The final version was published in: M. Leitner and A. Bonitz, "Authentication in the Context of E-Participation: Current Practice, Challenges and Recommendations," 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 2016, pp. 480-485. doi:10.1109/ARES.2016.82

Authentication in the Context of E-participation: Current Practice, Challenges and Recommendations

Maria Leitner and Arndt Bonitz

AIT Austrian Institute of Technology
Digital Safety & Security Department
firstname.lastname@ait.ac.at

Abstract—**Authentication as well as identification are key functions when it comes to online and democratic participatory processes that can be found in the context of e-participation. Until now, research has centered on the development of authentication and identification techniques. Why and how these techniques are currently used and what their benefits are in the context of e-participation is missing so far. In this paper, we aim to address these challenges by reviewing state of the art literature and practice in order to determine how current authentication techniques are used in e-participation. Furthermore, we conduct an expert survey in order to establish a baseline how current techniques are used and perceived. The results show that current practice focuses strongly on the use of the de facto standard user/password in e-participation. However, experts believe that multiple other authentication techniques such as biometrics or electronic signatures will become more important in future applications. Moreover, experts acknowledge the use of various authentication methods suitable for the level of participation, as opposed to current practice that often provides only one way of authentication. These findings will help to further develop and improve future technologies and applications to support participatory processes for citizens' involvement.**

Keywords–authentication; e-participation; electronic identities; security; survey.

I. Introduction

Electronic participation is the implementation of participatory processes for citizen involvement using electronic media (see [1], [2]). The engagement of citizens can be further categorized into levels of participation. For example in [3], the levels information, consultation (e.g., one- or two-way communication), co-operation (i.e. prepare results in a collaborative way) and co-decision (i.e. to vote on results or implementations) are specified. Information and communication technologies (ICT) are a key factor when it comes provide and support these levels adequately. In fact, security measures such as authentication and identification can vary between different levels of e-participation (cmp. [4], [5]).

ICT provide the use of digital identities in order to provide assurance, traceability, and non-repudiation and to prevent misuse. *Digital identity* (also called electronic identity (eID)) is defined as a set of data that uniquely describes a person, an organization, or a thing (usually referred as a subject or entity) and contains information about the subject's relationships to other entities in cyberspace [6]. The information about the subject is called attributes, including characteristics such as nationality, data of birth, height and so on. Attributes can be temporary (e.g. address, employer), long-term (e.g. a social security or passport number), and persistent (e.g. fingerprints and eye colour). Digital identities have been invented to solve three difficult problems in cyberspace, i.e. authentication, identification, and access. (1) **Identification** is the process of claiming an identity. For example, in order to login to a website one has to fill in a username (e.g., "user100"). (2) **Authentication** is the process of confirming an identity. In the example, to confirm that one is "user100" one has to type in a correct password. Identification is often a necessary element of transactions-driven domains such as e-government and e-commerce. (3) **Access** is the ability to permit or deny use to a certain resource (e.g., website, app). Identification requires authentication of identity; access to computer resources must be preceded by authentication.

The existence of eID benefits most of us in society: individuals can conduct their personal business and access services (e.g., e-government, e-commerce, e-banking, e-participation) online with less time and effort. Electronic identities can have different levels of quality and differ for example in levels of assurance (e.g., low assurance identities that can be created within seconds and have no verification if the person really exists (e.g., social network identities) or high assurance identities that can be issued by local authorities such as the Austrian Citizen Card).

In e-participation and e-government, eIDs are highly important to provide transactions that require a strong identity link. Research has specified various authentication techniques that can be used to confirm an identity. For example, a set of authentication techniques such as biometrics, one time password, electronic signatures; an overview can be found in [7]. What is missing so far is a comprehensive analysis which authentication techniques are actually used and could be used in the context of e-participation. Furthermore, we aim to investigate how technologies could be used in future application e-participation scenarios. In particular, we conduct a literature analysis in order to evaluate current state of the art and a short qualitative analysis of current technology used in selected e-participation examples. Lastly, an expert survey is performed to further determine current practice and future usage scenarios. This will help to identify current benefits of authentication techniques and further develop and improve future technologies and applications.

The rest of this paper is structured as follows: Section II summarizes the methodology used in this paper. Furthermore, Section III provides a literature analysis of current authentication techniques. Section IV analyzes selected examples and how they use authentication techniques. Section V lists the procedure and results of the expert survey. Lastly, Section VI summarizes the main findings and provides recommendations for future use.

II. Methodology

This paper aims to analyze current use and practice of identification methods in e-participation. Furthermore, its goal is to identify challenges for further research. To tackle this, we performed several steps: First of all, we provide a **literature review** on current state of the art of authentication methods. Therefore, we analyze current techniques and identify threats and challenges in the context of e-participation. Secondly, we perform a **short qualitative analysis** to identify the use and practice of authentication methods and related aspects in e-participation projects. In particular, we analyzed the offered use of electronic identities as well as the applied data protection and security features. Furthermore, we perform an **expert survey** in order to identify how identification methods could be used in e-participation settings and to evaluate future applications.

RQ1 How and why are identification methods in e-participation relevant?

RQ2 Which identification methods (and technologies) are commonly used in e-participation?

RQ3 Which identification methods could be used in future in e-participation?

III. Review of Authentication Techniques

According to [8] authentication techniques can be classified into:

- Token-based authentication (what you have) includes physical tokens such as smart cards, RFID chips or ATM cards.
- Knowledge-based authentication (what you know) contains specific information or knowledge possessed by the individual (e.g., password, pin code).
- Inherence-based authentication (what you are) centers on intrinsic properties of individuals (e.g., fingerprint, face, iris, voice).

Secure authentication can be a key factor for the use and trust of e-participation platforms. These authentication techniques provide the basis to confirm identities. In the following, we will revise current authentication techniques that can be used for e-participation. The categorization is based on an ENISA report on electronic identity authentication methods in the e-payment and e-finance services [7]. We chose this report as it provides a comprehensive overview of authentication mechanisms for the finance sector. Also, in e-participation, we aim for achieving a secure and trusted authentication as this is already established in the e-finance or e-commerce sector.

A. Login with password or PIN

The usage of a password or PIN is one of the most common authentication techniques. It requires an identifier (such as a username) and a secret pass-phrase (e.g., password or PIN). The drawbacks of passwords is that often humans use standard passwords (e.g., “1234567” or “password”) that make it easily crackable. However, further techniques exist to increase usability and use graphical passwords (e.g., [9], [10]).

B. Biometrics

This technique uses biometric features of the human body or the behavior for authentication [11].

- **Body biometrics**: Body features such as the fingerprint, voice, facial, or hand recognition can be used for authentication (e.g., [12]).
- **Behavior biometrics**: Another biometric authentication analyzes how the user behaves with a computer using for example keystroke dynamics or handwritten signature analysis.

The threats to biometrics are impersonation (i.e. attacker steals biometric information and constructs artificial biometric features), irrevokability (i.e. once compromised they cannot be updated or reissued) and exposure of sensitive personal information [13] e.g., health issues or pregnancy. To the best of our knowledge, we did not discover any biometric authentication in previous and current e-participation projects in literature and the web.

C. One Time Password

One Time Password (OTP) uses a secret pass-phrase to generate a random, different passwords that is valid for single use only (e.g., in a session or for a transaction) (see e.g., [14], [15]). OTP implementations can generate e.g., time-based or event-based OTPs (e.g., [16]). Static OTP approaches are typically based on TAN code lists. Dynamic OTP approaches typically consists of a token - either hardware-based (e.g., small OTP device) or software-based (e.g., located in the mobile phone). The token can generate an OTP using a secret key and a counter (or clock). In the following, selected OTP approaches are shortly outlined:

- **TAN code list**: Static OTP generation provides a list of OTPs that is sent by post office. A user can insert a TAN for one transaction in a web application.
- **SMS-based OTP**: The generated OTP is sent via SMS to an end users’ mobile phone that is registered at the authentication service. This is commonly used by e-banking services.
- **Hardware-based OTP**: A hardware device generates an OTP each time the user requests it.
- **Software-based OTP**: A software generates the OTP upon request for the user. The software can be installed on mobile phones (i.e. mobile OTP applications), personal computers or other devices (e.g., tablets).

OTPs is commonly used for two-factor identification (e.g., e-banking). There are various threats to different OTP approaches. For example, using a mobile OTP application can be circumvented by stealth attacks that leak information to attackers [17] or taking screenshots from the application displaying the OTP [18]. While hardware-based OTP approaches can diminish several risks that mobile-based approaches come with, they have also limitations. For example, they are more cost-intensive than software-based solutions and software on the physical devices is difficult to upgrade.

D. E-signature Certificate

In this authentication technique, end users are authenticated by electronic signatures. Each user has a private key that can be used to sign e.g., a transaction or a document. The private key can be stored on local hard drives (e.g., computers) or on other devices (e.g., USB stick, memory card, chip card, smart card, or mobile phone).

E. Device Authentication

The authentication process is safeguarded by registering the device that the user uses to access the e.g., web application. Therefore, the device name and e.g., device ID (e.g., MAC or IMEI) or IP address are stored to identify the device. Furthermore, mobile applications can be specifically developed for mobile customers (users) to access certain services. With device authentication, policies and guidelines have to be developed to ensure authentication only to users; also in the case of device theft, device change (e.g., upgrade) or loss.

IV. Authentication in E-Participation

This section examines the authentication technology use in selected e-participation projects.

1) Approach: We aimed to included only participation projects that contained an electronic exchange (e.g., web platforms). During our first search, we discovered that participation projects are often scattered over the web. There is no portal that summarizes or points out different participation procedures at national or EU-wide level (see e.g., [19]). That's why we decided to focus on regional participation procedures at first and will expand this investigation to international procedures as future work. Note that an extensive (multinational) analysis in [19] showed in similar results as the one in this paper.

As a first step, we've selected only projects located in the city of Vienna, Austria. In particular, we searched by using keywords (e.g., *E-Partizipation, Beteiligung, Wien, E-participation, Vienna*) to discover projects. In total, we've selected 5 regional projects in Vienna.

2) Analysis: In the following, we summarize the findings of the analysis.

The analysis shows that authentication is conducted using a local database with usernames and passwords; only one project uses no authentication at all. This is not surprising as some of the identification methods (e.g., biometry, device authentication or OTP) require more resources for the actual operation. For example, device authentication requires the purchase of hardware devices or biometrics often require a maintained database (e.g., fingerprints or portraits). Compared to these methods, the implementation of a login with passwords or PINs is rather facile. Even more, social networking sites such as Facebook, Google or Twitter provide application programming interfaces (APIs) that simplify the integration of these logins into websites.

Table I summarizes the social ID providers used in the selected projects. Many projects provide their own user database (referred to as "local database" in the second column of Table I). In addition, they support the use of various social identity providers.

TABLE I: Use of social IDs

No.	*Local database*	*Facebook*	*Google+*	*OpenID*
1	□	□	□	□
2	☒	☒	☒	□
3	☒	☒	□	☒ Yahoo, Google, AOL
4	☒	□	□	□
5	☒	☒	□	☒ Yahoo, Google, AOL

The top 5 of preferred digital channels in Austria[1] are Facebook, WhatsApp, YouTube, Google+ and Skype. Table I displays that the projects use social IDs that are frequently used.

Interpretation: The analysis shows that the e-participation examples focus on authentication with password. In addition, they provide optionally the use of social IDs in lieu of registering a local username. We believe that operators of e-participation should continue to provide various, adequate eIDs for their users in order to minimize the barrier of entry.

Furthermore, these projects aiming mostly at engaging citizens into participatory processes often depend on "free" (i.e. low-cost) alternatives such as pages at social networks or others. Choosing a third party provider might entail also acknowledging its privacy and data policies that might not align with national law. These solutions mostly use a single authentication method and are usually not offering additional authentication methods.

In the next section, we will further investigate these results with an expert survey to further identify possible challenges and drawbacks of authentication techniques in the context of e-participation.

V. Expert Survey

An online expert survey (see e.g., [20]) was used to complement the analysis to address research questions RQ2 and RQ3 (see Section II). The aim of the expert survey was to gain further insights into current practice in e-participation, to confirm typical authentication methods and to identify challenges and obstacles of authentication techniques in e-participation.

A. Procedure

The survey was distributed by email to experts in the area of e-government, e-participation, data protection and ICT security. In total, 17 people participated in the survey.

B. Results

The results of the survey are described in the following sections.

[1] See TNS Infratest, Digitales Österreich, URL: http://www.tns-infratest.com/presse/presseinformation.asp?prID=3458&titel=Digitales%20%C3%96sterreich

1) Secure authentication: The survey included the question “Which identification method would you categorize as secure?”. The experts answered in various ways. For example, several experts (7) categorized password/PIN as less secure (see Figure 1). On the other hand, experts weighted biometrics, OTP and electronic signatures as more secure.

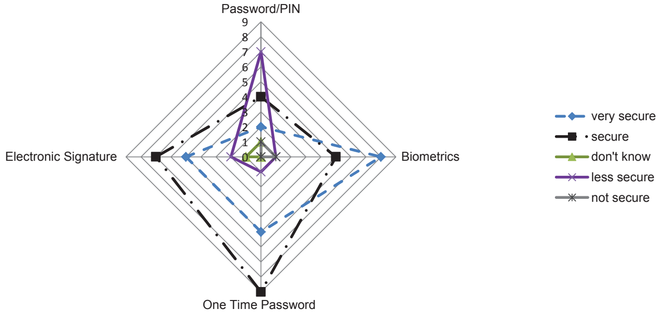

Figure 1: Results on secure authentication

Interpretation: The results indicate that experts valued the security of unique features such as can be found in biometric features or OTP (as the passphrase has an expiry date) as more secure than using passwords/PIN. We expect that this is due to mismanagement of users (e.g., lack of updating, creating easy passwords).

2) Registering an electronic identity: Figure 2 lists the results on the time to register an eID (specified by experts). It can be seen from the figure that username/password, social IDs and OTPs can be registered within two hours. On the other hand, state-based eIDs such as the Austrian Citizen Card can only be registered in one or more weeks. Experts had different opinions on biometric eIDs and have selected answers between less than 6 hours or more than one day.

Interpretation: We have obtained consistent results for the eIDs of local databases and social networks. However, we found diverse results for biometric eIDs and state-based eIDs. One of the reasons could be that we did only specify a category but not clearly which specific eIDs; i.e. experts could therefore categorize different eIDs having different requirements for the setup.

3) Use of authentication techniques in e-participation and other application domains: In order to evaluate how current techniques are used in practice, we asked the experts to define which techniques are currently used in which domains. The main findings are described in the following:

- Password/PIN is the de facto standard for authentication in software and applications (e.g., e-mail, social media, e-commerce, etc.). It is further used to unlock mobile phones.
- According to the experts, biometrics are often used to access highly secure areas, to unlock smart phones and can be found in many application domains (e.g., prosecution, military, border control).
- OTP is categorized as the technique that is mostly used in e-banking (also in combination with 2-factor authentication), e-mail sign-in and online gaming.
- E-signatures are often used in e-mails and e-government applications.

Figure 3 summarizes the results for the frequency of use of techniques in the context of e-participation. The experts rated password/pin as the most frequent method used in e-participation. In addition, the electronic signature is also rated as often used. Furthermore, biometrics (never) or OTP (rarely) are defined as seldomly used.

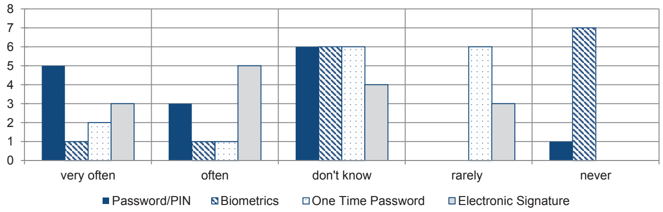

Figure 3: Results on use of authentication techniques in e-participation

Interpretation: The results display our results from the qualitative analysis. Most websites, if authentication is required, provide password/pin authentication while biometrics or OTP are almost never used.

Furthermore, experts think that identification is important as it (1) provides evidence that someone is behind this and prevents misuse through lobbyists (2) is de facto standard for user registration of websites and (3) has a low barrier. One expert notes that current technology for biometrics is rather expensive and requires an additional device and the maintenance and secrecy of TANs might require a higher effort.

4) Motivation for use of authentication techniques for e-participation: The motivation and background to use and provide different authentication techniques for e-participation can be manifold. In the following, we summarize the main points derived from the expert survey:

- High usability for users
- Fast creation of eIDs
- Data protection policies should be clearly specified
- Use of secure technologies and security measures
- Low acquisition cost
- Low maintenance on administrative side
- Clear terms of use

Interpretation: The results show that handling and management are important factors from the user and administration side. Furthermore, monetary aspects cannot be ignored for the use of authentication techniques.

5) Future use: For future use, experts expect that applications will use a set of different authentication techniques. The experts replied that it is important to provide a low barrier and to provide several authentication methods in order to provide different ways for identification. In addition, the experts noted that the use and application of national eIDs such as the Austrian Citizen Card are fundamental. Furthermore, e-participation could benefit from the use of e-signatures and TAN SMS in future projects. Even one expert noted that finger prints and iris scans could be possible future technologies.

Interpretation: The use of further authentication techniques in e-participation depends on various factors such as usability,

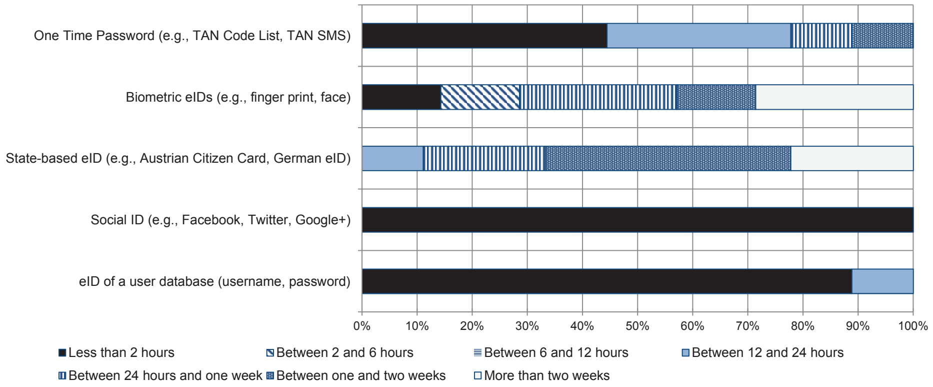

Figure 2: Results on time to register an eID

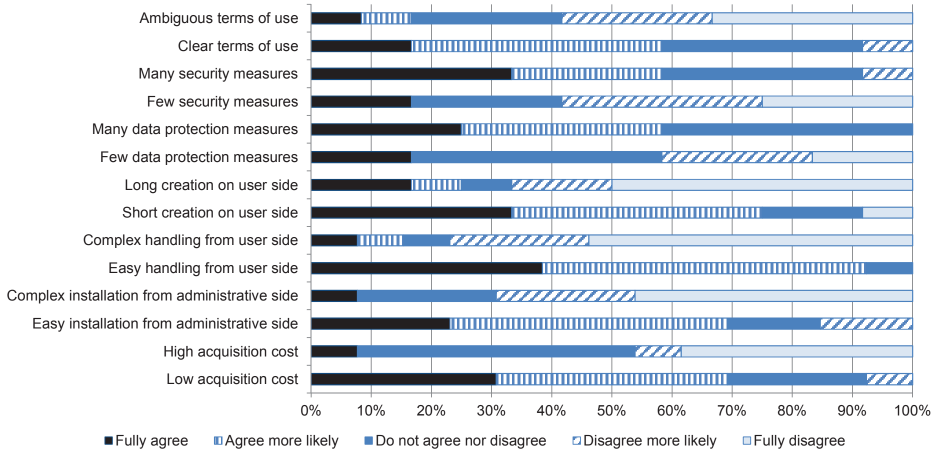

Figure 4: Results on motivation for use of authentication

maintenance and cost. Furthermore, they should have low barriers to entry and be developed together with users (i.e. human-in-the-loop).

C. Limitations

This survey has been designed as a short survey with 10 questions. To further elaborate on identification methods and their usage, a more in depth analysis with e.g., interviews is required. It further was out of scope to further investigate certain aspects and are subject to future work. Furthermore, the authors found that the choice of wording is essential in surveys. For example, we think that in a larger survey, we would specify the question outlined in Section V-B1 and would for example analyze unique characteristics for identification or authentication and further would analyze the technologies used to secure these characteristics.

VI. Discussion and Recommendations

Table II summarizes the main results of this paper. It displays a categorization of current practice and future use of authentication techniques in the context of e-participation. Based on the results of the previous sections, we specified current and future authentication techniques for the levels of e-participation. In the following, we will analyze each level of participation and the application of authentication techniques as shown in Table II.

Information is a level of e-participation that might not actually require the use of an authentication technique. As information in citizen involvement is often public and does not need authentication, we specified all authentication techniques as not adequate.

Furthermore, *Consultation* is about one- and two-way communication (e.g., commenting, rating and scoring of comments). So far, authentication is often provided by password. This way of communication does not require high authentication requirements. For example, OTP could be used; other techniques might be too expensive to adapt due to high acquisition cost and resources to maintain databases.

Co-operation is about creating and developing plans or tasks cooperatively. As stated above, biometrics and device authentication might not be suitable for this level. However, OTP and e-signature certificates could be used in future e-participation projects.

The level *Co-decision* provides voting mechanisms on plans or implementations (such as voting for different renovation plans of a park or public place). Co-decision can have stronger security requirements e.g., a participant is only allowed to vote once or that only a certain crowd is allowed

TABLE II: Current practice and future use

	Level of E-participation			
Technique	**Information**	**Consultation**	**Co-operation**	**Co-decision**
Password	⊟	⊠	⊠	⊠
Biometrics	⊟	⊟	⊟	⊡
One time password	⊟	⊡	⊡	⊡
E-signature certificate	⊟	⊟	⊡	⊡
Device authentication	⊟	⊟	⊟	⊡

Legend: ⊠ ... current practice; ⊡ ... future use possible; ⊟ ... not adequate

to vote (e.g., people living in a certain area, people having a certain age). Depending on these requirements, suitable authentication techniques could be selected.

In summary, the results showed that password is currently used as primary authentication technique in e-participation. This is not surprising due to low maintenance cost and available technology. However, further technologies are ready to be adopted in the context of e-participation. Their use and actual benefit should be analyzed beforehand and depends also on predefined security and privacy requirements.

VII. Conclusion

While e-participation is an emerging research field, the use and application of authentication techniques has only centered on standard techniques: password or pin. However, research and development provides several authentication techniques such as OTP, biometrics or e-signatures that could be used for e-participation. In this paper, we provided an analysis of possible authentication techniques and their current practice and conducted an expert survey to determine how these techniques are categorized in terms of security, availability and usability. The results showed that the use of authentication techniques for e-participation depends on several factors such as high usability, fast creation, low acquisition cost, or low maintenance. In future projects, these results can be used as a reference to diversify authentication and provide new ways for e-participation.

Acknowledgments

This work is part of the project eParticipation (845507) and is funded by the Austrian security research programme KIRAS and the Federal Ministry for Transport, Innovation and Technology (bmvit). The authors would like to thank the participants of the expert survey for their support and contribution.

References

[1] A. Macintosh, “Characterizing e-participation in policy-making,” in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004*, Jan. 2004.

[2] C. W. Phang and A. Kankanhalli, “A Framework of ICT Exploitation for e-Participation Initiatives,” *Commun. ACM*, vol. 51, no. 12, pp. 128–132, Dec. 2008.

[3] P. Parycek, “Positionspapier zu E-Democracy und E-Participation in Österreich,” White Paper EDEM-1.0.0, Jun. 2008. [Online]. Available: http://reference.e-government.gv.at/fileadmin/_migrated/content_uploads/EDEM-1-0-0-20080525.pdf

[4] P. Parycek, J. Schossböck, and B. Rinnerbauer, “Identification in E-Participation: Between Quality of Identification Data and Participation Threshold,” in *Electronic Participation*, ser. LNCS. Springer, Aug. 2015, no. 9249, pp. 108–119.

[5] O. Terbu, W. Hötzendorfer, M. Leitner, A. Bonitz, S. Vogl, and S. Zehetbauer, “Privacy and security by Design im agilen Softwareprozess,” in *Netzwerke: Tagungsband des 19. Internationalen Rechtsinformatik Symposions IRIS 2016*. Österreichische Computer Gesellschaft (OCG), 2016, pp. 457–464.

[6] P. J. Windley, *Digital Identity*. ”O’Reilly Media, Inc.”, Aug. 2005.

[7] ENISA, “eID Authentication methods in e-Finance and e-Payment services,” ENISA, Heraklion, Greece, Tech. Rep., Dec. 2013, 978-92-9204-077-2.

[8] M. Norshidah, *Critical Socio-Technical Issues Surrounding Mobile Computing*. IGI Global, Oct. 2015.

[9] B. Pinkas and T. Sander, “Securing Passwords Against Dictionary Attacks,” in *Proc. of the 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 161–170.

[10] X. Suo, Y. Zhu, and G. S. Owen, “Graphical passwords: a survey,” in *Computer Security Applications Conference, 21st Annual*, Dec. 2005, pp. 10 pp.–472.

[11] A. Jain, L. Hong, and S. Pankanti, “Biometric Identification,” *Commun. ACM*, vol. 43, no. 2, pp. 90–98, Feb. 2000.

[12] A. Weaver, “Biometric authentication,” *Computer*, vol. 39, no. 2, pp. 96–97, Feb. 2006.

[13] P. Tuyls and J. Goseling, “Capacity and Examples of Template-Protecting Biometric Authentication Systems,” in *Biometric Authentication*, ser. LNCS. Springer, May 2004, no. 3087, pp. 158–170.

[14] N. Haller, “The S/KEY one-time password system,” RFC 1760, Feb. 1995. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1760.txt

[15] N. Haller, C. Metz, P. Nesser, and M. Straw, “A one-time password system,” RFC 2289, 1998.

[16] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, “A password authentication scheme over insecure networks,” *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, Jun. 2006.

[17] S. Arzt, S. Rasthofer, and E. Bodden, “Instrumenting Android and Java Applications as Easy as abc,” in *Runtime Verification*, ser. LNCS. Springer, Sep. 2013, no. 8174, pp. 364–381.

[18] C.-C. Lin, H. Li, X. Zhou, and X. Wang, “Screenmilker: How to milk your android screen for secrets,” in *21st Annual Network and Distributed System Security Symposium (NDSS)*, 2014.

[19] I. Serov, M. Leitner, and S. Rinderle-Ma, “Current Practice and Challenges of Data Use and Web Analytics in Online Participations,” in *15th IFIP Electronic Government (EGOV) and 8th Electronic Participation (ePart) Conference 2016*, 2016, (to appear).

[20] K. Baxter, C. Courage, and K. Caine, *Understanding Your Users: A Practical Guide to User Research Methods*. Morgan Kaufmann, May 2015.