Security Levels for Web Authentication Using Mobile Phones

Anna Vapen, Nahid Shahmehri

Security Levels for Web Authentication using Mobile Phones

Anna Vapen and Nahid Shahmehri

Department of Computer and Information Science
Linköping University, SE-58183 Linköping, Sweden
{anna.vapen,nahid.shahmehri}@liu.se

Abstract. Mobile phones offer unique advantages for secure authentication: they are small and portable, provide multiple data transfer channels, and are nearly ubiquitous. While phones provide a flexible and capable platform, phone designs vary, and the security level of an authentication solution is influenced by the choice of channels and authentication methods. It can be a challenge to get a consistent overview of the strengths and weaknesses of the available alternatives. Existing guidelines for authentication usually do not consider the specific problems in mobile phone authentication. We provide a method for evaluating and designing authentication solutions using mobile phones, using an augmented version of the Electronic Authentication Guideline.

Keywords: Authentication, information security, mobile phone, security levels, evaluation method

1 Introduction

Most people today have multiple accounts and identities on the Internet, which they use in everyday life for a variety of purposes, from the inconsequential to the vital. To access these accounts, digital identities consisting of username/password pairs are commonly used [7]. Since users usually have many identities to remember, there is a risk that they will write the passwords down or choose the same password for several sites, which increases the risk of identity theft [12]. Users also tend to choose simple passwords that can be revealed to an attacker in an online guessing attack [3].

A hardware device can be used to ensure strong authentication by providing a tamper-resistant environment in which an authentication algorithm can run. Examples of hardware devices for authentication are smart cards, USB sticks, and devices with a display and a keypad [4]. Hardware devices for authentication are mainly used in online banking and other security-critical applications. The hardware is issued by the service provider and dedicated to a specific application [6]. Dedicated hardware can require additional equipment, such as cables or card readers. It may be inconvenient for the user to carry the device and other equipment at all times, especially for mobile users who use multiple computers

in different locations, for example at work, at home and at an Internet kiosk. Another option is to use a device that a user will already be carrying for a different reason. A mobile phone is an example of a device always available to the user. Furthermore, it does not require distribution to users, since most users already have access to a mobile phone [2]. Examples of authentication solutions where a mobile phone is used are:

- *2-clickAuth* [10], an optical authentication solution for identity providers;
- *Strong Authentication with Mobile Phones* [9], an authentication solution using SIM cards [8];
- *SWA* [11], authentication adapted specifically for untrusted computers.

Since authentication solutions for mobile phones differ significantly from each other, and since there are many choices with regard to data transfer and communication, it can be difficult to determine how secure a solution is. It is also difficult to design a new authentication solution with a specified security level in mind, since the choices of input and communication depend on the specific situation.

We propose a method for the evaluation and design of authentication solutions that use mobile phones as secure hardware devices. Our method focuses on mobile phones and also considers usability, availability and economic aspects, as well as security. The method uses the security level concept from the Electronic Authentication Guideline from NIST [4]. We also propose supplements to the guideline to include secure hardware devices that can communicate with a local computer or a remote authentication server.

The outline of this paper is as follows: section two describes aspects of the use of mobile phones in web authentication, section three describes the security level concept and shows our proposed supplements to the NIST Electronic Authentication Guidelines and section four explains our evaluation and design method. Section five describes case studies, section six describes related work, section seven describes future work and section eight concludes the paper.

2 Mobile Phones in Web Authentication

The variety of communication and input channels differentiates mobile phones from other hardware devices for authentication. The channels allow transfers of large amounts of data without time-consuming typing. The phone can also connect directly to a remote server via a long-range channel [9]. However, the location of the user affects the availability of the channel, e.g. whether a long-range channel can be reached and if it is costly to use. The availability of an authentication solution depends on whether the communication channels in the solution can be used without extra equipment and costs. Since users are mobile and authenticate from different places, the hardware they use will not be consistent.

An authentication solution that is available to the user and reaches the required security level should also be easy to use, regardless of the user's skill

level. Usability in a broader sense should also be considered, e.g. reduction of user actions needed to perform authentication.

There are also economic aspects to authentication, such as costs incurred by the user to access the long range communication channels and costs for purchase and distribution of equipment.

We discuss these factors in our design and evaluation method in section four. However, first we describe how the existing security levels can be adapted to mobile phones as authentication devices.

3 Proposal for New Security Levels

The Electronic Authentication Guideline from NIST [4] defines four security levels (1–4 where 4 is the highest) that can be used for evaluating the security of authentication solutions in general. Below is a short overview of the guidelines.

Level 1: Single or multi-factor authentication with no identity proof. Protection against online guessing and replay attacks.

Level 2: Single or multi-factor authentication. Protection against eavesdropping and the attacks from level 1.

Level 3: Multi-factor authentication with protection against verifier impersonation, MitM attacks and the attacks from level 2. Level 3 requires a token used for authentication to be unlocked by the user using a password or biometrics. Only non-reusable data (e.g. one-time passwords) may be used.

Level 4: Multi-factor authentication with FIPS-140-2 certified tamper-resistant hardware [1]. Protects against session hijacking and the attacks from level 3.

Since there are specific concerns related to phones, we suggest complementing the Electronic Authentication Guideline [4] so that it can handle phone specific issues, such as eavesdropping on short range (i.e. between a phone and a nearby computer) communication channels.

We propose two new levels between the existing security levels, to make the Electronic Authentication Guideline better suited for evaluating web authentication solutions, especially with mobile phones. We make the original levels more fine-grained by dividing levels 2 and 3 into two levels each, adding level 2.5 and 3.5. The goal is to be better able to compare authentication solutions to each other. With the current levels, two solutions with very different security may end up on the same level, which makes comparisons more difficult. When designing new solutions with a specific level in mind, a less secure design may be chosen since it is located at the same level as one that is more secure.

Since the Electronic Authentication Guideline is mainly intended for solutions where individuals are authenticated, identity proofing is required for all levels above 1. Identity proofing means that at registration the user must prove their physical identity, e.g. by providing their passport number and credit card number. Most web applications authenticate digital identities but are not concerned with physical ones. In such applications, security may be relevant even

if identity proofing is not. Furthermore, our interest lies in the technological aspects of mobile authentication, whereas identity proofing is an administrative issue. For these reasons, identity proofing is not relevant to web authentication. Requiring identity proofing would make most web authentication solutions end up on level 1, independent of the overall security of the solutions.

Level 2.5: The same requirements as for level 3, but with only one of phone locking or MitM protection.

Level 3.5: The same requirements as for level 4, but with a SIM or USIM card (or similar tamper-resistant module) that is not FIPS-140-2 certified.

When using a mobile phone for password storage, passwords may be strong and have high entropy, without any extra inconvenience for the user. Because it is possible to store a password securely on the phone and transfer it to a local computer without a risk of keylogging, such solutions meet the requirements of level 2, except for the identity proofing aspect. Since we consider identity proofing a separate issue, we consider these solutions to be at level 2.

For level 2.5, one of phone locking or MitM protection may be left out. An MitM attack is difficult to protect against, since such protection requires a side channel or the exchange of several rounds of data. Phone locking may be time-consuming for a user that authenticates often. Verifier impersonation lies in level 2.5 since it is a protocol issue that is unrelated to the properties of the phone.

Very few phones today can reach level 4, because of the hardware requirements. Level 3.5 requires both protection against verifier impersonation and that sensitive data transactions must be authenticated. However, a SIM or USIM card can be used in authentication, either in an EAP-SIM protocol [9] or for running authentication algorithms, e.g. calculating responses to a challenge. The SIM card may not be used in such a way that secret keys or other secrets are revealed to an attacker.

4 Evaluation Method for Mobile Phone Authentication

We provide a list of steps, outlined in Figure 1, to follow for evaluation and design of authentication solutions using any type of mobile phone, including

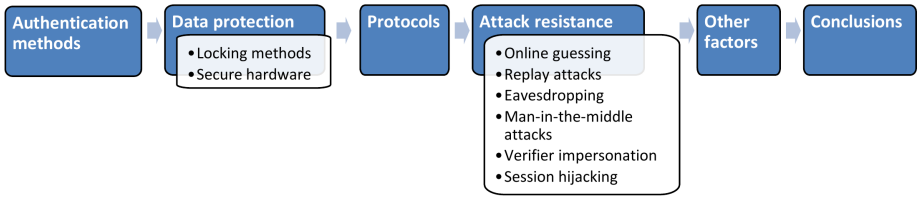

Fig. 1. Description of the evaluation and design method.

Table 1. Features of mobile phone communication channels

Features	Factors	Bluetooth	IR	NFC	Cable	Audio	Optical	Manual	Comments
Keylogger resistant	S	x	x	x	x	x	x	(x)	Manual input may be vulnerable to keyloggers when using passwords. Non-HID Bluetooth devices are not vulnerable to keyloggers.
Cannot spread malware	S					x	x	x	
For private environments	S	(x)	x	x	x	x	x	x	Bluetooth can be eavesdropped from outside a building.
For public environments	S	(x)	(x)	x	x	(x)	(x)	x	Channels in parenthesis can be eavesdropped and replayed by a nearby attacker, if the data is used several times.
For phone unlocking	S					x	x	x	In specific cases a touch screen or fingerprint reader could be used for biometric unlocking.
For noisy environments	U	x	x	x	x		x	x	
For users with poor eyes	U	x	x	x	x	x		x	
For users with shaky hands	U	x	x	x	x	x		x	
No extra equipment	AE					(x)	(x)	x	An optical channel from the phone to the computer requires a web camera. Audio channels require speakers and a microphone.

S: security factor, U: usability factor, A: availability factor, E: economic factor. x: the channel has this feature. (x): the channel usually has this feature, but there are exceptions that are noted in the Comments column.

smartphones. The list is used in conjunction with Table 1 to determine the highest security level that a solution can achieve or to suggest solutions for a chosen security level. Table 1 describes features present in the communication channels and makes it easy to compare the variety of communication channels for mobile phones, based on their features. The set of features is initial and will be extended. The features in the current set are the most important ones and can affect the security level of a solution.

1. **Authentication methods:** There are methods with reusable data (e.g. passwords) and with one-time data (e.g. one-time passwords).
   Evaluation: Identify the authentication method used in the solution. If a method with reusable data is used, level 2 is the highest level possible. For level 1, passwords must have reasonable security (see *online guessing* below). To reach level 2, passwords with at least 10 bit entropy are required [4]. Biometrics may not be used, according to the Electronic Authentication Guideline.
   Design: Choose the authentication methods that are feasible. For level 3 and higher, only methods with one-time data may be used. For level 2, passwords with 10 bit entropy are needed. Using a phone for password storage makes it possible to use a strong password that is difficult to remember.
2. **Data protection**
   (a) **Locking methods:** To protect the phone when it is not in use, it may be locked using biometrics (e.g. voice or face recognition) or a manual method (e.g. password or PIN).
   Evaluation: If the phone can be locked, the solution can reach level 3 or higher. Otherwise the solution can at most reach level 2.
   Design: For level 3 and higher, choose a locking method. This requires manual, optical or audio input on the phone, depending on the locking method.
   (b) **Secure hardware:** Tamper-resistant hardware in the phone can be used for data protection. Level 3 requires multi-factor authentication with a secure hardware device [1], a software token (e.g. software used for calculating non-reusable authentication data), or a one-time password device. Phones can be considered hardware devices, without the FIPS certification needed for level 4, but can also be seen as devices containing software tokens.
   Evaluation: If the phone uses secure hardware certified by the FIPS-140-2 standard (FIPS-140-2 level 2 overall security and FIPS-140-2 level 3 physical security) [4], the solution can reach level 4. If a SIM card is used as secure hardware, level 3.5 is possible. Otherwise level 3 is the highest level.
   Design: See *evaluation*.
3. **Protocols:** Depending on which protocol is used in authentication, the security of the solution may vary. The following authentication protocols may be used: proof-of-possession-protocols with either private or symmetric keys, tunneled or zero-knowledge password protocols and challenge-response password protocols.
   Evaluation: Challenge-response passwords can at most reach level 1. Tunneled or zero-knowledge password protocols, which are protocols that cannot be easily eavesdropped, reach level 2 at most. Proof-of-possession protocols can reach level 4.
   Design: See *evaluation*. On a mobile phone, proof-of-possession protocols require keys to be securely loaded into and stored in the phone.
4. **Attack resistance**

(a) **Online guessing:** Passwords must be strong enough not to be guessed.
Evaluation: For level 1 and 2, passwords must resist online guessing. This is achieved by using strong passwords and not sending them in the clear. The maximum chance of success of a password guessing attack must be 1/1024 for level 1 and 1/16384 for level 2, over the complete lifetime of the password [4]. Passwords are not used in levels 3 and 4.
Design: See *evaluation*.

(b) **Replay attacks:** In a replay attack, authentication data is reused by the attacker.
Evaluation: Resistance against replay attacks is required for levels 1–4. If passwords are sent in the clear, the solution does not reach level 1.
Design: To reach level 1, passwords must be tunneled or salted while sent over a network or phone channel.

(c) **Eavesdropping:** Table 1 shows which channels can be used in a private environment, i.e. a room without untrusted people present, and which channels can be used in a public environment, e.g. an open area with untrusted people present, without being eavesdropped by an attacker.
Evaluation: For non-reusable authentication data, the solution can reach level 4. For reusable data (e.g. passwords), use Table 1 to see if the channels are vulnerable to eavesdropping. If not, the solution can reach level 2. Otherwise the solution can reach level 1 at most. Level 2 also requires reusable data to be tunneled (e.g. using SSL) or otherwise protected, when sent from the local computer to a remote server.
Design: For reusable data, choose channels not vulnerable to eavesdropping and tunnel the communication to the remote server to reach level 2. For non-reusable data, any channel may be used and tunneling is not necessary.

(d) **Man-in-the-Middle-attacks (MitM):** If there are long range channels available, such as a phone network or Wi-Fi, they can be used as a secure side channel to protect against MitM attacks. Without long range channels, mutual authentication can be used to prevent MitM attacks.
Evaluation: With MitM mitigation the solution can reach level 3 and higher. For level 2.5, either MitM mitigation or phone locking must be present.
Design: See *evaluation*.

(e) **Verifier impersonation:** In this type of attack, an attacker claims to be the verifier in order to learn passwords and secret keys.
Evaluation: Resistance against verifier impersonation is required for level 3 and higher. The data sent should not give any clues on the secret key used in authentication.
Design: See *evaluation*.

(f) **Session hijacking:** An attacker modifies or reroutes parts of a session.
Evaluation: If there is a shared secret per session, this may be used to protect against hijacking. Such protection is required for level 4.
Design: See *evaluation*.

5. **Other factors:**
   Evaluation: Use Table 1 to learn about features not discussed in the Electronic Authentication Guideline. These features do not affect the security level, but may affect other aspects of the solution. For solutions in which third parties are involved, shared secrets must not be revealed to the third party, in order for the solution to reach level 2 or higher.
   Design: Choose channels based on the user's equipment, if known. Manual input is default for both computers and phones. If challenge-response is used as authentication protocol, data transfer in both directions between the computer and the phone is needed. If there is a risk of malware, users with poor eyes etc, check Table 1 for solutions that may be used in the specific cases. For level 2 and higher secrets must not be revealed to third parties.
6. **Conclusions:**
   Evaluation: Applying these steps will allow identification of the solution's maximum security level. This will also provide information about the properties that prevent the solution from reaching a higher level.
   Design: Given the preferred security level, this process will provide recommendations about possible channels, authentication methods and other features. An example of this would be one-time passwords or challenge-response with manual input and Wi-Fi as a side channel.

5 Case Studies

We now present four case studies that apply our method from section four and show design and evaluation.

5.1 Design Case Study: Password Storage

Consider a simple application in which the user stores their password on a mobile phone, in order to have strong passwords without having to remember them and type them on the keyboard. The goal of this password storage is to make the use of passwords as secure as possible, i.e. level 2. It should be possible to use it both in private and public environments.

1. **Authentication methods:** The default method is passwords that may reach level 2 if the passwords are tunneled or zero-proof passwords.
2. **Data protection**
   (a) **Locking methods:** Phone locking is not needed for level 2.
   (b) **Secure hardware:** For level 2, no secure hardware is needed.
3. **Protocols:** All protocols except challenge-response passwords may be used.
4. **Attack resistance**
   (a) **Online guessing:** Passwords must be strong enough to resist password guessing and dictionary attacks. They must also have at least 10 bit entropy.

(b) **Replay attacks:** Tunneling can be used for mitigating replay attacks over a remote network. For transmission between the phone and a local computer, choose channels from Table 1 that are not open to attacks in public environments.
(c) **Eavesdropping:** See *replay attacks*.
(d) **MitM:** Not needed for level 2.
(e) **Verifier impersonation:** Not needed for level 2.
(f) **Session hijacking:** Not needed for level 2.

5. **Other factors:** For transferring passwords from the phone to a local computer, manual input should be avoided in order to protect against keyloggers. In a public environment, NFC and a cable connection may be used. In a private environment IR, audio transfer and optical transfer may also be used.
6. **Conclusions:** One possible solution for this application would be to use strong, high entropy passwords (possibly automatically generated) stored on a phone and transferred to a nearby computer using a cable or NFC. Channels such as IR or Bluetooth are not appropriate since they are vulnerable to eavesdropping in a public environment. Finally, the password must be tunneled when sent over a remote network, or the solution would fail to reach even level 1.

5.2 Design Case Study: Online Banking

Consider a general online banking solution in which the user can perform several different tasks which require different levels of security. Examples of these tasks are: A) check account balance, B) withdraw money from the account and move it to another account, owned by another person and C) close the account. For A we assume that the security of a password is sufficient, given that there is additional protection against keyloggers and eavesdropping. Therefore, level 2 is chosen for A. For B, we aim for a higher security level than A. C is considered the most security-critical case and requires as high a level of security as is possible. We will now use our evaluation method to find suitable authentication solutions for A and B. For this scenario we assume Bluetooth access, a phone network, a phone camera and manual input. We assume that the solutions are to be used in public environments.

1. **Authentication methods:** A: All methods can be used. B: Only methods with non-reusable authentication data can be used.
2. **Data protection**
   (a) **Locking methods:** A: No locking needed. B, C: Manual or optical (biometric) input can be used for locking the phone.
   (b) **Secure hardware:** A and B: Secure hardware is not needed. If a SIM-card is used for secure storage, B may reach level 3.5. C: Secure hardware must be used, but is not present in phones.
3. **Protocols:** A: A strong password protocol such as tunneled or zero-knowledge password protocols may be used. Proof-of-possession protocols may also be used. B, C: A proof-of-possession-protocol must be used.

4. **Attack resistance**
   (a) **Online guessing:** A: Passwords must be strong and have a least 10 bit entropy. B, C: Passwords are not used.
   (b) **Replay attacks:** A: Bluetooth and optical data transfer should not be used for sending reusable data. Tunneling must be used for reusable data. All channels can be used for one-time data. B, C: All channels can be used.
   (c) **Eavesdropping:** A, B and C: The same as for replay attacks apply.
   (d) **MitM:** A: MitM protection is not needed. B, C: The phone network can be used as a side channel. Other mitigation methods can also be used.
   (e) **Verifier impersonation:** A: Not needed for level 2. B, C: If an attack occurs, the attacker must not get access to sensitive data. Eavesdropping resistance will suffice in this case.
   (f) **Session hijacking:** A and B: protection against this type of attack is not needed for levels 2-3. C: Session secrets can be used for protection against hijacking.
5. **Other factors:** A: Only manual input is available for reusable data, but not suitable for passwords (malware risk). B: No other factors apply. C: Data transactions must be authenticated.
6. **Conclusions:** For checking account balance (A), one-time passwords with manual input may be used. An alternative is to transfer data via Bluetooth instead of manual input. A challenge-response protocol can be used instead of one-time passwords. In that case the response may be sent optically. Otherwise, manual input or Bluetooth may be used. For withdrawing money and moving it to another person's account (B), the requirements for A applies, but with locking using manual or optical input and with additional MitM mitigation. For closing the account (C), the requirements for B applies, but with authenticated data transfer and session secrets. Since secure hardware is not available, sufficient security for C cannot be achieved with a mobile phone alone. The user can initiate the closing of the account with the solution from B, but then must add another method such as physically signing a form from the bank and sending it by mail.

5.3 Evaluation Case Study: 2-clickAuth

2-clickAuth [10] is an optical challenge-response solution that uses a camera-equipped mobile phone as a secure hardware token together with a web camera to provide fast, simple, highly available and secure authentication. Data is transferred both to and from the phone using two-dimensional barcodes.

1. **Authentication methods:** 2-clickAuth uses challenge-response with non-reusable data. Max level: 4
2. **Data protection**
   (a) **Locking methods:** 2-clickAuth can be used with a PIN-code to lock the phone. Max level: 4
   (b) **Secure hardware:** No secure hardware is used. Max level: 3

3. **Protocols:** A proof-of-possession protocol with shared keys is used. Max level: 4
4. **Attack resistance**
   (a) **Online guessing:** Passwords are not used. Max level: 4
   (b) **Replay attacks:** Non-reusable data is used. Max level: 4
   (c) **Eavesdropping:** Since 2-clickAuth is intended for use by mobile users in diverse locations there is a risk of eavesdropping, but the data cannot be used to gain knowledge about secret keys. Max level: 4
   (d) **MitM:** MitM protection is not used, due to availability. Max level: 2.5
   (e) **Verifier impersonation:** There is a risk of verifier impersonation, but since the authentication data transferred does not reveal any sensitive information, the impersonating attacker does not gain access to secrets. Max level: 4
   (f) **Session hijacking:** No session secrets are used. Max level: 3
5. **Other factors:** It should be possible to use 2-clickAuth in noisy environments such as public places, because it uses optical data transfer. Optical channels are also malware resistant, since data can only be sent as a direct result of user action. No secure hardware can be assumed. Secrets are not revealed to third parties.
6. **Conclusions:** 2-clickAuth may reach level 2.5 if used with a PIN code. To reach level 3, some kind of MitM mitigation (e.g. using SMS as a side channel) must be used.

5.4 Evaluation Case Study: Strong Authentication (SA)

The Strong Authentication (SA) solution consists of several variants wherein a phone operator is considered a trusted third party. A secret identifier stored on the user's SIM card and listed in the phone operator's user database is used to calculate session IDs and challenges. The user authenticates by using one of the following alternatives:

A: The user sends an SMS to the SA server acknowledging that a session ID shown in the computer's browser and one sent to the user's phone are the same.
B: The user sends an SMS to the SA server, containing a response calculated by the phone to a challenge shown in the computer's browser and typed into the phone by the user (or sent via Bluetooth). A variant is that the user receives the challenge via SMS and sends the response via the computer.
C: The EAP-SIM protocol is used for strong authentication via Bluetooth or SMS [9].

1. **Authentication methods:** A: Identifier based on a static value. Max level: 2. B, C: Non-reusable data, comparable to one-time passwords. Max level: 4
2. **Data protection**
   (a) **Locking methods:** Since the SIM card is used, a PIN code can be assumed for phone locking. Max level: 4

   (b) **Secure hardware:** SIM cards are used in all SA variants. Max level: 4
3. **Protocols:** A: Similar to using passwords. Max level: 2. B, C: Proof-of-possession. Max level: 4
4. **Attack resistance**
   (a) **Online guessing:** Non-reusable data is used. Max level: 4
   (b) **Replay attacks:** Authentication data can only be used during the session. Max level: 4
   (c) **Eavesdropping:** A: The session ID is based on a static identifier and may be eavesdropped. Max level: 2. B, C: Not vulnerable to eavesdropping. Max level: 4
   (d) **MitM:** A, B: Does not protect against MitM attacks, even if SMS is used for B. This is because the SMS channel is not used as a side channel, but as an alternative to short range channels. Max level: 2. C: MitM protection. Max level: 4
   (e) **Verifier impersonation:** A, B: Does not protect against verifier impersonation. Max level: 2. C: Verifier impersonation protection. Max level: 4
   (f) **Session hijacking:** A, B: Does not protect against verifier impersonation. Max level: 2. C: Verifier impersonation protection. Max level: 4
5. **Other factors:** SA requires the participation of a mobile phone operator. Shared secrets are not revealed to third parties in any of the SA variants. In A there are no shared secrets. Only C has authenticated data transfer. It is stated that SA needs to be usable. Bluetooth can spread malware between the phone and the computer. When there is a choice between SMS and Bluetooth, SMS is a better choice if it is feasible to use the phone network.
6. **Conclusions:** The session ID solution (A) is a simple solution that reaches level 1. Challenge-response solutions (B) reaches level 2 and EAP-SIM solutions (C) reaches level 3.5.

6 Related Work

The NIST guidelines for authentication [4] cover different areas of authentication and discuss technical details and formal security requirements. However, in their guidelines, security is the only factor. In this paper, the aim is to combine the well known and accepted security levels from NIST with factors such as availability, usability and economic factors. This should help developers and evaluators make the best choice among several solutions that meet the same security requirements.

There is no comparison of authentication channels and methods made specifically for mobile phones. However, for the authentication system Strong Authentication with Mobile Phones, which uses a phone's SIM card in authentication, there is a comparison between the different modes of the system in which different channels are used. The comparison shows how the different modes compare to each other when it comes to factors such as cost, infrastructure, security and usability [9]. Cost and infrastructure, e.g. which equipment and networks are needed, are not factors that are explicitly discussed in this paper.

There is also work in progress on evaluating authentication solutions in the area of IMS (IP Multimedia Subsystem). The IMS evaluation method considers several different factors such as security, simplicity and userfriendliness [5].

7 Future Work

Our evaluation and design method can be extended to include cryptographic methods as well as examples of trusted hardware modules and their usage. We will introduce new factors, such as infrastructure and learnability to make the method more detailed.

We have already taken into account the cost issues regarding the use of phone networks and equipment that the user may need for short range communication via specific channels. We intend to investigate other cost issues, such as factors related to deployment and running of authentication systems. We will integrate these factors into our method to help developers create economically feasible solutions. Our method will also be adapted for different types of applications and user groups as well as for services and parts of services. We will also investigate the possibility of designing authentication solutions in which the user can actively change the authentication level, based on other requirements such as the current situation and application.

8 Summary and Conclusions

Hardware devices can help increase the security of authentication solutions. The mobile phone is a flexible and capable device with several channels for transferring authentication data. Different channels and authentication methods influence the level of security of authentication solutions, but it may be difficult to get an overview of all combinations of channels and methods. We provide a method for evaluating authentication solutions where mobile phones are used as hardware devices. This is different from the case where a user authenticates to a web site using the phone's browser (i.e. the phone is used as a handheld computer). In that case the phone itself becomes untrusted.

Our method is related to the Electronic Authentication Guideline, but has been adapted to apply to the specific problems of mobile phone authentication, especially considering communication channels. We have also introduced intermediary security levels to improve the granularity at which authentication methods can be compared. To the best of our knowledge, there are currently no other evaluation methods for phone authentication.

The method is to be extended and can be used both for evaluating existing authentication systems and for designing new solutions. The goal is to help developers create secure authentication, taking availability, usability and economic factors into account.

References

1. Security requirements for cryptographic modules. Technical Report 140-2, National Institute of Standards and Technology, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
2. F. Aloul, S. Zahidi, and W. El-Hajj. Two factor authentication using mobile phones. *AICCSA 2009*, pages 641–644, May 2009.
3. J. Bonneau and S. Preibusch. The password thicket: technical and market failures in human authentication on the web. pages 1 –10, 2010.
4. W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. Technical Report 800-63, National Institute of Standards and Technology, 2008. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
5. C. Eliasson, M. Fiedler, and I. Jorstad. A criteria-based evaluation framework for authentication schemes in IMS. In *Proceedings of the 4th International Conference on Availability, Reliability and Security*, pages 865 –869, 2009.
6. A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. *IEEE Security & Privacy*, 4(2):21 –29, March-April 2006.
7. M. Mannan and P. C. van Oorschot. Using a personal device to strengthen password authentication from an untrusted computer. In *Financial Cryptography and Data Security*, pages 88–103. Springer Berlin / Heidelberg, 2007.
8. K. Rannenberg. Identity management in mobile cellular networks and related applications. *Information Security Technical Report*, 9(1):77 – 85, 2004.
9. D. van Thanh, I. Jorstad, T. Jonvik, and D. van Thuan. Strong authentication with mobile phone as security token. In *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, pages 777 –782, 12-15 2009.
10. A. Vapen, D. Byers, and N. Shahmehri. 2-clickAuth - optical challenge-response authentication. In *Proceedings of the 5th International Conference on Availability, Reliability and Security*, pages 79–86. IEEE Computer Society, February 2010.
11. M. Wu, S. Garfinkel, and R. Miller. Secure web authentication with mobile phones. In *Proceedings of DIMACS Workshop on Usable Privacy and Security Software*, 2004.
12. J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: empirical results. *IEEE Security & Privacy*, 2(5):25 –31, September-October 2004.