September 2015

Authentication Via Multiple Associated Devices

Jean-Baptiste Subils
University of South Florida, subils@mail.usf.edu

Authentication Via Multiple Associated Devices

by

Jean-Baptiste Subils

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Science
Department of Computer Science and Engineering
College of Engineering
University of South Florida

Major Professor: Jay Ligatti, Ph.D.
Dmitry Goldgof, Ph.D.
Yao Liu, Ph.D.

Date of Approval:
May 26, 2015

Keywords: Security, access control, authorization

ACKNOWLEDGMENTS

I am grateful to Cagri Cetin, Dr. Jay Ligatti, and Dr. Dmitry Goldgof for their precious and constant help on this project. I would like to thank Glenn Whichard, William Munnerlyn, Sarah Murphy, and Nair Gayatry, for their help through the patent application process. I also would like to thank Ian Markwood and Benjamin Dunn for their help with proofreading and revisions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This thesis presents a practical method of authentication utilizing multiple devices. The factors contributing to the practicality of the method are: the utilization of devices already commonly possessed by users and the amenability to being implemented on a wide variety of devices. The term “device” refers to anything able to perform cryptographic operations, store data, and communicate with another such device.

In the method presented herein, multiple devices need to be associated with a single user to provide this user an identity in the system. A public key infrastructure is used to provide this identity. Each of the devices associated with a user possesses a public and private key which allow cryptographic operations to be performed. These operations include signing and encrypting data and will prove the identity of each device. The addition of these identities helps authenticate a single user.

A wide variety of devices qualifies to be used by this authentication method. The minimum requirements are: the storage of data such as a private key, the ability to communicate, and a processor to perform the cryptographic operations. Smart devices possess these requirements and the manufacture of such devices can be realized at a reasonable cost.

This method is malleable and implemented in numerous authentication protocols. This thesis illustrates and explains several instances of these protocols.

The method’s primary novelty is its resistance to theft-based attacks, which results from the utilization of multiple devices to authenticate users. A user associated with multiple devices needs to be in possession of these devices to correctly perform the authentication task. This thesis focuses on the system design of this novel authentication method.

CHAPTER 1

INTRODUCTION

Access control is a critical feature of a secure system, aiming to protect against unauthorized access. Diverse authentication methods are used to determine the identity of an entity, which is authorized to access the secure system depending on the authentication results. An entity is any active agent capable of performing computation where any sort of computation is included, and the active agent computation can be a result of a human's action [1]. The authentication results are used by an access control system to determine the permission of the entity requiring access.

1.1 Authentication

Authentication methods are diverse but generally belong to three main categories. Each uses a particular attribute of the entity requiring access in order to identify it. These three attributes, or factors, correspond either to something the entity knows (i.e. knowledge), something the entity has (i.e. possession) or something the entity is (i.e. inherence) [2]. Although these categories are the most prevalent, others have been developed [3]. For example, Denning and MacDoran [4] present a location-based authentication which could be categorized in where the entity is (i.e. location).

A popular form of authentication is the pairing of a login and a password, which is used by the majority of web services and organizations. However, some companies recognize the weakness of a password and use an additional factor to identify individuals. This factor is generally a security token but can also be a biometric trait. These authentication methods are subject to many vulnerabilities [5]. Biometrics, passwords and tokens are subject to theft.

The most common knowledge-based authentication method is the utilization of a unique combination of a login and a password. For example, to access a email account users have an unique identifier and a secret password to validate their identity. This method can determine the identity of a specific user, however the knowledge of a user can be used to determine the affiliation of this user with a specific group. For example the utilization of CAPTCHA attempts to separate human from Artificial Intelligence [6].

A physical key is a prevalent object to gain authorization to access a system. This old technique is still in use and efficient. Physical objects have evolved as technology has been developed. Users now have magnetic cards and electronic devices in their possession to be identified. Many implementations have been developed, which serve diverse purposes, using magnetic cards or electronic devices.

The inherence of a human can be, but is not limited to, the biometrics associated with this particular human. Biometrics are the various measurements of biological and behavioral traits specific to a human [7]. Authentication methods utilizing biometrics have been implemented and are used. The common features used to identify a person are the following: Voice, Eye, Face, and Fingerprint.

A multi-factor authentication method combines different factors from the three categories presented previously. An example of multi-factor authentication is the utilisation of Automatic Teller Machine (ATM). These machines require a card and Personal Identification Number (PIN). So the two factors combined are:

- Possession (the card)

- Knowledge (the PIN)

Any combination of two or more of these categories presented can be considered as multi-factor methods. If another category is introduced it can also be argued that the combination of this new category with any of the previous is multi-factor.

1.2 Emergence of Technology

Smart devices (e.g. smart watches, smart television) are popular, and even if they currently remain expensive, they are becoming more affordable over the years. Most people will soon possess multiple electronic devices [8].

Since people start using multiple device the authentication method presented can be applied because it utilizes at least two devices in order to identify a user. The term "device" refers to anything able to perform cryptographic operations, store some data, and communicate with another such device. The requirements for a device to perform this authentication method are not stringent and allow a broad range of devices to be used.

1.3 Approach

This thesis presents a novel, practicable, and robust method of authentication utilizing multiple devices.

The factors contributing to the practicability of the method are: the utilization of devices, commonly possessed by users and the amenability to implement on a wide variety of devices. This method utilizes only one factor, twice.

A user can be associated with n devices and is required to perform the authentication with m devices. m need to be greater than two, in order to maintain the robustness against the theft of one device property of this authentication method. This authentication method is robust against the theft of k devices with $k < m$. m can also be less than n to allow loss of devices. A user can lose $n - m$ and still be able to perform the authentication task because this user still possess m devices.

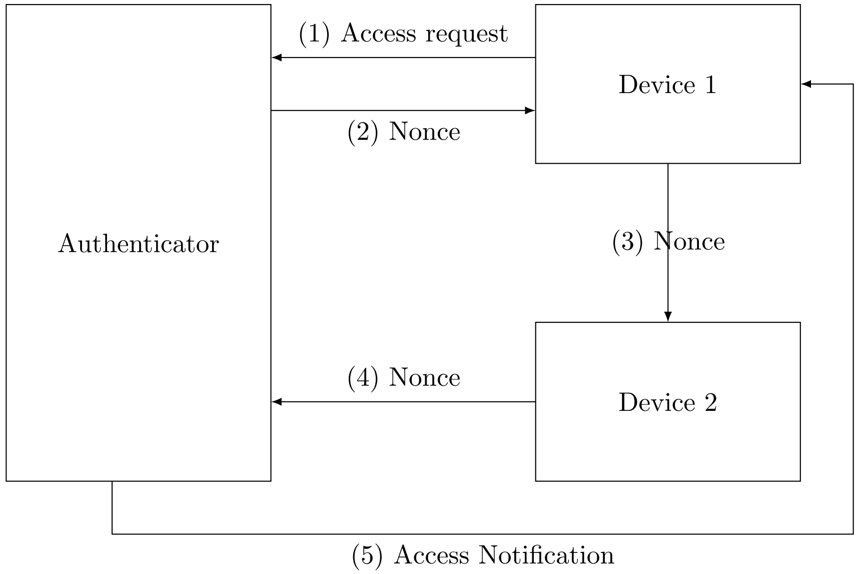

Figure 1.1. Overview of a specific simple authentication performed.

In a two-factor authentication method, if one factor is accessible by an attacker then this attacker would still need the second factor. The authentication method presented here uses a similar idea; if a user's device is stolen, the attacker will still need a second device associated with the stolen one. This method only uses one factor, but it can also be combined with other factors.

In the Figure 1.1, an example of a protocol based on the authentication method presented herein is illustrated. This specific protocol requires two devices to perform the authentication task. The authenticator is the service in charge of authenticating the entity requiring access to some protected resource(s). Any access request is redirected to this service. As shown in the Figure 1.1, Device 1 is requesting access to some resource(s) through the authenticator. Then the authenticator send back a nonce to Device 1. Now, Device 1 has to transmit this nonce to Device 2. To complete the authentication task, Device 2 needs to send the nonce to the authenticator. Finally, the authenticator notifies Device 1 if it can access the resource(s) requested depending on whether or not the information received is correct. These communications are signed and/or decrypted by the private key stored on each device during the registration phase. The communication between Device 1 and Device 2 does not necessitate these cryptographic operations since the authenticator is not monitoring it.

This approach is generalized to an arbitrary number of devices. Instead of one response from the additional device, the device which is not requesting access, the authenticator requires multiple responses. This will be further explained in Chapter 4.

1.4 Attack Vector

An attacker could attempt to usurp a user's identity by stealing a paired device. This attacker would gain access to the private key associated to this device, which is the primary tool to identify a user. Thus, in this paper, the theft of one device can also refer to the theft of only the private key.

To effectively usurp the identity of a user, an attacker needs to gain access to multiple devices associated with this user. The exact number is the number of devices required to perform the authentication task. This number can vary depending on the specification of the protocol, which will be explained in details in the following chapters.

1.5 Summary

This thesis focuses on the system design of this novel authentication method. Cagri Cetin's thesis focuses on the implementations of the authentication method presented herein [9]. The novelty of this method is not the multiple utilization of the same factor, but how this factor is used.

Various factors can be used in an authentication protocol, and the authentication protocols presented herein utilize the possession factor. This factor has advantages and disadvantages further explained Chapter 2 and Chapter 5.

This work provides evidence supporting the thesis that there exists a method of authentication based on n devices that is secure against the theft of $k < n$ devices. The n devices are the devices required to perform the authentication task. These n devices are, in the method presented herein, associated with a specific user. This association allows the authenticator, which is the entity verifying the identity of a user, to determine whether or not a specific user can access some resource(s).

The remainder of this thesis is organized as follows: Chapter 2 reviews the prior state of the art, Chapter 3 details multiple protocols, using two devices, resulting from the authentication method presented, Chapter 4 also details multiple protocols, but using three devices, and then generalizes to an arbitrary number of devices, Chapter 5 analyzes the current state of the novel authentication method, and then illustrates different instances of utilization of this authentication method, and finally Chapter 6 proposes future research and improvements that can be explored, and finally concludes.

CHAPTER 2

RELATED WORK

Access control is an important field in which authentication is a crucial component. Both academia and industry are actively working on improving current authentication methods. There are several good textbooks surveying the field of access control [1, 10, 11, 12, 13].

2.1 Knowledge

Authentication methods can use specific knowledge to determine the identity of a user. The most popular knowledge-based authentication method is the combination of a login and password, but other popular methods using the knowledge of a user have been developed. For example, challenge-response authentication methods provide a challenge, usually an image or a question, that needs to be answered, by either identifying the image or answering the question.

Some of the protocols implemented from this model are used to identify specific users [10]. However, not all the methods are used to verify the identity of a specific user; for example, CAPTCHAs only differentiate humans from Artificial Intelligence [6].

2.1.1 Advantages

The popularity of passwords comes from the simplicity of implementation and deployment of this method. Indeed, the minimum requirement is for the users to remember a string of characters that the system also knows. This string can be restricted by the number or by the type of characters in it, but this is an optional enforcement. This authentication method can be implemented at a low cost.

Another advantage for users is the possibility to reuse passwords for multiple systems. Users can choose a universal password for all the applications they use. This factor is mainly used for web services, with the combination of a login and a password. Thus, this method allows users to access resource(s) from remote locations and with most electronic devices. Sharing a password can also be considered an advantage. Two users may need or want to share access to the same resource(s) and, therefore, can share a password to access it.

2.1.2 Disadvantages

Passwords need to be memorized, which can cause insecure behavior from the users. A user can choose an easy password and reuse it for multiple systems. A password that is easy to remember is often also a password easy for an attacker to guess. An attacker could either use social engineering or brute force. Social engineering could be used to manipulate users to give information from which that attacker would deduce their passwords. The re-utilization of a password for different systems is not a good practice because if an attacker has a user's password for a specific system, then the attacker can access all systems where the user reused this password.

CAPTCHA has been implemented in various ways. However, some of these implementations do not successfully distinguish humans [14, 15].

2.2 Possession

A physical key is the most popular token used in an authentication method. Tokens have evolved and are present now as magnetic cards or electronic devices, often called security tokens. The mechanisms used to verify the validity of tokens are various. For example, doors usually require a physical key to unlock and the verification mechanism is the pins inside of the lock that will open the door when aligned by the specific cuts on a key.

Magnetic cards can be used to unlock doors, and they became a popular alternative to physical key due to the programmability of the card itself and the door readers. Magnetic cards are a good solution for many organizations that need rekeyable locks, such as lodging organizations.

Security tokens have been recently developed and have different implementations. These security tokens have to be carried by users to prove their identity. Two main implementations can be distinguished: symmetric and asymmetric key cryptography. In symmetric key cryptography, a shared seed is used to generate a random number, and in asymmetric key cryptography a private key is used to sign an authentication message [10].

2.2.1 Advantages

The noticeability of usurpation with this form of authentication is an undeniable benefit. A missing object used to authenticate into a system can alert the user of a possible attack. Also copying a security token can be argued as more difficult than the copying of a password. Security tokens are supposed to be constantly carried by users, therefore an attacker must physically access the tokens, which the users would notice.

2.2.2 Disadvantages

Many flaws persist in the actual electronic tokens available. Indeed, Biryukov, Lano, and Preneel [16] have exploited some of the vulnerabilities specific to RSA SecurID, a popular security token used in many organizations [3]. Also, providing an additional device to users leads to inconveniences both on the user side and the provider side. The main inconvenience for a user is the obligation to carry the token at all times; and if the user does not, the security of the system is greatly weakened. On the provider side, the cost of the token is the main issue.

Losing the token used to authenticate is inconvenient. The user cannot access the system anymore and another token needs to be issued. This issuance of a new security token can be long, and this loss represents a cost for the provider.

2.3 Inherence

Inherence is a fundamental aspect of an entity. For a human, inherence can be a biological trait or a behavioral feature. Various authentication methods have been implemented using these aspects [7]. Some authentication methods use fingerprints, eyes, or faces to recognize a specific user [17, 18, 19]. These biological traits are considered unique in order for an authenticator to verify the identity of users. Biological traits are not the only inherence factors used; behavioral features can be used. Signatures, for legal documents, are an example of a behavioral characteristic. The combination of both behavioral and biological aspects can be used such as voice recognition [20].

2.3.1 Advantages

An attractive aspect of this factor is its uniqueness. Biometric and behavioral traits used in authentication protocols have been argued as unique for every human. Similarly to the security token, some of the biometric traits can be noticed if stolen or copied. For example, copying the iris of someone cannot be done by simply taking a regular picture of someone's face. The biometrics of human is also attractive because every human is supposed to have the trait required.

2.3.2 Disadvantages

The cost of implementing authentication methods using biometrics, in particular, is usually expensive. Complex readers need to be developed and deployed to accept such factors. Also, in some cases it is possible for someone to not have the biometric trait required. The behavior of users is used as an inherence factor and argued as unique. For example, the typing patterns called keystroke dynamics have been argued as unique and are used by some authentication methods. However, Meng, Gupta, and Gao [21] proved, through a teaching tool named Mimesis, that it is relatively easy to learn the keystroke dynamics of a user in order to mimic them. Thus, even if a trait is unique it should also not be easy to reproduce. Signature authentication methods possess flaws because signatures need to be checked. This verification can contain false positives. Indeed, M Kam, G Fielding, R Conn, and K Gummadidala exposed this false positive presence in the verification process of signatures [22, 23, 24].

2.4 Multi-factor Authentication

A multi-factor authentication method refers to a method combining different factors from the three categories presented previously. A novel authentication method can be argued as using a different factor than the ones presented, therefore any combination of this novel factor with any of the three main factors can be considered a multi-factor authentication. Bank cards are a good example of the combination of possession and knowledge. To use a bank card, a user needs this card and also a secret that is either a Personal Identification Number (PIN) or a signature. The possession factor is the bank card itself and both the PIN and the signature are knowledge factors.

2.4.1 Advantages

Multi-factor authentication methods carry on most of the advantages of the factors combined. In the example of a bank card, the noticeability of usurpation is present, if the card is stolen, and using a signature or a PIN keeps the implementation simple. Also, since multiple factors are used it creates multiple barriers to go through for an attacker. Thus, any proper combination of two factors can be considered more secure than the use of only one of these factors.

2.4.2 Disadvantages

Similarly, the advantages brought by combining factors, multiple factor authentication carries on the weaknesses of the factors combined. Also, multi-factor authentication implementations are less user-friendly than implementations using only one of the factors used in multi-factor authentication. Combining a password and a security token is less user-friendly than using only a password or only a security token.

2.5 Contribution to the State of the Art

The authentication method presented in this thesis utilizes the possession factor multiple times. The advantages procured by the possession factor, such as noticeability of usurpation, are present in this method. Some of the disadvantages brought by the possession factor, such as the cost associated with tokens, is diminished by the utilization of devices already in the users' possession. The user-friendliness is enabled here by the possibility of not requiring any action from the user. The access request, as well as the challenge, can be triggered by a proximity based mechanism in some implementations. In the case where a user loses a device, this user can still access the system if the number of devices required to perform the challenge is less than the number of devices associated with this user. The method presented can have various implementations, therefore some of these implementations may be inconvenient in the case where a user loses one device. However, it is possible to design a protocol in such a way that if some devices are lost, it does not affect the user as much as a single security token protcol would. This specific design will be further discussed later on.

CHAPTER 3

SYSTEM DESIGN FOR TWO DEVICES

This chapter presents the design of the authentication method. The authentication protocol resulting can differ, and this chapter presents only one specific protocol using two devices. This authentication protocol necessitates the users to have their identities established. The identity establishment, which is explained in detail in Section 3.1, is assumed to be performed properly and the proper devices are associated. This protocol also utilizes the public key infrastructure to provide an identity for each device which then provides the identity of the entity using these devices. Therefore the public key infrastructure is considered sound and secure against network attacks. These assumptions are expected to hold in any scenario and application of the method presented in this thesis.

The number of devices associated with a user depends on the specifications of the protocol used. A minimum of two devices is required to perform the authentication task in order to maintain the robustness against the theft of one device. The number of devices required to perform the authentication task should not be greater than the number of devices associated with each user, otherwise the authentication will not be possible. The maximum number of devices associated with each user is set to two in this section.

This set is limited to two devices for simplicity and clarity, and in Chapter 4 the authentication method is generalized to an arbitrary number of devices.

3.1 Identity Establishment (Device Registration)

In the multi-device authentication system presented each user needs to have an identity in order to be authenticated. As explained previously two devices will be associated with a single user throughout this chapter. During this identity establishment private keys will be generated for the associated devices. This thesis does not focus on the identity establishment which can be done in various ways and is assumed to be performed properly.

3.2 Authentication Protocol

All authentication methods could be viewed as requiring a response to some challenge. For example, the challenge can be to know a specific combination of a login and a password. In another example, the challenge could be to provide a magnetic card containing unique information. In a final example, the challenge can be to provide a specific fingerprint. The challenge to resolve in this method consists of transmitting a nonce through the associated devices. This nonce is subject to cryptographic operations in order to validate the devices used.

The claim made in this thesis states that the authentication method presented is robust against the theft of k devices with k being less than the number of devices required to perform the challenge. In this specific protocol only two devices are required to perform the challenge, thus k is equal to one.

3.2.1 Protocol

The high level process of the authentication protocol is illustrated in Figure 3.1 and the low level cryptographic operations are detailed in the next section. In Figure 3.1, A represents the Authenticator, D_1 and D_2 represent respectively Device 1 and Device 2.

The communications (2), (3), and (4) are all labeled nonce to understand that the nonce needs to remain the same. However, cryptographic operations compute this nonce to verify the validity of the devices used. These communications also contain extra information, such as timestamps and unique identifiers for each device, which aid the identification of each device.

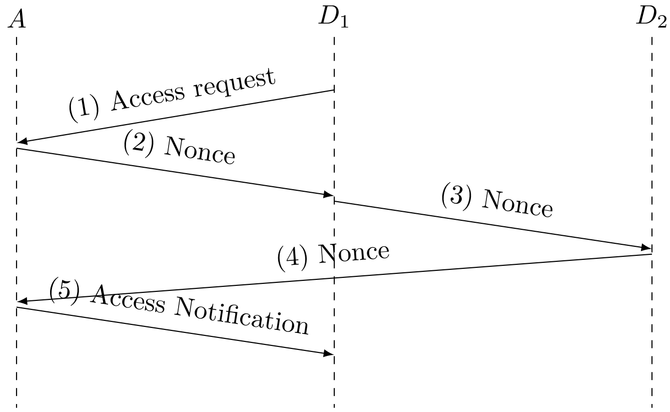

Figure 3.1. Authentication protocol requiring two devices with the nonce sent to the first device.

3.2.2 Cryptographic Operations

In order to determine the validity of the devices performing the challenge, the Public Key Infrastructure is used. Timestamps are used to detect relay attacks. The details of each of the communications in Figure 3.1 include the following:

(1) Access Request

This communication is the notification to the Authenticator that Device 1 is attempting to access the system. This device needs to send a minimum amount of information to the authenticator in order for the authenticator to retrieve the information associated with it. The information includes the public key of this device and may include the second device associated with Device 1 along with other information such as an identifier (e.g. a username).

(2) Nonce

This message contains the nonce but is encrypted with the public key of the recipient device of this message. This encryption allows verification of the identity of the device receiving the message. Without the private key the following communications will not happen because the device needs to extract the nonce from this encrypted message.

(3) Nonce

The designed proposed allows with or without any encryption and/or signature of this communication, similarly to the previous or next communication. The encryption would preserve the secrecy of the nonce but the authenticity is not monitored by the authenticator during this communication. Therefore, this communication can differ depending on the need and the implementation of the authentication protocol.

(4) Nonce

This communication is signed by the private key of the device sending the nonce. This digital signature is used to prove the authenticity of the device. The signature of the nonce can be verified with the public key of the second device.

(5) Request Notification

This communication is simply a notification of the authentication result. The device will be granted access if the information received matches. If the information does not match the authenticator can notify the device of the denied access, but could also not send any notification. The protocol function with or without this last communication.

All communications, with the authenticator, in the protocols presented, are encrypted and/or signed. Thus, if a communication is sent to an associated device, from the authenticator, this communication is encrypted using its public key. If a communication is received from an associated device this communication is signed with its private key. The several protocols presented herein follow the same analogy in terms of cryptographic operation.

3.3 Alternative of the Authenticator Response

Answering directly to an inquiry is the norm, in regard to this convention the nonce is sent to the device requesting access. However, the nonce could be sent to the second device.

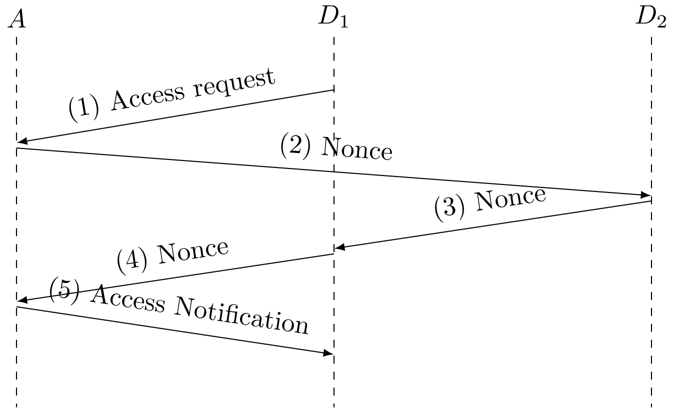

Figure 3.2. Authentication protocol requiring two devices with an alternative flow.

In Figure 3.2 an alternative of the authentication protocol is illustrated. The difference with the previous protocol is that the second communication is not sent to the first device but to the second device. This communication needs to be encrypted to verify the identity of the second device, then the second device needs to forward the nonce to the first device which has to sign this nonce to prove its identity. If the information received by the authenticator match and is correct the first device can be granted access. All the communications of this protocol need to follow the logic of the cryptographic operations described previously.

3.4 Communication Between Devices

The communication between the devices can be of various types. Any kind of communication which allows the transmission of data can be used. The following presents a non-exhaustive list of communication that could be used:

- Radio frequency

  Bluetooth and Near Field Communication (NFC) are two protocols using radio frequency to exchange data [25, 26].

- Sound waves

Data can be exchanged through sound waves and these sound waves can be at a frequency not audible by humans to avoid annoyance [27].

- Visual

  An example of visual data exchange are Quick Response codes, which are machine-readable images that contain information and can therefore be used for one direction communication [28].

- Vibration

  Vibrations can be used to transmit a message. The message transmitted should be short otherwise this communication would be cumbersome. Some animals do communicate through vibration [29], thus this technique could be researched.

The communication between devices is flexible, and can be done via one of the previously mentioned protocol of communication. This flexibility allows the idea proposed in this thesis to be malleable, and accept a wide variety of devices.

CHAPTER 4

SYSTEM DESIGN FOR MULTIPLE DEVICES

This chapter presents a specific protocol with three devices which is then generalized to an arbitrary number of devices.

4.1 Identity Establishment

In the novel authentication method presented in this thesis, each user needs to be associated with some devices depending on the specifications of the protocol implemented. These devices constitute the identity of each user. The identity establishment remains similar for any number of devices. The identity establishment is not the concern of this thesis and will be assumed to be performed correctly. Also a user without the required number of devices associated can not perform the challenge required to be authenticated.

4.2 Authentication Protocol for Three Devices

In this section three devices are associated with each user in the protected system. The authentication protocol is illustrated requiring also a minimum of three devices to perform the challenge. In the case of a system associating three devices and requiring only two devices to perform the challenge then the protocol is the same as previously presented in Chapter 3. Thus, in the following section $n = m = 3$, with m being the number of devices required to perform the challenge and n the number of devices associated with each user.

Since three devices are necessary to perform the challenge, the authentication protocol, in this section, is robust against the theft of two devices. Thus, in this instance $k = 2$.

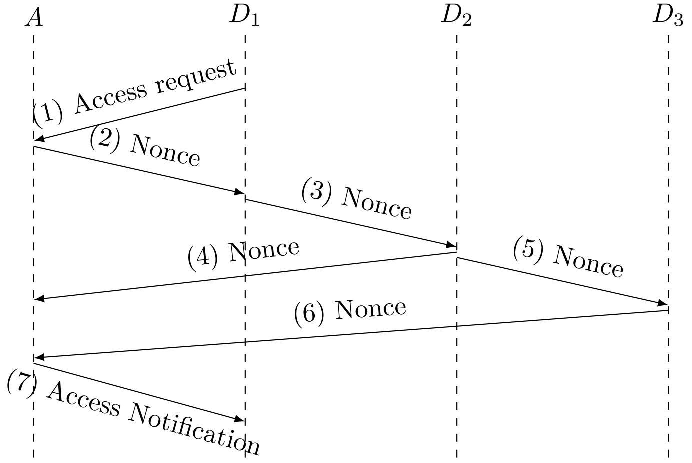

Figure 4.1. Authentication protocol requiring three devices.

4.2.1 Authentication Protocol Details

An example of a protocol using three devices is illustrated in Figure 4.1. This protocol works as follows; The first device requests access to some resource(s), then the authenticator sends the encrypted nonce to the first device, the first device needs to then forward the nonce to the second device which has to forward to the third device and sign the nonce before sending it to the authenticator, then the third device needs to sign the nonce and send it to the authenticator. The access notification will notify the first device if the access is granted or denied. The second device can first sign and send it to the authenticator and then forward the nonce not signed to the third device.

This illustration is a specific example of the protocol requiring three devices to perform the challenge. Different choices can be made on this protocol and these choices will be covered in detail in the upcoming sections.

4.2.2 Alternatives of the Authentication Protocol

Similar to the alternative protocol presented in the previous chapter, the response from the authenticator does not have to be addressed to the device requesting access. Also, since there are more than two devices the nonce does not have to be sent from one device to another following a specific order.

The nonce can be transmitted in a different order from device to device. The only necessary information to authenticate a user is the response of each device. Indeed, each device needs to send to the authenticator credentials that allow the authentication of the user. These credentials are explained in detail in Section 3.2.2.

Figures 4.2 and 4.3 are examples of these alternative protocols. The difference between these two protocols is the fourth communication. This communication is sent from the third device in Figure 4.2 and from the first device in Figure 4.3.

The response of the Authenticator does not have to be addressed to the device requesting access. This alternative is similar to the idea presented in Figure 3.2 but in this case three devices are used.

Figures 4.4 and 4.5 illustrate this alternative for three devices performing the challenge. In Figure 4.4 the authenticator sends the nonce to Device 2, and in Figure 4.5 the authenticator sends the nonce to Device 3.

4.3 Generalization of the Authentication Protocol

This section generalizes to an arbitrary number of devices associated with each user.

As previously stated a registration of the devices associated with a user needs to be performed and this registration can be similar for any number of devices.

4.3.1 System Design for Multiple Devices

The authentication method presented in this thesis can result in various protocols. The protocols presented can be extended with more devices. Each user can be associated with n devices and the challenge can be performed by a specific number of m devices. m needs to remain less than or equal to n; otherwise it would not be possible for a user to perform the challenge.

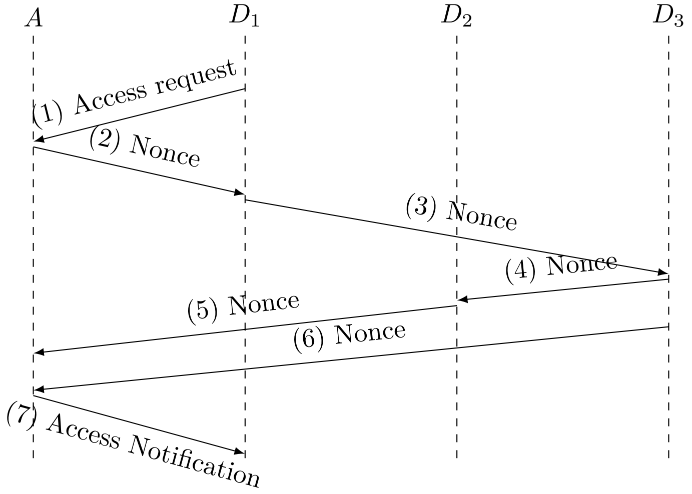

Figure 4.2. First three devices protocol with alternative order of transmission.

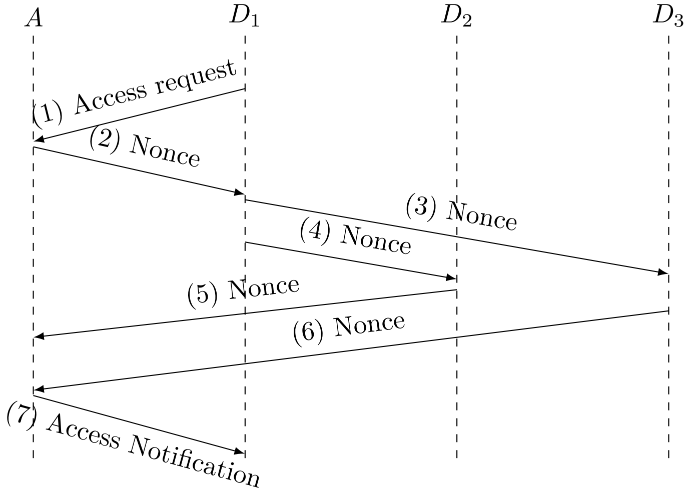

Figure 4.3. Second three devices protocol with alternative order of transmission.

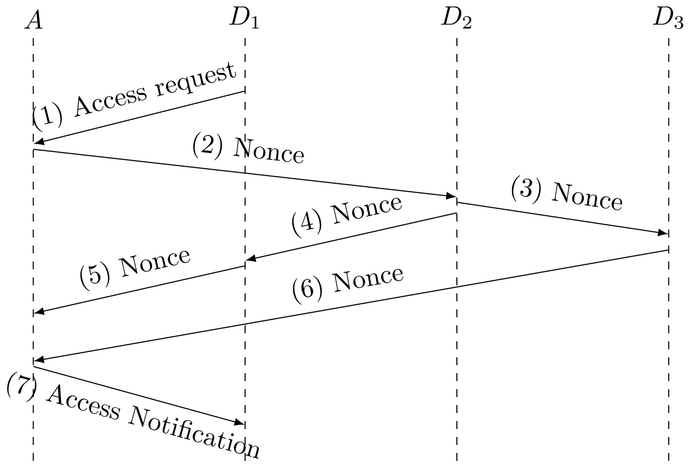

Figure 4.4. First three devices protocol with alternative responses.

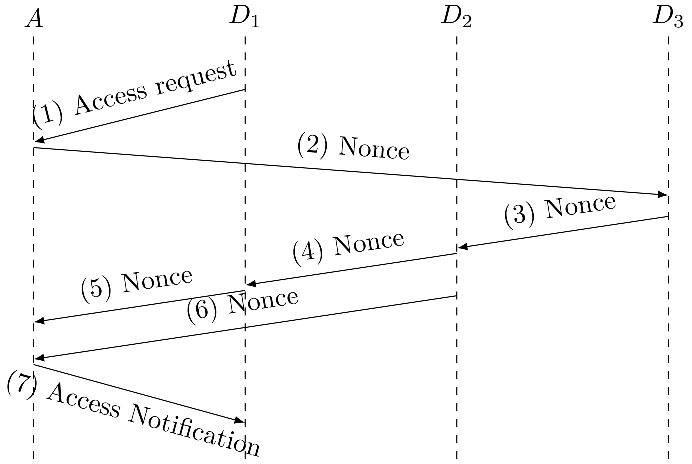

Figure 4.5. Second three devices protocol with alternative responses.

This method remains secure against theft of k devices where k is strictly less than the number of devices required to perform the challenge. Thus $k < m$.

For example, each user is associated with five devices, and is required to perform the challenge with three devices, thus $n = 5$ and $m = 3$. In such system a user can lose two devices and still be able to perform the challenge. Also an attacker needs to steal three devices to usurp a user's identity therefore this specific method is robust against the theft of two devices.

A user still can be able to perform the challenge even after the loss of $n - m$ devices. The number of devices that an attacker needs to steal in order to usurp a user's identity is m, thus authentication methods similar to the one presented are robust against theft of k devices where $k \leq m - 1$.

From the constraints enumerated previously the following inequation ensues: $k < m \leq n$.

4.3.2 Alternatives of the Authentication Protocol

The alternatives presented previously on the authentication protocol can be applied for a greater number of devices.

The response from the authenticator can be sent to any device associated with the user of the device requesting access. This alternative is not always convenient because the user is now required to perform the challenge with the device which received the nonce. The user may not have originally planned to use this device to be authenticated.

The nonce can also be transmitted from one device to another in any order. This alternative is presented in Figure 4.2 and Figure 4.3 for three devices but can be generalized to an arbitrary number of devices.

CHAPTER 5

ANALYSIS AND APPLICATIONS OF THE NOVEL AUTHENTICATION METHOD

The authentication method presented in this thesis is malleable and can be implemented for various purposes. Applications of the authentication method are non-exhaustively presented in this chapter.

5.1 Analysis

An analysis of the idea presented in this thesis is done in this section.

5.1.1 Identity Establishment

Identity establishment is the process of giving an identity to users. This process is also called registration. In the method presented, the identity establishment consists of associating a user with multiple devices. This association can be performed by storing an unique identifier, for example an email address, to represent the user and an unique identifier for each device associated with this user, for example the media access control address (MAC address) of these devices. In another method, for example, where the authentication is done through the verification of a combination of a login and a password, the identity establishment is the creation of this combination.

The identity establishment has been assumed secure. This assumption results from the complexity of the Public Key Infrastructure establishment. Attacks during this phase are possible.

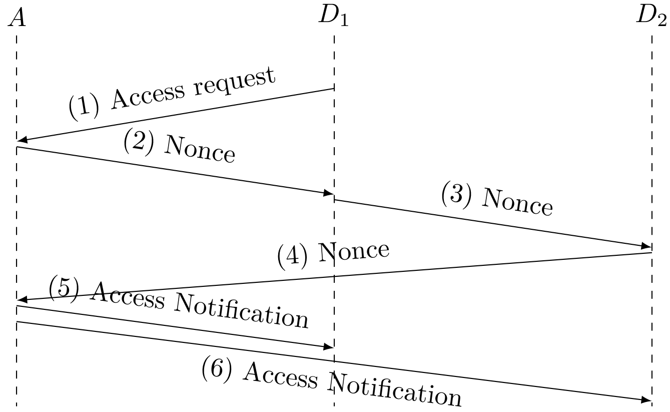

Figure 5.1. Authentication protocol requiring two devices with two access notifications.

5.1.2 Authentication of All Devices Performing the Challenge

The protocols presented only notify the device requesting access of the authentication result. Thus, only this device is granted access in successful scenarios. Alternatively, other devices performing the challenge with the device requesting access could be considered as authenticated and granted access.

If a user wants to access some resources through two devices, the authentication needs to be performed twice even if both devices are used for the first authentication. This alternative can have advantages but needs to be studied to understand if any additional attack vector ensue.

In Figure 5.1, both devices are notified of the authentication result. This notification can allow both devices to access the resources requested by the first device.

5.1.3 Authenticator Response

Instead of answering to the device requesting access, the authenticator could send the nonce to a different device associated with the same user. This alternative can create inconveniences for users. If the number of devices required to perform the challenge is less than the number of devices associated with each user, then the authenticator could send the nonce to a device that the user did not intend to use.

For example, Alice has three devices D_1, D_2, and D_3. In this example, the protocol requires $n = 3$ and $m = 2$ (with m being the number of devices required to perform the challenge and n the number of devices associated with each user). In this particular case Alice may want to only use D_1 and D_2 to perform the challenge however, the authenticator could decide to answer on D_3. This scenario is not convenient for Alice, who now has to use D_3.

5.1.4 Sound Waves as a Communication Between Devices

The devices used during the authentication can communicate through various channels. Sound waves have been mentioned but not studied in this thesis. It is possible for devices possessing a microphone and a speaker to communicate between each other. Also this communication can be inaudible by humans [27].

5.2 Applications for Various Type System

The type of systems that can be protected by the authentication method presented herein is wide. Any physical or digital resource(s) can be protected. The system needs to have an authenticator and a database containing information about the devices associated with each user. The authenticator and the users' devices need to be able to perform computation, store data and communicate with each other. The ability to communicate is also not stringent because, as explained in Section 3.4, the communication can be of various forms, and, as explained in Section 6.3, the devices can communicate with the authenticator through another device.

5.2.1 Vehicles

Any kind of vehicle can be protected with this authentication method. Car, boat or aircraft security can be enforced. Vulnerabilities on modern cars and their keyless entry system have been demonstrated [30]. Thus, the implementation of this method for vehicles can be explored and analysed to determine how suitable it is.

5.2.2 Building Access

Most buildings are already protected by a type of access control. Most of them utilize the possession factor through a physical key or a magnetic card for the authentication protocol installed.

Magnetic cards are often used for their re-programmability property. This advantage is present in the method explained. Users can be stored in a database managed by the authenticator, therefore this database can be modified.

This method may not be suitable for personal houses because of the higher degree of complexity compared to a physical key. Personal homes currently do not require a high-level of security. However, some people could decide to implement this method for houses.

5.2.3 Web Services

Web services requiring authentication for users often use a combination of a login and a password. This authentication method can be replaced by a version of the authentication method presented herein. The protocol can be implemented in diverse manners depending on the platform protected. An email service may not require the same degree of security as an online banking service.

5.2.4 Personal Devices

A personal laptop can require a password in order to be accessed. The utilization of additional devices, such as a tablet and a smartwatch can be the requirement to access a laptop instead of a password or in addition to it. Any device similar to a laptop can also be protected.

In this instance, such protection is similar to a Digital Right Management protection (DRM). Thus, DRMs can be replaced by this method. For example, a Compact Disc (CD) could require the user to authenticate before being accessed. However, the implementation needs to be well thought-out to avoid any harmful side effects [31].

Even if this method is robust, DRM will always be vulnerable to attacks because attackers have physical access.

5.2.5 Various Protocol Configurations

This authentication method is malleable and can be implemented in various configurations. This malleability results from the possibility to use a wide variety of devices. The minimum requirements are: the storage of data (such as a private key), the ability to communicate, and a processor to perform the cryptographic operations.

Table 5.1 illustrates a non-exhaustive list of configurations where the authentication method presented herein could be implemented. Also, Device 1 requests access to the protected system and permutation between devices is allowed if they can still communicate with each other. Some communications are unidirectional, for example QR code.

Table 5.1. Examples of configuration using two devices.

System protected	Device 1	Device 2	Device 3	Communication between devices
Office	Smartphone	Smartwatch	None	Bluetooth
Car	Smartphone	Smartwatch	None	Bluetooth
Web service	Smartphone	Smartwatch	Laptop	Sound waves
Web service	Smartphone	Smartwatch	Tablet	Bluetooth
Web service	Smartphone	Laptop	None	Bluetooth
Web service	Laptop	Smartphone	Smartwatch	QR code

In every configuration, the authenticator can be included in the system protected. However, the authenticator can also be a separate entity which is only in charge of the identification. The authenticator is assumed to be able to communicate with at least one of the devices. In the case where the authenticator cannot communicate with one of the devices, the other device will be used to relay the communication as presented in Section 6.3.

In the configurations where smartwatches or cars are used in combination with Bluetooth, the assumption is made that either the authenticator can communicate through Bluetooth or the communication is relayed by the other device. Also, smartwatches and vehicles can possess WiFi in addition to Bluetooth.

5.3 Permissions

Most resources protected by an access control mechanism often possess methods to define permissions and access rights for users. A popular example is a file system which can have complex and well construct permissions. Another example is the Grey system [32] which can assign access rights for office doors. This system uses electronic devices, more specifically smartphones, to manage these rights.

The Grey system could be combined with the authentication method presented herein to protect office doors. Other permission systems can also be combined to enable more usability.

CHAPTER 6

DISCUSSION

This chapter proposes future research and improvements that can be explored, and then concludes.

6.1 Future Work

This section presents the ideas that can be explored in order to extend the authentication method presented herein.

6.2 Device Duplication

A device can be purposefully duplicated to serve as a backup or as an alternative to sharing a device with a user presented in Section 6.4. Doing so imparts both advantages and disadvantages.

The advantages of duplicating a device include using the duplicated device as a backup or as a shared device with another person. In the case of a shared device, only the main user possesses the original device and does not have to lend it. This is desirable because the original device may be a personal device that the user does not want anybody to access, so having a separate device to lend is useful.

One disadvantage is an additional attack vector for each duplicated device. Also, the authenticator is not aware of such duplication because the action of duplicating the private key of a device cannot be monitored. In an instance where devices have been duplicated, an attacker only needs access to one of the duplicated devices, which is easier than accessing all devices.

6.3 Relayed Communication

In Figure 6.1, an authentication protocol is presented where the first device is used as a relay for the communication between the authenticator and the second device. There are two possibilities of how this protocol can function. The first one functions as follows: the nonce is addressed to the first device; therefore, the communications (2) and (3) are the same as in Figure 3.1, and the communications (4) and (5) are actually the exact same communication. The first device is used only as a relay to transmit the communication to the authenticator. The second possibility is analogous to the first.

In a protocol implemented as illustrated in Figure 6.1, the timestamps need to be implemented accordingly since the communication is relayed. For example, the fifth communication should not be allowed to be sent within a greater time interval than the others.

This protocol can be useful when a device cannot directly communicate with the authenticator but can communicate with another device. An example of this scenario is the case of a smartwatch that currently has only Bluetooth to communicate. Therefore, the authen-

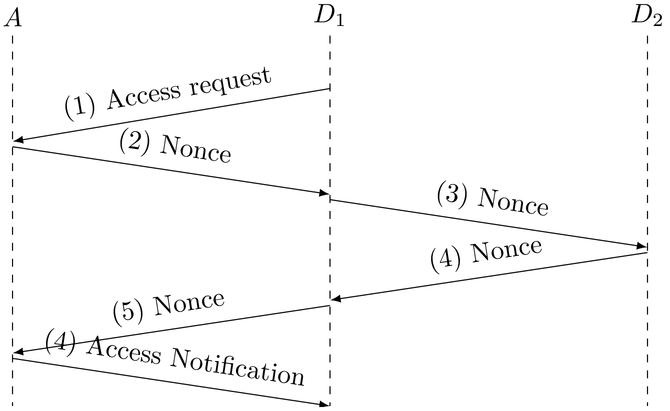

Figure 6.1. Authentication protocol requiring two devices with a relayed communication.

ticator may not be able to communicate through Bluetooth, but with this specific protocol the communication would be relayed by another device.

6.4 Shared Association of Devices

In some implementations a device could be shared between two users. A device can be shared between both Alice and Bob. In this case the assumption is made that Alice will not attempt to usurp Bob's identity. Indeed, in the case of shared devices an insider attack is possible.

For example, if Alice has D_1 and D_2 for associated devices and Bob has D_2 and D_3, they can both access the system with D_2 and their respective additional device. However, the authentication cannot be successfully performed by using only D_1 and D_3.

This situation can occur when the system to protect is a car, and the car's key could be the shared device. Alice and Bob would have their own respective additional devices to perform the authentication task.

6.4.1 Usability

The usability of the authentication method should be studied. This study could be done on diverse implementations of this method in comparison with existing methods. For example, the experimentation could measure the user-friendliness of the implementations.

6.4.2 Authentication from an Unknown Device

A desirable restriction in the authentication method presented in this thesis is that the device requiring access must be an associated device. However, a user could want to access resource(s) from a non-associated device. For example, in a computer lab, the computers are shared between strangers.

In such scenario, the cryptographic operations need to change and be studied to reduce the attack surface.

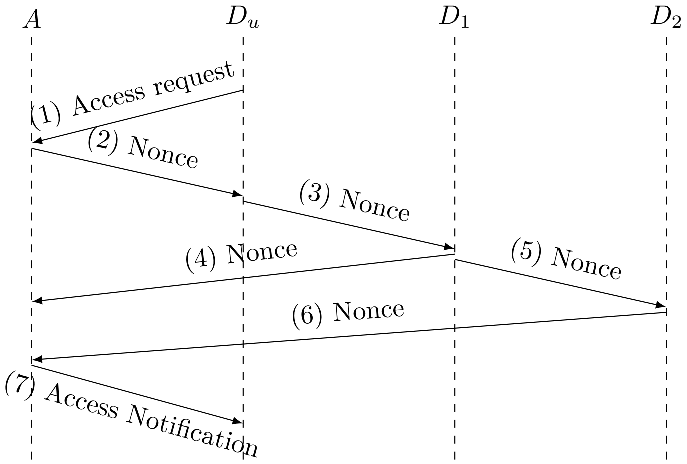

Figure 6.2. Authentication protocol through an unknown device.

Figure 6.2 illustrates a specific example of an authentication protocol from an unknown device. This protocol can vary according to the alternatives presented in Chapter 4.

6.4.3 Modification of the Set of Provers

The set of provers contains the devices associated with a specific user. To enable more usability the possibility of adding or deleting devices should be possible. However, this functionality creates a wide attack surface that needs to be studied. It should not be easy for an attacker to usurp the identity of someone by obtaining access to one person's devices, adding the attacker's devices, and then deleting the devices of the victim.

6.4.4 Continuous Authentication

A continuous authentication protocol can be implemented with this method. This authentication method can either require an action or not from the user; thus the user could be continuously authenticated. The server task would be to send the nonce within time intervals and disconnect the user if one of the challenges is not performed properly. Any minimal action from the user or none can be required. In continuous authentication methods, the task required to be performed by a user needs to not be obtrusive. For example, entering a password every minute is not convenient for a user.

An instance of continuous authentication protocol could be a user with two associated devices, a laptop and smart glasses, with the challenge being a QR code to scan. The user would have to look at the screen of the laptop when the QR code appeared in order to complete the authentication. The action is minimal and non-obtrusive. This instance requires an action from the user, but if the protocol implemented uses Bluetooth communication, the user is not required to perform any action.

6.4.5 Multi-factor Authentication

The method presented herein utilizes only one factor, which is the possession factor. Thus, implementation of this authentication method could combine multiple factors. The advantages brought by such combination should be studied and experimented.

6.5 Summary

This thesis focuses on the system design of a practical method of authentication utilizing multiple devices. This practicality results from the malleability and the possibility of implementation on various devices of this method. Furthermore, the devices already in possession of users can be used. The authentication method presented herein associates devices to specific users to identify them. Each device possesses a private key which is used to perform cryptographic operations. These operations authenticate each device and the addition of each of these authentications allows the identification of the associated user.

This method is robust against theft-based attacks of k devices. Each user is associated with n devices and then m devices are required to be authenticated. The following inequation needs to hold: $k < m \leq n$.

The authentication method presented herein is malleable and can be implemented in various ways. These implementations could replace many existing authentication protocols, from the combination of login and password overused for web services, to simple locks protecting houses, vehicles, and buildings. This authentication relies on the possession of multiple electronic devices from users, which is becoming more common.

LIST OF REFERENCES

[1] Messaoud Benantar. *Access control systems: security, identity management and trust models*. Springer Science & Business Media, 2006.

[2] Thomas D Wu et al. The secure remote password protocol. In *NDSS*, volume 98, pages 97–111, 1998.

[3] John Brainard, Ari Juels, Ronald L Rivest, Michael Szydlo, and Moti Yung. Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 168–178. ACM, 2006.

[4] Dorothy E Denning and Peter F MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security*, 1996(2):12–16, 1996.

[5] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 173–186. ACM, 2013.

[6] Luis Von Ahn, Manuel Blum, Nicholas J Hopper, and John Langford. Captcha: Using hard ai problems for security. In *Advances in CryptologyEUROCRYPT 2003*, pages 294–311. Springer, 2003.

[7] Benjamin Miller. Vital signs of identity [biometrics]. *Spectrum, IEEE*, 31(2):22–30, 1994.

[8] Reza Rawassizadeh, Blaine A Price, and Marian Petre. Wearables: has the age of smartwatches finally arrived? *Communications of the ACM*, 58(1):45–47, 2014.

[9] Cagri Cetin. Design, testing and implementation of a new authentication method using multiple devices. Master's thesis, University of South Florida, 2015.

[10] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, 2011.

[11] Matt Bishop. *Computer security: art and science*, volume 200. Addison-Wesley, 2012.

[12] Ross Anderson. *Security engineering*. John Wiley & Sons, 2001.

[13] Dan M Bowers. *Access control and personal identification systems*. Butterworth-Heinemann, 2013.

[14] Jeff Yan and Ahmad Salah El Ahmad. A low-cost attack on a microsoft captcha. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 543–554. ACM, 2008.

[15] Philippe Golle. Machine learning attacks against the asirra captcha. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 535–542. ACM, 2008.

[16] Alex Biryukov, Joseph Lano, and Bart Preneel. Recent attacks on alleged securid and their practical implications. *Computers & Security*, 24(5):364–370, 2005.

[17] Charles Beumier and Marc Acheroy. Automatic 3d face authentication. *Image and Vision Computing*, 18(4):315–321, 2000.

[18] Siew Chin Chong, Andrew Beng Jin Teoh, and David Chek Ling Ngo. Iris authentication using privatized advanced correlation filter. In *Advances in Biometrics*, pages 382–388. Springer, 2005.

[19] Nalini K Ratha, Ruud M Bolle, Vinayaka D Pandit, and Vaibhav Vaish. Robust fingerprint authentication using local structural similarity. In *Applications of Computer Vision, 2000, Fifth IEEE Workshop on.*, pages 29–34. IEEE, 2000.

[20] Chang-Mok Park, Devinder Thapa, and Gi-Nam Wang. Speech authentication system using digital watermarking and pattern recovery. *Pattern Recognition Letters*, 28(8):931–938, 2007.

[21] Chee Meng Tey, Payas Gupta, and Debin Gao. I can be you: Questioning the use of keystroke dynamics as biometrics. The 20th Annual Network & Distributed System Security Symposium (NDSS 2013), 2013.

[22] Moshe Kam, Gabriel Fielding, and Robert Conn. Effects of monetary incentives on performance of nonprofessionals in document-examination proficiency tests. *Journal of forensic sciences*, 43(5):1000–1004, 1998.

[23] Moshe Kam, Gabriel Fielding, and Robert Conn. Writer identification by professional document examiners. *Journal of Forensic Sciences*, 42(5), 1997.

[24] Moshe Kam, Kishore Gummadidala, Gabriel Fielding, and Robert Conn. Signature authentication by forensic document examiners. *Journal of Forensic Sciences*, 46(4):884–888, 2001.

[25] Roy Want. Near field communication. *IEEE Pervasive Computing*, 10(3):0004–7, 2011.

[26] Brent A Miller and Chatschik Bisdikian. *Bluetooth revealed: the insider's guide to an open specification for global wireless communication.* Prentice Hall PTR, 2001.

[27] Jie Yang, Simon Sidhom, Gayathri Chandrasekaran, Tam Vu, Hongbo Liu, Nicolae Cecan, Yingying Chen, Marco Gruteser, and Richard P Martin. Detecting driver phone use leveraging car speakers. In *Proceedings of the 17th annual international conference on Mobile computing and networking*, pages 97–108. ACM, 2011.

[28] ADC Denso. Qr code essentials. *Retrieved fr om http://www. nacs. org/LinkClick. aspx*, 2011.

[29] Peter M Narins. Vibration communication in vertebrates. In *Ecology of sensing*, pages 127–148. Springer, 2001.

[30] Aurélien Francillon, Boris Danev, Srdjan Capkun, Srdjan Capkun, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *NDSS*, 2011.

[31] J Alex Halderman and Edward W Felten. Lessons from the sony cd drm episode. In *USENIX Security*, 2006.

[32] Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-enabled authorization in the Grey system. In *Information Security: 8th International Conference, ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 431–445. Springer, September 2005.