Economic Aspects of Web Authentication

Arul mozhivarman Govindarajan Muhammad Adnan
Email: {arugo208, muhad308}@student.liu.se
Supervisor: Anna Vapen, {anna.vapen@liu.se}
Project Report for Information Security Course
Linköpings universitet, Sweden

Abstract

Nowadays the web is a comprehensive source of information and a place where communication takes place. However, such wide use of the web for storing and sharing personal and sensitive information leads to a need of strong authentication while web users are communicating with each other. Authentication helps in reducing attackers stealing personal information. In addition, many different methods for web authentication are in practice. The most popular among them is password-based authentication. While implementing authentication solutions many different aspects need to be considered, one among them is the economic aspect which includes both direct and indirect costs.

1. Introduction

Today people all over the world like to have products, services and solutions which are simple and flexible with high security. Before the technology era, a man cannot live without water and food, but now to this he adds Internet and mobile communication which leads to new challenges and problems. Around 5 billion people use mobile phones around the world and this figure is increasing day by day [6]. In this report we are going to investigate economical aspects of web authentication with a focus on mobile phones.

Today people want products; support and solutions right at their doorstep but in the process the major concern is regarding the privacy and security of the data they share. These services are acquired mostly online through the Internet where a strong setup of authentication needs to be employed to address the concerns of the customer, which as a result would have a greater economic impact on the business. In general, authentication is a process to check for an exact match of a person or a thing. Web authentication is a process where the authentication takes place over the web and authentication data is sent over a remote network. In web authentication passwords are commonly used, which can be weak and open to attacks. The world has advanced quite a lot in the field of data communication which has raised the mobile phone usage up to 5 billion users [6] and now 3G technologies are providing high speed web access on the move. So the threat level to mobile internet users is the same as for home Internet users risking their privacy, commercial transactions and corporate data [18].

The problems to be addressed in this report:

- What are the possible attacks that can be used against authentication solutions?
- Which are the multiple features supported by mobile phones?
- How can we provide secure web authentication using mobile phones?
- What are the economic effects on web authentication using mobile phones?

2. Various Authentication Methods

In this section we explain the different types of authentication methods. Authentication is a process through which the identity of an entity is declared, it plays an important role in the field of computing [10]. Several websites and other online services such as e-mail use authentication. In section we discuss different web authentication methods while in the sections following 2.1 we discuss improvements of methods.

2.1 Identifier and Password

Password-based authentication is the most common method of authentication on the web. In this method, before using the application, the user must enter his username or similar identifier. The next step is to enter his password, to verify whether the entered user is allowed to

access the application or not. User inputs are compared with entries stored in a database. If it matches, the user is allowed to access the application, otherwise not.

A more secure alternative to passwords are one-time passwords (OTPs). When using this approach usually a random password is generated by the user. OTPs expire automatically after being used once, so OTPs are resistant to replay attacks since they are non-reusable. They are also resistant to password guessing (online guessing) [12, 13].

Other ways to make password-based authentication more secure are to keep locking the login screen after a specific idle time, close the session automatically, and make the system lockup after a specific number of invalid login attempts. Tunneling is another approach used to increase the security of password-based authentication.

2.2 Biometrics

Biometrics is an authentication method based on physiological or behavioral characteristics of a person.

Physiological characteristics: Finger or hand prints, face recognition, iris recognition, voice recognition etc.
Behavioral characteristics: Signature verification, speech verification, key stroke verification.

While a user logs in to an application using a biometric reader, the reader compares the currently captured sample with the stored biometric sample. If it matches the user is allowed to access the application. The main advantage of this method is that it is resistant to online guessing, since it requires the use of the physical characteristics of the actual user [12]. However, when sending biometric authentication data over a network it can be captured and replayed by an attacker.

2.3 Hardware Authentication Tokens

There are several groups of *authentication factors* of which knowledge factors (e.g. passwords) and inherence factors (i.e. biometrics) are two. A third type of factor is the ownership factor. A common ownership factor is the hardware authentication token, a hardware device which can store or generate authentication data and that is carried by the user. Mobile phones can be used as hardware authentication tokens. Hardware authentication devices are also used in web authentication [12, 16, 17].

By using another authentication factor together with the hardware authentication device, the security can be increased [16].

3. Possible Attacks against Authentication Methods

Password-based authentication is the most widely used authentication method on the web. The most common attacks against this authentication method are brute force attacks, and eavesdropping on web communication to reveal passwords [7].

SQL injection is another type of attack used by attackers to compromise web sites [8, 9]. In this case, the attacker inputs malicious SQL code in a web site form, which can be executed by the server and result in a security breach, for example passwords being revealed to the attacker.

Biometrics can be a more secure form of authentication than passwords since it requires the attacker to use the physical characteristics of the actual user. If an attacker gets a fingerprint sample of the user, it can be used to login to such biometric systems. However, the attacker does not need to capture physical samples if the biometric identifier is sent over a network. In that case, the attacker can capture the authentication data (e.g. the biometric data) during transmission and replay it to act as the user.

If we look especially at mobile phones for authentication the physical security of the devices is important. If the mobile phone is stolen or lost, it can be used by anyone to authenticate them.

One specific type of replay attacks take place when corrupt data is being provided between the sensor and the processor in a biometric system. A replay attack is a multi-level procedure which involves getting hold of data from the sensor then altering it and replaying it in the end. Encrypting the data will solve the problem as intermediate decryption and modification would be required before replay and the required technique will make the system less prone to attacks [18]. This is however not the most common type of replay attack. Replay attacks usually occur over a network when an attacker reuses a user's authentication data to act as the user.

3.1 Shortcomings in Existing Authentication Systems

Computers are usually used by customers to authenticate themselves for online shopping, payments, business etc. Computers usually does not provide the security required

in these cases, and in case a fraud occurs, it is difficult to identify whether the fraud was done by customers, banks systems or a network security breach. For example, recently fraudulent security certificates were issued through the Comodo security firm, which were being used to spoof genuine websites such as Google, Yahoo and Skype, to capture passwords and other sensitive information [1]. This security breach occurred due to the lack of robust security in web browsers. The responsibility lies on many people, not only the Comodo security firm, but also on browser developers. It is difficult to pin point the blame on a single entity. This is also the case in many other scenarios [2, 3]. The main problem is that the user cannot always trust a service provider [3].

4. Mobile Phones and Authentication

4.1 Mobile Phone Features

In this section, we discuss the main features of mobile phones and the different authentication methods supported by mobile phones. The growth of the Internet leads to the development of various web based applications, which people use in their day to day life. If people need various devices for different purposes such as using a telephone to make a call, using a PC or laptop to access websites, using an MP3 player to listen music, using a card reader for online banking, or using a camera to take a photo or record a video, the users need to buy and maintain a lot of equipment. Now one single device, the mobile phone, can be used for all these purposes. This provides convenience and lowered cost to end user.

4.2 Mobile Phones as Authentication Devices

Mobile phones do not only provide many different services in one single device. They can also be used as authentication devices, providing the following authentication methods to the user:

1. Mobile phones can provide knowledge based authentication using passwords.
2. The mobile phone supports biometrics authentication since:

- It has an audio recording device and speakers. Therefore voice recognition authentication can be provided.
- It has a video capture device i.e a camera. Thereby image recognition authentication can be provided.
- Some mobile phones can support external biometric devices for authentication purposes such as fingerprint scanners [11].

The above methods can be used both for authenticating to the phone itself and for storing credentials and running authentication algorithms. In the latter case the mobile phone can be used as an external device for web authentication.

We can even say as the mobile phone is providing hardware token authentication, since a mobile phone is an ownership factor. An ownership factor alone cannot provide security, it need some technique to provide the security. If a hardware token, (e.g. a mobile phone) is combined with a password allocated to a user, it will form an authentication method which can provide security.

5. Possible Solutions to Improve the Security in Authentication Systems

Mobile phones can be used to not only authenticate users but also to store the authentication information. For example a bank can provide authentication software for the user's mobile phone, this can then enable this particular user to use this mobile for authentication for online shopping etc. General authentication with mobile phones requires the following [3, 4]; we apply this strategy also for web authentication;

1. The user must have a device which can support keyboard input, storage of data in encrypted form and display. The device must have the ability to encrypt and decrypt the data.
2. This device can be used by service provider to store user authentication information in it.
3. For security critical applications, the device must authenticate the user by using biometric information such as finger prints, so that unauthorized people cannot use this device. For less critical applications the device can authenticate the user by password authentication.

For ensuring security of data following techniques needs to be followed:

Security Association

For secure exchange of data while ensuring privacy, security associations among system blocks should be

developed. The arrangement is provided by many algorithms of which some imply public key infrastructure whereas some use symmetric keys.

Replay Protection
The user's privacy is shielded from attacks by any interferer during authentication, so chances of unauthorized use and accessing private information can be minimized.

6. Economic Aspects

Economic aspects on web authentication should not only be based on the end user's side, but also from service provider view. The economy factor deals with how trustworthy identity management for web authentication is being implemented between a mobile phone and to a service provided by the service providers. Based on this prices are framed. Today mobile phones are very flexible and portable and can support various web authentication services. If the service provider makes a proper trustworthy identity management plan, which makes if feasible to use a mobile phone as a trusted authentication agent, this will reduce other hardware costs [19].

Using mobile phones can decrease the expenses occurring due to the maintenance and issuing of different hardware such as smart cards, credit cards and RFID chips, and instead the cost shift to the user, who has to buy a device such as mobile phone to be able to authenticate themselves [4].

7. Conclusions

In this article we discussed the different aspects of web authentication. We identified the major authentication methods currently used and their drawbacks. We also discussed the possible attacks which can be targeted against these methods. We discussed a possible solution which can help in improving the security of web authentication system using mobile phones and its economic effects.

The future of authentication methods is quite diverse. One possible future is using mobile phones as a standard for authentication [4]. Beside its advantages to provide multi-level authentication, reduction in cost, convenience for the end user, there are also drawbacks such as the security of the physical device [4]. Using mobile phones for authentication will decrease the cost of deploying systems and software and their maintenance.

References

[1] E. Mills and D. McCullagh. (2011) "Google, Yahoo, Skype targeted in attack linked to Iran". [Online]. Available: http://news.cnet.com/8301-31921_3-20046340-281.html?tag=mncol;txt, accessed: 2011-03-23.

[2] A. Herzberg, "Payments and banking with mobile personal devices," *Communications of the ACM,* vol. 46(5) n.5, pp. 53-58, May 2003.

[3] A. Gaurav, A. Sharma, V. Gelara and R. Moona, 2008, "Using personal electronic device for authentication-based service access," in *IEEE International Conference on Communications*, 2008, pp. 5930-5934.

[4] P. Lin, H.-Y. Chen, Y. Fang, J.-Y. Jeng and F.S. Lu, "A secure mobile electronic payment architecture platform for wireless mobile networks," *IEEE Transactions on Wireless Communications*, vol. 7(7), pp. 2705-2713, July 2008.

[5] W. E. Burr, D. F. Dodson, W. T. Polk, "Electronic Authentication Guideline", *National Institute of Standards and Technology*, *U.S Department of Commerce.*

[7] C. Adams, G. Jourdan, J. Levac and F. Prevost, "Lightweight protection against brute force login attacks on Web applications," in *Eighth Annual International Conference on Privacy Security and Trust (PST)*, pp.181-188, 17-19 Aug. 2010.

[8] X. Wang, L. Wang, G. Wei, D. Zhang and Y. Yang, "Hidden web crawling for SQL injection detection," *3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, pp.14-18, 26-28 Oct. 2010.

[9] A. Tajpour, M. J. Z. Shooshtari, "Evaluation of SQL Injection Detection and Prevention Techniques," *Second International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*, pp. 216-221, 28-30 July 2010.

[10] Motorola corporation. (2011) "Mobile Biometric identification". [Online]. Available: http://www.motorola.com/web/Business/Products/Biometrics/Mobile%20AFIS/Mobile%20AFIS/_Documents/Static

%20Files/Mobile%20Identification%20White%20Paper.pdf?localeId=33

[11] M. Bishop, "*Computer Security: Art and science,*" Addison-Wesley, 2002.

[12] EMC corporation (2011) "One Time Password". [Online]. Available: http://www.rsa.com/glossary/default.asp?id=1064

[13] F. Corella. (2007) "Protecting a Multiuser Web Application against Online Password-Guessing Attacks". [Online]. Available: http://pomcor.com/whitepapers/protecting_against_password_guessing_attacks.pdf

[14] Aladdin corporation. (2008) "Two-Factor Authentication". [Online] Available: http://www.r2technologies.com/pdf/Whitepapers/Security/Secure/Secure%20Computing%20-%20Two%20Factor%20Authentication%20TCO.pdf

[15] Symantec corporation. (2011) "Two-Factor Authentication". [Online] Available: http://www.verisign.com/static/029263.pdf

[16] C. Roberts. (2006) "Biometric attack vectors and defences". [Online] Available: http://otago.ourarchive.ac.nz/bitstream/handle/10523/1243/BiometricAttackVectors.pdf

[17] Hasan, J. Jähnert, S. Zander and Burkhard Stiller. (2001) "Authentication, Authorization, Accounting, and Charging for the Mobile Internet". [Online] Avilable: http://www.tik.ee.ethz.ch/~mobydick/papers/TIK-Report114.pdf

[18] L. Elbaz. (2002) "Using public key cryptography in mobile phones". [Online] Available: http://www.discretix.com/PDF/Using%20Public%20Key%20Cryptography%20in%20Mobile%20Phones.pdf

[19] R. Mallavarapu. (2010) "Trustworthy Identity Management for Web Authentication". [Online] Available: http://www.cse.hut.fi/en/publications/B/11/papers/mallavarapu.pdf