Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Notat

# Previous and Related Research on Usability and Accessibility Issues of Personal Identification Management Systems

Note no. DART/10/2010

Authors Kristin Skeide Fuglerud, Till Halbach Røssvoll

Date October 11, 2010


**Norwegian Computing Center / Norsk Regnesentral**

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. NR's clients range from industrial over commercial to public service organizations, on both the national and international market. Our scientific and technical capabilities are further developed in cooperation with The Research Council of Norway, European Research Programmes, and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers. Please visit our website for further information.

http://nr.no

| | |
|---|---|
| Title | Review of Literature on Usability and Accessibility Issues of Personal Identification Management Systems |
| Authors | Kristin Skeide Fuglerud, Till Halbach Røssvoll |
| Quality assurance | Ivar Solheim |
| Date | 2010-10-01 |
| Publication number | DART/10/2010 |

**Abstract**

The overall objective of the e-Me project is to provide new knowledge that can significantly improve the usability and accessibility of identity management and authentication mechanisms in electronic services and social networks without compromising privacy, security, or offending legal frameworks.

This document introduces the terminology, concepts, and research issues related to usability and accessibility of identification mechanisms and related systems. In particular, this topic is placed in the context of the increasing use of social media.

| | |
|---|---|
| Keywords | Literature review, e-Inclusion, accessibility, usability, universal design, design for all, authentication, security mechanisms, identity management, IDM, IMS, disabled, impairments |
| Target group | Researchers |
| Availability | Open |
| Project | e-Me |
| Research field | e-Inclusion, Universal Design |
| Number of pages | 24 |

## Norsk Regnesentral

Norsk Regnesentral (NR) er en privat, uavhengig stiftelse som utfører oppdragsforskning for bedrifter og det offentlige i det norske og internasjonale markedet. NR ble etablert i 1952 og har kontorer i Informatikkbygningen ved Universitetet i Oslo. NR er et av Europas største miljøer innen anvendt statistikk. Det jobbes med svært mange forskjellige problemstillinger slik som estimering av torskebestanden, finansiell risiko, beskrivelse av geologien i petroleumsreservoarer og overvåking av klimaendringer. NR er også ledende i Norge innen informasjons- og kommunikasjonsteknologi på områdene sikkerhet og personvern, e-inkludering og multimedia. Problemstillinger kan være å overvåke inntrengning i datasystemer, utforming av digitale systemer for bruk av alle, integrering av datateknologi i markedsanalyser samt anvendelser av multimedia på forskjellige plattformer og ulike kanaler. NRs visjon er forskningsresultater som brukes og synes.

http://nr.no

## Sammendrag

Det overordnede målet for e-Me-prosjektet er å gi ny kunnskap som kan bedre brukervennlighet og tilgjengelighet til systemer for identifisering og håndtering av elektroniske identiteter uten å svekke personvern, sikkerhet eller krenke juridiske rammer.

Dette dokumentet introduserer begreper og forskningsproblemstillinger knyttet til brukervennlighet og tilgjengelighet av identifikasjonsmekanismer og systemer for håndtering av identiteter. Spesielt blir dette sett i sammenheng med den økende bruken av sosiale medier.

| | |
|---|---|
| Emneord | Litteratur, digital inkludering, tilgjengelighet av IKT, brukervennlighet, universell utforming, design for alle, autentisering, sikkerhetsmekanismer, identitetshåndtering, funksjonsnedsettelse, handikap |
| Målgruppe | Forskere |
| Tilgjengelighet | Offentlig |
| Prosjekt | e-Me |
| Prosjektnummer | 320457 |
| Satsningfelt | e-Inkludering, universell utforming av IKT |
| Antall sider | 24 |

# Content

# 1 Introduction

Electronic services and social networking services have been experiencing exponential growth in recent years, and there are currently no signals that this development will not continue in the years to come. As they become more and more pervasive and “mission critical” in many aspects of people's daily life, it is vital that those services are accessible to virtually all users, including persons with motor, sensor, and cognition impairments. The first step during the use of a social networking service is typically identification and authentication, which often makes a huge hinder for user in the aforementioned target groups who wish to participate in the digital life.

Some problems and aspects concerning accessibility and usability of identity management and authentication mechanisms in social networking services have been addressed by previous research. The intention of this document is to summarize existing literature and related research to draw a picture which can be used as a starting point for further research. This document introduces terminology, concepts, and research issues related to usability and accessibility of identification mechanisms and systems of identity management.

The project named e-Me provides the setting for this review: The project's overall objective is to provide new knowledge that significantly can improve the usability and accessibility of identity management and authentication mechanisms in social networking services and electronic services without compromising privacy or security, and simultaneously avoiding to offend legal frameworks.

# 2 Terminology and concepts

Here, we introduce the terminology and a few concepts that are frequently used in the subsequent Review section.

## 2.1 Human-related terms

### 2.1.1 User

A person that is using a system to gather information or to complete a particular task. In the context of social networks, a user can be member of one or several communities.

### 2.1.2 User profile

A collection of user data and related attributes such as name, address, skills, disabilities, preferences, and behavior. Can also contain data unknown to the user, like machine-generated data.

### 2.1.3 User preferences

Parameters that summarize a user's personal likings for a particular aspect in a given setting like font-size, color contrast ratio, etc. Does not necessarily correlate with a user's needs.

### 2.1.4 Impairment

A functional deficit compared to what is commonly viewed as “the norm”. Impairments are usually decomposed into one of the classifications motor, sensor, and cognition.

### 2.1.5 Target group

Group of users with one or several commonalities, such as socio-ethnic and cultural background, geographical proximity, interests, skills, knowledge, age, gender, (dis)abilities, literacy, etc. Also known as focus group.

### 2.1.6 User experience

A term for the overall impression and “feeling” a user has while using a particular service or product.

## 2.2 System-related terms

### 2.2.1 Social-networking service

Primarily Web-based service for users providing means to interact with other users. May also denote the social-networking parts of an ordinary service. Also known as social networking site.

### 2.2.2 Electronic service

An online service offered to citizens and customers of companies and organizations. Examples are tax specification, online banking, and membership management.

### 2.2.3 Web 2.0

An umbrella term to describe web services that handle user-generated content, such as social networking sites, and allow a great deal of interactivity with other users. Also refers to web applications like mail services.

### 2.2.4 User interface

Means to enable interaction of humans and machines like computers and other technical devices. Can be built as both software and hardware, such as computer peripherals.

### 2.2.5 Device

An electronic piece of hardware, also sometimes referred to as gadget, for use in daily life. The term includes TV set-top boxes, personal digital assistants, mobile phones, smartphones, and others.

## 2.3 Digital inclusion-related terms

### 2.3.1 Accessibility

In the context of ICT, accessibility describes the degree to which a solution is accessible by as many people as possible, in particular those with impairments.

### 2.3.2 Usability

Denotes the usefulness of a product or service and the ease with which people can use it.

### 2.3.3 Universal design

In the current context, refers to the design of ICT solutions such that they can be used by as many people as possible. Also known as design for all.

### 2.3.4 Assistive technology

Technology, both hardware and software, with the meaning to assist the user in order to reach a particular goal. Typically tailored to her/his special needs, such as blindness.

## 2.4 Security- and privacy-related terms

### 2.4.1 Privacy

An individual's ability to reveal themselves selectively by controlling the amount of information shared with others.

### 2.4.2 Security

In the current context, security means to protect a system or information from unauthorized access.

### 2.4.3 Risk

Generally speaking the deviation of a future result from its previously anticipated value. In this context, the danger that an unauthorized person gains access to a system or information.

### 2.4.4 IDM, IMS

Identity management refers to techniques for establishing and organizing the identity of the user in order to grant access to a particular service or data, or to authorize the execution of a certain task. Identity management systems are implementations of identity management routines. An IDM example is the management of user profiles in a social-networking site like Facebook.

### 2.4.5 User-controlled IDM

Identity management where the user defines the policy for what information about the user is revealed and when.

### 2.4.6 PIM

Personal identification mechanisms are systems providing means to determine the identity of the user. As such they are part of an IMS. An example is the login procedure for web applications like Gmail or Flickr.

### 2.4.7 Identification

The process of establishing a user's identity. See also authentication.

### 2.4.8 Digital identifier

A representation of an individuals identity in a digital context. A single user may have more than one digital identities.

### 2.4.9 Electronic identifier

See digital identifier.

### 2.4.10 Authentication

The act of confirming a person as authentic, that is, confirming that a person is the one she/he claims to be.

### 2.4.11 Login

A method used by machines to determine a user's identity. Typically involves the input of a user's credentials, such as user name and password.

### 2.4.12 Phishing

An umbrella term for methods to get hold of private information from a user, such as credentials and credit card number. Resembles the word “fishing” (of data).

## 2.5 Other technology-related terms

### 2.5.1 Multimodality

The notion of multiple paths from machines to humans and vice versa. In human-machine interaction, the term generally refers to a sense or a sensor of a human or machine.

### 2.5.2 CAPTCHA

An image-based method deployed by machines to be able to tell apart humans and other machines. Commonly used to suppress automated submissions of electronic forms. Based on the underlying assumption that a machine cannot easily establish an image's semantic.

### 2.5.3 Personalization

The act of tailoring a product or service to a particular user, i.e. a user's needs, preferences, and behavior. Typically enables a particular system feature or user interface. Is often accomplished by means of user profiles.

### 2.5.4 Profiling

The process of managing user information in so-called user profiles. See also Personalization.

### 2.5.5 Adaptation

Refers to a system's inherited property to adapt to the preferences and needs of a user by altering its user interface and underlying functionality.

### 2.5.6 OpenID

Denotes both a protocol for decentralized authentication and a digital identifier. OpenID is an open standard.

# 3 Previous and related research

We have split the literature review into several logical sections to ease the overview.

## 3.1 Electronic services & social-networking services

The use of electronic services and social-networking services is tremendously expanding. Currently, Wikipedia lists 195 social-networking services as the world's most popular ones [Wikipedia 2010], and the number of users who actively participate in such services grows fast. As an example, the social-networking service Facebook, which was launched in 2004, had more than 500 million users in July 2010, according to the service's founder [Zuckerberg 2010]. The service reaches 70% of all 15 to 29 year olds in Norway on a daily basis [Futsæter 2010]. As a result, the number of services visited by the average person also grows, even though no exact numbers to validate this claim are found in the literature.

## 3.2 Users

The group of users is very heterogeneous of nature. However, one of the few things all users have in common is that their physical and mental capabilities change over time [Hansen et al. 2008], meaning that not only disabled users will profit from accessible and usable systems but also the everyday user. Understanding the challenges of disabled users provides a clue to understanding accessibility challenges of all users in general [Halbach 2010].

The majority of users seeks to get things done with the least possible effort [Dhamija et al. 2008]. Albeit this seems to be obvious, its consequences might be severe with regard to users compromising the security mechanisms of the system in order to get things done. This supports the well known fact that the user often is the weakest element in the chain of security elements.

While users with impairments sometimes visit special forums particularly targeting those users, e.g., to exchange experiences and discuss, in most situations special-needs users may prefer not to reveal their impairment or needs to other users [Zubal-Ruggeri 2007]. This sets limits for exposing user data from user profiles, and is a strong argument for systems where the user controls what data are visible to others in what situations [Fritsch et al. 2008].

## 3.3 Accessibility

It is always a challenge to design a product or system so that all potential users are able to access it. In other words, it is of great concern not to exclude large user groups such as people with disabilities. However, it is our impression that research about how to design accessible ID-technology seems to be very limited. This is also the conclusion of Sauer et al. [2010] who reports that the number of studies regarding accessibility and security is extremely limited.

There are many indications that a great deal of IDM systems are inaccessible to many, in particular to users with disabilities and elderly [Fritsch et al. 2008, Fuglerud et al. 2008, Fuglerud et al. 2009, Hochheiser et al. 2008]. One study found that 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]. Another study involving people with poor reading and writing skills showed that passwords created by choosing several pictures in a certain order worked better and faster than the use of character-based passwords or PINs [Schmidt et al. 2004].

Authentication mechanisms which consist of so-called captcha images are a huge barrier for many vision-impaired users [Ahn et al. 2004, Jameel et al. 2007, May 2005]. Consequently, recent research deals with more accessible CAPTCHA codes. One example with picture-based CAPTCHAs is described in [Fuglerud et al. 2009]. Other promising work was done by Sauer et al. [2010] who developed a tool which combines audio and matching images, supporting both visual and audio output. This new form of CAPTCHA was preferred to previous forms of text-based CAPTCHAs when tested with five sighted and five blind users. The solution is, according to the authors, accessible for users with visual impairments, and at the same time it has the benefit of easy adaptation for different languages and cultures.

## 3.4 Usability

It is generally acknowledged that poor accessibility and usability of authentication mechanisms is a major source of flaw and risk [Adams et al. 1999, Braz et al. 2006, Dhamija et al. 2008, Halpert 2005, Jendricke et al. 2000, Whitten et al. 1998]. It is also established knowledge that any technology for secure ICT solutions is only as secure as the settings within which it is deployed [Dourish et al. 2004].

Universal design can increase the user experience concerning the use of a particular product or service considerably, meaning that a solution becomes more accessible to ideally all potential users with a different background, such as skills, knowledge, age, gender, (dis)abilities, literacy, etc. A central issue in universal design of ICT solutions is the development of flexible multimodal user interfaces that can meet a user's different needs, abilities, situations, preferences, and devices [Fuglerud 2009, Hellman 2007a, Hellman 2007b, Honkala et al. 2006, Reeves et al. 2004, Sarter 2006].

## 3.5 Privacy

For identification and authentication purposes, users sometimes have to reveal personal data such as the social security number when using electronic services. The concerns to give up information privacy here have to be weighted against the benefits of information disclosure. Often, the user makes the decision without a proper understanding of the implied consequences and possible risks [Kai-Lung et al. 2006, Schrammel 2009].

Next, most identification solutions of electronic services imply personal profiles and some degree of personalization. Profiling and adaptation both have privacy implications [Kobsa 2007] as user data can be stolen and abused, as pointed out by [Huang 2005] and [Solove 2006].

Also adaptive dynamic profiling systems introduce new privacy threats. As [Kobsa 2007] argues, profiling and personalization have privacy implications; user profiles contain sensitive information about a user’s preferences and (dis)abilities. Universally

designed systems' privacy requirements transcend normal privacy concerns, due to profiling of possible sensitive and disability-related information about the users. This could be misused, as pointed out by [Huang 2005] and [Solove 2006]. There is thus the demand for privacy-enhancing technology and privacy-preserving technologies as detailed by [Fritsch 2007]. There is current research on usable and privacy-aware applications such as [Fischer-Hübner 2009] and [Kosta 2010]; however, it appears that the universal-design aspect of many privacy-enhancing technologies has not been studied to a satisfactory extent for the time being.

## 3.6 Security

Cyber criminals are increasingly targeting social-networking sites and other Web 2.0 technologies [Krebs 2008, AFP 2010]. This is due to these services' great popularity, and because of their technical possibilities and complexity.

As mentioned before, poor accessibility and usability of IDM systems is a major source of flaw and risk. Examples are identity theft caused by the vulnerability of electronic identifiers [Levy et al. 2005], identity spam, and a plethora of other security challenges [Klingsheim et al. 2008] such as phishing. This also includes the generation of fake profiles of other people hoping that people will link with them. Such profiles are sometimes loaded with various forms of malicious software as part of a phishing attack.

Another aspect is that many people with impairments are bound to use assistive technology in addition to regular solutions in order to access a particular service such as an ATM. Such technology means additional security implications as they come with a separate set of flaws and risks. Also, malicious systems sometimes mask as assistive technology and may as such compromise authentication information and thus violate the user's security [Jaeger 2004, Hochheiser et al. 2008]. Universal design can reduce the need for assistive technology by developing a solution for a wider spectrum of target groups [Keates 2006].

## 3.7 User-controlled IDM

User-controlled identity management tools have been suggested as a response to the need to handle an ever increasing number of identities in new digital services [Camenisch et al. 2002; Jendricke et al. 2000]. However, usability experts warn about exposing the user to such highly complex systems [Fritsch et al. 2008]. The complexity is likely to confuse even users without disabilities (Pettersson et al. 2005). Therefore, user-controlled IDM cannot be recommended for deployment from a usability point of view.

## 3.8 Evaluation criteria

Service providers are in need of systems to handle digital identities. This includes identification means, also referred to as automated personal identification mechanism or APIM.

However, there are many types of APIMs and a number of different identity management systems, and it is not straight forward to decide which concept is most suitable for a given scope. According to [Palmer 2008], there is a lack of a commonly agreed upon set of factors concerning which to deploy in an evaluation of APIMs.

The work also lists over 200 possible evaluation criteria to aid the selection of the most appropriate identification mechanism for a given context. The criteria are chosen to expose strategic issues and risk management aspects that influence the objective of organizations and their policies for introducing such mechanisms. The author developed a number of criteria to acquire functional and performance requirements for the intended user community, ranging from technological efficiency to accessibility issues and usability effectiveness. They may also be used to describe the characteristics of competing solutions.

The author is unclear, however, about how to measure the criteria, and admits that some of them may require further decomposition, refinement, or re-organization, which remains for further research.

## 3.9 Registration in social-networking sites

A study examined the registration process for several social networking sites [Meiselwitz et al. 2009]. The sites were evaluated according to their compliance with Section 508 of the Rehabilitation Act. The evaluation also included the use of CAPTCHAs and the use of mail for user identification. The author found that out of 22 sites, 9 sites were marginally inaccessible, 12 were moderately inaccessible, and 1 site was substantially inaccessible. No site was completely accessible, according to the used definition of accessibility. The author refers to common web development tools to improve the situation.

## 3.10 Decentralized IDM

Decentralized identity management has been suggested as a solution to the problem of having one account (typically comprising user name and password) for a multitude of sites requiring a login. Examples are Oasis WS-Federation, OpenID, Liberty Alliance's Security Assertion Markup Language, Microsoft's Cardspace, and the Higgins Project. However, as [Dhamija et al. 2008] pointed out, these techniques increase the cognitive burden on the user and introduce a couple of concepts a user may not be familiar with, such as web addresses or URIs.

## 3.11 Open vs. closed systems

In contrast to closed identity management systems that are based on proprietary solutions, open systems like OpenID aim at providing more transparency to the user and thereby increase a user's trust. [Vanderheiden 2007] discusses accessibility aspects of this and concludes that "[...] the trend toward closed systems, for digital rights management or security reasons, is preventing individuals from adapting devices to make them accessible, or from attaching assistive technology so they can access the devices", advocating the deployment of open systems.

## 3.12 Need for security education and awareness amongst users

The need for educating users is a common thread in usable security research [Raja et al. 2009]. Even for IT security practitioners and other experts, it turns out that access control and other security tasks often are secondary, performed irregularly, and without necessarily proper training [Botta et al. 2007].

Dourish et al. [2004] advocate for making security technologies "highly visible" so the user can always inspect and understand the current security configuration.

Other studies have shown that users have a very limited understanding of risk and security features of technology. [Dhamija et al. 2006] showed that 23% of the participants in their lab study concerning phishing web sites did not pay attention to indicators such as the address bar or the security padlock when evaluating the legitimacy of a site. The participants only looked at the content of the web page to evaluate site authenticity. Moreover, Wu et al. [2006] found that users did not understand anti-phishing toolbars, i.e. tools which visually indicate that a site might not be legitimate.

[Strater et al. 2008] found that the users' expectations of the outcome of their privacy settings did not match what actually happened, which is likely to result in accidental information disclosure. As users continue to download new applications in their digital habitats of social networks, join new networks, or disclose new information, they rarely revisit their privacy settings to ensure that their configurations appropriately cover their growing profile [Strater et al. 2008].

Helkala [2010] has studied how to rank and strengthen methodologies for user-generated passwords by educating users in generating stronger passwords. The education had a very strong positive effect directly after the training. However, the training's effect vanished in time if the users were not reminded of how to generate good passwords. The author concludes that users continually need reminders, and she suggests that a system for tutoring and evaluation should be implemented in systems using password authentication.

Studies such as those referred to above suggest that security and privacy features are often misunderstood by users. Probably, a combination of more usable and accessible user interfaces together with accessible and interactive education of the users is needed.

# 4 Other literature

The work by [Palmer 2008] gives a very good overview of literature concerning research dealing with issues regarding usability aspects of security and privacy matters of ICT solutions.

# 5 Conclusion

This literature review has shed light on previous and related research given the topic usability and accessibility of identity management systems as defined by the superordinated e-Me project. The work can be used as a starting point in the quest to significantly improve usability and accessibility of ICT solutions that require identity management without compromising privacy, security, or offending legal frameworks. In particular, the work is placed in the context of the increasing use of social-networking services.

After the definition of terminology and the introduction of concepts, we review a number of publications based on a classification into various subtopics.

In the literature, poor accessibility and usability of identification management solutions has been identified as a major culprit for system flaws and security risks. Universally designed products and services have been proposed to remedy or at least reduce the extent of the problem. The system development should incorporate the development of flexible and personalized multimodal user interfaces. The privacy issues encountered with user profiling should be solved by applying privacy-enhancing technology while simultaneously maintaining good accessibility and usability.

The list of references includes a number of additional publications to complete the overview of research in this area.

# 6 Abbreviations

| | |
|---|---|
| APIM | automatic personal information mechanism |
| ATM | automated teller machine |
| CAPTCHA | completely automated public Turing test to tell computers and humans apart |
| DART | Department of Applied Research in Information Technology |
| ICT | information and communication technology |
| IDM | identity management |
| IIDM | inclusive identity management |
| IKT | informasjons- og kommunikasjonsteknologi |
| IMS | identity management system |
| IT | information technology |
| NR | Norsk Regnesentral |
| PET | privacy-enhancing technology |
| PIM | personal information mechanism |
| PIN | personal identification number |
| URI | uniform resource identifier |

# 7 References

The following list of references compounds all aforementioned citations and

additionally a number of other references for completion purposes.

J. L. Abad, P. Steiger, and P. Steiger, “Making electronic commerce easier to use with novel user interfaces,” Electronic Markets, vol. 8, no. 3, pp. 8-12, 1998.

A. Acquisti, “Identity Management, Privacy, and Price Discrimination,” vol. 6, no. 2, pp. 46-50, 2008.

A. Adams, and M. A. Sasse, “Users are not the enemy: Why users compromize computer security mechanisms and how to take remedial measure.,” Commun. ACM, vol. 42, no. 12, pp. 41-46, 1999.

AFP, “Cyber Criminals Target Social Networks”, Discovery News, accessed Oct. 2010, http://news.discovery.com/tech/cyber-criminals-social-networks.html

P. L. Agostini, and R. Naggi, "Selecting Proper Authentication Mechanisms in Electronic Identity Management (EIDM): Open Issues," Interdisciplinary Aspects of Information Systems Studies, pp. 391-397, 2008.

R. J. Anderson, Security in Clinical Information Systems, 1996.

A. Ansper, S. Heiberg, H. Lipmaa et al., "Security and Trust for the Norwegian E-Voting Pilot Project E-valg 2011," Identity and Privacy in the Internet Age, pp. 207-222, 2009.

A. I. Anton, J. B. Earp, and J. D. Young, “How Internet Users' Privacy Concerns Have Evolved since 2002,” Security & Privacy, IEEE, vol. 8, no. 1, pp. 21-27, 2010.

R. Ariel, “Personal knowledge questions for fallback authentication: security questions in the era of Facebook,” in Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2008.

E.-A. Baatarjav, R. Dantu, and S. Phithakkitnukoon, “Privacy Management for Facebook,” in Proceedings of the 4th International Conference on Information Systems Security, Hyderabad, India, 2008.

S. Balasubramaniam, G. A. Lewis, E. Morris et al., "Identity management and its impact on federation in a system-of-systems context." pp. 179-182.

S. Balfe, E. Gallery, C. J. Mitchell et al., “Challenges for Trusted Computing,” Security & Privacy, IEEE, vol. 6, no. 6, pp. 60-66, 2008.

L. Bauer, L. F. Cranor, M. K. Reiter et al., “Lessons learned from the deployment of a smartphone-based access-control system,” in Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2007.

R. Bernard, “Information Lifecycle Security Risk Assessment: A tool for closing security gaps,” Computers & Security, vol. 26, no. 1, pp. 26-30, 2007.

R. Borrino, M. Furini, and M. Roccetti, “Augmenting social media accessibility,” in Proceedings of the 2009 International Cross-Disciplinary Conference on Web

Accessibililty (W4A), Madrid, Spain, 2009.

D. Botta, R. Werlinger, A. Gagne, K. Beznosov, L. Iverson, S. Fels, B. Fisher, “Towards Understanding IT Security Professionals and Their Tools” Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

S. Bratus, C. Masone, and S. W. Smith, “Why Do Street-Smart People Do Stupid Things Online?,” Security & Privacy, IEEE, vol. 6, no. 3, pp. 71-74, 2008.

C. Braz, and J.-M. Robert, “Security and usability: the case of the user authentication methods,” in Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine, Montreal, Canada, 2006.

C. Braz, A. Seffah, and D. M’Raihi, "Designing a Trade-Off Between Usability and Security: A Metrics Based-Model," Human-Computer Interaction – INTERACT 2007, pp. 114-126, 2009.

G. Conti, and E. Sobiesk, “Malicious Interfaces and Personalization's Uninviting Future,” Security & Privacy, IEEE, vol. 7, no. 3, pp. 64-67, 2009.

H. Cormac, “So long, and no thanks for the externalities: the rational rejection of security advice by users,” in Proceedings of the 2009 workshop on New security paradigms workshop, Oxford, United Kingdom, 2009.

L. F. Cranor and S. Garfinkel, Security and Usability: Designing secure systems that people can use.: O'Reilly, 2005.

J. D'Arcy and J. Feng, “Investigating Security-Related Behaviors Among Computer Users With Motor Impairments”, Symposium on Usable Privacy and Security (SOUPS) 2006

R. Dhamija, J.D. Tygar, M. Hearst, “Why phishing works”, CHI 2006, April 2006, Montréal, Québec, Canada

R. Dhamija, and L. Dusseault, “The Seven Flaws of Identity Management: Usability and Security Challenges,” Security & Privacy, IEEE, vol. 6, no. 2, pp. 24-29, 2008.

G. Dhillon, “Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns,” Computers & Security, vol. 20, no. 2, pp. 165-172, 2001.

P. Dourish, E. Grinter, J. D. d. l. Flor et al., "Security in the wild: user strategies for managing security as an everyday, practical problem," Pers Ubiquit Comput vol. 8, Springer-Verlag, 2004, pp. 391-401.

S. Egelman, J. King, R. C. Miller et al., “Security user studies: methodologies and best practices,” in CHI '07 extended abstracts on Human factors in computing systems, San Jose, CA, USA, 2007.

Fidis, FIDIS Deliverable D7.2: Descriptive analysis and inventory of profiling practices,

2005.

S. Fischer-Hübner, Christina Köffel, Erik Wästlund et al. “HCI Research Report - Version 1”, PrimeLife Project, Feb. 2009, http://www.primelife.eu

I. Flechais, C. Mascolo, and M. A. Sasse, "Integrating security and usability into the requirements and design process," 1, Inderscience Publishers, 2007, pp. 12-26.

I. Flechais, and M. A. Sasse, “Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science,” International Journal of Human-Computer Studies, vol. 67, no. 4, pp. 281-296, 2009.

L. Fritsch, “State of the art of Privacy-enhancing Technology (PET)”, Technical Report D2.1 of the PETweb project, Nov. 2007, http://publ.nr.no/4589

L. Fritsch, K. S. Fuglerud, and I. Solheim, “Towards inclusive identity management,” in Identity in the Information Society Workshop, Arona, Italy, 2008.

K. S. Fuglerud, A. Reinertsen, L. Fritsch et al., “Universal design of IT-based solutions for registration and authentication”, Norwegian Computing Center, Oslo, 2009.

S. Furnell, “Why users cannot use security,” Computers & Security, vol. 24, no. 4, pp. 274-279, 2005.

S. Furnell, “Making security usable: Are things improving?,” Computers & Security, vol. 26, no. 6, pp. 434-443, 2007.

S. Furnell, V. Tsaganidi, and A. Phippen, “Security beliefs and barriers for novice Internet users,” Computers & Security, vol. 27, no. 7-8, pp. 235-240, 2008.

S. M. Furnell, “Using security: Easier said than done?,” Computer Fraud & Security, vol. 2004, no. 4, pp. 6-10, 2004.

S. M. Furnell, A. Jusoh, and D. Katsabas, “The challenges of understanding and using security: A survey of end-users,” Computers & Security, vol. 25, no. 1, pp. 27-35, 2006.

Knut-Arne Futsæter, “Media trends and use of SNR in Norway”, presentation, April 2010, http://www.intermedia.uio.no/mediatized

L. F. C. S. Garfinkel, Security and Usability: Designing secure systems that people can use.: O'Reilly, 2005.

S. Gaw, and E. W. Felten, “Password management strategies for online accounts,” in Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

J. Gilbert, Y. McMillian, K. Rouse et al., “Universal access in e-voting for the blind,” Universal Access in the Information Society, 2010.

J. Goecks, W. K. Edwards, and E. D. Mynatt, “Challenges in supporting end-user privacy and security management with social navigation,” in Proceedings of the 5th

Symposium on Usable Privacy and Security, Mountain View, California, 2009.

J. B. Gross, and M. B. Rosson, “Looking for trouble: understanding end-user security management,” in Proceedings of the 2007 symposium on Computer human interaction for the management of information technology, Cambridge, Massachusetts, 2007.

J. Hagen, “Human Relationships: A Never-Ending Security Education Challenge?,” Security & Privacy, IEEE, vol. 7, no. 4, pp. 65-67, 2009.

T. Halbach, “Towards Cognitively Accessible Web Pages”, International Conference on Advances in Computer-Human Interactions , St. Maarten, Netherlands Antilles, Feb. 2010

B. J. Halpert, "Authentication Interface Evaluation and Design for Mobile Devices."

K. Han-Gyu, K. Seung-Hyun, and J. Seung-Hun, "Usability Enhanced Privacy Protection System Based on Users' Responses." pp. 1-6.

M. Hansen, A. Pfitzmann, and S. Steinbrecher, Identity Management throughout one's whole life, 2008.

K.M. Helkala, “Authentication in Health Services”, PhD thesis, University of Oslo, Norway, Aug. 2010

H. Hochheiser, J. Feng, and J. Lazar, “Challenges in Universally Usable Privacy and Security,” in Symposium On Usable Privacy and Security (SOUPS) 2008, Pittsburgh, PA, USA, 2008.

S. Hosio, H. Kukka, and J. Riekki, “Leveraging social networking services to encourage interaction in public spaces,” in Proceedings of the 7th International Conference on Mobile and Ubiquitous Multimedia, Umeå, Sweden, 2008.

H. Jameel, Taxonomy of Human Identification Protocols, U-security Research Group, Ubiquitous Computing Laboratory, Kyung Hee University, Korea, 2007.

U. Jendricke, and D. Gerd tom Markotten, “Usability meets security - The Identity-Manager as your Personal Security Assistant for the Internet,” Proceedings of the 16th Annual Computer Security Applications Conference, 2000.

J. Johnston, J. H. P. Eloff, and L. Labuschagne, “Security and human computer interfaces,” Computers & Security, vol. 22, no. 8, pp. 675-684, 2003.

Simeon Keates, “Design for Accessibility. A Business Guide to Countering Design Exclusion”, CRC press, 2006

J. King, and A. McDiarmid, “Where's the beep?: security, privacy, and user misunderstandings of RFID,” in Proceedings of the 1st Conference on Usability, Psychology, and Security, San Francisco, California, 2008.

A. Kobsa, "Tailoring Privacy to Users’ Needs," User Modeling 2001, Lecture Notes in

Computer Science, pp. 301-313: Springer Berlin / Heidelberg, 2001.

T. Koelsch, L. Fritsch, M. Kohlweiss et al., "Privacy for Profitable Location Based Services," pp. 164-179, Boppard: Springer, 2005.

E. Kosta, “D8.1 Legal, economic and technical evaluation of the first platform and community prototype”, Picos Project, Apr. 2010, http://picos-project.eu

H. Krasnova, O. Günther, S. Spiekermann et al., “Privacy concerns and identity in online social networks,” Identity in the Information Society, vol. 2, no. 1, pp. 39-63, 2009.

B. Krebs, “Hackers' Latest Target: Social Networking Sites”, The Washington Post, Aug. 9, 2008, accessed Oct. 2010, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html

J. Krumm, “A survey of computational location privacy,” Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

M. Levi, and D. S. Wall, “Technologies, Security, and Privacy in the Post-9/11 European Information Society,” Journal of Law and Society, vol. 31, pp. 194-220, 2004.

G. L. Lohse, and P. Spiller, “Electronic Shopping: Designing online stores with effective customer interfaces has a critical influence on traffic and sales.,” Communications of the ACM, vol. 41, no. 7, pp. 81-88, 1998.

M. Mahemoff, A. Hussey, and L. Johnston, "Pattern-based Reuse of Successful Desigs: Usability of Safety-Critical Systems."

B. Matt, and A. F. Deborah, “Achieving Learning Objectives through E-Voting Case Studies,” Security & Privacy, IEEE, vol. 5, no. 1, pp. 53-56, 2007.

A. Mauren, "Hackere kan bruke kamera-info til ran," Aftenposten, 2002, p. 3.

G. Meiselwitz and J. Lazar, “Accessibility of Registration Mechanisms in Social Networking Sites ”, Online Communities, LNCS 5621, pp. 82–90, Springer, 2009

G. Müller, and K. Rannenberg, Multilateral Security in Communications, München: Addison-Wesley-Longman. ISBN 3-8273-1360-0., 1999.

T. Nabeth, “Social web and identity: a likely encounter,” Identity in the Information Society, vol. 2, no. 1, pp. 1-5, 2009.

C. A. Neff, “A verifiable secret shuffle and its application to e-voting,” in Proceedings of the 8th ACM conference on Computer and Communications Security, Philadelphia, PA, USA, 2001.

A. Newell, and S. H. A., Human problem solving, Carnegie-Mellon University, Pittsburgh, PA: Englewood Cliffs, NJ: Prentice-Hall, 1972.

J. Nielsen. "Personalization is Over-Rated," 05. February, 2001; http://www.useit.com/alertbox/981004.html.

J. Nielsen. "Security & Human Factors," 27.11.2000, 2000; http://www.useit.com/alertbox/20001126.html.

J. S. Olson, J. Grudin, and E. Horvitz, “A study of preferences for sharing and privacy,” in CHI '05 extended abstracts on Human factors in computing systems, Portland, OR, USA, 2005.

A. J. Palmer, “Criteria to evaluate Automated Personal Identification Mechanisms,” Computers & Security, vol. 27, no. 7-8, pp. 260-284, March 2008, 2008.

J. Peeters, and P. Dyson, “Cost-Effective Security,” Security & Privacy, IEEE, vol. 5, no. 3, pp. 85-87, 2007.

J. S. Pettersson, S. Fischer-Hübner, N. Danielsson et al., “Making PRIME usable,” in Proceedings of the 2005 symposium on usable privacy and security, Pittsburgh, Pennsylvania, 2005.

K. Poulsen, “Hackers Assault Epilepsy Patients via Computer,” WIRED News, 28. Mars, 2008.

F. Raja, K. Hawkey, and K. Beznosov, “Revealing hidden context: improving mental models of personal firewall users,” in Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, California, 2009.

M. Reichenbach, H. Damker, H. Federrath et al., "Individual Management of Personal Reachability in Mobile Communication." pp. 164-174.

S. Rieger, and B. Neumair, "Towards usable and reasonable Identity Management in heterogeneous IT infrastructures." pp. 560-574.

RSA, "Enterprise single sign-on solutions reduce IT helpdesk calls but raise concern amongst security experts, reveals RSA Security," Press Releases, new & Events, [2008-08-25, 2006].

G. Sauer, J.Holman, J. Lazar , H. Hochheiser, J. Feng , “Accessible privacy and security: a universally usable human-interaction proof tool ”, Univ Access Inf Soc (2010) 9:239–248, Springer

A. Schmidt, T. Kölbl, S. Wagner, and W. Straßmeier, “Enabling Access to Computers for People with Poor Reading Skills”, UI4All, LNCS 3196, pp. 96–115, Springer 2004

H. Schmidt, and I. Wentzlaff, "Preserving Software Quality Characteristics from Requirements Analysis to Architectural Design," Software Architecture, pp. 189-203, 2006.

G. Schryen, and E. Rich, "Security in large-scale internet elections: a retrospective analysis of elections in Estonia, the Netherlands, and Switzerland," 4, IEEE Press,

2009, pp. 729-744.

A. Sears, J. Lazar, A. Ozok et al., "Human-Centered Computing: Defining a Research Agenda," 1, Taylor & Francis, 2008, pp. 2 - 16.

R. Sekar, A. Pujari, E.-A. Baatarjav et al., "Privacy Management for Facebook," Information Systems Security, Lecture Notes in Computer Science, pp. 273-286: Springer Berlin / Heidelberg, 2008.

A. Shah, A. Farooq, and K. Talib, "User-oriented identity management model for web-services." pp. 1-8.

P. B. v. Solms, “Corporate Governance and Information Security,” Computers & Security, vol. 20, no. 3, pp. 215-218, 2001.

K. Strater and H. Richter Lipford, “Strategies and Struggles with Privacy in an Online Social Networking Community”, in Proceedings of HCI, Liverpool (UK.), Sep. 2008

F. Tari, A. A. Ozok, and S. H. Holden, “A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords,” in Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA., 2006.

I. Tjøstheim, K. S. Fuglerud, K. Boge et al., Online-consumers and privacy - a national study of what the e-consumers are willing to share of personal information, NR report Report no. 979, Norwegian Computing Center, Oslo, 2001.

U. Topkara, M. Topkara, and M. J. Atallah, “Passwords for everyone: secure mnemonic-based accessible authentication,” in 2007 USENIX Annual Technical Conference on Proceedings of the USENIX Annual Technical Conference, Santa Clara, CA, 2007.

D. Trepess, and T. Stockman, “A classification and analysis of erronoeous actions in computer supported co-operative work environment,” Interacting with Computers, no. 11, pp. 611-622, 1999.

D. van Rooy, and J. Bus, “Trust and privacy in the future internet—a research perspective,” Identity in the Information Society, vol. 3, no. 2, pp. 397-404, 2010.

G. Vanderheiden, “Fundamental Principles and Priority Setting for Universal Usability ”, Proceedings of the Conference on Universal Usability (CUU), Nov. 2000

J. Viega, and B. Michael, “Guest Editors' Introduction: Mobile Device Security,” IEEE Security and Privacy,, no. March/April, pp. 11-12, 2010.

S. Viller, J. Bowers, and T. Rodden, “Human factors in requirements engineering: A survey of human sciences literature relevant to the improvement of dependable systems development processes,” Interacting with Computers, vol. 11, no. 6, pp. 665-698, 1999.

L. von Ahn, M. Blum, and J. Langford, “Telling humans and computers apart

automatically", Communications of the ACM, Feb. 2004/Vol. 47, No. 2, pp. 57-60

P. Wauters, and P. V. Durme, Online availability of public services: How is Europe progressing?, Prepared by: Capgemini For: European Commission Directorate General for Information Society and Media,, 2005.

C. S. Weir, G. Douglas, M. Carruthers et al., "User perceptions of security, convenience and usability for ebanking authentication tokens," Computers & Security, vol. In Press, Corrected Proof, 2007.

A. Whitten, and J. D. Tygar, Usability of Security: A case study, CMU-CS-98-155, Carnegie Melon University, Pittsburgh, PA 15213, USA, 1998.

A. Whitten, and J. D. Tygar, "Why Johnny can't encrypt: a usability evaluation of PGP 5.0," in Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, Washington, D.C., 1999.

Wikipedia, "List of social networking websites", accessed Oct. 2010, http://en.wikipedia.org/wiki/List_of_social_networking_websites

WSC. "Web Security Context Working Group home page," 14. Dec., 2009; http://www.w3.org/2006/WSC/.

M. Wu, C. M. Robert, and G. Little, "Web wallet: preventing phishing attacks by revealing user intentions," in Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2006.

M. E. Zurko, and K. Johar, "Standards, Usable Security, and Accessibility: Can we constrain the problem any further?," in Symposium On Usable Privacy and Security (SOUPS) 2008, Pittsburgh, PA, USA, 2008.

R. Zubal-Ruggeri, "Making Links, Making Connections, Internet Resources for Self-Advocates and People With Developmental Disabilities", Intellectual and developmental disabilities, 45 (3): 209-215. June 2007.

M. Zuckerberg, "500 Million Stories", accessed Oct. 2010, http://blog.facebook.com/blog.php?post=409753352130