Camera Based Authentication Methods

Rizwan Azhar
Email: rizaz830@student.liu.se
Supervisor: Anna Vapen, annva@ida.liu.se
Project Report for Information Security Course
Linköpings Universitet, Sweden

Abstract

There are many areas where camera based authentication methods are used. These areas involve online banking operations and device authentication etc where a user can be presented with authentication data and capture the data by using a phone camera or another camera equipped device. In this paper we will focus on current research on camera-based authentication and compare the different authentication methods. Finally, we will perform a risk analysis on camera-based authentication and suggest mitigations to possible threats.

1. Introduction

With the passage of time password based authentication is becoming popular due to ease of use. However, it creates a lot of issues [4]. For example, consider a person who has many accounts which are accessed through password based authentication. In this case the user has to remember all their usernames and passwords, which will be difficult. On the other hand, if the person uses one password for all the accounts it will be a single point of failure. Another alternative is to use a camera based authentication method. These methods use means of optically transferring data, which can be combined with other methods like for example optical challenge-response and one time passwords (OTP).

In camera based authentication, different variants of equipment is used such as web cameras, camera equipped mobile phones and dedicated devices. Camera equipped mobile phones would be a good choice in camera based authentication methods as they are available to all users at all times and thus provide high availability. Dedicated devices provide high security and high usability, on the other hand these devices needs to be distributed to all users [13].

Mobile phones have several communication channels which include Infra Red (IR), Bluetooth, Wireless Fidelity (Wi-fi), camera, manual input and sound. Infrared is a short range channel for radio communication which works around 1 meter [3]. It is replaced by Bluetooth technology which is most common today. In radio communication Bluetooth addresses three security concerns which are confidentiality, authentication and authorization by using encryption techniques. WiFi provides high speed internet (11 mbps to 200 mbps theoretical) via radio waves [14].

Optical channels are useful when we have to transfer bulky data in a short interval of time without typing the information. Also, these channels are more efficient and less error prone than sound when work in noisy environment. Moreover Bluetooth, WiFi and Infrared which are also common. On the other hand, cameras are becoming more common in computers, laptops, mobile phones etc [13].

1.1 Methodology

Our focus is to address the questions and problems highlighted in section 2. Section 3 describes the background regarding our project. Section 4 describes different case studies of authentication methods, their security problems and mitigations. In section 5 we compare camera based authentication methods. In section 6 we perform risk assessment. In section 7 we suggest future work and finally in section 8 we draw our conclusion.

2. Questions/Problems

Our report will be based on the questions below.

- How is camera-based authentication used today?
- What are the problems related to camera based authentication methods?
- What mitigations are needed to avoid problems with camera based authentication methods?
- What are the risks involved when using camera-based authentication?

3. Background

There are many authentication methods that can be applied in different situations. We choose to study camera based authentication methods because cameras are becoming popular in devices like computers, laptops, mobile phones etc, thus provide high availability, usability and has the tendency to perform secure cryptographic operations [13].

We have chosen to study Seeing-is-Believing, pixel mapping and optical character recognition in our project on camera based authentication methods. There are also other methods available like 2-clickAuth, QR-TAN and commercial solutions which are described below.

3.1 2-clickAuth

This method is based on optical challenge response solution in which a webcam and camera equipped mobile phone is used for the purpose of authentication. This solution uses two-dimensional bar-codes to provide communication between camera-equipped mobile phone and webcam. This solution has high usability due to its ease of use and easy distribution to users. This solution can be implemented with an identity management system to solve the issues of those users having many passwords and IDs to remember [13].

3.2 QR-TAN

Quick Response Transaction Authentication Numbers is a flavor of TAN which use one time password to make the transaction more secure compare to the static password. QR-TAN uses a method which is best suited for web based applications; it uses two dimensional QR codes based on transaction-signing with the help of a trusted device. This device can be a mobile phone with a display and a camera with a modest resolution. Transactions can be performed completely offline without any network connection if smart card technology is used with QR-TANs. By not requiring network capabilities on the trusted device, mobile TANs properties can be improved. It provides security by using secure encryption techniques in case if an attacker gains access to the trusted device [8].

3.3 Commercial Solutions

There are some commercial solutions available for camera based authentication methods. Two of them are discussed below.

3.3.1 Flicker TAN

In this solution encrypted flickering images are used to perform the secure transaction. This solution is quite similar to the German CAP system (HHD 1.3) [7] with respect to versatility and security features. It is easier to use because there is no need to type the information twice thus increases usability. On the other hand this solution needs a specific hardware device and a card to perform the secure transaction. Flickering images may be annoying for some users and may cause epilepsy if the refreshing rate is between 3-60 Hz [8].

3.3.2 Cronto Photo TAN

This solution uses encoded custom 2-D barcodes to perform the secure transaction. This solution is more flexible than German CAP system (HHD 1.3) as it allows free text. This solution includes mobile phones having features like Java, Blackberry, Android, Symbian, iPhone, etc. The mobile phone usage is personal so in this sense it is more protected. It is used by Commerzbank [8]. Online banking instructions for mobile application customers can be securely verified with the help of photoTAN. The risk for authorization of deceptive transactions and difficulty for manual transactions can be eliminated by Cronto visual signing technology [9]. The encrypted visual channel is created for the authentication of secure transactions. A graphical cryptogram comprises a set of colored dots which is displayed on the customers monitor. The customer then captures the graphical cryptogram by using a mobile phone camera. Cronto software which is already available in mobile phones is then used for authentication [15].

3.4 Authentication Factors

The authentication methods categorizes in three ways. These methods can be combined with each other to provide multimodal authentication [16].

- Knowledge factors: some-thing you know (Passwords, PIN etc)
- Ownership factors: some-thing you have (Smart Cards, Tokens etc)
- Inherence factors: some-thing you are (Biometrics etc)

3.4.1 Knowledge Factors

Knowledge factors include passwords, one time passwords (OTP), PIN etc. These methods are mostly used for authentication purposes. In password based authentication method the user provides an identity and secret to authenticate him/her self. If the

combination of id/password is correct then the user will be authenticated, otherwise rejected [10].

3.4.2 Ownership Factors

Common examples of ownership factors are smart cards, USB-sticks, dedicated devices etc. Let us consider smart card to understand the concept of ownership based authentication. Smart cards are quite similar to a credit card (all credit cards are not smart cards) having an embedded programmable micro chip for secure user authentication. In this method user put the card into the card reader, the card reader reads the user information through chip and use that information for authentication purposes. Smart cards are mostly use in online banking and need a card reader for performing secure transactions [12].

Ownership factors can be combined with one time passwords (OTP) and challenge response methods. In these kinds of authentication methods the user provides username and the authentication server generates random challenge in response. The user uses this challenge with his card and four digits PIN to generate result with cryptographic operation. This result is then sent to the server. The server verifies the result by performing the same operation, if the result of the user and server matches, the user will be authenticated [20].

3.4.3 Inherence Factors

These factors involve physiological or behavioral characteristics of users for the purpose of authentication. Physiological characteristics include finger print, facial characteristics, retina scan etc; however behavioral characteristics include key stroke dynamics, traits etc. The biometric samples of these characteristics are enrolled in database which then compared with the given sample to authenticate specific user. During authentication false acceptance and false rejection may occur. False acceptance rates can be decreased by allowing less variation while false rejection rates can be decreased by allowing variation. Both types of failures can be reduced by balancing allowed variation [11].

4. Case Studies

This section describes different case studies to explore the problems and mitigations related to camera based authentication methods.

4.1 The Untrusted Computer Problem and Camera-Based Authentication

The first case study is regarding untrusted computer problem and two camera based authentication methods which solve this problem. Let's consider a user uses an untrusted computer (via an Internet cafe etc) to contact a bank in order to manage her stocks and placing orders. In fact the user is interacting with a Trojan horse without knowing as the interface looks exactly as expected and has no idea what's going on inside the computer. The Trojan horse can store users's password, can simulate the whole session with the bank and it show misleading information. The untrusted computer has access to all information user enters and what is displayed to the user.

Consider a user having trusted personal device. The trusted proxy which is connected to the trusted banking server. User, device and proxy can interact through a channel which corresponds to the untrusted computer. Mostly the channel is faithful but not always. The user, trusted device and proxy have shared secrets for cryptographic operations [1].

4.1.1 Camera Based Solution

Two camera based authentication methods to solve the untrusted computer problem have been proposed. Both of these proposed implementations user must be used with a camera based device to monitor untrusted computer screen. The content displayed on the screen would be in image form.

4.1.1.1 Pixel Mapping

In this method the camera equipment is supposed to be completely still on the screen during the dedicated authenticated session because pixel mapping is done by capturing very detailed image. During the initial calibration phase, mapping between screen pixels and camera based pixels have been reformed. The device will use this mapping to rebuild the screen content. At the bottom of the screen the small area will be chosen to transmit the nonce, a one time password and a MAC.

During *downward authentication* the proxy sends information, encrypted nonce, encrypted one time password and MAC to the user, which looks like an image. The device then compares information received from proxy to the information it calculates from the screen through camera. If both information matches then one time password will be displayed on the device screen. After reading the one time password from screen it is sent to the proxy via upward authentication, this is called *secure approval*. For *upward authentication* all the information is directly sent to the proxy as the user types on the utrusted computer.

Calibration: This process is used to validate the screen content with the camera content in order to check whether the untrusted computer has tampered

the information or not. During this process camera must be still. The mapping between screen pixels and camera pixels is established if each screen pixel is seen by at least one of the camera pixels. These valid pixels later used to generate the screen image [1].

4.1.1.2 Optical Character Recognition (OCR)

In this method it is assumed that the user's device is equipped with a camera and has an infrared link to the untrusted computer. This link is used to exchange data with the proxy, via the untrusted computer, to take advantage of the large amount of data available at the proxy. The information is stored in the image, by using OCR function in user's device that information is retrieved. This information is later used for authentication purposes [1],[17].

Downwards Authentication: During downward authentication the proxy send information in image form to the untrusted computer which appears on the screen. The device takes a picture of the screen and calculates the encrypted nonce and MAC. After that via infrared link all this information including the picture is sent to the proxy in the form of a data packet for verification purposes. The proxy checks the MAC and nonce, if all checks passes it means by performing OCR on the received picture, the text displayed on the screen was genuine. The proxy acknowledge to the device in the form of (yes, encrypted nonce, MAC). The device again check the nonce and MAC, if all check passes then it shows the green light.

Upwards Transmission: The user types commands with the help of the untrusted computer. All those commands are sent to the proxy directly.

Secure Approval: The user accepts the data on the screen by using the device. The device takes a picture of the screen, and sends ("accept", picture, encrypted nonce, MAC ("accept", picture, encrypted nonce)) to the proxy. By using downwards authentication the proxy verifies the message. If all the checks pass then it approved the picture [1].

4.2 Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication

Day by day the use of mobile phones is increasing due to the fact that mobile phones are merging all the technologies from multimedia to computing [5]. In this way the availability of computing increases but on the other hand it also increases the possibility of security threats. Today's mobile phones have enhanced features which includes a high quality display, a good quality camera, and a range of communication technologies like Infrared, Bluetooth and Wi-Fi. Also, modern phones are strong enough to carry out secure cryptographic operations.

4.2.1 Barcode Authentication

Mobile phones with an integrated camera have potential of taking images and analyze those images. Two-dimensional barcodes such as QR-codes [19] can be used to create a visual channel between the mobile phone camera and communicating device. Quick response (QR) codes are good enough because they are fast, reliable, simpler and easier to use, while capturing images with mobile phones. In order to create a visual channel with the help of QR-bar-codes, the user creates a bar-code encrypted with the public RSA key of other user and display this encrypted bar-code on the electronic screen whereas the other user then acts as view finder and capture the encrypted bar code while positioning the camera, now the bar code recognition algorithm process starts and the image is decrypted with the user private RSA key [2].

4.2.2 SiB Versatility

In the SIB protocol different kinds of devices exist, which include camera with display, camera only, display only and barcode sticker. These devices can connect in different ways such as camera only devices connect with barcode stickers or camera with display devices connect with bar code sticker, thus creating different levels of security. Let's consider one example where both devices have the same capabilities which are camera and display. In this particular scenario both devices can mutually authenticate each other as they both posses a camera, moreover they have the potential to use long term public key or exchange the public key in any instance while showing the newly generated barcode on their electronic screen [2].

4.2.3 SiB Protocol

The SiB protocol starts with the discovery of neighboring devices through wireless medium like Bluetooth on their own devices. The discovery process can be accomplished with the friendly names given to the wireless devices so that the users easily recognize each other. It is also necessary that one device should be listening when the other device is connecting to this device. Now the user at each end of the communication channel estimate channel a commitment to their public keys and then encrypts a barcode with this information. This key can be used for the whole session or the key can be regenerated

by following the same procedure. Then the pre-authentication stage begins in which both users capturing an image of a barcode from the other user's device. The order of capturing images is not so important. After the pre-authentication stage both devices possess commitments to the other device's public key. These devices then execute the same commitment on the other device's public key to make sure about the previous result of the commitment, thus providing mutual authentication. These authenticated keys can then be used with other public key protocols like SSL etc on the wireless medium. In this way SiB provide demonstrative identification between the communication devices.

4.2.4 SiB and TPM

Presence of Trojans and other malware cannot be neglected. They will steal the secrets of the running program and cause damage to the system. A mobile phone having a keypad, a display and a typical operating system like Symbian, can be insecure if the communication is performed via keypad input. Therefore there is a need to create trusted path modules (TPM). Because of phone keyloggers and other malware, one solution is that the mobile phone camera securely configure the TPM and in order to securely configure the TPM we need to involve Trusted Computing Group(TCG). TCG is a non profit organization which is developed to define standards for trusted computing based on an open, vendor-neutral approach [18].

In the TPM scenario the mobile user only input the Owner Authorization Data (OAD) via keyboard, and according to the TCG specification each TPM comes with public/private endorsement key pairs. The public key is used for encryption and the private key for decryption while connecting with the TPM [2].

5. Comparison

In this section we compare the camera based authentication methods which we have used in our report. These methods include pixel mapping, optical character recognition (OCR) and Seeing-is-Believing (SiB). Table 1 below shows a comparison of camera based authentication methods. We have chosen these features based on the facts that these are the most important in the camera based authentication methods which we have chosen to study in our project. An encrypted nonce prevents from replay attacks as well as active attacks. Bidirectional authentication is required for both parties to authenticate each other in order to prevent from intruders. Trusted platform modules ensure the information integrity within the device by using public/private keys. Calibration and fixed camera is required in SiB while in OCR calibration is not require and the camera can move. SiB is more flexible in the sense that it does not require camera based devices on both ends of communication however pixel mapping and OCR must require camera based devices at user end. Usability involves ease of use which is much higher in pixel mapping and OCR due to the fixed device configurations. Availability is high in all methods because devices which we have used are mobile phones. If dedicated devices are used instead of mobile phones, availability will be low.

Features	**Camera based authentication methods**		
	Pixel Mapping	**OCR**	**SIB**
Encrypted Nonce	Yes	Yes	Yes
Active/replay Attacks	No	No	No
Bidirectional Authentication	Yes	Yes	Yes
TPM	No	No	Yes
Calibration	Yes	No	Yes
Device Capabilities	Fixed	Fixed	Flexible
Usability	Higher	Higher	High
Availability	High	High	High

Table 1: Authentication methods comparison

6. Risk Analysis

Risk measurement in online banking and device authentication on camera based authentication methods is challenging due to high security requirements [6]. In this section we have followed risk management framework (RMF) to perform the risk analysis [16]. RMF consists of five stages. We performed the risk analysis by using these fundamental activity stages.

i. Understand the business context

This stage involves understanding of business goals, priorities and circumstances, which are helpful to identify risks. Business goals may include business revenue, reduce development cost and give high Return On Investment (ROI). The business context includes ease of use, device availability and interoperability.

ii. Identify Business and technical risks

Business risks may include *usability* and *device availability*. Risks related to *usability* are that the devices are becoming more complex, so in this case devices may not provide ease of use which might affect business. However the risk involved with *device availability* is that if we use dedicated devices instead of mobile phones then users have to carry those devices which may affect business, as without those devices user cannot perform his operations.

Technical Risks involved with OCR are image capturing distortions which may leads to *false rejection*. In OCR higher requirements are needed for *camera resolution* and computation power may which leads to infeasibility of implementation on current mobile phones which results in availability risks. As in OCR the users device has an infrared link to the untrusted computer to contact the proxy. This link provides *weak security checks* so an intruder may attack by exploiting this channel.

The risk involved with SiB is that the attacker may try to read the *pixels of the QR code* and then display this code to the user while using malicious applications. Another risk associated with SiB is that the attacker may vary the *lighting condition* of the authenticated environment and disrupt the process of SiB which may lead towards the denial of service.

iii. Synthesize and prioritize risks

In this stage we have prioritized both business and technical risks while considering the criticality of those risks. Risks priorities are assigned below.

1. Device availability
2. Usability
3. False rejection
4. Pixels of QR code
5. Weak security checks
6. Lightening conditions
7. Camera resolution

iv. Define the risk mitigation strategy

Risk mitigations are described in this stage. In order to mitigate risks regarding device availability, mobile phones, smart phones and PDAs should be used. In this way the user doesn't carry extra dedicated devices which increase device availability. With respect to usability the device should provide ease of use with a user friendly interface which will increase usability. False rejection rate can be decreased by using reasonable picture quality and distortion reduction techniques. In order to reduce the risk regarding pixels of the QR code, the window manager ensures that other application doesn't read the pixels of the screen and the user specific application pixels must be inaccessible to other applications.

The risk of weak security checks by using an infrared link in OCR can be reduced by using Bluetooth, as it contains a strong security mechanism during data transfer which minimizes the risk. However there are risks involved with Bluetooth as well. These includes, eavesdropping which may results in unauthorized access by attacker. The lightening conditions risk can be mitigated by ensuring that the light sensitivity of authenticated devices works only with a certain threshold of sensitivity and besides this threshold these devices doesn't work. The camera resolution risk can be mitigated by using pixel mapping as it does not require high resolution. Pixel mapping can work with black and white images.

v. Fix the Problems and Validate the Fixes

This is the last stage of risk analysis. In this stage we try to refine the mitigation strategy that we have developed in stage iv. If the dedicated devices are used, they must ensure a user friendly interface and portability factors. False rejection rate is mostly related to distortion, so by implementing distortion reduction techniques it can be decreased.

7. Future work

There are different types of camera based authentication which can be used in different environments depending on the specific requirements. In camera based authentication methods mobile phones are becoming more popular. Today mobile phones are equipped with advanced features. However, it increases the complexity of mobile phones. It in turn leads towards the malware risks where malware can steal or corrupt sensitive information on mobile phones. In future work the risks regarding malware need to be considered to avoid stealing/corruption of sensitive data.

The complexity of mobile phone is increasing day by day which may decrease the usability. Thus by advancing the features of mobile phones the concept of usability should be considered. This can be studied in future to enhance the usability aspects. More systems can be evaluated in more detail i.e. QRTAN, Cronto photo TAN, Flicker TAN and 2-clickAuth.

8. Conclusion

In this paper we have discussed how different camera based authentication methods are used these days by describing 2clickAuth, QRTAN, Cronto photo TAN, Flicker TAN, pixel mapping, OCR and SiB. However our main emphasis relies on pixel mapping, OCR and SiB. We found that the problem of user authentication via untrusted computer can be removed by using pixel mapping, OCR and SiB. The comparison of these methods shows that SiB is more appropriate and secure.

9. References

[1] M. Burnside et al, M. V. Dijk, "The Untrusted Computer Problem and Camera-Based Autentication" PP 114-124, 2002.

[2] J. M. McCune, A.Perrig, M.K. Reiter "Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication" PP 43 – 56, 2009.

[3] Infrared Data Association http://www.irda.org [Accessed: May 4, 2010]

[4] Password based authentication http://www.ece.cmu.edu/~adrian/projects/usenix 2000/node2.html, [Accessed: March 23, 2010]

[5] Cell phone usage. [Online], Available http://www.cellular-news.com/story/30323.php [Accessed: March 20, 2010]

[6] Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment", 2001

[7] S. Drimer, S. J. Murdoch, and R. Anderson, "Optimised to Fail: Card Readers for Online Banking", December 29, 2009 Berlin Germany

[8] G. Starnberger, L. Froihofer and K. M. Goeschka, "QR-TAN: Secure Mobile Transaction Authentication", International Conference on Availability, Reliability and Security, 2009

[9] Business Wire,"CRONTO". [Online]. Available: http://www.businesswire.com/portal/site/home/ template.PAGE/permalink/?avax.portlet.tpst= c3eb0ec6c81ef7157972709ddb808a0c_ws_MX& javax.portlet.prp_c3eb0ec6c81ef7157972709ddb 808a0c_newsLang=en&javax.portlet.prp_c3eb0 ec6c81ef7157972709ddb808a0c_viewID=news_ view&javax.portlet.prp_c3eb0ec6c81ef7157972 709ddb808a0c_newsId=20081113005401&bean ID=1933350696&viewID=news_view&javax. portlet.begCacheTok=com.vignette.cachetoken &javax.portlet.endCacheTok=com.vignette.cach etoken [Accessed: March 15, 2010]

[10] SANS Organization, "Authentication Methods". [Online]. Available: http://www.sans.org/reading_room/whitepapers /authntication/overview-authentication-methods-protocols_118 [Accessed: March 15, 2010]

[11] National Institute of standards and Technology, "Biometric Authentication". [Online]. Available: http://www.itl.nist.gov/div893/biometrics/Biom etricsfromthemovies.pdf [Accessed: March 16, 2010]

[12] Tech Target, "Security token and smart card authentication". [Online]. Available: http://searchsecurity.techtarget.com/tip/0,289 483,sid14_gci1338503,00.html [Accessed: March 15, 2010]

[13] A. Vapen, D. Byers, N. Shahmehri,2-clickAuth-Optical challenge-Response Authentication, ARES, 2010

[14] IEEE Standard Association. [Online]. Available: http://standards.ieee.org/getieee802/802.11.html [Accessed: March 18, 2010]

[15] Cronto Limited. [Online]. Available: http://www.cronto.com/visual_cryptogram.htm [Accessed: April 13, 2010]

[16] Risk Management Framework. [Online]. Available: https://buildsecurityin.uscert.gov/bsi/articles /best-practices/risk/250-BSI.html [Accessed: April 16, 2010]

[17] M. Alzomai, B. Alfayyadh, and A. Jøsang, Display Security for Online Transactions, University of Oslo, Norway

[18] Trusted Computing Group. [Online]. Available: http://www.trustedcomputinggroup.org [Accessed: April 10, 2010]

[19] Denso Wave Inc, "QR Code.com". [Online]. Available: http://www.denso-wave.com/ qrcode/index-e.html [Accessed: April 15, 2010

[20] Building internet firewall. [Online], Available http://docstore.mik.ua/orelly/networking/firewa ll/ch10_03.htm. [Accessed: April 27, 2010]