UNIVERSITY OF OSLO
Department of Informatics

Authentication methods

INF5261

Midterm report

Hans-Joachim
Jelena Mirkovic
Ivica Milanovic
Øyvind Bakkeli

Spring 2010

Contents

1. Introduction

With mobile devices constantly taking a bigger part in our everyday life, the convenience of accessing a bank account, paying for any services or even checking medical journals independently of current place and time is getting more and more feasible. Having in mind that these kinds of services require access to user's personal information, the logical major requirement is high security and strong user authentication methods.

Through our project we want to address following questions:

- What are most common and accepted authentication methods for mobile services?
- What are differences, opportunities and challenges concerning user authentication for mobile services compared with traditional stationary computers?
- How do people accept them and what are their opinions regarding security on mobile device?
- Evaluation of a security / usability / privacy trade offs for different authentication mechanisms.

We recognize the potential of new mobile services that are emerging (e.g. mHealth, mBanking, mLearning), but we would like to find out if security is on a level high enough to provide adequate support for them or they can provide more threats and problems to users than benefits.

2. Methods

The first phase of our project was to perform research on what is already developed and available in the area of user authentication for mobile service. For research we used Internet browsing, as well as search of research databases (IEEE, ACM, Elsevier…). We saw that field of user authentication for mobile device is very wide and try to organize our findings in four groups:

- Authentication methods based on something that user know
- Authentication methods based on something that user has
- Authentication methods based on something that user is
- Authentication methods based on user location

For every group we tried to capture main characteristics and summarize the theory findings through covering four main topics: implementation for stationary devices, implementation for mobile devices, security level that is provided, and usability issues. Based on that it was easier for us detect main challenges, advantages and problems regarding each specific authentication approach. Results of the performed research are described in section 3.

Beside theory overview that gave us background information on what is done in the area of authentication for mobile devices and enable us to detect main characteristics of each of it, we wanted also to gain knowledge about users and their acceptance of authentication methods on mobile devices. For this purpose, we created questionnaire for usability testing of mobile users. Using the questionnaire we plan to identify main requirements and satisfactions with different user authentication methods. Also we would like to find out what are their impressions about authentication requirements for different types of services, what they view as sufficiently secure for different services and what difficulties usually arise when they interact with (mobile) authentication methods. Descriptions of questioner and testing scenario are in section four.

At the end of the project our plan is to evaluate and summarize our findings and present different types of authentication methods looked from different angles (e.g. security they provide, usability for users, type of service they are intended, type of users they are intended). We plan to find out which authentication methods are more suitable for mobile devices and if there are some authentication mechanisms that are developed just for mobile devices by utilizing their specific characteristics. We also want to see whether usability and security represent two opposing sides of a continuum, what the required balance between them is, and how they are related to types of the services or applications and privacy issues. Some of the preliminary discussions based on the work that we did so far are given in section five.

3. Authenticate methods used on mobile and stationary devices

3.1 Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be [1] Authentication processes are common these days, as online banking, online services (email, facebook) or even online access to medical journals and similar become more and more usual. The traditional way of authenticating per today depends on three factors that could be something you have, something you are and something you know[2]. The authentication process could include one of these factors or a combination of them all.

3.2 Something that user know

Something that user knows is often associated with a password, multiple passwords, or a combination of a password and a username [3]. User usually choose password before he/she starts using the service. This same static password has to be provided by user for every future use of service.

3.2.1 Stationary computer approach

In computer-security systems this is the most common method for authentication for users. For most of web applications and services password authentication presents well enough solution. Even though this authentication mechanism does not provide high level of security, it is very easy for implementation, and user is usually free to choose password that is easy for him/her to remember.

3.2.2 Mobile device approach

Based on success of password authentication on stationary devices, same approach is also adopted and used on mobile devices. The first example you can see when you turn on your mobile phone. The first thing that usually happens is that you are prompted for PIN code, before you can start using your mobile phone. On that manner user is authenticated to the mobile network, and he/she is protected from lost and theft of the mobile phone.

3.2.3 Security level

Security level provided by this approach is not very high. There are numerous of attacks that can jeopardize user confidentiality and security. Some of the attacks are brute force attacks where attacker try to log in to the service with every possible password until he/she succeed, dictionary attack where user try only passwords from the previous prepared lists and rainbow attach that present more sophisticated version of dictionary attack where passwords are hashed before attack and these values are used for attacks. Additionally, more threats can emerge if original password that is provided by user during registration is stored in an inappropriate manner.

One major problem with password and security is user factor. In most cases user is required to choose password that he/she will use on the system and remember it. Password that is chosen can greatly influence security of the user, and because of that it is very important for user to choose strong password. On the other hand if user is made to choose complicated and inconvenient password, there is another problem with writing down and forgetting it.

3.2.4 Usability issue

We saw that authentication using passwords provide really low level of security. But also we said that this approach is very popular and widely accepted for stationary and mobile device. The biggest reason for this is high usability and easy implementation. From user it is required to remember password that he/she choose, and there is no complicated and demanding authentication process and privacy issues.

3.3 Something the user has

User authentication in this case is based on something that user has, a physical object. An object could be a mobile device or a token. Using this approach, a user is not required to reveal any private information about him/her (like in biometrics) nor is it required remembering some secret information (password).

3.3.1 Stationary device approach

A token could be a small physical device[3]that is often used to authenticate on website or a similar service. They are used to prove one's identity electronically, and they exist in different sizes and shapes, and are often small devices that can easily be carried around. Tokens can store different kind of data that is often implemented in a chip and can perform various authentication methods. The four types[4] of tokens are; static passwords, synchronous dynamic passwords, asynchronous

passwords and challenge response. The tokens could work as stand alone, or they can be connected to a computer using the USB mechanism or some kind of wireless technology like Bluetooth. Mobile phone also can be used as a token for user authentication for services and applications on stationary devices.

3.3.2 Mobile device approach

This approach for user authentication is especially suitable for authentication of the user for mobile applications and services. The biggest reason for this is that mobile device is usually considered as private device that belong just to one person, and because of that is ideal example of “something that user has”. On that manner mobile device is in the same time terminal that provide service and user authentication token.

There is couple of possibilities how this authentication method can be implemented on mobile phones. The biggest difference is how user’s private authentication information is stored or delivered to mobile phone. The possible approaches are:

- private information is stored on hardware on the mobile phone(e.g. SIM card),
- private information is stored on the specific file on the mobile phone file system, and
- private information is received through mobile service operation (SMS message)

Authentication of user based on private information stored on a SIM card is usually used by network operator to authenticate subscribers. This approach provides very high level of security because user private information is stored on the tamper resistant cards. For this reason, this approach is becoming more and more popular for authentication of the user for different mobile services (e.g. mobile banking). The biggest disadvantage is that all changes and additions to SIM cards must go through network provider.

Authentication of user based on private information stored on mobile phone memory is not dependent on the mobile network provider and user or service provider can more freely install and/or store user’s authentication information on mobile device. The secret information can be in different format depending on the type of the services. For example, the user can use certificate that is stored on the mobile phone for authentication or install specific application that contain user’s private information and generate authentication token based on this information. The problem with this approach is that private information is stored on the mobile phone, so if user changes mobile phone he/she has to acquire private information again.

One example of authentication of the user based on private information that is received through mobile service operation is using SMS messages. The most common scenario is that One Time Password (OTP) is delivered to user during authentication process, which afterwards must be inputted in the log in screen in the original application. But also other scenarios are developed. For example, when user receives a SMS message with the OTP he/she just reply to the SMS message on the mobile phone. In this approach user is not required to retype OTP, but utilize the telephone network for the second factor of authentication [phone factor authentication]. Even thought this approach provides great usability to regular users (there is no need to use complicated application and functionalities of the mobile, but just SMS service that is well known to everybody), there are great trade-offs that this approach introduce[5]. First, there are problems with latency of the SMS services especially during peak SMS usage as holidays. Another one is that text is transferred without any encryption and is visible to service provider. Also, service provider has right to store SMS messages on their side (for example when user is not accessible, so the message can be forwarded later on). Finally, there are also serious security vulnerabilities that this kind of authentication introduces e.g. man-in-the-middle [5]

3.3.3 Security level

Security level that is provided by using only this method is not so high. Attacker that steals user's token or mobile device can gain full access to user's private information and services. And today it is not so unlikely scenario that mobile phone is lost or stolen because of their small size and wide deployment in people everyday life. Mainly for this reason, this approach for user authentication is usually used in combination with some other authentication method (most commonly with authentication based on something that user know e.g. password, PIN number). This approach is called two-factor authentication and is frequently used for user authentication for mobile services.

3.3.4 Usability issue

Usability of this authentication approach can vary greatly depending on the type of token that is used. For example, if authentication token is chosen well and user is always in possession of token (for example if toke is mobile phone) whole authentication process can be very simple and easy for user. But on the other hand we have example where token is some stand-alone device that user do not use very frequently and do not carry it always with herself/himself, and user is very often in situation that can not use service because he/she do not have token in that moment.

3.4 Something that user is

Ways to authenticate a user based on something he or she is are often based on scanning and analysis. These methods, referred to as biometrics, centers around authentication based on that person's unique traits. Traits can be physical, such as fingerprints or behavior, such as walking patterns or typing patterns.

Biometric authentication methods have been developed to counter the possibility that unauthorized persons may gain access when traditional security methods like security pass cards or passwords are used[6] states the most critical flaw of these systems is that since they do not use any inherent characteristics or attributes of the individual user, they are unable to differentiate between an authorized personnel and an impostor who have fraudulently come to possess the token or knowledge (such as stolen credit card or lost password)." For this reason, methods to discern legitimate users various biometric methods have been developed, which today includes "fingerprint-based systems and iris, retina, face, palm print, voice, handwriting and DNA technologies"[6]

3.4.1 Stationary device approach

Several computer or keyboard models come equipped with finger-print-readers. They offer an alternative to authenticate the user of the machine in addition to traditional passwords. There are also some solutions that require the user to swipe their finger in order to get access to an area or similar. In these cases the readers are attached to or close to doors.

3.4.2 Mobile device approach

In addition to desktop computers, many laptop models ship with fingerprint scanners that can be used for user authentication. With mobile phones, a few models are available with fingerprint scanners[7]

There have been and is ongoing research in this area, and as the technology improves, biometric scanners on mobile devices might be more widespread than what it is today. Some experiments, such as [6] have been able to authenticate users based on palm print scanning using a mobile camera. Also ongoing research are conducted on authentication of users by scanning their wrist veins [8] and recognizing their handwritten signature [9]

3.4.3 Security level

As with all security solutions there are good and bad implementations. Some readers are easy to fool, requiring only a glove with an attached fingerprint according to Veum and Flesland. Some scanners

may also accept cut-off fingers. Other scanners are more thorough and will not fall for simple tricks as this.

In addition, biometric solutions may pose a treat to the user itself. Imagine if unauthorized persons wanting access become aware that the only thing the user needs in order to gain access is to swipe one of his or her fingers. The user now runs the risk of having one of his fingers removed in order for the unauthorized persons to be able to gain access.

Biometrics might be best suited for additional security, or as a second factor in an authentication process, rather than being used on its own.

3.4.4 Usability issue

The use of biometrics can be quick and effective. Since it is based on something the user is, it is virtually impossible to loose or forget like tokens or passwords. After all, the user will have his or her finger available for scanning. However, disabled people might not be able to utilize all biometric solutions. For instance a user in a wheelchair might not be able to utilize solutions based on walk patterns or a person with a broken arm will have trouble with maintaining the typing pattern he or she would have with both hands available.

Some people might value their privacy more than the ability to use a convenient authentication method such as fingerprint scanning. Since this is unique information that might be tied to a single person, their concerns may be justified. For a given solution, which information and how detailed as well as who might have access to this information might affect how a user reacts to such solutions. For one, it might be limited who really needs to store biometric information, like when entering schools [10], Disneyland[11] or even gyms[12].

Another concern is if their information is somehow compromised, the users will not be able to change their fingerprint, like they would their password.

3.5 Location based authentication

Location based authentication is not used much directly in present times, other than for instance limiting access for services such as ATMs. We choose to focus on authentication related to mobile devices. Other methods could for instance involve using optical devices to recognize users.

To find the users location some suggested methods involve using GPS capable devices, for instance a newer cell phone, relying on the cell network or using Bluetooth or other range limited technology as

a beacon. The different methods have advantages, disadvantages regarding granularity and range and different uses.

3.5.1 Stationary device approach

For stationary use one can see if the user is in proximity of the device being used. One method [13] presented suggests using IP geo location services to get the terminals location. This can then be used directly as a part of the authentication, the user's phone and the terminal has to be in proximity to get authentication. It can also be used to suggest what level of authentication one need, if the location is in a workplace or similar perhaps a one-factor authentication could be enough.

One of the patents[13] also suggest multiple mobile device works together with authentication on a stationary device, but one can be in possession of multiple mobile devices and one can check if these are in proximity of each other.

3.5.2 Mobile use

When interacting with a terminal of some sort (using a mobile device for payment or similar), the stationary and mobile methods overlap.

When applied purely in a mobile context, location based authentication would probably move toward determining if a user is at a location. Using some form of automatic positioning systems are one option, using passphrases or secrets located at the location is another.

3.5.3 Security

The security achieved by using mobile devices for authentication depends on the method of determining a user's location. For instance GPS devices can be tampered with, and depends on the client side environment. Using a cell phone network and checking what antenna a user is connected to be better, but has low granularity. Signals emitted from a beacon can be spoofed and transmitted to other places.

Some privacy concerns may arise when considering how location is found. Constantly tracking the users would give good precision and security.

3.5.4 Usability

Location based authentication can be transparent for the user, so when it comes to usability it isn't really an obstacle. However, considering the low degree of usage and support today, one can think that location based authentication processes would be dependent on third party application.

These applications may not integrate well with the devices, and then exclude certain user groups. When using some knowledge that only exists at the location however, there may be some challenges.

3.6 Summary

From research that we conducted and summarized in previous part of the paper, we can see that there are many approaches for performing user authentication, both for mobile and stationary devices. We saw that there is no unique solution that is appropriate to every situation. There are numerous factors that must be taken in consideration when selecting authentication method, as for instance: usability, security, specific functionality of the application/service, privacy, user requirements. The biggest challenge is finding the right balance between these factors, and selecting the authentication method that is suitable for specific service and accepted by users.

4 Questionnaire

Next step of our project is to involve user and found out what are their thoughts on this topic. We want to determine what users would expect and tolerate to protect their personal information. For this purpose we made questionnaire we will use to find out user's acceptance of different authentication methods described in previous chapter.

4.1 Usability testing – process description

We made questionnaire that we plan to distribute to users as hard copies and in online version. We do not want to pose any limitation on respondents for taking part in our questionnaire, but because of time and resource limitation the major part of people that will take part in our questionnaire will be between 18 and 40 years old. We decided on this because the most mobile users are from this age group regarding research[14] and we hope to get the more valuable feedback from users with more experience in using mobile devices. Only stipulation is the respondents should be current or previous users of mobile handsets.

During our literature search we found some articles that are addressing very similar issues, and we use their descriptions of procedures and questions in questionnaire as base for creating our questionnaire. In the papers[15, 16] it is described the results of the survey that as goal had to find out opinions of subscribers regarding the need for security in mobile devices, their acceptance attitudes toward current and possible future alternative methods.

During development of the questionnaire, we tried to find the right questions for users, and do not ask more than it is absolutely necessary for our research. Also we tried not to ask any questions that user might experience as privacy violations. User is not required to respond to all questions, and can leave some of them unanswered if he/she wants.

4.2 Questionnaire description

In the Appendix we enclose the current version of the questionnaire that we made. We plan to perform some final changes and improvements before creating online version and start usability testing. Also, we plan to first perform usability testing on group of students on this course, to gain both answers to questionnaire and feedback about content of questionnaire, and detect possible bad formulation and misunderstanding of questions.

Now we will describe questionnaire in more details and explain what we want to find out with each question.

Age and group questions are usually starting point in every questionnaire and we plan to see how responds of the rest of the questionnaire depends of the age and the sex of the participants.

With questions about factors that influence choice of network operator and mobile handsets, we plan to find out how aware users are about security issues and with what they relate security with.

Questions about current and future usages of mobile phones will show us how much users are acquainted with their mobile phones and their capabilities and are they interested in future deployment.

In the next set of questions we will ask users about current authentication methods: which are used, on what manner, do they think there is need for higher level of security and would they accept other authentication methods.

Also we have one question that address privacy issue, and what do user think about storing their private information on different places (mobile phone, network…).

5 Discussion

From the previous two parts we can see which user authentication methods are used today for mobile and stationary device, what are their characteristics, how we plan to gather additional information about user acceptance of them. Here we will describe some preliminary topics for discussions based on performed research.

5.1 Differences between mobile devices and traditional computers

As stated earlier, services like banking becomes frequently more available to smartphones and other mobile devices rather than being reserved for stationary computers. It is therefore important to look at how authentication is handled on these mobile devices and what risks or challenges are present on mobile devices compared to traditional computers.

According to a whitepaper by Trend Micro[17] companies are starting to use mobile devices to access business applications such as Customer Relationship Management (CRM) or Enterprise Resource Planning (ERP), which can frequently include sensitive data. With this kind of access through mobile devices, employees might access these services from anywhere. Trend Micro[17] suggest the company network protected by a central firewall is no longer sufficient, but these devices need to be protected as well.

Trend Micro[17] identifies some of the main risks with mobile devices as:

- They are at higher risk to be stolen or lost, which might lead to compromised data.
- problems caused by malware
- spyware compromising data
- cracking or Denial of Service

If a device is lost or stolen from an employee, sensitive data stored on it might be exposed. Though some sensitive data will only be stored in encrypted form it is still not desirable that these devices should fall into the wrong hands. Trend Micro suggests unauthorized access to data can be thwarted by erasing or encrypting the data on the device" in order to protect data. On some devices it might be

possible to remotely erase data on a lost or stolen device; however this process might fail if the device is not available to receive the command. Instead the device might set policies to wipe all stored data e.g. after an amount of failed login attempts. Trend Micro[17] considers encryption and policy based solutions for erasing data best practices for this scenario. In addition the company should have policies for how old devices and data store on them are handled, for instance when upgrading or replacing equipment.

While computers have a known history of dealing with viruses and malware, far less problems have been recorded with mobile devices. However, this might be an increasing problem in the years to come. Since mobile devices such as a Smartphone might have access to both the home network and company network in addition to others, malware might spread rapidly. Trend Micro (2007) also lists examples where viruses have spread by sending themselves to all the numbers in a user's address book or sending large number of SMS-messages, either simply spamming or trying to manipulate the receiver by phishing.

Similar to malware, the dangers of spyware in the form of key loggers or similar have been known on the PC platform. However such programs are no less capable of recording keystrokes, passwords or offer unauthorized access to a mobile device. Trend Micro[17] defines spyware as malware (...) used to steal confidential data with intent to sell it or cause harm to an organization". Information gathered from spyware may be sold to competitors or used to damage the company, the company's customers or employees.

In addition, if the mobile device, the operating system or the services it run contains flaws, these might be exploited by crackers. They will also be susceptible to Denial of Service attacks, in which the device or service receives more requests than it can handle, thus rendering it unusable as long as the DoS attack lasts.

It is important to note that secure solutions do not consist of purely technical solutions. In addition to technical means such as anti-malware protection, transfer data of secure connections and firewalls, Trend Micro (2007) lists the establishment of clear policies for use of mobile devices, authentication of users and devices for data access. In addition, training of users and increase risk awareness.

5.2Differences between different authentication methods

Findings from the research until now we summarized in the Table 1.

	Security	Usability	Privacy	Mobile implementation
Something that user know	Low level of security. Numerous attacks exist.	Medium. There is no complicated authentication process but user must memorize password.	Good. User is not required to reveal any private information about him/her.	Yes. Widely deployed in mobile application/services world.
Something that user has	Used as only factor provide medium level of security, but usually used in two-facto authentication.	Vary. Depend on the selection of the token.	Good. User is not required to reveal any private information about him/her.	Yes. More and more used for mobile service because the mobile phone can be in the same time authentication token and terminal for accessing the service.
Something that user is	High. Attacker can not that easy impersonate regular user, but attacks exist.	Medium. Regular user can always prove who he/she is, but there is problem with physically impaired people.	Low. User must provide information about his/hers unique physical characteristic.	Yes, but not much. There are some phones with fingerprint reader, and there are also researches about other types of biometrics authentication for mobile phones.
Were user is	Depend on the method.	High. User is not required to perform any additional tasks.	Low. User must reveal information about his/hers location in the moment of authentication.	Not yet, but there are research projects in this field.

Table 1. Characteristics of different security methods

In the table we can see the strongest and the weakest points for each approach. For the future research we plan to add more columns in the table to be able to better preview the whole situations. Some of the other aspects we want to address here are: suitability for different kind of services, user acceptance, law regulations addressing required authentication methods, resource and performance requirements.

6 References

1. *Authentication*. 2007; Available from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html.
2. Council, F.F.I.E., *Authentication in an electronic banking enviroment.* 2001.
3. Bordea, D.d., *Selecting a two-factor authentication system.* Network Security, 2007. **2007**(7): p. 17-20.
4. From Wikipedia, t.f.e. *Security token*. Available from: http://en.wikipedia.org/wiki/Security_token.
5. From Wikipedia, t.f.e. *Two-factor authentication*. Available from: http://en.wikipedia.org/wiki/Two-factor_authentication#SMS_One_Time_Password.
6. Fang, L., M.K.H. Leung, and C.S. Chian, *Making Palm Print Matching Mobile.* International Journal of Computer Science and Information Security (IJCSIS), 2009. **Vol. 6**: p. 001-009.
7. *Cellphones / PDAs / GPS / Portables / Assistants personels / GPS*. Available from: http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_pdaphones.htm.
8. NGT. *CScout Exclusive: Mobile Vein Authentication*. 2009; Available from: http://www.mobilebehavior.com/tag/authentication/.
9. *BioWallet Signature*. Available from: http://www.mobbeel.com/en/mobbeel/Products/biowallet.html.
10. From Wikipedia, t.f.e. *Fingerprint*. Available from: http://en.wikipedia.org/wiki/Fingerprint#Privacy_issues.
11. Harmel, K. *Walt Disney World: The Government's Tomorrowland?* 2006; Available from: http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments.
12. Vinson, J. *Cracking your Fingers*. 2009; Available from: http://thedailywtf.com/Articles/Cracking-your-Fingers.aspx.
13. Ashfield. *Patent Application Publication*. 2008; Available from: http://www.freepatentsonline.com/20100022254.pdf.

14. *Consumers in the 18-to-24 Age Segment View Cell Phones as Multi-Functional Accessories; Crave Advanced Features and Personalization Options.* 2007.

15. Clarkea, N.L., et al., *Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices.* Computers & Security, 2002. **21**(3): p. 220-228.

16. Furnell, N.L.C.a.S.M., *Authentication on users on mobile telephones – A survey of attitudes and practices.* Computers & Security, 2005. **24**(7): p. 519-527.

17. Micro, T. *Enterprise Mobile Security Protecting Mobile Data and Increasing Productivity*. 2007; Available from: http://emea.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/mobilesecurity/wp03_tmms_071212us.pdf.

7 Appendix A (Questionary)

Questionnaire - Authentication methods for mobile devices

1. Age

   ☐ Below 18 ☐ 18-24 ☐ 25-34 ☐ Above 34

2. Gender

   ☐ Male ☐ Female

3. Education Level:

   ☐ Grade school

   ☐ High school

   ☐ Bachelor degree/ Diploma

   ☐ Master degree and above

4. What are your considerations when choosing a network operator?

	Low	Medium	High
Choice of handsets	☐	☐	☐
Network coverage	☐	☐	☐
Operator loyalty	☐	☐	☐
Prices, deals etc.	☐	☐	☐
Reliability	☐	☐	☐
Security features	☐	☐	☐

5. What are your considerations when choosing a mobile handset?

	Low	Medium	High
Brand	☐	☐	☐
Battery	☐	☐	☐
Accessories	☐	☐	☐
Games	☐	☐	☐
Security	☐	☐	☐

Infrared/Bluetooth	☐	☐	☐

6. Which functionalities do you use one your phone?

	Yes	No	Not available
Information services	☐	☐	☐
Internet browsing	☐	☐	☐
Email	☐	☐	☐
E-commerce	☐	☐	☐
Music	☐	☐	☐
MMS	☐	☐	☐
GPS	☐	☐	☐
Additional games	☐	☐	☐
Mobile banking	☐	☐	☐
Applications	☐	☐	☐
Calendar/Organizer	☐	☐	☐

7. What functionalities do you think you would use in the future?
   - ☐ Mobile health
   - ☐ Mobile learning
   - ☐ Video conferencing
   - ☐ Mobile payment
   - ☐ Video on demand
8. What kind of authentication methods you use today and what you think about its usability and security?
   - PIN number /Password
     - Usage: ☐ Mobile device ☐ Stationary device
     - Usability: ☐ High ☐ Medium ☐ Low
     - Security: ☐ High ☐ Medium ☐ Low
   - Token
     - Usage: ☐ Mobile device ☐ Stationary device
     - Usability: ☐ High ☐ Medium ☐ Low
     - Security: ☐ High ☐ Medium ☐ Low
   - SMS message
     - Usage: ☐ Mobile device ☐ Stationary device

- Usability: ☐ High ☐ Medium ☐ Low
- Security: ☐ High ☐ Medium ☐ Low

- Fingerprint
  - Usage: ☐ Mobile device ☐ Stationary device
  - Usability: ☐ High ☐ Medium ☐ Low
  - Security: ☐ High ☐ Medium ☐ Low
- Location based
  - Usage: ☐ Mobile device ☐ Stationary device
  - Usability: ☐ High ☐ Medium ☐ Low
  - Security: ☐ High ☐ Medium ☐ Low
- Others:

  _____
  - Usage: ☐ Mobile device ☐ Stationary device
  - Usability: ☐ High ☐ Medium ☐ Low
  - Security: ☐ High ☐ Medium ☐ Low

9. If you use password authentication, do you utilize possibility of your phone to remember password for you?

☐ Yes, always ☐ Sometimes ☐ Depend on the service ☐ No, never

10. If you lose your phone, what will you consider as biggest problem:
    - ☐ Lost of contact list
    - ☐ Lost of SMS messages
    - ☐ Lost of pictures/other media on mobile phone
    - ☐ Lost of other private information stored on the mobile phone
    - ☐ Lost of authentication token for other kinds of services
    - ☐ Expenses (higher bill due to misuse, buying new phone)
11. Do you think that there is need for higher security for mobile services

    ☐ Yes ☐ No ☐ Don't know

12. Do you think that using biometrics on the mobile phone is needed?

☐ Yes ☐ No ☐ Don't know

13. Would you use these types of authentication for mobile services?
    - ☐ Fingerprint
    - ☐ Face recognition
    - ☐ Hand recognition
    - ☐ Iris scanning
    - ☐ Voice recognition
    - ☐ Keystroke analysis
    - ☐ Location based
14. Where the original data that is used in authentication should be stored?
    - ☐ SIM card
    - ☐ Memory of the phone
    - ☐ External device
    - ☐ Network
    - ☐ Don’t know