Improving Usability of Password Management with Standardized Password Policies

Henning Klevjer[1], Bander AlFayyadh[2], Per Thorsheim[3], Audun Jøsang[1]

University of Oslo[1], Queensland University of Technology[2], Evry[3]

Presented by Henning Klevjer, hennikl@ifi.uio.no

May 23, 2012

Agenda

- Password policies
- Problems with passwords
  - Password fatigue
  - Password selection
- Survey of password policy characteristics
- Proposal
- Benefits of the proposal

Password policies

- Private, informal policies used for various online services
  - Usually not cleverly developed
  - Too hard for the user to understand the level of security
- Official standards enforced by governments, European Union, etc.

Password selection

Figure: Password selection

Password selection

Figure: Password selection

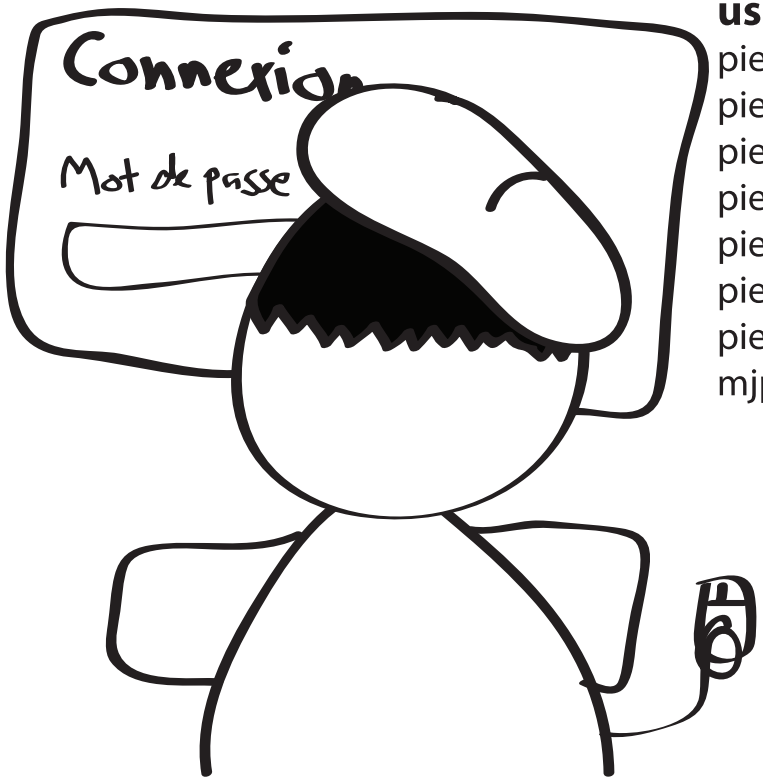
Password selection

Figure: Password selection

Password fatigue

Figure: Password fatigue / identity overload

Password fatigue



username	password
pierre2000	%_Dl# _!£$
pierre	password
pierremja	password
pierre	baguette99
pierremja	Cro1$$4nT
pierre2000	%_Dl# _!£$
pierre2000	baguette99
mjpierre	123456

Figure: Password fatigue / identity overload

Password fatigue

username	password
pierre2000	%_Dl# _!£$
pierre	password
pierremja	password
pierre	baguette99
pierremja	Cro1$$4nT
pierre2000	%_Dl# _!£$
pierre2000	baguette99
mjpierre	123456

Figure: Password fatigue / identity overload

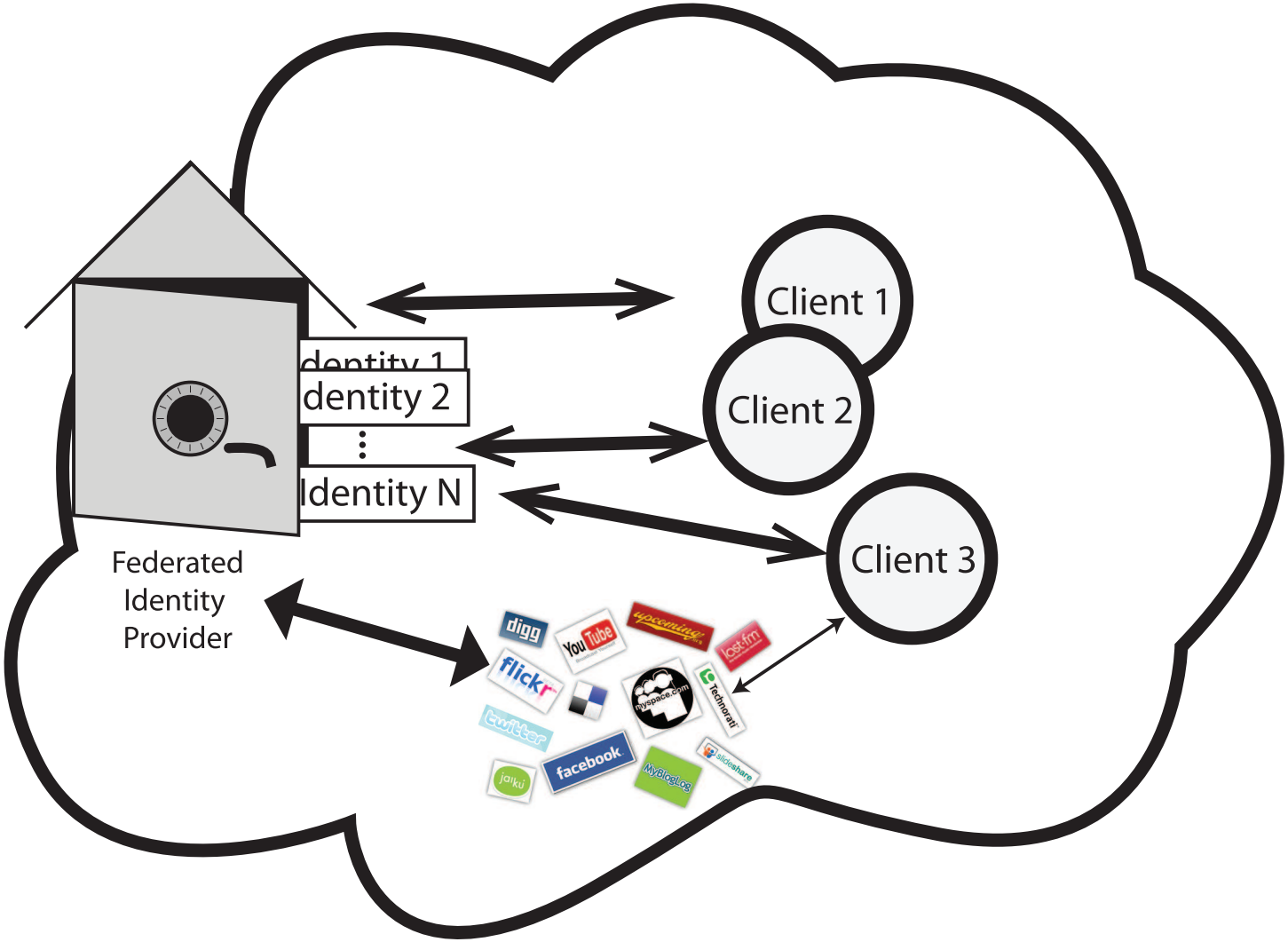
The problem with passwords

- Reuse
- Writing down

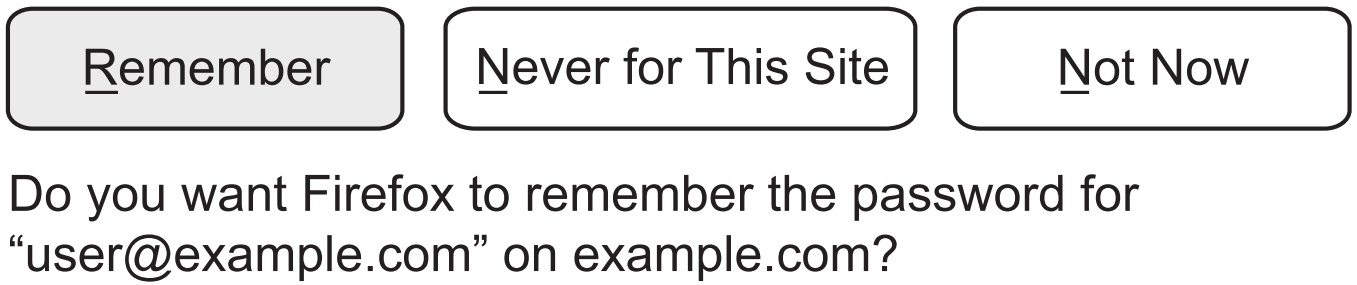
Identity management

- Identity management is usually the concern of the user.

Solutions

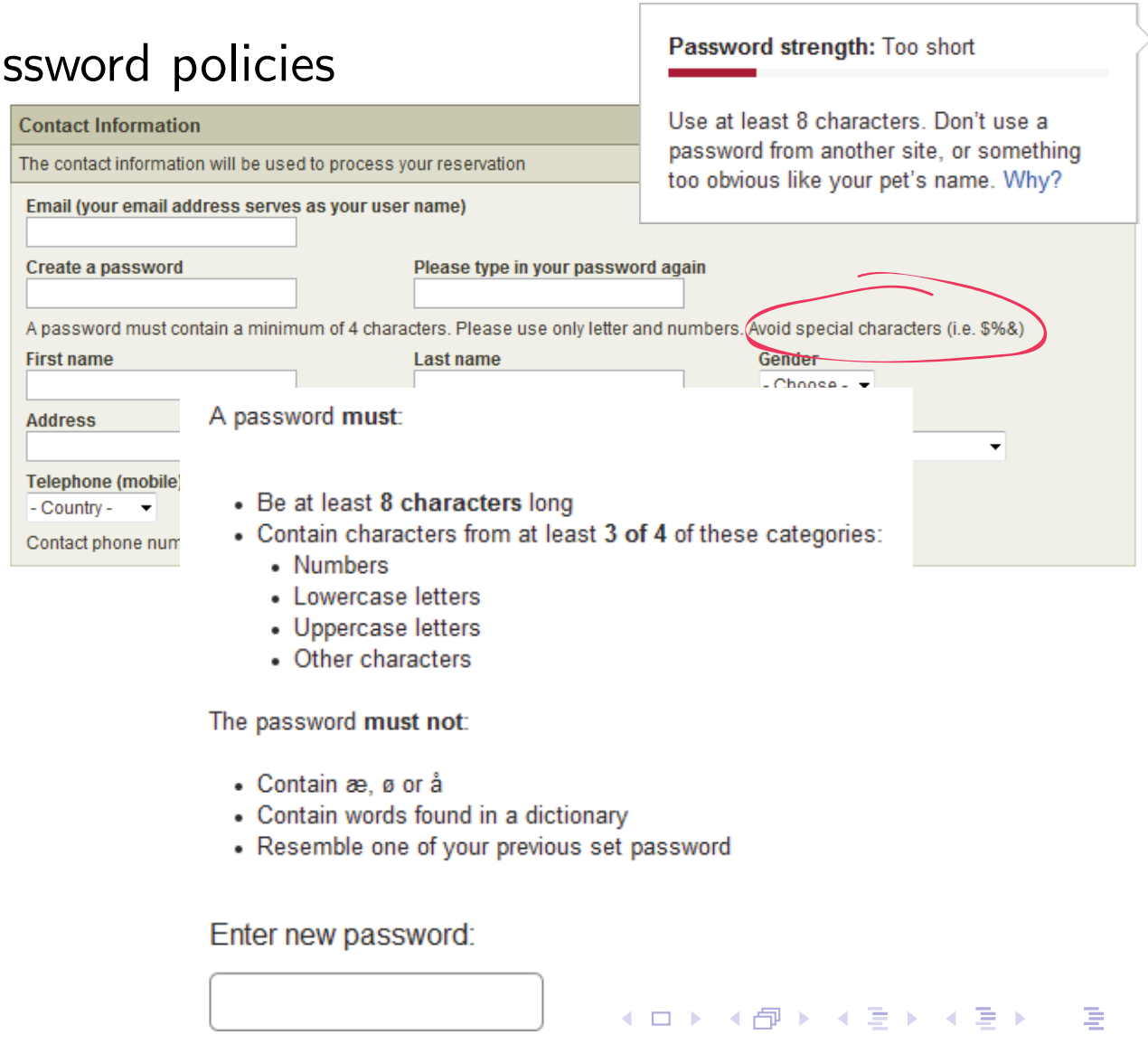

Client 1
Client 2
Client 3
dentity 2
Identity N
Federated
Identity
Provider
digg
YouTube
flickr
twitter
facebook
jaiku
MyBlogLog
Technorati
last.fm
slideshare

Solutions


Remember
Never for This Site
Not Now
Do you want Firefox to remember the password for
“user@example.com” on example.com?

The problem

Heterogeneous password policies



Critique

Too many password policies

- Only governments enforce strict standardized policies
- Private policies are too different, do not consider "security level"

Authentication Assurance Level

Authentication Assurance is the degree of confidence that the service provider can have in the veracity of the user

- The user is who he says he is
- The consequence of a false identity defines the assurance level


Jägermeister
Jägermeister promotes responsible drinking.
To access our Jägermeister websites, you must be of legal drinking age. Please enter your date of birth below.
Norway
15
08
1769
ENTER
DRINK RESPONSIBLY
Mast-Jägermeister SE, E-Mail: international@jaegermeister.de
For media requests please write to press@jaegermeister.de
Contact · Newsroom · Legals

US NIST SP800-63 password policy

- AAL1 — "Little or no assurance"
- AAL2 — "Some assurance"
- AAL3 — "High assurance"
- AAL4 — "Very high assurance"

EU IDABC password policy

- AAL1 — "Minimal assurance"
- AAL2 — "Low assurance"
- AAL3 — "Substantial assurance"
- AAL4 — "High assurance"

DET KONGELIGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Norwegian FANR password policy

- AAL1 — "Little or no assurance"
- AAL2 — "Low assurance"
- AAL3 — "Moderate assurance"
- AAL4 — "High assurance"

Australian Government

Department of Finance and Deregulation

Australian NeAF password policy

- AAL0 — "No assurance"
- AAL1 — "Little or no assurance"
- AAL2 — "Low assurance"
- AAL3 — "Moderate assurance"
- AAL4 — "High assurance"

Similarities

Similarities in many respects

- Each policy is generalized
- Applicable and available to any identity provider

Similarities

Similarities in many respects

1. 0^{th} and 1^{st} AAL: *Better than nothing; isolate users*
2. 2^{nd} AAL: Additional security, randomized passwords
3. 3^{rd} AAL: 2-factor authentication (e.g. OTP + password)
4. 4^{th} AAL: 2-factor, might require physical handover of one factor

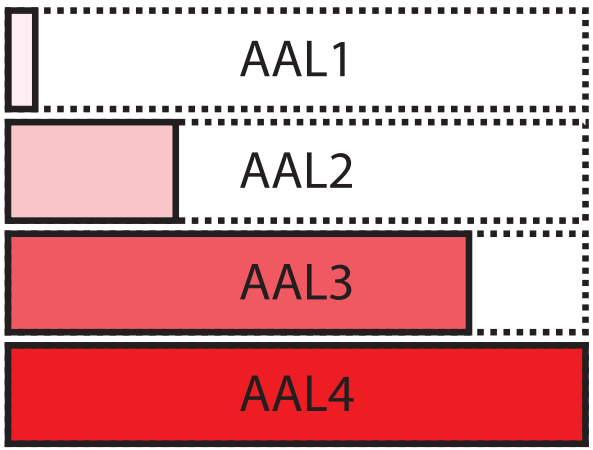
Authentication Framework	***Authentication Assurance Levels***				
NIST (USA) 2006	Little or no assurance (1)		Some (2)	High (3)	Very High (4)
IDABC (EU) 2007	×	Minimal (1)	Low (2)	Substantial (3)	High (4)
FANR (Norway) 2008	Little or no assurance (1)		Low (2)	Moderate (3)	High (4)
NeAF (Australia) 2009	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)

Correspondence between authentication assurance levels in authentication frameworks

Proposal

Proposing a generic, all-inclusive password policy

- Four assurance levels (AAL1-4)
- A generalization of the four governmental policies into one
- Applicable for both governments and private service providers
- (May not fit for all)



Benefits

Benefits to the user

- Intuitive policies ease password selection
  e.g. —*This service requires strong authentication: Your password must follow these constraints: . . .*
- No need to guess the sensitivity of the service
- Only four different policy levels to deal with

Benefits

Benefits to the service provider

- Easy to adapt to an assurance level fit for the service's assurance level
- No need to define own policy

Thank you

Questions?