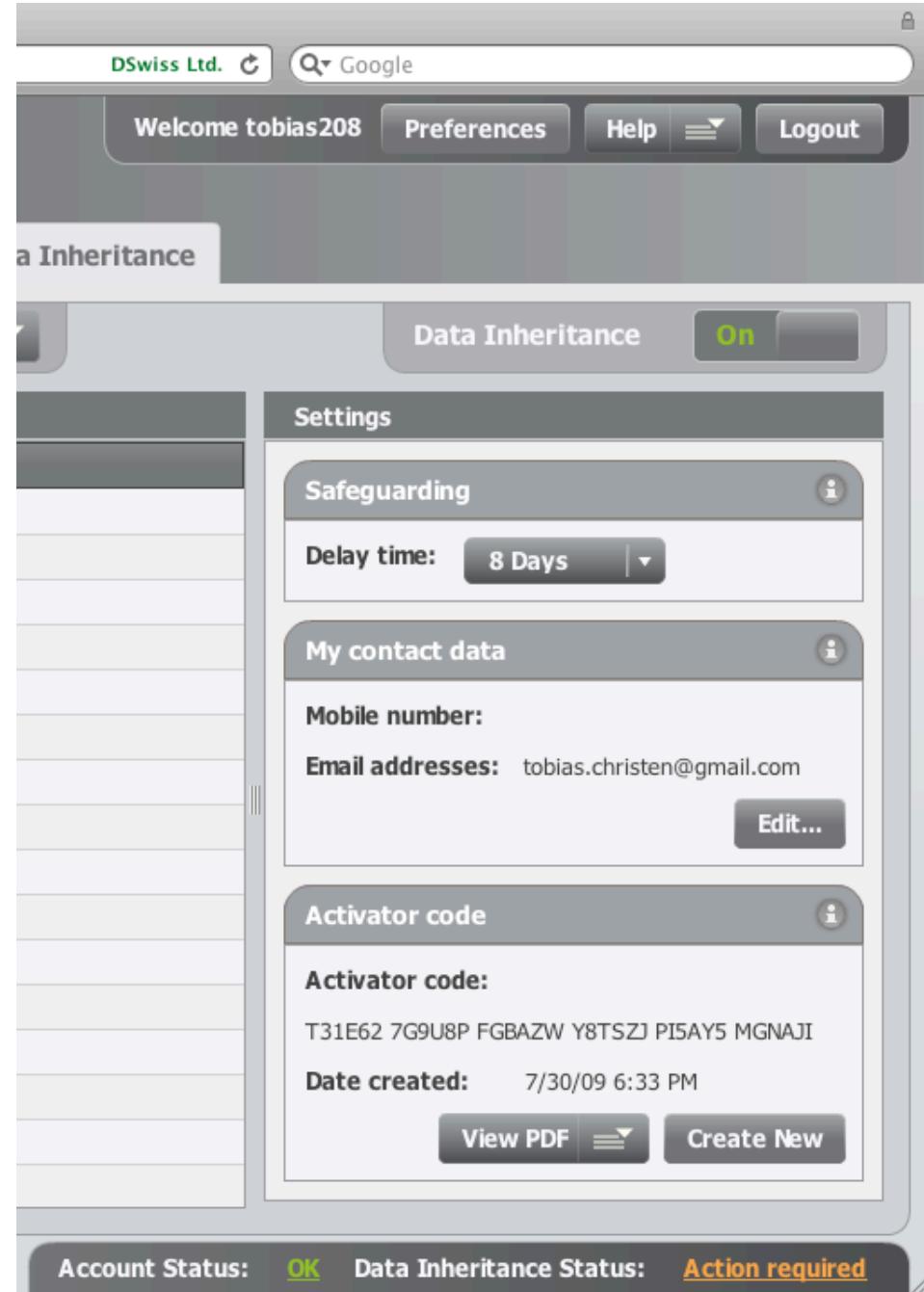
Guidelines
Re-Usable Panels
Consistency Checks

LEARN



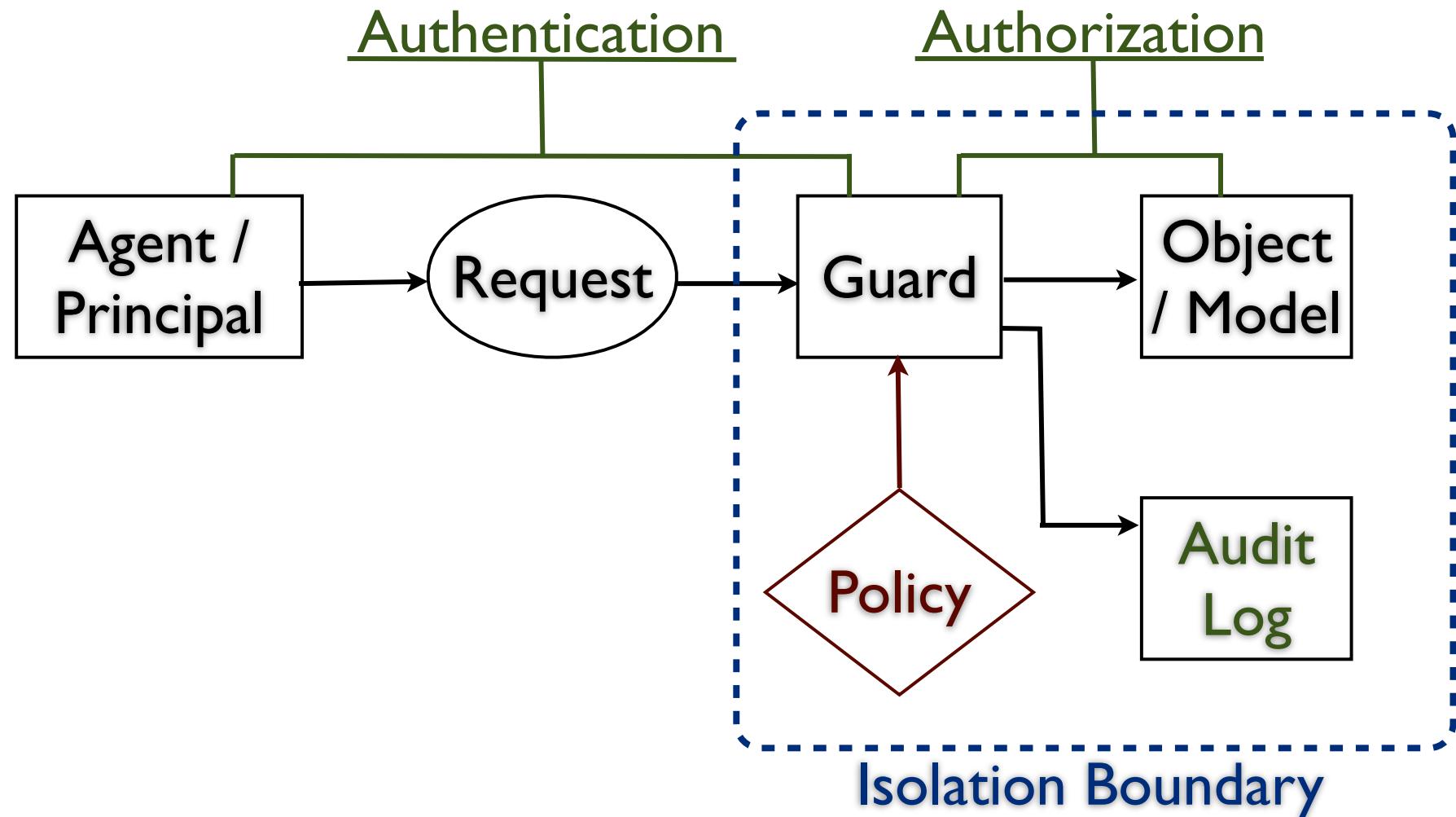
Feedback Driven Small Improvements

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



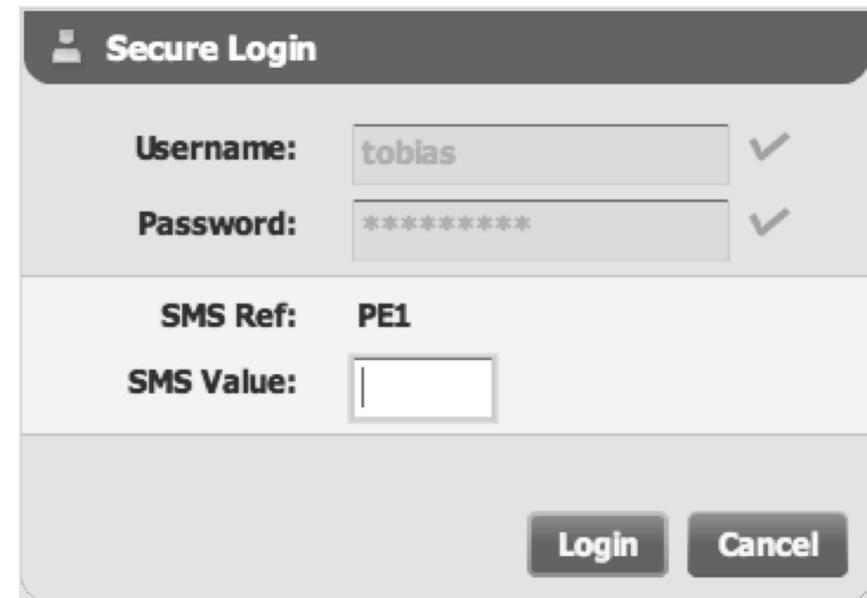
Security
Operations



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

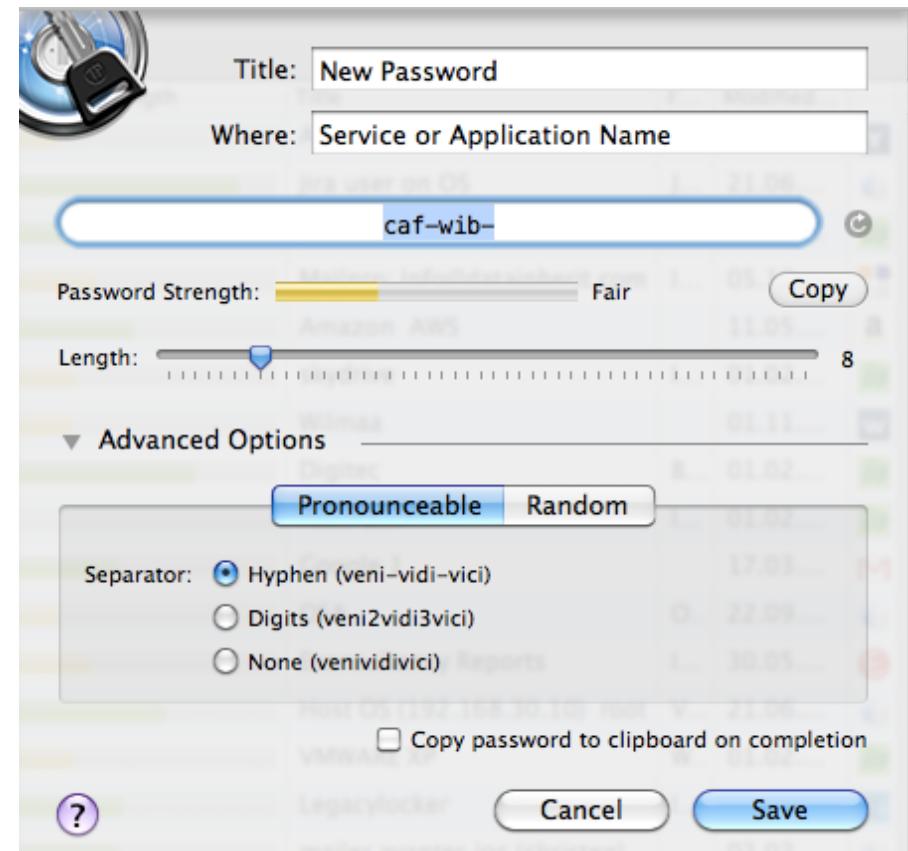


The image shows a 'Secure Login' interface. At the top, there is a header with a user icon and the text 'Secure Login'. Below the header, there are two text input fields: 'Username' containing 'tobias' and 'Password' containing a masked value. To the right of each input field is a checkmark icon. Below these fields, there are two more fields: 'SMS Ref' with the value 'PE1' and 'SMS Value' with an empty input field. At the bottom right of the form are two buttons: 'Login' and 'Cancel'.



Password helpers

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



Discussion

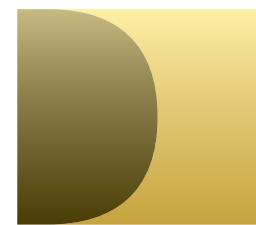
Where did you see the lack of usability in security?



Literature

- <http://simson.net/ref/2009/2009-10-29-HCI-SEC.pdf>
- <http://cacm.acm.org/magazines/2009/11/48419-usability-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

