

Accessibility of registration and authentication

e-Me seminar
22. March,

Norwegian Computing Center (NR)
Oslo

Kristin S. Fuglerud
Senior Research Scientist, NR

e-Me

**e-Me – inclusive identity management
in new social media**

**The e-Me project is funded by the VERDIKT
program, the Research Council of Norway.**

Content

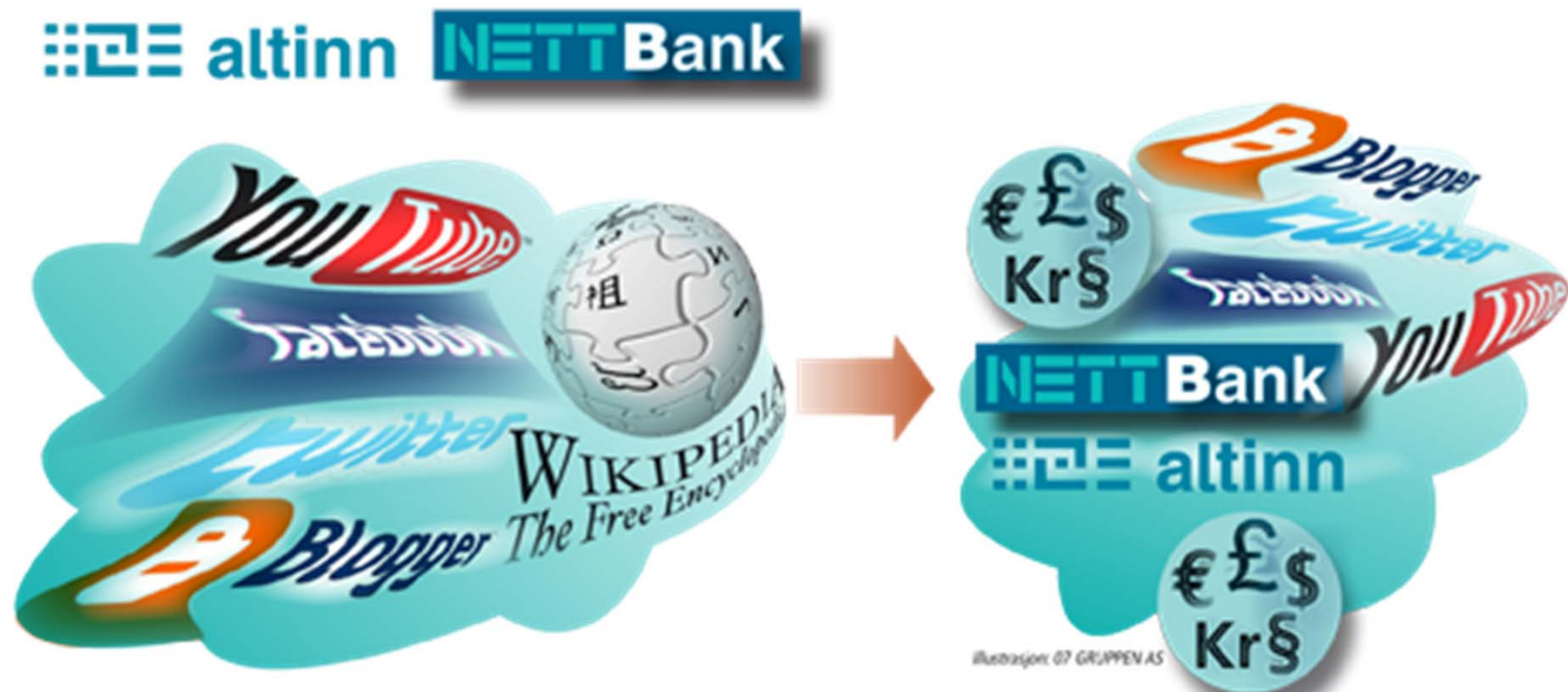
- ▶ Background, the e-Me-project
- ▶ Related work: usability and accessibility of ID technologies
- ▶ The authentication process
- ▶ Authentication examples
- ▶ Challenges and summary

Background, the e-Me-project (1)

- ▶ Identity (ID) technologies makes it possible to identify persons in the information society. The ability to use ID technologies is a precondition for using many ICT services.
- ▶ Low usability of ID technologies has been found to be a major source of flaw and risk.
- ▶ In previous projects we experienced that there are major accessibility barriers to security and ID technologies
- ▶ There is a broad political awareness and pressure towards e-Inclusion.
- ▶ Legislation requiring universal design in ICT

Background, the e-Me-project (2)

- ▶ Increasing use of Social media
- ▶ Integration of services with different use context (private, commercial and public) and thus security/privacy requirements



Background, the e-Me-project (3)

- ▶ Our main approach is universal design, i.e. the goal is that ID technologies shall be usable and accessible for as many people as possible, ideally all people.
 - Interaction style shall depend on the users sensory, motor and cognitive abilities, situations and devices.
 - using different modalities, such as: text, pictures, illustrations, symbols, sounds, voice, vibration
 - make sure that it can be used together with various types of assistive technology
 - A person in a constraining situation may produce similar requirements to a system as an impaired person

- ▶ This leads to many choices and complexity, which calls for personalization and adaptation which in turn calls for usable and accessible identity management solutions that fulfils privacy and security requirements while complying with legal frameworks

Need for inclusive ID technologies

- ▶ Precondition for use of many ICT services
- ▶ Each person is using an increasing number services, and each person have an increasing number of devices that communicates with the environment.
- ▶ Increasing number of security barriers (code passwords Security tokens, cards, biometric)
- ▶ ID technologies are necessary for personalisation and adaptation.
- ▶ Even ICT experts are not able to understand privacy and security settings



Related work – usability and accessibility of ID technology

- ▶ Users seek to get things done with the least possible effort, users do shortcuts
- ▶ Users use weak passwords, and engage in risky behavior
- ▶ Security and privacy features are often misunderstood by users.
 - Wrong conceptual models is a major source of risk and erroneous usage
 - Often, the user makes the decision without a proper understanding of the implied consequences and possible risks
- ▶ The number of studies regarding accessibility and security is extremely limited
- ▶ Current ID technologies are inaccessible and difficult to many user groups, in particular to elderly and users with disabilities

Related work – accessibility of ID technology

- ▶ Users with motor impairments use simple, non-complex passwords that are usually short in length due to their difficulty using the keyboard (D'Arcy et al. 2006).
- ▶ Some studies experimenting with non-textual visual passwords.
- ▶ Security software might be in direct conflict with assistive technology.
- ▶ User-controlled identity management tools are developed, but usability experts warn about exposing the user to such highly complex systems.

- ▶ Developers need more knowledge about accessibility
- ▶ Security technology must be more understandable
 - Help users develop good conceptual models – this requires all the skills of the designer and appropriate working methods:
- ▶ User centered development, knowledge of use context
 - Observe the users in their use context
 - Understand what the users do not understand....
 - Creativity – make prototypes
 - Test and refine
- ▶ Need for security education and awareness among users
 - Interactive education of users with reminders

What is authentication?

Authentication is a four stage process*, consisting of:

1. Enrollment/registration – matching the user with a secret (the authentication key). The key can be issued by the system or provided by the user, with the latter being more common.
2. Authentication – the user is challenged by the system to provide the key. The provided key is compared to the stored key. If they match the user is granted access.
3. Replacement – this occurs if the user forgets the key and needs to have a new one issued.
4. De-registration – the user should have the right to close his or her account together with all details removed from the system.

1. Enrollment /registration

Dato	Underskrift	Tlf. privat	Tlf. arbeid
PIN-kode A: 12345	PIN-kode B: 23456	PIN-kode C: 34567	SMS PIN-kode: 45678
D: 32101	E: 97876	F: 89786	
G: 43123	H: 23465	I: 98989	

- ▶ Dependent on context
 - Username and a user generated password
 - Captcha
 - Letter in post with pins
 - Many codes – confusing
 - Thin paper with weak ink colour

1. Enrollment /registration Captcha

Choosing a word relating to several images:

ESP-PIX - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ESP-PIX

The CAPTCHA Project

150 ways to play Solitaire

P Z B S

Credit and debt
Credit cards

Choose a word that relates to all the images.

cake
butterfly
cake
camera
card
cat
cheese
church
clock
coin
cow
cup
dog
doll
drop
egg

TIP: You can use the arrow to move up or down

© 2004 Carnegie Mellon University, all rights reserved.

1. Enrollment /registration

Image and audio based Caphca: HIPUU*

17

Play Audio CAPTCHA



Please Input Answer 1
Here



Please Input Answer 2
Here

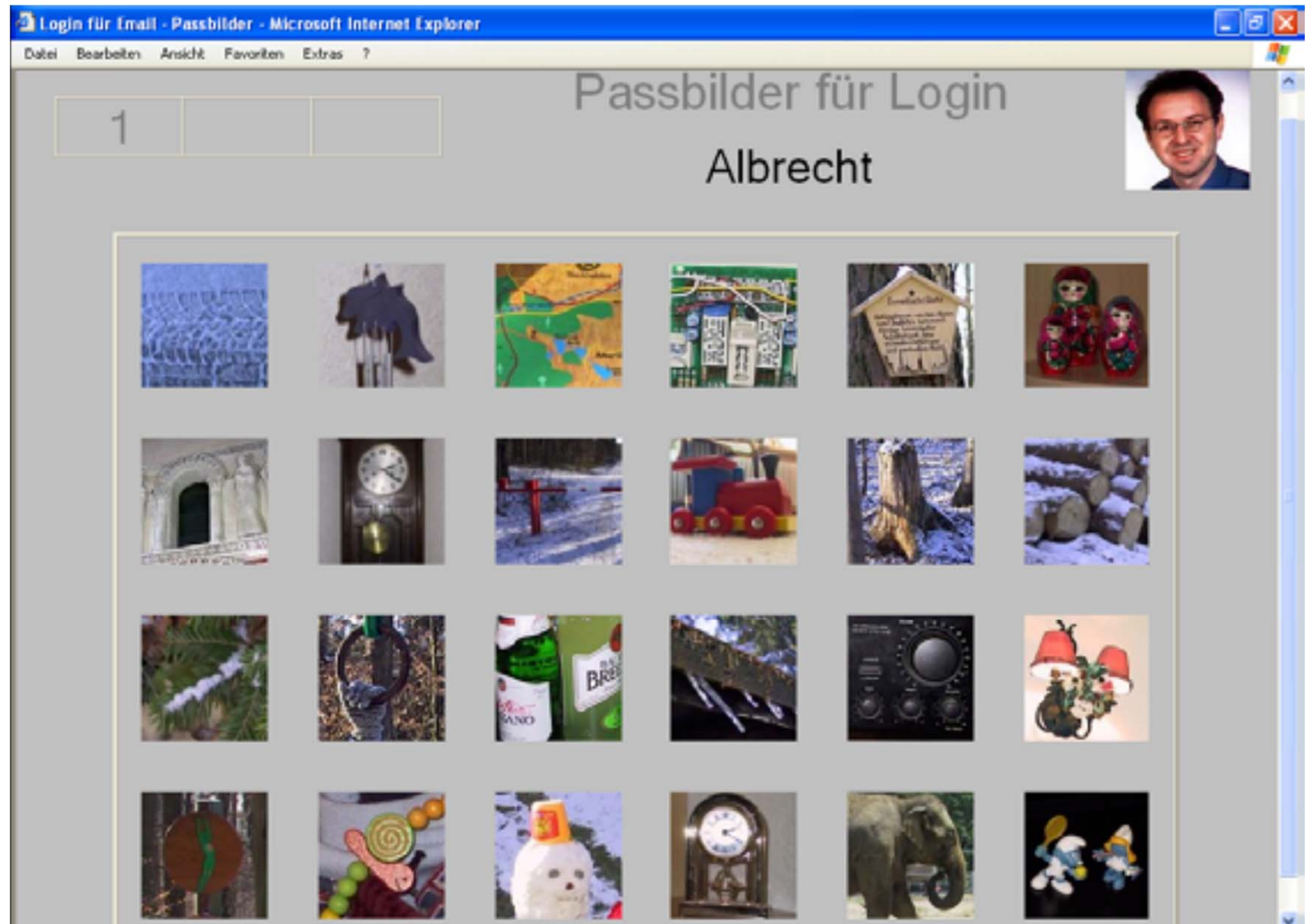


Please Input Answer 3
Here

Submit

2. Authentication Visual passwords

18



2.

Sound based
"kodes"

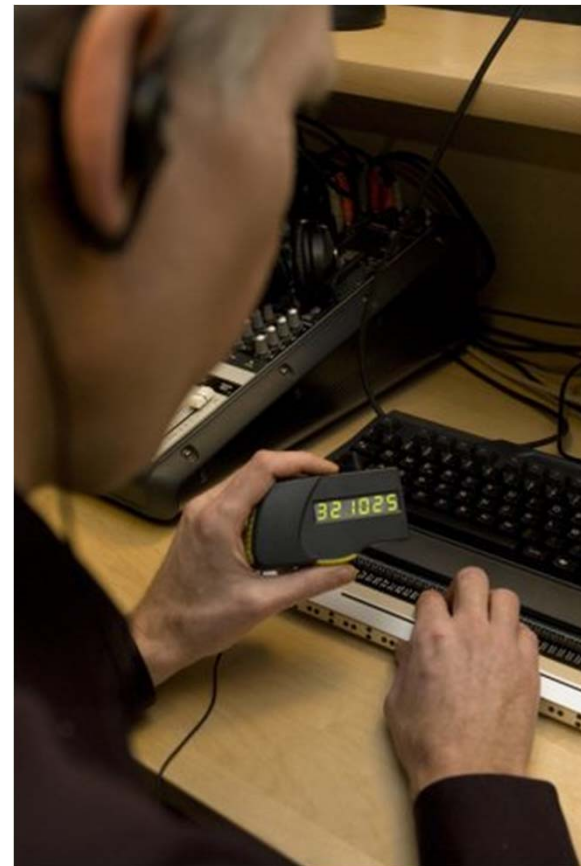
PhD work of
Garcia Gibson



2. Authentication (1) Security tokens



- ▶ Hardware code generator (DNB Nor provides with big display and audio)



2. Authentication Biometrics

21

Common biometrics

- Fingerprints
- Iris recognition
- Signature
- Speech/voice recognition

Other methods:

- Hand geometry
- Vein geometry
- Facial recognition
- Gait recognition/ walking

Illustration from:

<http://accessit.nda.ie/it-accessibility-guidelines/smart-cards/guidelines/smart-card-guidelines/authentication>



fingerprint recognition;



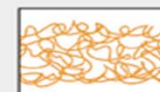
iris recognition;



face recognition;



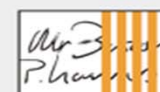
hand geometry recognition;



vein recognition;



voice recognition; and



dynamic signature recognition.

2. Authentication Challenges with biometrics

22

- ▶ Not all people have the same physical features.
- ▶ Might need different readers (expensive equipment) at an access point
- ▶ The physical feature may be temporary or permanently damaged by disease or accident
- ▶ Inaccuracy: Sometimes it just fails for no explainable reason
- ▶ Biometrics usually have higher failure rates with old people. As people get older, ageing processes tend to degrade biometrics.

2. Authentication: need for alternatives

Method	Feature	Visually Impaired	Hearing Impaired	Physical Impaired	Cognition Impaired	Dyslexia
Passwords	Text token	●	●	✗	✗	✗
Text Captchas	Distorted Text	✗	●	✗	✗	✗
Smart cards	Small card with chip; card reader	✗	●	✗	●	●
Number tokens	Challenge-Response	✗	●	✗	✗	✗
Fingerprint scanning	Small scanner	✗	●	✗	●	●
Voice recognition	Microphone on computer system	●	✗	●	●	●

Challenges

- ▶ Diverse user groups
- ▶ Flexibility of authentication methods, present alternatives
 - How can these alternatives be presented in a usable and accessible way?
- ▶ User behaviour in different contexts, elicit users conceptual models
- ▶ How to introduce appropriate and efficient conceptual models
- ▶ User centred development in a interdisciplinary group: collaboration within areas such as security, privacy and legal.

Challenges

- ▶ Privacy/security is rarely a primary goal for users:
 - Most users do not care about privacy/security until it is broken.
 - a study itself may introduce bias by having the participant focus more on security than outside an experimental setting.
- ▶ Qualitative methods such as observation have been used successfully in a number of studies but have limitations:
 - ethical issues in unobtrusive/covert real life studies
 - significant inconsistency with what people say they do and what they actually do.
- ▶ Lab experiments have its limitations:
 - Security focus bias
 - When using dummy data users do not act to protect their data as if it is their own.
 - Privacy and ethical challenges of having users using their own data

Thank you for your attention!

- ▶ Questions?
- ▶ Contact information:

Kristin S. Fuglerud
Norwegian Computing Center
e-mail: Kristin.Skeide.Fuglerud at nr.no
Phone: +47 22 85 25 00

Referanser

- [1] K. S. Fuglerud et al., Universell utforming av IKT-baserte løsninger for registrering og autentisering, Norwegian Computing Center, Oslo, 2009.
- [2] Renaud, K. & Angeli, A. D., Visual passwords: cure-all or snake-oil? *Commun. ACM*, 52 (12): 135-140, 2009.
- [3] Sauer, G.; et al. Towards A Universally Usable Human Interaction Proof: Evaluation of Task Completion Strategies. 2 (4): 1-32, 2010.
- [4] J. D'Arcy, and J. Feng, "Investigating Security Related Behaviors Among Computer Users with Motor Impairments," Symposium on Usable Privacy and Security (SOUPS), 2006.
- [5] Schmidt, A., Kölbl, T., Wagner, S. & Straßmeier, W. (2004, June 28-29, 2004,). Enabling Access to Computers for People with Poor Reading Skills. 8th ERCIM Workshop on User Interfaces for All, Vienna, Austria. Springer-Verlag Berlin Heidelberg. 96–115 s.