2017

Leveraging bluetooth as a second factor in two-factor authentication

Cimone Le Wright-Hamor
Iowa State University

Leveraging bluetooth as a second factor in two-factor authentication

by

Cimone Le Wright-Hamor

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Co-majors: Computer Engineering; Information Assurance (Secure and Reliable Computing)

Program of Study Committee:
Zhenqiang (Neil) Gong, Major Professor
Doug Jacobson
James Davis

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this thesis. The Graduate College will ensure this thesis is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2018

DEDICATION

I would like to dedicate this thesis to my family, friends, and colleagues without their support I would not have been able to complete this work. I would also like to thank my friends and family for holding me accountable and providing me with critical feedback.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

ACKNOWLEDGMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. Neil Gong for his guidance, patience, and support throughout this research and the writing of this thesis. Dr. Gong enabled me to do things at my own pace, which helped me find my confidence in research. His insights and resources have empowered me and revived my hopes for completing my graduate education. I would also like to thank my committee members for their efforts and contributions to this work: Dr. Doug Jacobson and Dr. James Davis. I would additionally like to thank Mr. Aaron Bertram and Ms. Hardeep Obhi for their guidance throughout the various stages of writing this thesis. I would also like to thank my husband, Andrew Hamor, for supporting me by taking care of everything that was not directly related to school or my thesis. This work was financially supported by the National GEM Consortium, Iowa State University George Washington Carver Fellowship, and the Iowa State University Cyber Corps Scholarship for Service.

ABSTRACT

Passwords have been the dominant single-factor authentication method for decades but are no longer sufficient to validate a user's identity. The simplistic nature of passwords perpetuate their existence and makes them an easy attack vector. However, Two-Factor Authentication (2FA) augments passwords and adds a layer of security. Although 2FA has the potential to increase security, traditional second factors require user interaction at every login attempt, which may contribute to slow adaptation. Traditional second factors drastically alter the user authentication experience and typically require the user to navigate away from the login screen. Therefore, we present a new second-factor method that leverages Bluetooth technology called Ambient-Discovery. Our protocol is designed to provide security assurances comparable to or greater than the traditional second factors while keeping the user experience the same as password-based authentication. There is no user interaction, as the second factor restricts communication between a mobile application and a computer browser. Therefore, Ambient-Discovery provides an additional layer of security while limiting user interaction.

CHAPTER 1. OVERVIEW

1.1 Introduction

The ubiquitous, simplistic, and disposable nature of passwords makes them the preferred Single-Factor Authentication (1FA) method because all other methods are too complex. Passwords are perceived to be insufficient due to the increasing number of successful high profile attacks on password databases [2, 3, 4]; thus, making Two-Factor Authentication (2FA) a preferred method because it increases complexity for an attacker. 2FA is a two-layered verification process in which users provide proof of their identity, usually via username and password, and additional means of authentication from a different factor such as a physical token or a fingerprint. According to the Federal Deposit Insurance Corporation (FDIC), authentication methods typically fall into one of three categories:

- *Knowledge Factor*: Something known, such as a Personal Identification Number (PIN), a password, or a shared secret
- ***Possession Factor***: Something owned, such as an Automated Teller Machine (ATM) card, Radio Frequency Identification (RFID) badge, or a token generator
- *Inherent Factor*: Something biologically inherent, such as a fingerprint, facial recognition, or a keystroke pattern

The combination of any two factors listed above is 2FA. Usually, the user provides identification via knowledge factor in combination with another factor, the additional factor is known as second factor. This additional method may not be within the same category; therefore, repetition of the same method is not allowed. For example, a password-based and a PIN are not the same method but are both within the knowledge factor category. Therefore, it is not permitted.

For this reason, we cannot do away with passwords, but second factors have been created to augment them [5]. The number of successful high-profile attacks on password databases makes 2FA a preferred method because it adds a layer of security. However, there are still some security flaws with the current second factor methods.

1.2 Traditional Second Factors

There are various second factor methods actively being used in the industry today, such as Short Message Service (SMS), email, tokens, biometrics, and security questions [6]. The issues with popular 2FAs are that they have security flaws and usability impediments. SMS is easy for an attacker to intercept the messaged [7]. Email is hidden behind a 1FA, which undermines the 2FA [8]. Token-based requires the user to carry an additional item. Biometric related authentication, such as fingerprints or eyeballs, do not present a reasonable security trade-off; once compromised they cannot be replaced [5]. Security questions are not ideal because an attacker could social engineer the user to gather the answer to the security questions. All these traditional second factor methods require additional user action.

Existing second factors are *active*, which means the user is required to perform additional interaction upon every login attempt. The additional user interaction typically requires you they suffer from security flaws. The additional user action required by traditional second factors decreases the usage of traditional 2FA because customers dislike the extra engagement required to use them [9]. A commonly held perception is that users are willing to trade the additional layer of security offered by 2FA for convenience, this trade off maybe a contributing factor to the infrequent usage of 2FA. Researchers have been focusing on alternative 2FAs that are *passive*, which do not require additional user interaction. These newly proposed second factor have usability, deployability, and security issues. Despite the issues presented by second factors, they add a second layer of security. Therefore, 2FA is preferred to increase security. Developing a passive 2FA has the potential to increase the usage of 2FA by removing the inconvenience for users.

An ideal second factor method would provide a protocol that does not require additional user interaction or equipment, nor disrupt the current environment. Such a method should reinforce user validation and be easy to deploy. In this paper, we introduce **Ambient-Discovery**, a new passive possession-factor protocol that leverages Bluetooth technology in smartphones and computers.

1.3 Geolocation

A naive approach of validating if two devices are within the proximity of each other is to request their Global Positioning System (GPS) locations and validate that they are within an acceptable range of each other. While most smartphones have GPS sensors, not all computers come equipped with GPS capabilities. The more recent browsers expose geolocation Application Programming Interface (API)'s [10]. Unfortunately, this does not guarantee that the information is accurate. An adversary may dissimulate their location by utilizing a Virtual Private Network (VPN), which undermines using GPS to validate that the devices are in close proximity of one another. Despite the fact that devices can obfuscate themselves behind a VPN many website still attempt to retrieve the GPS location available. The GPS information is used and logged the locations a user has authenticated in from.

1.4 Our Contribution and Organization of this Thesis

In this thesis we developed an innovative second factor authentication method that leverages Bluetooth technology in smartphones and computers. The system can effectively provide accurate information about the proximity of two devices. Furthermore, it does not require the user to carry additional items, which has the potential to decrease the usage of the system requiring additional items to authenticate. Ambient-Discovery leverages existing items to provide a passive form of authentication, which does not require user interaction. By design the mobile application communicates directly with the browser, thus achieving a passive form of authentication.

Ambient-Discovery does not require additional user interaction or equipment and does not disrupt the environment. We made the following contributions:

- We proposed the Ambient-Discovery protocol, a novel proximity-based 2FA mechanism for websites that does not require additional user interaction.
- We implemented the prototype of our solution for Android and a standard website login page.
- We evaluated the effectiveness of the prototype by measuring the additional time required to authenticate. We also conducted a comparative study to show its perceived usability, deployability, and security based on Bonneau's Framework [1].

This thesis is organized as follows: chapter 2 establishes and evaluates a list of previous efforts at creating passive 2FA. Chapter 3 provides a formal description of the problem and establishes goals an idea solution would achieve. Next, we provide details about the practical implementation and overview of the Ambient-Discovery protocol in chapter 4. Then, in chapter 5 we provide an evaluation of our implementation and evaluate Ambient-Discovery using Bonneau's Framework [1]. Finally, present our conclusion in chapter 6.

CHAPTER 2. RELATED WORKS

2.1 Sound-Proof

Sound-Proof is a proximity-based second factor mechanism that does not require user interaction [11]. The mechanism leverages audio frequencies and recording abilities in computers and smartphones. In order to use Sound-Proof, the user completes the standard username and password login on a website; upon successful user verification, the computer and smartphone simultaneously record an audio frequency. The browser encrypts the audio it recorded and sends it the server, the server forwards the encrypted audio to the phone. Then, the phone decrypts and computes the similarities of two sample noises. If the audio frequencies are within an acceptable range, the user will be authenticated. Otherwise, the user not authenticated. While Sound-Proof does not require additional user interaction, the audio frequency used for authenticating is within audible range of the human ear, which disrupts the environment. This disruption could potentially decrease the usability of this second factor mechanism. The audio has the potential of disturbing the user or other in the vicinity. Sound-Proof is limited in scalability because it operates within human audible range, thus restricting the number of devices connected to an account. SlickLogin is another second factor method that leverages audio frequencies by utilizing non-audible frequencies to authenticate a users [12]. This method was found to have a decreased usability because it would require high-quality speakers.

2.2 PhoneAuth

PhoneAuth is a proximity-based 2FA mechanism that leverages Bluetooth technology [13]. In order to use PhoneAuth, the user enters their username and password into a website; the credentials are relayed to a server. Then, the server generates a login ticket; the ticket serves as an identity assertion. Following that, the browser forwards that ticket to the user's phone. The phone validates

the ticket, and if the ticket is valid, the phone signs the ID assertion and sends the assertion back to the browser. Following, the browser forwards the assertion to the server, and the server validates the signature. If the signature is valid, the server authenticates the user by setting a cookie. While PhoneAuth does reduce the cognitive load on the user, it has the potential to create another attack vector.

The implementation utilizes Bluetooth technology to pair user's phone with a computer that may be malicious. PhoneAuth also requires a proprietary browser, which creates deployability issues. If a user does not have administrative access to the computer, they will not be able to download the required proprietary browser. As a result, they will not be able to use PhoneAuth.

Ambient-discovery is similar to PhoneAuth because they are proximity-based authentication mechanism that leverage Bluetooth technology within computers and smartphones. However, unlike PhoneAuth, Ambient-Discovery uses characteristics about Bluetooth in authentication. Additionally, we use the Internet as a medium of communication and attributes associated with Bluetooth technology to validate that two devices are proximal.

2.3 Bonneau's Framework

Bonneau's framework provides objective criteria for evaluating the effectiveness of website authentication methods [1]. This framework is used to Ambient-Discovery. The framework evaluates the usability, deployability, and security of authentication schemes, which encompasses 25 "benefits" an ideal website authentication method should possess. Based on the authenticating schemes evaluated in the original paper, it was found that no scheme examined is perfect or relatively close to being perfect. The results showed that passwords are more deployable than every other scheme, which could contribute to their longevity. The schemes evaluated were not eminent over passwords. Therefore, replacing passwords with any scheme means exchanging benefits. Bonneau's framework will be used to evaluate our proximity-based second factor protocol.

CHAPTER 3. PROBLEM STATEMENT AND DESIGN GOALS

Traditional 2FA authentication mechanism require additional interaction from the user. Usually, this additional action requires the user to navigate way from the login screen to answer a security question. This question usually requires the user to retrieve information from memory, another account, or a device. The information is either randomly generated data or the answer to a question set by the user when the account was created. Requiring the user to input information is prone to errors. Answering the question incorrectly, typically requires the user to restart the authentication process over. This process can lead to user frustration and decrease the chance the user using 2FA. Despite the fact that 2FA increases security, it appears that users are willing to trade security for convenience.

An ideal 2FA authentication mechanism would not require the user to sacrifice security for convenience. A mechanism that does require the user to input anything, is browser and server comparable would make it easy to use and deploy. The security provided by this mechanisms would be greater than or compatible to password-based authentication.

The goal of this project is to design a 2FA that provides the following benefits:

1. does require additional user interaction upon every login attempt
2. compatible with current browser and server setups
3. provide security greater than password-based authentication

CHAPTER 4. SYSTEM DESIGN

4.1 Hardware Requirements

Ambient-Discovery requires a computer and a smartphone with Bluetooth 5.0 or higher. Ambient-Discovery relies on the Bluetooth Low Energy (BLE) protocol introduced in Bluetooth version 5.0. BLE 5.0 only advertising data of 1650 bytes [14]. Most smartphones come equipped with Bluetooth 5.0 functionality [[15]], the smartphone must also have an operating system of Android 8.0 or higher to run the application. Within the smartphone market, Android has the largest market share at 86%, because Android holds majority of the market our application was developed for Android [16]. We used Android 8 (Oreo) because of the new BLE functionality [17]. A server is required to host the website, a database, and control the flow of communication.

4.2 Software Requirements

Ambient-Discovery depends on Firebase to initiate server side communication with the Mobile Ambient-Discovery. The nodeJS node-web-bluetooth library enables the browser to scan for BLE devices in proximity and programmatically select a device. Chrome browser version 57 or higher is required to leverage the web Bluetooth functionality. The Android application was developed using the Bluetooth LE BluetoothLeAdvertiser library and required the Bluetooth_Admin permission to be set in the manifest file.

4.3 System Components and Design Decisions

There are four main components to the system: browser, Mobile Ambient-Discovery, Firebase, and server. Our system has been integrated with a standard login webpage, as shown in Figure 4.3. The website has a client and back-end server, our code into both the client and the back-end server.

4.3.0.1 Browser

The browser is responsible for standard username and password form, generating a random string ($RS1$), as well as retrieving Bluetooth data, $bBlt$. The nodeJS node-web-bluetooth library enables the browser to scan for BLE devices and retrieve the device data.If authenticated, the browser stores the token and adds it in the header of every request. The browser was developed in JavaScript using React and Redux, and is hosted on an instance of Elastics Compute Cloud (EC2) Amazon Web Services (AWS).

4.3.0.2 Mobile Ambient-Discovery

We created an Android application, Mobile Ambient-Discovery, that generates a public and private key pair, and a unique identification for each device that has the application installed. The public and private key pair, and unique identification are denoted as $mPub_k$, $mPriv_k$ and $ID_{Android}$, respectively. The Android unique identification is a 128-bit value. Mobile-Discovery uses the BLEAdvertiser library to advertise BLE data to all devices within range. The code for BLE running as a service. Therefore, it does not require the user interaction. The BLE 5.0 has the capability to transmit 257 bytes of data in the AdvData payload [18].

4.3.0.3 Firebase

The role of the Firebase component is to allow the server to initiate conversation with the Mobile Ambient-Discovery. The Mobile Ambient-Discovery registers with Firebase and is provided a unique identification number that we will denote as $ID_{Firebase}$. Firebase generates a unique identification number for each software installation associated with each Firebase project [19]. Additional code is appended in the Android application to create a Firebase service. The service is a facility for the application that tells the system about something going on in the background, this allows Firebase to initiate communication with the Mobile Ambient-Discovery at any point in time. The Firebase service is responsible for forwarding information form the server to Mobile Ambient-Discovery. Firebase has a maximum message payload of 4KB [19].

4.3.0.4 Server

The server is responsible for validating user credentials, making calls to Firebase, collecting data, and returning the result to the browser. Firebase unique identifiers ,$ID_{Firebase}$, is the only thing stored on the server in plaintext. Transportation Socket Layer (TLS) protocol is used to secure communication between the browser and the server. The primary responsibility of the server is to validate data used to authenticate the user.

4.4 Two-Factor Authentication

Ambient-Discovery is a 2FA mechanism that is divided into to phases, registration and authentication. The registration phases is not a recurring phase and is only required upon initial use of Ambient-Discovery. While, the authentication phase is occurs upon every login attempt.

4.4.1 Registration Phase

The user is required to download the application on their smartphone and register their device. Once the application is downloaded, the user is required to provide an email address and a password as seen in Figure 4.1. The application will generate a public and private key pair, and a unique identification number per device. The username, password, public key, and identification number are denoted as $mPub_k$, $mPriv_k$ and $ID_{Android}$, respectively. The public and private key pair, and the identification number of the mobile device are 128-bit values. Mobile Ambient-Discovery will be send the username, password, public key, and identification number to the server. A service will register the device with Firebase, which will provide the application with a unique Firebase identification number, denoted as $ID_{Firebase}$. The application identification number and the Firebase identification number are not the same, these numbers are used for different purposes.

Following registration, the user will not be required to access this application again, but it must remain on the device. This is the only part of the protocol that requires human interaction and only needs to be completed once per device. Following registration, the server will be able to initiate communication with Mobile Ambient-Discovery by using Firebase.

Figure 4.1 Registration Screen of Mobile Ambient-Discovery

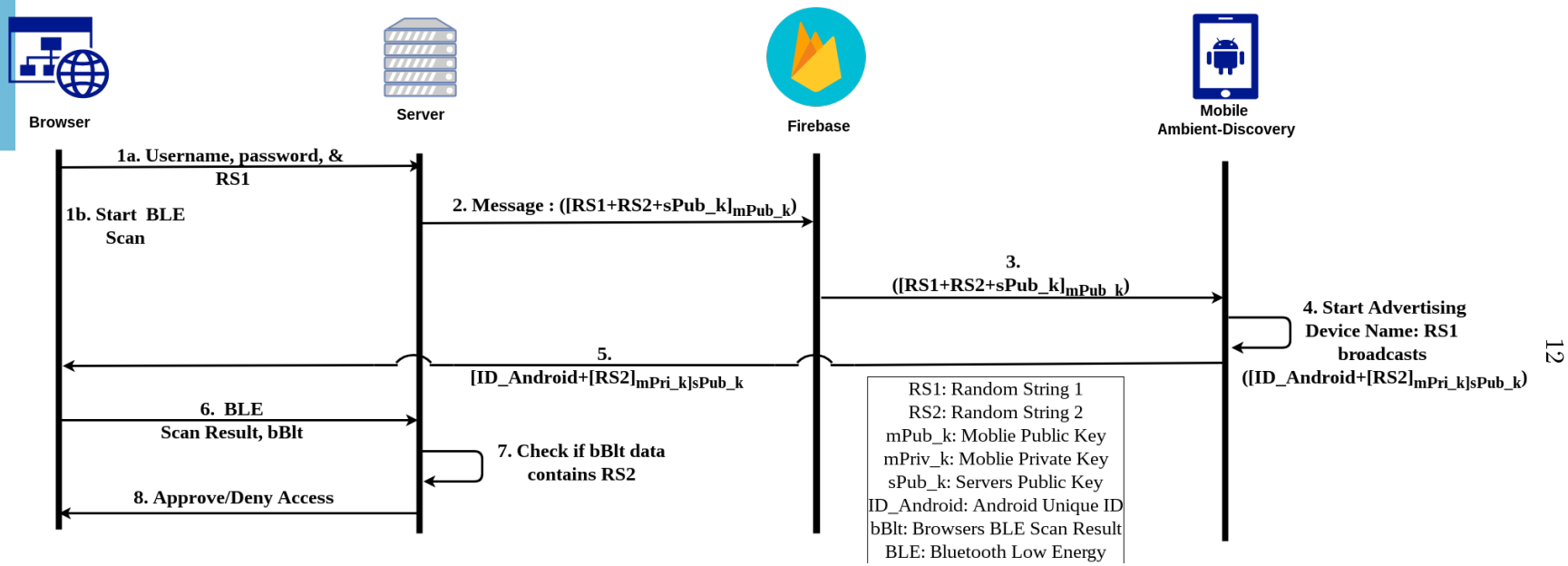

Figure 4.2 Ambient-Discovery Protocol Diagram

4.4.2 Authentication Phase

The authenticating phases of Ambient-Discovery is a reoccurring phase that will be initiated upon every login attempt. A general overview of the protocol can be seen in Figure 4.2. The steps of the Ambient-Discovery protocol are as follows:

Step 1: The user inputs their username and password into the website, as shown in Figure 4.3. Once the user submits their credentials, the browser generates a random string denoted as $RS1$ and begins scanning for a BLE device with $RS1$ as a device name. Then the user credentials, along with a random string, are sent to the server.

Step 2: The credentials are validated on the server. Is this a valid user?

FALSE: The server denies the login attempt and the protocol will terminate. Once terminated, the user will be returned to the login page and may attempt to login again.

TRUE: The server will request Firebase to forward a message to Mobile Ambient-Discovery. The details of this step is provided in section 4.4.3.

Step 3: Firebase forwards the message:= $[RS1 + RS2 + sPub_k]_{mPub_k}$ to Mobile Ambient-Discovery.

Step 4: The Mobile Ambient-Discovery will decrypt the message received from Firebase and advertise data to all devices found within range. More details for this step is provided in section 4.4.4.

Step 5: The browser will receive advertising data from Mobile Ambient-Discovery. The data received through the browser is denoted as $bBlt$.

Step 6: The browser will forward the information received from the BLE scan to the server.

Step 7: The server will search for a decrypt of the information from the browser and validate that it matches the information sent. More details are provided in section 4.4.5.

Step 8: Return authentication result to browser

DENY: If the information does not match, the server will reject the login attempt and the user can attempt to reauthenticate.

APPROVE: If the information matches, the server will generate and send a session token. The user is now authenticated.

4.4.3 Step 2: TRUE

In this step the user credentials are correct and the server will generate a unique 256-bit public and private key pair per device registered. This key pair of the server are designated as $sPub_k$ and $sPriv_k$, respectively. Two 128-bit random strings are generated, random string one and random string two, $RS1$ and $RS2$, respectively. Random string one and two are appended to the servers public key. All strings are concatenated and encrypted using the public key of Mobile Ambient-Discovery to create a message. The message is then sent to Firebase. The message that is sent from the server is constructed as follows $[RS1 + RS2 + sPub_k]_{mPub_k}$.

4.4.4 Step 4

Mobile Ambient-Discovery will decrypt the following message:= $[RS1 + RS2 + sPub_k]_{mPub_k}$ using its private key as follows: $[[RS1 + RS2 + sPub_k]_{mPub_k}]_{mPriv_k}$. Then, the application will temporarily change the devices name to $RS1$. Using the server's public key, the application will encrypt the unique id and $RS2$ as follows, $[ID_{Android} + [RS2]_{mPri_k}]_{sPub_k}$, to generate advertising data. The data will then be advertised to all BLE devices within range for a maximum of 15 seconds.

4.4.5 Step 7

The server will decrypt the data from the browser, $bBlt$. The message is expected to be in the following format $bBlt$:=$[ID_{Android} + [RS2]_{mPri_k}]_{sPub_k}$. The $bBlt$ is decrypted using the servers private key as follows $[[ID_{Android} + [RS2]_{mPri_k}]_{sPub_k}]_{sPriv}$. The Android ID, $ID_{Android}$, is extracted

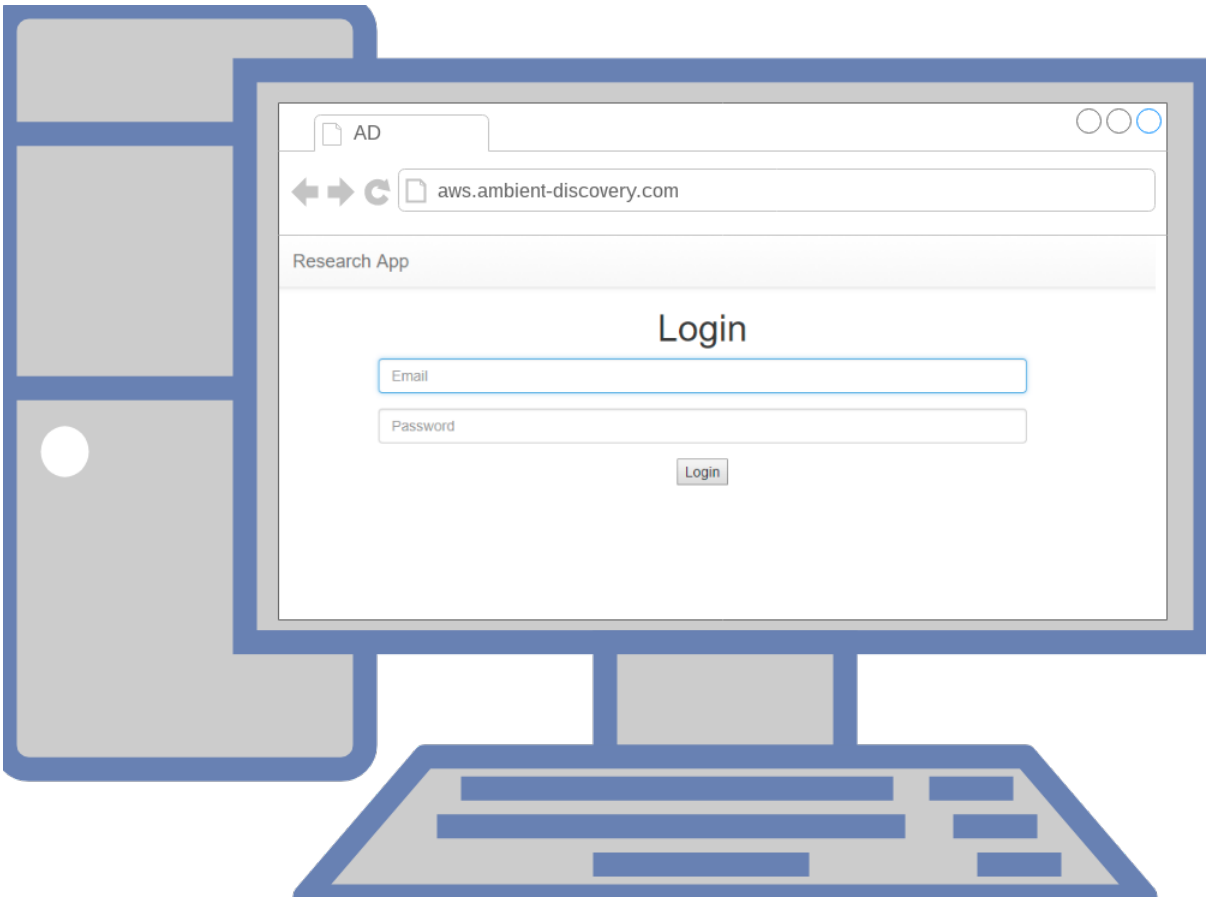

Figure 4.3 Website Login Screen

to identify which public key and $RS2$ to retrieve from the database. The $RS2$ received from the browser, $RS2_B$, is then compared to the $RS2$ stored on the server, $RS2_S$.

CHAPTER 5. EVALUATION

Our evaluation was broken up into two categories, experimental and comparative. The experimental evaluation is a series of experiments that were designed to evaluate the additional time required by Ambient-Discovery. The Bonneau's framework [1] is used to evaluate the effectiveness of Ambient-Discovery as a 2FA mechanism. In this section we will detail the setup and goals for each experiment.

5.1 Experimental Setup

To test the reliability and performance of the protocol we design automated scripts to perform the login attempts. An AWS database was created and preloaded with one million pre-generated fake usernames and passwords. The function randomly choose a number between 1 and a million, this number was used to indicate which user would be used in the login script. The login script would get the user credentials and proceed to login, like a user would. These scripts were made in Python and interacted with the browser to simulate a normal user and keep consistency. For simplicity, all users were connected to same mobile device. The testing was conducted with a HTC u11 smartphone, a DELL Latitude E6540 laptop, a BLE 5.0 adapter, and AWS as a hosting service. The client and back-end server were developed in JavaScript and hosted on an EC2 AWS.

Tests were performed for four different settings to determine the reliability and additional time required by Ambient-Discovery. All tests were conducted using a Python script that performed 50 login attempts. Passwords-based authentication was used in every test. The following settings were given for each experiment:

1. 1FA: This test was designed to gather data about the reliability of password only authentication. Only the password portion of the protocol was used in this test. This test showed

that the script was able to successfully login the user on every attempt and capture the time required to authenticate the user.

2. 2FA with Computer Bluetooth Disabled: In this test the Bluetooth capabilities on the computer is disabled, thus preventing the browser from being able to scan for BLE devices. In this test the Bluetooth capabilities on the phone are enabled.

3. 2FA with Smart Phone Bluetooth Disabled: In this test the Bluetooth capabilities on the smart phone were disabled to measure the response. While the computer has Bluetooth enabled allows the browser to scan for BLE devices in range.

4. 2FA with Bluetooth Out of Range: This test had two factor authentication setup with Bluetooth enabled on the smartphone, but not within range of the browser. The range was 15 meters. Communication outside of that range may not be reliable. Most smartphones have a Bluetooth range of 10 meters, so tests beyond this point were used to demonstrate what would happen if the device was out of range [20]. The computer's Bluetooth was enabled, thus enabling the browser to scan for BLE devices within range.

5. 2FA with Bluetooth in Range: This test has Bluetooth enabled on both the computer and the mobile device. The mobile device is also within range of the computer, thus allowing the browser to discover the BLE advertisement from the mobile device. During this test the mobile device was within one meter of the computer.

5.2 Data Collection

The data was collected and exported using JavaScript file. The following items were collected during every test: time stamp and a boolean to indicate if the server authenticated the user successfully.

5.3 Performance

We investigated the reliability of different settings, this test was designed to gather information about the additional time required in various settings. The time was captured from the moment the login button on the webpage was clicked and ended when the server responded indicting if the user was authenticated or not.

1. 1FA: Time is captured from when the user submits credentials until the password authentication protocol is complete. This test showed that the standalone password authentication required less than 2 seconds to respond.

2. 2FA with Computer Bluetooth Disabled: Time is captured from when the user submits credentials and the server responded to the browser with authentication results. This test showed that when Bluetooth is disabled on the computer, the browser responded with a time close to password authentication, the time required less than 16 seconds to respond.

3. 2FA with Smart Phone Bluetooth Disabled: Time is captured from when the user submits credentials and the server responded to the browser with authentication results. This test showed that the time required to complete the 2FA was less than 16 seconds to respond.

4. 2FA with Bluetooth Out of Range: Time is captured from when the user submits credentials and the server responded to the browser with authentication results. This test showed that the time required to complete 2FA with these settings was less than 16 seconds to respond.

5. 2FA with Bluetooth in Range: Time is captured from when the user submits credentials and the server responded to the browser with authentication results. This test showed that the time required to complete the 2FA was less than 14 seconds to respond.

The results for these experiments are within Table 5.1. These results show that the protocol requires additional time, but within reason.

Table 5.1 Time Performance for Authentication Scenarios (n=50)

Authentication Mechanism	Mean (s)	Standard Deviation
1FA (Password-Based Authentication)	2.1	0.0024
2FA with Computer Bluetooth Disabled	15	1.0391
2FA with Smart Phone Bluetooth Disabled	15.2	0.0158
2FA with Bluetooth Out of Range	15.2	0.032
2FA with Bluetooth in Range	13	3.0261

5.4 Bonneau's Comparative Framework

5.4.1 Usability: Ambient-Discovery

The usability of Ambient-Discovery provides *MemoryWise-Effortless*, *Easy-to-Learn*, and *Easy-to-Use* due to the fact that it does not require the user to memorize or learn anything new. Since the protocol can support multiple devices and accounts, we believe that it is *Scalable-for-Users*. The user must have their smartphone with them in order to authenticate with Ambient-Discovery, for this reason we stated that it does not meet *Nothing-to-Carry* criteria. Ambient-Discovery does offer the *Quasi-Nothing-to-Carry* benefit since smartphones are a regular carried item. *Infrequent-Errors* was listed as somewhat provided because the system will provide errors if the password is incorrect or if the phone does not have Internet access. Since registration is required to authenticate and multiple devices can be registered per user this gives the protocol a *Easy-Recovery-from-Loss* benefit. The passive authentication nature of Ambient-Discovery makes gives the protocol the *Physically-Effortless* benefit.

5.4.2 Deployability: Ambient-Discovery

Ambient-Discovery does not require the user to install plugins on their browser. The Chrome browser comes with BLE scanning capabilities, therefore it is *Browser-Compatible*. Ambient-Discovery does not interfere with password based authentication, therefore it is accessible. The protocol requires adding a function to an existing server design that supports password-based authentication, thus it is *Server-Compatible*. This protocol does not require anyone to pay royalties

and is simple to implement, therefore it provides *Non-Proprietary* and *Negligible-Cost-pre-User* benefits. Due to limited resources we were unable to deploy this protocol on a large scale, therefore, Ambient-Discovery has not undergone a stress test to qualify for the *Mature* benefit.

5.4.3 Security: Ambient-Discovery

The security benefits of Ambient-Discovery are more lucrative than passwords. Ambient-Discovery is *Resilient-to-Physical*, *Resilient-to-Targeted-Impersonations*, and *Resilient-to-Phishing* because no user interaction is required. Therefore, there is nothing to physically watch or mimic. The benefit of *Resilient-to-Throttled-Guessing* and *Resilient-to-Unthrottled-Guessing* is provided because all communication is encrypted. The messages exchanged between the mobile application and server change upon every login attempt. The results of evaluating Ambient-Discovery using the Bonneaus's framework can be seen if Table 5.2.

5.4.4 Ambient-Discovery Comparison to Password-based Authentication

Based on the evaluation from Bonneau's framework, we believe that Ambient-Discovery fares well. In Table 5.2, we evaluated Ambient-Discovery method against password-based authentication scheme. As stated in chapter 3, an ideal protocol would provide security without requiring additional user interaction. We argue that Ambient-Discovery is ideal based on the Bonneau Framework. As seen in the Table 5.2, Ambient-Discovery is more secure than passwords alone. Ambient-Discovery provides nine security benefits compared to passwords five. Our 2FA mechanism provides usability comparable to password-based authentication, Ambient-Discovery provides two more benefits than passwords. The user is not required to retrieve their phone out of their pocket, thus not inconveniencing the user by requiring them to navigate away from the login screen. Removing the need to pair with the browsers enables this protocol to be used on with any computer, thus the easing the deployment and removing the need to track if this computer is a personal device.

Table 5.2 Comparison of Ambient-Discovery against password-based authentication using the Bonneau's framework [1]. 'y' := benefit provided, 's' := benefit somewhat provided, ' ' := benefit not provided

	Scheme	Usability								Deployability					Security									
Password	Memorywise-Effortless	y	Scalable-for-Users		Nothing-to-Carry		Quasi-Nothing-to-Carry	y	Physically-Effortless	y	Easy-to-Learn	y	Easy-to-User	y	Infrequent-Errors	s	Easy-Recovery-from-Loss	y	Accessible	y	Negligible-Cost-per-User	y	Server-Compatible	s	Browser-Compatible	s	Mature	y	Non-Proprietary	y	Resilient-to-Physical-Observation	y	Resilient-to-Targeted-Impersonation	y	Resilient-to-Throttled-Guessing	y	Resilient-to-Unthrottled-Guessing	y	Resilient-to-Internal-Observation	s	Resilient-to-Leaks-from-Other-Verifiers	y	Resilient-to-Phishing	s	Resilient-to-Theft	y	No-Trusted-Third-Party		Requiring-Explicit-Consent	y	Unlinkable	y
Ambient-Discovery		y		y		y		y		y		y		s		y		y		y		y		s				y		y		y		y		y		y		y		y		y		y		y	

5.5 Challenges and Limitations

5.5.1 Bluetooth

We chose Bluetooth as a means of identification because it comes standard with most Internet connectable devices; such as smartphones, tablets, laptops, wireless audio devices, car connectivity devices, fitness products, household appliances, as well as new technologies. In 2015, more than 3 billion Bluetooth devices were shipped, and Bluetooth is projected to continue increasing in usage with nearly 5 billion to be sold in 2019 [21]. Most smart phones come equipped with Bluetooth technology [15]. BLE 5 requires that both devices have Bluetooth 5.0 in order to make this protocol work. Bluetooth facilitated the passive feature of Ambient-Discovery.

5.5.2 Smartphone

Android phones require the application to request permission within the manifest file in order to access anything related to Bluetooth. The required manifest file provides Android with essential information about the application being installed, including a list of required permissions [22]. Due to the fact that Media Access Control (MAC) address are designed to be globally unique and typically cannot be altered, Android has disabled the ability to programmatically access the MAC address. If a third party application attempts to access the Bluetooth MAC address programmatically through the *BluetoothAdapter* class, the device will return the follow default value *02:00:00:00:00:00*. As a result, we were required to change the protocol. Android does not allow access of the Bluetooth MAC Address, we decided to use BLE instead of classic Bluetooth.

5.5.3 Web Bluetooth

Initially, the browser was responsible for scanning for nearby Bluetooth devices. Chrome Bluetooth functionality is built off the Generic Attributes (GATT) protocol. GATT is restricted to BLE devices and does not support classic Bluetooth. The design limitation of the GATT forced use to BLE. Bluetooth web functionality is in the early stage of development and is not stable. The functionality provided volatile and subject to change without notice.

5.6 Future Work

The Ambient-Discovery prototype for this thesis did not fully explore the possibilities of authentication problems it could solve. This protocol could be adapted to support Internet of Things (IoT) devices. Most IoT devices leverage Bluetooth as a medium of communication between the device and a mobile application. While some IoT devices utilize BLE, it is not guaranteed. Ambient-Discovery would require adaptation to accommodate this restriction.

CHAPTER 6. CONCLUSION

We proposed a new 2FA mechanism for websites. Ambient-Discovery leverages Bluetooth technology, to verify if a user is within the area of the browser being logged into. The unique aspect of Ambient-Discovery is that is leverages technology within the users smartphone to determine their proximity, therefore making it a possession-based authentication factor. The user would not be required to interact with their phone, therefore they can keep their phone in their packet. Although Ambient-Discovery increases the login time, the additional time required is negligible and can be decreased with optimization. Ambient-Discovery adds a layer of security without increasing user interaction.

Acronyms

1FA Single-Factor Authentication.

2FA Two-Factor Authentication.

API Application Programming Interface.

ATM Automated Teller Machine.

AWS Amazon Web Services.

BLE Bluetooth Low Energy.

EC2 Elastics Compute Cloud.

GATT Generic Attributes.

GPS Global Positioning System.

IoT Internet of Things.

MAC Media Access Control.

PIN Personal Identification Number.

RFID Radio Frequency Identification.

SMS Short Message Service.

TLS Transportation Socket Layer.

VPN Virtual Private Network.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," pp. 553–567, May 2012.

[2] J. Pagliery. (2016, May) Hackers selling 117 million linkedin passwords. [Online]. Available: http://money.cnn.com/2016/05/19/technology/linkedin-hack/

[3] C. McGoogan. (2016, Aug.) Dropbox hackers stole 68 million passwords-check if you're affected and how to protect yourself. [Online]. Available: http://www.telegraph.co.uk/technology/2016/08/31/dropbox-hackers-stole-70-million-passwords-and-email-addresses/

[4] K. Conger. (2016, Oct.) Weebly hacked, 43 million credentials stolen.

[5] C. Everett, "Are passwords finally dying?" *Network Security*, vol. 2016, no. 2, pp. 10 – 14, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485816300174

[6] (2017, October) Double up on security. [Online]. Available: https://duo.com/product/trusted-users/two-factor-authentication

[7] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y. Choong *et al.*, "Draft nist special publication 800 63b digital identity guidelines."

[8] S. Khandelwal. (2017, Mar.) One million stolen gmail and yahoo acconts for sale on dark web. [Online]. Available: https://thehackernews.com/2017/03/gmail-yahoo-password-hack.html

[9] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking,"

Computers and Security, vol. 30, no. 4, pp. 208 – 220, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404810001148

[10] (2017, Mar.) Html5 geolocation. [Online]. Available: https://www.w3schools.com/html/html5_geolocation.asp

[11] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun, "Sound-proof: Usable two-factor authentication based on ambient sound," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 483–498. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/karapanos

[12] G. Kumparak. (2014, Feb.) Google acquires slicklogin, the sound-based password alternative.

[13] A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and D. Balfanz, "Strengthening user authentication through opportunistic cryptographic identity assertions," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 404–414. [Online]. Available: http://doi.acm.org/10.1145/2382196.2382240

[14] (2017, Aug.) Ble advertising. [Online]. Available: https://source.android.com/devices/bluetooth/ble_advertising

[15] (2017, Aug.) Mobile phones and smart phones. [Online]. Available: https://www.bluetooth.com/what-is-bluetooth-technology/where-to-find-it/mobile-phones-smart-phones

[16] (2017, October) Global mobile os market share in sales to end users from 1st quarter 2009 to 1st quarter 2017. [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

[17] (2017, March) Open wonder: Introducing android 8.0. [Online]. Available: https://www.android.com/versions/oreo-8-0/

[18] W. Warne. (2017, Feb.) Exploring bluetooth 5 - what's new in advertising? [Online]. Available: https://blog.bluetooth.com/exploring-bluetooth5-whats-new-in-advertising

[19] (2017, October) About fcm message. [Online]. Available: https://firebase.google.com/docs/cloud-messaging/concept-options

[20] J. Wright. (2007, Sept.) Dispelling common bluetooth misconceptions. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/bluetooth

[21] D. kleiner. (2015, April) That's a wrap, bluetooth world 2017. retrieved from bluetooth. [Online]. Available: https://blog.bluetooth.com/thats-a-wrap-bluetooth-world-2017

[22] (2017, October) App manifest. [Online]. Available: https://developer.android.com/guide/topics/manifest/manifest-intro.html