Economic aspects of web authentication

Pernilla Stolpe Johansson
Email: perst718@student.liu.se
Supervisor: Anna Vapen, {anna.vapen@liu.se}
Project Report for Information Security Course
Linköping University, Sweden

Abstract:

In year 2008, 51.3 % of the world population owned a mobile phone, today probably being significantly higher the figure. To be able to reach a good enough security level, a hardware authentication device might be the only option. But since this means that the user needs to bring an extra item all the time it is argued that the mobile phone could be used as a hardware authentication device. But using the mobile phone in web authentication means different types of costs than with another type of hardware authentication device and this is therefore analysed in the study. A model is presented that can be used when evaluating web authentication in general and with mobile phones in specific. It concludes with the fact that it is difficult defining a specific cost since it depends on many variables, but by using the model one should be able to reach a good estimate in each situation.

1. Introduction

Web authentication is the way to prove who we are on the web. For example, when entering the bank in an errand, the bank clerk will check your ID-card prior helping you to assure that you are the one posing to be. In the same way we need to identify ourselves on the web when we try to enter certain accounts or modifying certain information so that the addressed system is assured that you are the person that you state to be.

According to Matt Bishop there are 4 different ways of doing so; through something you know, through something you have, through who you are, and finally, through where you are [1]. Something you know can for example be the password you use to log into your e-mail account, and something you have could be your bank security device.

Depending on the way you choose, or which combinations you use, the security level of the web authentication will reach different levels. In the former example, having a hardware authentication device such as a bank security device is more secure than a reusable password to your e-mail account. The problem with the bank security device, and other hardware tokens, is that you need to keep it with you. If you use one device to access all your files and programs at work and you forget it at home one day you simply will not be able to work; quite a hassle just to ensure security.

This hassle would be evaded if the separate hardware authentication device was not needed. But since this is the case to assure the security level the question is rather if it is possible to merge it with something that we always keep with us – the mobile phone.

According to statistics from the UN [2], 51.3 % of the world population had a mobile phone in 2008; looking only at the countries within Europe this population owns 1.02 mobile phones each with Estonia topping the list with 1.88 units per person. This is therefore a strong indication that a mobile phone would be a hassle-free way to always keep the hardware authentication device with you.

1.1 Scope of the report

This article therefore focuses on web authentication using mobile phones. Since this is a field already quite covered with research, another approach has been used. Information security is an area which a company can invest quite a lot of money in, but what if the cost of information protection reaches higher levels than the revenue of the company itself – is not that then the real threat? Therefore, the aim of this report is to paint a better picture of what costs web authentication with mobile phones incur. Another aim is to provide a model or mindset of what factors that needs to be reviewed before the implementation of a new web authentication system to assure that all costs are covered and analyzed, specifically with mobile phones in mind. Furthermore, as mentioned in the article by Vapen and Shahmehri [3], this report hopefully sheds some light over the costs that can be cut by using mobile phones in web authentication.

To help reaching the goal of the study, the following questions are used as a guide while exploring the area:

- What are the general economic aspects related to web authentication?
- What are the extras needed for using a mobile phone for web authentication?
    - Hardware, network costs, protocols etc.
    - What costs do these extras incur (or cut)?

- What are the most important factors to analyze from an economic aspect?

1.2 Outline of the report

In chapter 2.1 a literature study is performed of the topic, thereafter in chapter 2.2 practical cases are presented. The cases describe how hardware authentication devices that could be exchanged for mobile phones are used in web authentication.

Thereafter, the cases are compared and analysed in chapter 3, with the aim to find out how to convert the mobile phone into a security device to reach different levels of security.

Thereafter, the scope has been narrowed down even further, and investigates what these factors imply in costs.

At last, in chapter 4, conclusions of the findings have are made.

1.3 Method of work

To reach the aim of the study a literature study is performed of existing articles and books, firstly the course literature and secondly a screening of existing articles on the topic.

To connect the literature to real life a review of methods and implementations already in use is taken place.

1.4 Limitations

This report does not analyse if the mobile phone is, or is not, a feasible tool for web authentication. The report is only based on the fact that it can be used and then further analyse effects, possibilities and economical factors. This is to limit the scope of this report and therefore be able to focus more on the scope.

2. Background

As a background, several sources, theoretical as practical, is reviewed to reach a good-enough base of information to proceed to the analysis.

2.1 Literature study

Divided in shorter chapters, the basic literature on the subject is presented.

2.1.1 Four ways to authenticate

According to Matt Bishop [1], authentication is defined as "…the binding of an identity to a subject." But for the system to be able to bind the identity, the subject needs to provide something in order to be authenticated. According to Bishop this can be made in providing one or more of the following:

1. Something that the subject knows
2. Something that the subject possess
3. Something that the subject is
4. Where the subject is

To translate this into more specific terms, examples of each follow:

1. A password or a secret answer to a question
2. A door passing card or another hardware authentication device
3. Fingerprints or other biometric entities
4. On what network, on which computer

These four authentication factors reaches different levels of security and risks related to them, for example, a password depends on its entropy if it is to survive a dictionary attack. A door passing card is secure as long as the right person possesses it, if it is not possible to use the card information at a distance. Fingerprints have a small error margin built in to the algorithm calculating if the fingerprint is correct or not. And finally, it is possible that someone manages to be in the right place. By combining several of these measures, it increases the possibility of a good-enough security level. For example, the possibility that someone else manage to get their hands on the hardware authentication device *and* the password for it is less likely. By combining two different authentication factors you will therefore get a two-factor authentication, strengthening the security of you solution [1].

2.1.2 Four security levels

According to the Electronic Authentication Guideline provided by NIST [5], there are four levels of assurance according to the degree of confidence that the user is the one he or she is posing to be. A brief summary of the security levels presented in the NIST guideline is listed below:

1. Little or no confidence in the asserted identity's validity. There is no need for identity proofing[1] on this level, on this level it is sufficient with a simple password challenge-response protocol. Risk: Eavesdropping and thereafter replay attack
2. Some confidence in the asserted identity's validity. "Level 2 provides single factor remote network authentication."[5] At this level there is a need for identity proofing and need for a secure authentication protocol to prove the identity. No longer a risk with eavesdropping, but with online-guessing attacks and Trojan attacks.
3. High confidence in the asserted identity's validity. "Level 3 provides multi-factor remote network authentication." [5] At this level there is need for a proof of possession and a minimum of two authentication factors.
4. Very high confidence in the asserted identity's validity. "Level 4 is intended to provide the highest practical remote network authentication

[1] Identity proofing refers to a person presenting a physical evidence in order to proof his or hers identity.

assurance." [5] At this level there is need for proof of possession through a cryptographic protocol.

Regarding identity proofing when considering web authentication solutions, that is not a realistic requirement due to the natural constraint a web service have to proof the identity, at least not in a feasible way. Therefore the requirement of proof the identity on level 2 and higher will not be regarded when evaluating web authentication.

2.1.3 An attacker's possibilities

There are many different attacks a person could choose to use in order to access information that does not belong to said person. Below are descriptions of four types of attacks. We have chosen these four since they are quite common and paint an easy-to-understand image of attacks that threat web authentication.

1. **Eavesdropping**
   This method is known as a passive method, and means that the attacker simply listens to the traffic and tries to pick up useful information [6].
2. **Man-in-the-Middle (MitM)**
   In this method, the attacker goes for the authentication protocol and positions him/herself between the communicating parties and can therefore read and/or alter all information travelling between the parties [4].
3. **Phishing**
   This method is basically just asking for the password, in one or more ingenuous way. For example by posing to be a support centre, re-directing the user to an identical page and capture the password when the user tries to log on [7].
4. **Dictionary attack or online guessing attack**
   This is a guessing attack where the attacker most commonly has a list of strings, which are either words or just probable letter combinations, and do trial and error guesses based on that list [1].

2.1.4 Five ways to authenticate with a mobile phone

To increase the security on the authentication process a hardware authentication device can be used. But instead of using a separate device a mobile phone can be used as the hardware authentication device. In their article "Strong Authentication with mobile phone as a security token", van Thanh et al [3] display four different solutions of using the mobile phone as a hardware authentication device. There are also many other solutions offered that use the mobile phone as a part of the authentication process. One such solution is ActivIdentity [9]. Below is a list of these five different solutions, which serves as a representative sample of all the different solutions that exist.

1. **SMS authentication with Session ID verification**
   A session ID is sent both to the user's computer, and is shown in the web browser, as well to the user's mobile phone. The user then verifies that the session IDs are duplicates and confirms by returning a text message to the sender [4].
2. **One-time password from PC to SMS**
   When the user tries to login, the authentication server generates a challenge which is then sent to the user's web browser, and moreover an OTP. The person enters the challenge in the mobile phone which has an OTP applet installed. This applet generates an OTP and returns an answer to the authentication server through an SMS. If the answer is correct, i.e. if it matches the first OTP generated, the user is logged in [4].
3. **One-time password from SMS to PC**
   In this solution, when the user tries to login, the authentication server generates and sends an OTP in an SMS to the user's mobile phone. The user types this OTP into the web browser and is by this authenticated by the authentication server [4].
4. **SIM strong authentication via mobile phone**
   This solution is using the EAP-SIM protocol, which means that the protocol communicates directly to the SIM-card and authenticates the SIM through the international mobile subscriber identity (IMSI). It can be used automatically or manually depending on the Bluetooth availability, see note below [4].
5. **Software token in the mobile phone**
   In this solution a software token application is downloaded to the mobile phone. The token generates OTPs that are used to access the system or service in question. This solution therefore involves manual input of OTPs, but no information is sent via additional channels such as via SMS [8].

Note: Solution 1-4 it is also worth to mention that if the mobile phone and the computer are linked with Bluetooth the user do not need to verify the session IDs; the user only needs to make sure that the Bluetooth connection is working. Otherwise some kind of traffic over the GSM network will take place, either through SMS or data traffic, depending on the solution.

Further on, van Thanh et al discuss how vulnerable these four solutions are, and they find six potential weak spots, being: the mobile phone, the Bluetooth connection, the computer, the Internet connection, the connection between web browser and authentication server, and finally the GSM network. For the fifth solution all of these weak spots are applicable, except the GSM network and the Bluetooth connection.

2.2 Practical Experiences – Cases

In this chapter three different commercial use cases are presented, that involve web authentication in one way or another. There are no statistics behind the choice of the three examples, only that we regard them as three common situations, chosen to serve as a reference point in the chapters to come. Moreover these cases are general cases, not necessarily used from a mobile phone.

2.2.1 Case 1 – Internet banking security device

An internet banking security device is a hardware authentication device that is used to login on the online banking site, authenticating transactions and payments. The hardware authentication device contains an algorithm that generates an OTP, but only after the user has authenticated the usage with a personal PIN-number. When logging in or confirming a transaction the user therefore enters the PIN-number into the internet banking security device and retrieves an OTP. The OTP is thereafter entered in the web browser and the bank service authenticates the user [9].

2.2.2 Case 2 – Online payment with credit card with MasterCard SecureCode[2]

When using a MasterCard credit card to make a transaction online, the transaction is given an extra step, in which the user will be prompted with a screen where the user enters the SecureCode. When registering the card for SecureCode the user needs to enter the card details and the 4 last digits in his or hers personal id number (if the card issuer is a Swedish institution [11]) and thereafter enter the password that the user will use in all future transactions with that card when the merchants participate in SecureCode [10].

It should be noted that SecureCode is not more secure than any other password; it has just been given this name by MasterCard and might give a feeling of something more than a password.

2.2.3 Case 3 – Reach work mail externally/foreign computer

If the user needs to access the e-mail account when for some reason not being able to use the local Outlook client (or any other locally installed mail software), the mail can still be reached with Microsoft Outlook Web App (or any other web based mail service). This way the user can connect to the mail server from a foreign computer using only username and password. Thereafter the user can send and receive e-mails as if the user were sitting at the local computer.

[2] The same basic principal applies to credit cards issued by VISA as well, with Verified by VISA. The MasterCard solution is chosen only randomly to have a more narrow case.

3. Analysis of questions

Until now the report consists of a literature study and three commercial examples or cases. These will now be analyzed from the light of the questions presented in chapter 1.1. The aim of analyzing the first question is to conclude with an evaluation model to be used for evaluating web authentication solutions, to reach an estimation of cost.

3.1 What are the general economic aspects related to web authentication?

When considering the economical aspects of web authentication, one first has to consider what level of security that is needed. And also, what the service will be used for and from where.

If we start by looking at the cases presented in chapter 2.2, case 1 is the most secure of the three cases presented. But even though it is the most secure out of the selection, it only reaches level 2 in the NIST guidelines since it is still vulnerable to MitM-attacks. To be able to reach level 3 the web service would need to authenticate itself to the user (or use any other MitM mitigation technique) to so that the user is assured that there is not a MitM-attack.

Case 2 reaches level 2 when the SecureCode already is in place, but since there is really no proof of possession when one registers for the SecureCode, one can argue that the case 2 only reaches level 1. That is because in the registration process one needs to enter card details, that anyone possessing the card would know, but without the guarantee that it is the correct person possessing it and thereafter one has to enter the last 4 digits in the personal id-number (in the Swedish case) which an attacker most likely can retrieve on beforehand, or if not, at least guess the 4 digits quite easily. This is easy since the 4 last digits in the personal id-number are following a set of rules and the entropy his not very high of a password of 4 digits with no limit of trials. But since this means that someone needs to steal the card, which would probably lead to a quick deactivation of the card if the cardholder is vigilant of its possessions, it is argued that the case 2 reaches level 2 anyway.

Finally, case 3 reaches level 1 or 2 since only a password is needed to login, and it is therefore up to the entropy of the password to decide the level. Since case 3 is regarding accessing work e-mail from the web we might presume that the company has a password policy to reach certain entropy so that we can assume that case 3 reaches level 2. Risks might be eavesdropping or threat of a guessing attack. Since the breach of the security in case 3 can lead to information leakage the security level might be considered too low.

Summarizing these three cases one sees that all cases end up at level 2, even though their security differ from each other. Case 1 is the most secure and is very close to reach level 3, and case 2 and 3 are on level 2 but fluctuating between the middle of level to down to the margin of level 1

depending on the control of password that is performed when the user chooses password, for example minimum length, demand of at least one upper case letter, a number etc.

So depending on the level of security, different solutions need to be in place. For example, between the three cases, case 1 that reaches the highest security level also requires a hardware authentication device. Looking at the costs for this, one can not only see the cost of the hardware itself, but also the development of the algorithms behind the hardware authentication device or the license costs of these, and the demanding administration around the release of a hardware authentication device so it is sure that the right person receives it. It is also a matter of indirect cost in the case when the hardware authentication device is forgotten and needed in an urgent matter. First of all, the cost of building a support organization around it but also the indirect cost of lost opportunities etc.

For case 3 there is a need for a secure storage for the passwords but also a software assuring that all employees in the company changes password on a regular basis and chooses passwords that reaches certain entropy. On the other hand, changing password might sometimes give a false feeling of security, since changing password a lot might lead to more simple passwords, passwords written on notes besides the computer etc. to facilitate for the user. Case 2 also needs a secure storage but do not demand changing of passwords nor any software or person controlling the entropy of the SecureCode.

Taking one step back, basically all web authentication solutions would need a server containing the passwords, algorithms etc. and different layers protecting this information. And the cost of this does not only depend on the security level that is aimed for, but also what equipment one already possesses. It is important to see that a web authentication solution can be very costly or not at all, depending where you start out, empty-handed or with a full server room. Of course you also have to consider opportunity costs since you might lose an alternative income when using the servers for your internal web authentication solution instead of selling the capacity.

The costs will also depend on field of use and the roles of the users. Case 3 is probably ok for a low risk person[3] not handling any sensitive information but should probably not be used for a role handling a lot of sensitive data, where the leakage of such information would be devastating for the company. Therefore, on cannot only consider the actual and direct costs involved, but all the alternative costs if a security breach happens.

[3] A low risk person do not imply a specific role in a company, it refers more to the access rights the person has. That means that a consultant with access to only public information is a low risk person but a consultant with access to sensitive information means a higher risk.

To be able to do a structured evaluation, we propose an evaluation model in the following chapter, which will give an overview of the possible costs of web authentication.

3.1.1 Evaluation model of economic aspects related to web authentication

The evaluation model that we propose to get an overview of the costs is as follows:

1. Which security level do we need to reach?
2. Where will the solution be used (i.e. in a closed network, public WiFi, from certain computers only or an open web cafe etc.)
3. Who will be using it? What role and what kind of information does the person possess?
4. What are the opportunity costs [12] of the solution and the cost of a security breach?
5. What equipment do we already have in-house (can be treated as a sunk cost [12] or as a resource affecting the decision).

3.2 What are the costs related to using a mobile phone as a hardware authentication device?

When using a mobile phone as a part of the web authentication, there are other costs that need to be considered, but the model presented in chapter 3.1.1 is however still applicable. Going through step by step the different costs related will be analyzed:

1. Depending on the channels and protocols that are used, the solution will reach a different level. For example if all traffic is channeled through the same channel we will get the same effect as in case 1, and have a risk of MitM-attacks, and the solution will therefore only reach level 2. But on the other hand, if the information is in different channels and authenticate the user as well as the service, it will reach level 3, since that solution creates a two factor authentication. That is for example the case in the examples shown in chapter 2.1.4. So when deciding what security channel that one wants to reach, it is important to see what the web authentication solution with a mobile phone acting as the hardware authentication device uses in protocols and channels to assure the correct security level.
2. This is an especially interesting question when one is considering a mobile phone solution. Since many of the alternatives listed in chapter 2.1.4 use SMS and data traffic over the GSM network in their solution, one needs to consider the cost of that/those data traffic/SMS. If the user will be abroad when using the solution an added roaming cost will be issued and if the user needs to log on

frequently this will also create a cost. The aspects of where the solution will be used therefore need to be considered especially important.

3. Since extra costs as SMS etc is applicable to this type of solution there might be some roles where it is unnecessary with such an added cost; one role might need to re-login frequently which generates high costs. Therefore an evaluation about roles needs to be done in two aspects. Is the person important enough so it is defendable with the extra cost? And does the person posses any sensitive information that requires a higher security level although that person's role might not defend the cost.
4. By looking at the opportunity cost and cost of a security breach, one can from the roles in step 3 decide if the role needs the higher security level that the mobile phone solution implies. The alternative cost can for example be that instead of using mobile phone web authentication, the user needs to be at a certain location if the company chooses to use a closed intranet that cannot be accessed from outside the net. Although that might not be so common, it will serve as an example of alternative costs. The alternative cost would then be the trip there (both monetary and time wise) instead of investing in the mobile phone solution. A solution is either to raise the security level to be able to have an external access path or take the cost of travel. The security breach cost is for example if someone manages to guess the password of an important person sitting on a lot of confidential and sensitive information, the loss this will generate for the company if that information would be spread also needs to be considered.
5. The convenience of using a mobile phone is that no extra hardware authentication device is needed, although this creates a value of convenience to the user it is not necessarily most cost beneficial. If a solution using Bluetooth is chosen it can be quite costly if not the computers and mobile phones already have Bluetooth. If the computer lacks the Bluetooth it is possible to buy a separate blue tooth adapter (costing approximately € 15[4]), but then again an extra item is needed, that also occupies one USB port which might be inconvenient for the user.

Costs for authentication servers and service providers have not been provided in the analysis since it is considered this being unnecessary since they are basically default in any web authentication solution.

[4] http://www.dustinhome.se/pd_5010129433.aspx, exchange rate €1=9,02 SEK, 2011-04-10

The benefits of having the mobile phone as a hardware authentication device is that it is more convenient for the user not keeping many separate items in its possession, and it also means no extra issuing of hardware authentication devices. Also, that the identification of the user, i.e. the proof of possession, already is done when registering the mobile phone through the phone contract.

4. Conclusion

This report identifies the economical aspects regarding web authentication with a mobile phone as the hardware authentication device. The report ends up with an evaluation model with the steps of narrowing down the biggest cost factors regarding web authentication in general and using mobile phones in specific. The conclusion of the report is that it is an area hard to define since the costs depend so much on different variables. The most important variables to look at is need of security level, where it will be used, who will use it, what opportunity costs that can be found and at last, but not the least, what equipment that is already a resource at the company. By using this model, the costs should be possible to map in each case.

References

[1] M. Bishop, *Computer Security: Art and science*. Boston: Addison-Wesley, 2008

[2] UN data – A world of information. (2008) "Mobile cellular telephone subscriptions per 100 population." [Online] Available: http://data.un.org/Data.aspx?d=MDG&f=seriesRowID:756

[3] A. Vapen and N. Shahmehri. "Security levels for web authentication using mobile phones." *PrimeLife/IFIP Summer School Post-proceedings*, Springer, 2011 (In Press).

[4] 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, 2009.

[5] W. E. Burr, D. F. Dodson, 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>

[6] D. Gollmann, *Computer Security*. West Sussex: John Wiley & Sons Ltd, 2003

[7] D. van Thanh, T. Jønvik, B. Feng, D. van Thuan, I. Jørstad. "Simple Strong Authentication for Internet Applications using Mobile Phones." *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008.*

[8] ActivIdentity. *ActivIdentity_SoftT#5C7F992*. [Online] Available:

http://www.actividentity.com/download/document/171 [2011-04-09]
[9] ActivIdentity. *OTP tokens.* [Online] Available: http://www.actividentity.com/products/authenticationdevices/OTPTokens/ [2011-04-09]
[10] MasterCard. *SecureCode Support*. [Online] Available: http://www.mastercard.us/support/securecode.html [2011-04-09]
[11] Danske Bank. *Så här registrerar du ditt kort.* [Online] Available: http://www.danskebank.se/sv-se/privat/vardagsekonomi/Kort/Internethandel/Pages/Registration2.aspx [2011-04-09]
[12] R. Brealey, S. Myers, F. Allen, *Principles of Corporate Finance – Global edition*. McGraw-Hill Irwin. 10th edition, 2011