East African Scholars Journal of Engineering and Computer Sciences
Abbreviated Key Title: East African Scholars J Eng Comput Sci
ISSN 2617-4480 (Print) | ISSN 2663-0346 (Online) |
Published By East African Scholars Publisher, Kenya

OPEN ACCESS

Volume-2 | Issue-1 | January-2019 |

Review Article

E-Commerce Authentication

Shamik Palit

Assistant Professor, Manipal Academy of Higher Education , Dubai Campus, Dubai International Academic City, Dubai, United Arab Emirates

*Corresponding Author
Shamik Palit

Abstract: One-Time Passwords, or OTPs, and a few other techniques, such as the use of proprietary tokens, have been instituted as a counter measure to authentication & authorization attacks on Internet services especially for transactions on E-commerce, as well as a counter to phishing. OTP is commonly used for many different websites and applications. However, OTPs are not as secure as they seem. They can be vulnerable to heavy attack, especially by Trojans; even those that are encrypted. In this research, I shall analyze and study the architectural integrity of OTPs when it comes to security and the attacks that could pose a threat to authorization and authentication services. I will detail why OTPs can no longer be deemed as secure, and propose technologies that make authentication and authorization in E-commerce a much secure process.

Keywords: e commerce, authentication, transactons, e business, authorization, security

Chapter 1: Introduction

There are a handful of security measures that are used for online transactions in e-commerce. OTPs are a widely used measure, as an additional fall-back technology in a multi-factor authentication system. Users must enter their received OTP after they have logged in using their credentials, i.e. their username and password. They are frequently used for verification purposes in online transactions. SMS OTP, like mTan (mobile Transaction Authorisation Number) is quite commonly used. This is used for the authorisation of online transactions.(Mulliner, C *et al.*,2013, July). However, OTPs are not quite as secure as they seem to be. For example, SMS OTPs depend on the privacy of the SMS messages. But these SMS messages rely on cellular network security. Attacks on GSM and 3G networks have proven that SMS security cannot be guaranteed. Another vulnerability which is exploited by attackers is mobile phone security. Criminals have advanced their methods and created specialised Trojans. These Trojans obtain the SMS OTPs sent to devices and are used to access the victims personal accounts. When it comes to E-commerce especially, this is can pose a major threat to the security of customer finances.

In its current state, one-time password security needs to be improved. It can be done by first investigating attacks that can be used against OTPs and analysing those attacks that have taken place in the real world. Through analysis we would be able to conclude that the notion OTPs are still secure is false. Based on the outcome of the analysis, we can contemplate new security improvements and policies that can be implemented to improve the current state of OTPs.

One of the major improvements is a system that requires the connectivity of a mobile phone to the device which is used to access a website. This utilises location services as well as the implementation of Bluetooth Low Energy (R. van Rijswijk-Deij 2010) which also works well with Apple‟s iBeacon technology. This system would ensure that the device being used for the authentication exists in the same confined vicinity of the device that is used for access.(Aloul, F., Zahidi, S & El-Hajj, W., 2009) A secondary solution would be image based authentication. This authentication utilises images chosen by a user that are representative of certain keywords evaluated by the system. So, when asked to select the images after login, the system would generate images based on the keywords (so they are not exactly the same as the one that the user chose, but similar). After successfully choosing the right image, OTP would be validated and verification would be complete.

Quick Response Code

Journal homepage:
http://www.easpublisher.com/easjecs/

Article History
Received: 14.12.2018
Accepted: 25.12.2018
Published: 15.01.2019

DOI: 10.36349/easjecs.2019.v02i01.003

Chapter 2: E-commerce Security

2.1 Introduction

Security and privacy concerns are at the top of the list for e-commerce stores. These e-commerce web applications are usually in charge of the payments that a customer would make to them. The methods of transactions include the use of credit cards, debit cards, electronic transactions and even online wallets like PayPal. Because so many transactions take place online on these e-commerce websites, they have become a lucrative target for hackers and thus are more likely to be targeted than most other kinds of websites.

The e-commerce industry is slowly and constantly trying to deal with the security issues that they must face. Educating customers on adequate behavior that could keep their account safe is not enough, and as a result the e-commerce industry have to scramble to properly strengthen their security infrastructure.

2.2 The Need for Security

With the ever increasing exponential growth of online shopping, security is of utmost concern for all of the e-commerce stores; not just the retailers, but also for any business that utilises the internet for crucial transactions. It is a very convenient method of spending money to buy desired goods and services. But to ensure the trust and the continued patronage of the consumers, these e-commerce websites must be able to provide above-average security to their customers in order to make it a secure place to shop where threats to customer information, both personal and financial, should be ideally non-existent.

2.3 Existing Security Measures

Common methods used in e-commerce authentication are as follows:

Tokens are possessed by a user that is used to authenticate their identity. In e-commerce authentication, users authenticate themselves through the system or the application in a network. This token must be kept secret and well protected.

Fig. No. 1: A Sample Token

1. Passwords & PINs consist of various combinations of symbols, and alphanumeric values which is more secure than a typical password. Utilizing and implementing TLS and SSL during the transmission creates encrypted channels to exchange data and therefore protect information. However, a majority of attacks occur on services that rely purely on password based authentication.(https://web.archive.org).

SMS-based authentication is when a user of an e-commerce website or banking service receives a password, called One-time password, via an SMS message. Mobile phones are everywhere, so, this technique is highly preferred and the most used.

Symmetric-key authentication is where the user must share a unique key with the server that authenticates. This is when a user sends a challenge that is encrypted to the authentication server, only if the shared secret key is matched to the message that is provided by the server. When this occurs, the user is authenticated (https://web.archive.org).

2.Public key authentication is where there exists two parts of the authentication process; one being the private key known only to the user, and the other is a public key(www.e-authentication.gov.hk).
Biometric authentication involves the use of physiological elements of a user. They include but are not limited to retina scans, fingerprints, signatures, voice recognition and facial scans; the most commonly used biometric authentication being the fingerprint (https://web.archive.org/).

Chapter 3: One-time Password

3.1 Introduction

An OTP, or one-time password, is that which has a lifetime of a single login session, or, as commonly used, for transactions. OTPs were designed to overcome the various limitations that were evident with the static passwords that are used for authentication. They have also been used to integrate two-factor authentication systems (2FA) online, that utilise physical objects that a person possesses, like mobile phones, smartcards, or proprietary tokens to validate the one-time passwords.

The greatest benefit of implementing OTPs as a security measure is that they are invulnerable to replay attacks; network attacks that maliciously repeat or delay data transmissions. So, if an attacker were to obtain an OTP that had already been used to log in, or authorise a transaction, they would not be able to use it, as its validity would have expired. Another benefit is that those users who tend to use a similar password for every account are not as vulnerable. Attackers who obtain any of these passwords would find it unusable if they don"t have access to the OTP.

OTPs are created using generation algorithms that ensure randomness of the password generated. This would make it undoubtedly harder for any potential attackers by making it impossible for them to predict an OTP. Hash functions are used to derive values that cannot be backtracked, thus making it difficult for attackers to gain access to the data used in the hash.

There are different types of generation methods of OTPs. Time synchronisation is one, where there is a relation between an authentication server and the client responsible for the password. Another method is using mathematical algorithms to create passwords related to their previous iterations, or passwords based on a challenge given to the user.

There are differing methods of OTP distribution as well. These include security/proprietary tokens that a user must physically have with them that provide them with the OTP required. Another is a common method, using mobile phones of users that utilises software or SMSes.

However, despite all this, OTPs are still quite insecure. OTP technology has remained unchanged for a long time, but attacker technology has improved. Tactics such as Man in the Middle attacks, wireless GSM interception, and the worst of all, mobile phone Trojans have rendered OTP technology no longer secure.

3.2 Generation of OTP

3.2.1 Time-synchronized

Time synchronised OTPs are most commonly related to security tokens, that provides users with a token that is specific to them. It would look like a key fob or a tiny calculator, that displays the OTP. These devices have an accurate internal clock, that has been synchronised with the same clock on the authentication server.(Kalaikavitha, E., & Gnanaselvi, J.,2013).Time plays a vital role in the generation of these OTPs as a part of the algorithm. The generation of the time synchronized OTPs are independent of any previous OTPs generated. Tokens can themselves vary from requirement to requirement; it may be a proprietary token, or software that runs on a user"s mobile phone.

A standard of time synchronised OTP is TOTP, or Time-based One Time Password.

Fig. No. 2: A Time-synchronised Token by SecurePass

3.2.2 Mathematical Algorithms

Using mathematical algorithms, an OTP may be generated as a derivation from a previously generated OTP. A popular algorithm that incorporates this is the one created by Leslie Lamport. (L. J. Iacone., 2009) His algorithm utilises a one-way function. The working is as follows: (Kalaikavitha, E., & Gnanaselvi, J.,2013)

First, a seed, or starting value is chosen. E.g.: s.

Hash function is then used repeatedly to the chosen seed value. This can happen any number of times, even a thousand. So, for example, f¬500(s) is stored in the system.

The user"s first login will then us a password by using f 499 times to the seed. The system can then validate the password as the correct one. The generated value that is stored is then replaced by the password, thus allowing the user to log in.

The succeeding log in must then be f498 (s). This is further validated as a result of the hashing done that provides the password from f499(s), i.e. the value of the previous log in. So, the newly created value has now replaced the password, and the user is then allowed to log in.

This process can be done 497 more time, and every time validation occurs by checking after it has been hashed; the value of the previous log in has been stored. Hash functions have been created in such a way that they can be very tricky to reverse, thus making it so that the attacker requires knowledge of the initial seed s to calculate potential passwords. If the set for seed value s has been exhausted, then a new seed value is chosen, and this way passwords can continue to be generated,

Some algorithms allow users to give the server a static key to be used for encryption, by sending just an OTP.

Challenge response OTPs are also used, in which users are required to provide a solution to a challenge. To steer clear of duplicates, counters are utilised, so, duplicate challenges that warrant a response would generate distinct one-time passwords. These computations don"t rely on the existence of preceding OTPs. In other words, either algorithm is used, but not both.

3.3 Delivery of OTP

There are various ways to deliver OTPs to users that they"ll need for authorization.

3.3.1 Proprietary Tokens

Chip Authentication Program is a new kind of challenge-response algorithm that is coming in to play in European markets, instigated by EMV. Another technology being used is RSA Security"s SecurID that uses time synchronization methodologies for their tokens; HID Global is another.

Fig. No. 3: ActivID Token – HID Global Security Tokens

Tokens like these are undoubtedly inconvenient. They are likely to get lost, stolen or damaged. Other factors can play a part as well, such as battery exhaustion, especially on those tokens without the functionality that allowed users to recharge the battery.

To combat these inconveniences, a new kind of proprietary token was suggested by RSA that could be used for ubiquitous authentication. The proposal was to partner with different manufacturers and add physical components,

Secure ID chips, to devices, like cell phones. Soon after, OTP tokens came to be in the credit card form, where electronic parts related to regular keys for OTP tokens were embedded.

3.3.2 Mobile Phones

There is a significant portion of users who have access to the Internet, and those who utilise e-commerce services, who already have mobile phones. The utilisation of something that a user already possesses is beneficial as it keeps costs low. The fact that this reception of OTPs on mobile phones require very little computation power or storage. A single mobile phone application can provide the user with multiple OTPs, allowing users to receive and thereby authenticate multiple services and transaction right from a single device. After every transaction is confirmed, they would be asked to check their mobile phones for the OTP.

Fig. No. 4: ActivID OTP from HID Tokens

3.3.3 Text Messages

The most common form of OTP delivery used in e-commerce transaction security is text messaging. Text messaging is preferred by most organizations as it is an absolute ubiquitous communication channel that is used by so many users of mobile devices worldwide, thus deemed as a low cost solution. So, naturally an OTP system implemented using this technology is desirable.

Fig. No. 5: Example of an SMS OTP

However, there is a major flaw with delivery of OTPs over text messaging. OTP over text is commonly encrypted using A5/x standard protocol. But, it has been reported that several hacking groups over the years have been successful in decrypting it within minutes or seconds. Sometimes the OTPs may not even be encrypted by the service provider. When a user's service is set to roaming, different service-providers must be trusted as well. The utilization of such information can and has led to many man-in-the-middle attacks.

3.4 Hash Chains

A Hash chain is used to apply successive iterations of a cryptographic hash function to data fragments. This is used to generate multiple one-time passwords from a single password. The hash function may be applied continuously to more fragments of data to keep a track of data chronology and its existence.

The hash function h(x) is applied successively to string x.

So, h(h(h(h(x)))) would give a hash chain length of 5, that is usually denoted by h5(x).

Leslie Lamport proposed the idea that hash chains could be used for password protection, especially in situations that demanded more security.(Lamport, L.,1981).Authenticating servers store the hash chains, instead of the alternative of storing a text password, to thereby prevent password theft during transactions or right from the server.

If, for example, a server stores h1000(password) that the user provides, and then requires authentication, h999(password) must be provided to the server. The server then calculates h(h999(password)) = h1000(password) and validates the matches with that which the hash chain has stored. h999 is then stored for when the user decides to authenticate next.

Eavesdroppers that see h999(password) being communicated with the server cannot re-transmit similar hash chains for authentication and validation by the server, as the server is now expecting h998(password). It stops becoming a feasible process for eavesdroppers to backtrack hash functions to gather fragments of earlier hash chains. Here, user authentication can occur a 100 times until the hash chain expires; every time the value is unique so, ideally, they cannot be replicated by any potential hackers (M. Y. Rhee., 2009).

Binary hash chains are another commonly used technique related to hash trees. What it does, is that it takes two different hash values for input values, merges them together and then applies the hash function to what is resulted. This produces a 3rd hash value.

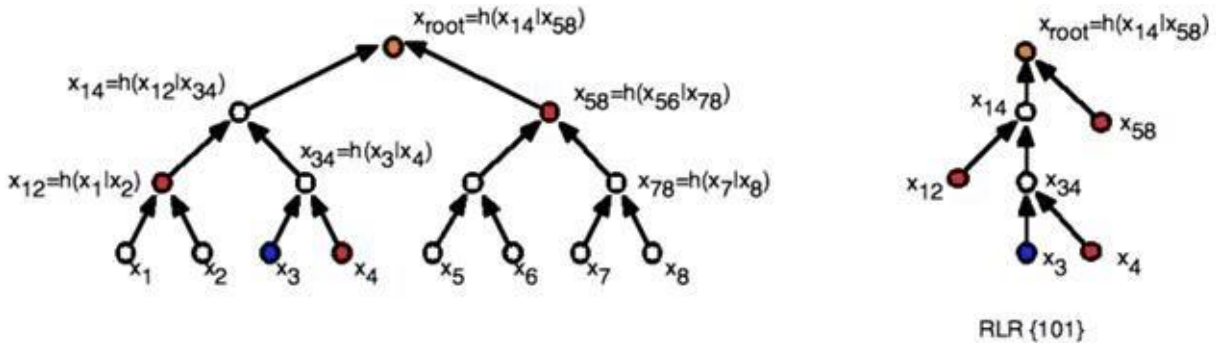

Fig. No. 6: Binary Hash Chain Working

Here we see a hash tree with eight leaves and a hash chain on the right that represents the 3rd leaf node. It is important to note that the concatenation order also has an effect on the complete hash chain.

3.5 Encryption

3.5.1 AES Algorithm

AES is a symmetric and iterative key block cipher which utilises 128, 192, and 256 bit keys strengths. The encryption and decryption process takes place in 128 bits blocks. The max block size is restricted to 256 bits, but it is important to note that these key sizes don't have any theoretical maximums. This isn't like the public key ciphers that uses different keys to decrypt and encrypt the data. What the user must do is select the AES decrypt or encrypt on their data. The encryption tool enables them to convert plaintext input to cipher text through continuous repetitions that are reliant on the encryption key provided (Kalaikavitha, E., & Gnanaselvi, J.,2013).On the other hand, the decryption method for AES has a similar process which involves changing the cipher text back to plaintext, in our case, the OTP. It

is a quite difficult encryption to defeat, and a hash is implemented in order to prevent the loss of encryption key secrecy resulting from any brute force attacks. It is widely used in securing information online and is used to secure e-commerce transactions by banks or e-commerce websites.

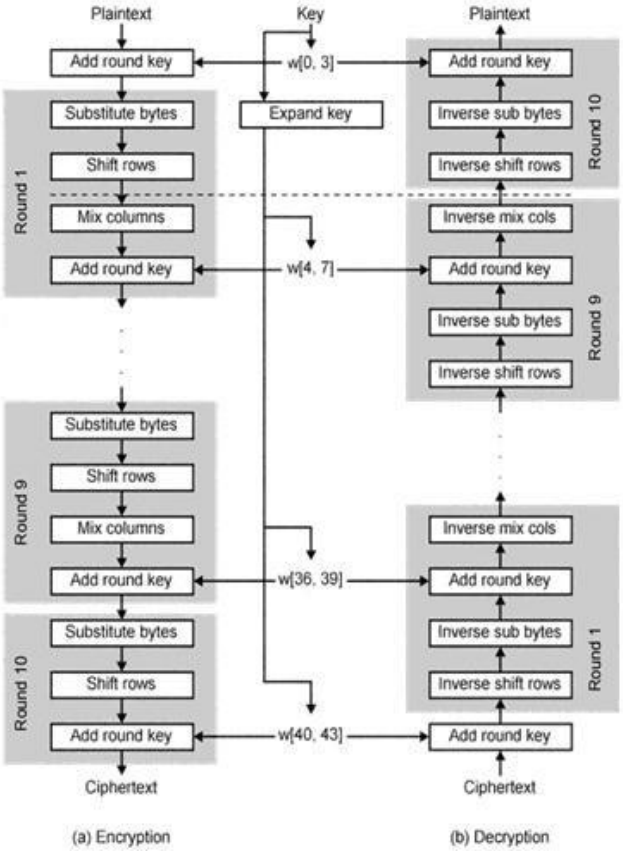

Fig. No. 7: The Process of AES Encryption & Decryption

3.5.2 A5/1

A5/1 is a type of stream cipher that enforces privacy for over the air communication in GSM standard. GSM transmissions are arranged through burst sequences. In a specified channel and direction, a burst is sent every 4.6 ms containing 114 information bits. It is used to create a 114-bit keystream sequence with XOR applied on the bits before the modulation. The initialization of A5/1 is done with a 64-bit key and a public 22-bit frame.

A5/1 revolves around the use of 3 LFSRs which have unorthodox clocking systems. The 3 shift registers are as follows:

Table No. 1: Linear Feedback Shift Registers

LFSR number	Length in bits	Feedback Polynomial	Clocking bit	Tapped bits
1	19	$^{19} + ^{18} + ^{17} + ^{14} + 1$	8	13, 16, 17, 18
2	22	$^{22} + ^{21} + 1$	10	20, 21
3	23	$^{23} + ^{22} + ^{21} + ^{8} + 1$	10	7, 20, 21, 22

The indexing of bits occurs in order of the LSB. These registers are clocked in a way that allows for go and stop using the rule of majority. Every cycle, the majority clocking bit of the registers is calculated. (Dubin, J)A register is thus clocked only when the bit agrees with the majority. Therefore, 2-3 registers are clocked with a step probability of 0.75.

After the initial zero value of the registers, for 64 whole cycle, the 64-bit key is added to the following:

In a cycle from 0 to 64, the ith bit is added to the LSB using XOR for every register.

$$R[0] = R[0] \Phi K[i]$$

Following this, every register becomes clocked. Likewise, the frame"s 22-bits are done in 22 cycles. After completion, the cipher can create 2 114 bit sequences of output keystream; the 1st 114 for downlink, and the last 114 for uplink.

3.6 Verification of OTP

Those applications that require OTP authentication for secure login and access to services initiates an OTP challenge. Depending the requirements of the challenge and the secret code that is necessary, the generation algorithm that was used can also be used to analyse the one-time password passed on by the server for verification.

The database of the server that contains for every user, a one-time password that was used for the latest successful authentication, or the first of nascent sequence. Thus, to complete the authentication of the user, the generator sends OTPs to the server where it is decoded into a 64-bit key. Then, the key is checked by running it through a secure hash function. If the check concludes with a match with a previously stored OTP, the authentication is a success and the OTP is then stored for later use.

Chapter 4: Security Threats

4.1 Man-in-the-Middle

A phishing website is that which is made to closely resemble those of an existing bank or an e-commerce store. What it does is that it obtains user credentials, including ID and password, thus enabling the hacker to login when they desire to maliciously use the account for their personal financial gain. OTPs tend to make this process harder however, as it is a constantly changing number which would most likely be changed by the time the hacker logs in.(Barkan, E & Biham, E.,2005)

Man-in-the-middle attacks is what hackers have started to use to make the process easier. The attacker would utilise a server that acts as a „middleman" between the user and the original website. This server communicates with user and website simultaneously to retrieve the login information that includes the OTP values as it is received by the user. As this technique revolves around real time hacking and retrieval of the token, its security features become useless.

In 2006, the first successful OTP attack had taken place using this real-time MITM attack. Russian hackers had successfully breached Citibank using this technique. In January of 2007, a different hacking group developed a tool that would copy the website and design of the legitimate websites of banks or e-commerce stores, create false URLs that seemed true, and would set up a server to relay credential information in real time to the attackers. This kit was quite openly sold on the internet.

Once susceptible victims were able to be lured into these fake websites using the fake URLs, via, for example, spam emails, and logged in to the website, the information would be immediately sent to the original website so that the attackers could easily siphon off the money in the victim"s account.

4.2 Wireless Interception

Current GSM technology is not secure. It has several flaws, including its lack of mutual authentication, as well as encryption algorithms that are not up to par. There have been several studies that have showed the evident weaknesses in the communication that takes place between phones and base stations. They can be eavesdropped on, and the weaknesses in protocols can be exploited and decrypted by hackers/attackers.(Golde, N. *et al.*,R,2012)[14] It has also been proven that femtocells, miniature base stations that are installed in user homes, can be hacked and used to intercept communication, especially SMS messages.(Dr. Igor Muttik.,2011) The attack is executed through installed firmware on the femtocell that is a modified version. This modified firmware is capable of sniffing and intercepting communication.

The TR-069 protocol is the most frequently used protocol for managing femtocells. However, this protocol is quite vulnerable. The problem femtocells are that they are run as root most of the time to run effectively. Therein lies the

problem. So attackers who exploit this can gain full access.(Binsalleeh *et al.*,2010) These femtocells contain a lot of information as well, private information, such as subscriber ID, the IMSI, & the ID of the phone, the IMEI. Femtocells most often have a configuration web page which can also be hacked into to alter configurations. It had also been reported, in BlackHat 2011, that some femtocells collate logs that are not encrypted to be sent to the operator using FTP. The log details user activity as well.

Service providers that utilise SMS OTPs blindly expect high security for the MNOs, but as is evident, security is not guaranteed. Countries like India do not have network traffic encrypted by default. (Mulliner, C *et al.,* 2013) Network operators may disable their encryption deliberately to decrease network load. In these situations, hackers with appropriate tools may be able to take advantage and capture OTPs OTA.

4.3 ZeuS in The Mobile

Trojans, in mobile phones are a great threat to OTP transaction security. There are Trojans created just for the purpose of intercepting SMS messages that provide users with the OTP to complete their transactions. These Trojans have been an increasing threat, and was created by hackers and criminals for this sole purpose of stealing money.

The ZeuS toolkit was developed by hackers to create several kinds of Trojans that were made to steal information and thus, to damage. This kit is openly available online as well. It was first created it 2007, but since then it continues to grow and wreak financial havoc as more and more Trojans are created. ZeuS has become a crime-ware tool of choice for attackers thanks to its competitive pricing and easy to use user interface.(Etaher, N. *et al.*,2015) Theft of banking details or login details is quite terrible for a person, however attacks such as these can tarnish the reputation of the banks as well.

ZeuS-in-the-mobile (ZitMo) is a mobilised version of the Trojan. It is a ZeuS botnet that transcended into the mobile phone space to target online banking and online transactions. Utilising social engineering methods, it is capable of stealing mTANs that are sent to users through SMS messages, by the service provides and the e-commerce agents. Using trickery, the attackers are able to install a security question malware, which is actually a ZitMo bot. Zitmo supports a variety of mobile OS, such as Symbian OS, Window Mobile, Android, and BlackBerry.(Maslennikov, D.,2011)

The ZitMo Trojan first started spreading in the time of the ever popular Symbian OS, specifically designed to intercept SMS messages containing mTANs. Its binary was delivered as a normally signed application for the OS and contained crucial capabilities that would enable it to e register itself with the Symbian operating system; so that it could retrieve the SMS messages when they arrived from the network. The SMS message would then be forwarded to a predefined phone number. ZitMo is also capable of deleting text messages. The hackers utilise this capability efficiently, by deleting the SMS after it has been forwarded to the predefined mobile number. This way the user who is the victim of the attacker, is totally unaware of the fact that an SMS was sent to him/her in the first place. This keeps victims clueless about the attack until it"s too late. The ZitMo Trojan can also be used by the attacker to configure settings of the infected phone, and to change, for example, the destination number to which an SMS would be forwarded.

In 2011, a ZeuS version was created for the Windows Mobile OS which came to replace the Symbian OS. It was named the Trojan-Spy.WinCE.Zbot.a [19] It had the same basic functionalities as the ZitMo. A similar Trojan exists for the Android OS, as well as the BlackBerry OS by RIM.

The Android Trojan that are able to intercept the SMS OTPs were MMarketPay.A Trojan. This Trojan was a tad different. It would buy goods from online stores, then intercept the OTPs that were required to verify the transaction that were sent to a user"s mobile device by accessing their SMS messages.

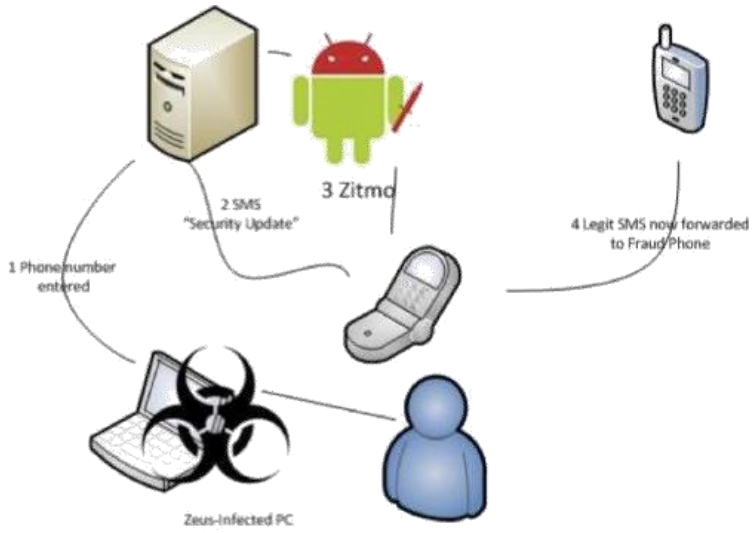

Fig. No. 8: The ZitMo Cycle

A lot of OS manufacturers provide developers with the ability to access SMS messages with an API. They can also aid in the delivery of these SMS messages to the mobile device. If this is a possibility, then attackers could utilise the same framework to obtain, modify, delete and forward the SMS messages to their own mobile phone without the user having a clue of what is going on.

Mobile phones in the past used a system where only a single CPU would run the OS and the baseband, i.e. the cellular interface. However, now, have two separate systems, on specifically for the OS, and one specifically for the baseband. Older phones had very restrictive measures to improve the security of the baseband as a result of manufacturers trying to protect their OS as well. It helped protect the SMS messages. (Mulliner, C 2013) But, due to the separation of the two, mobile phone manufacturers are not concerned with the security of the baseband anymore. As a result, manufacturers were very open with their OS, and provided developers with the API to access SMS messages, whereas previously, access to SMS messages was unavailable to them, not even Trojans. This end-to-end security is no longer available on current phones. Nowadays, iOS and Android applications require permission to be granted by the user to be able to access the SMS messages, but unfortunately many users just grant this permission so that they can get on with using the application.(Bloomberg.,2014)

4.4 E-commerce Attacks in the Real World

4.4.1 CurrentC

CurrentC is a mobile payment method rival to Apple Pay and Android Pay. It is supported by popular retailers like Wal-Mart. A security breach in 2014 led to hackers gaining access to the emails of all the clients of CurrentC's program. MCX, the developer of the software, stated that their email service provider had been hacked too. Prior to this occurrence, the mobile payment system that they were working on was breached as well.(http://www.it-security-inc.com)

4.4.2 Staples

Another attack in 2014, where a giant retailer, Staples lost the details of 1.2 million credit cards of their consumers to hackers. It was a major security breach that occurred between July & September. After a thorough investigation of the incident, it was revealed that these hackers used specially designed malware to infiltrate the system thus granting the attackers access to transaction information. The credit card information that was stolen included the cardholder's name, the numbers, expiration dates, and the verification codes. This was followed by several reports of fraudulent usage of the cards.(C. Cawley.,2014)

4.4.3 JP Morgan & Chase

Online banking mobile applications are so commonplace these days that it's hard to imagine oneself being the victim of identity theft. A security breach took place on JP Morgan and Chase Company in 2014, where attackers were able to access their servers through the root. With this, the attackers were able to release information of customers, transfer funds to external accounts, create new accounts, and also shut down whichever accounts they want. This incident has been considered to be one of the largest attacks on a corporation in US history. The information accessed was stolen from about 76 million families, and 7 million businesses.(C. Cawley.,2014)

4.4.4 eBay

This widely used, international e-commerce giant with its trustworthy reputation was attacked with a major security breach where millions of passwords of user were stolen. And, right after this attack another one occurred using a Cross Site Scripting or XSS. This involves inserting malicious code to redirect users to fake websites. There the user entered their credentials and in doing so the attackers would have immediately gained access to their accounts.(https://esj.com)

Chapter 5: Analysis

5.1 The Need for Change

Nowadays, 100s of millions of people rely on this outdated and insecure method of verification and authentication. As is evident, e-commerce providers and banks need to replace, or at the least modify, the OTP system used as a means of security.

The headlines are proof of this. The most popular and widely used OTP system manufacturer, RSA‟s CEO came out to inform everyone that their servers had been hacked. SecurID tokens had been obtained by the attackers, and this indicated to them that the effectiveness of this authentication system has dwindled as a result of lacking innovation.

Many OTP service providers have been ripping off their customers as well. Organisations pay a lot for the OTP systems, for little actual value.(W. Morrison., https://www.logintc.com)Some of them lack proper encryption techniques, while others may be using outdated encryption algorithms.

The inconvenience of one-time passwords is quite apparent. One-time passwords need their applications to be constantly changing to protect them, and this brings about many limitations. The users would need to copy the OTP from wherever the user has received it, and quite often these passwords are not simple ones.

There is also a terrible assumption made by many, if not all, OTP providers. It‟s that they falsely assume the security provided by mobile network operators. They assume that SMS messages cannot be hacked into by attackers. Those users that utilize the roaming feature are also quite vulnerable as they will have to trust many networks. Many networks in 3rd world countries may not even be encrypted.

Mobile malware, as described, is another problem; and a very obvious threat by now. Cellular network security and encryption is known to be weak. So, attackers have exploited this weakness thoroughly to use malware, such as Trojans specifically, to intercept the SMS messages that contain vital OTP information that most often is used to protect user transactions.

In its nascent stages, OTPs were never created as an additional factor for security. It was designed to combat replay attacks that were at large during its time when majority of communication through networks were unencrypted and password sniffing was problematic. (https://www.whatsapp.com/)

Chapter 6: Mobile Phone Improvements

6.1 Introduction

Changes can be made to the hardware utilization in a system that requires OTP. Existing hardware, like mobile phones, which is a common device used for the retrieval of OTP can definitely use some improvements. All the problems associated with receiving OTP on a mobile phone imposes a great security threat to both the user and the e-commerce website service.

For starters, the connection to the device in question would need to be made more secure, to ensure that the data is only accessed by the user and none else. An end-to-end encryption is what is required of this communication, as well as a dedicated channel that is responsible for handling OTP that is received through SMS messages. Another feature of a majority of smartphones nowadays are severely underutilized. The feature is the Bluetooth Low Energy & iBeacon for iOS. These connectivity features are seldom used by the users of the devices that support them. And, when they are used, they are for meagre tasks. These features can be utilized quite well if they were implemented into security protocols in e-commerce.

6.2 End-to-end Encryption

End-to-end encryption is slowly being implemented by giants like WhatsApp.(https://developer.android.com) They used this encryption on all media and messages to prevent them from being accessed by potential hackers. What end-to-end encryption basically does is that it ensures that the only communication that occurs is between two *ends*, so to speak. Every message that is passed would be locked, and the only way a recipient would be able to access the data is through a special key that they would possess.

So, OTP messages sent via SMS would be locked using this encryption method, thus preventing any interception. Application private storage is something that is available on all smartphones and mobile operating systems. This storage is private storage that any application is only allowed to use, and store data. [1] Platforms such as Android, iOS, Windows Phone, and J2ME has this kind of storage. The developers at Android themselves has stated that, "You can save files directly on the device's internal storage. By default, files saved to the internal storage are private to your application and other applications cannot access them (nor can the user). When the user uninstalls your application, these files are removed. "(https://technet.microsoft.com) Both iOS and Windows Phone also have similar functionalities.

So, what occurs in an end-to-end encryption is that when an OTP is generated by its respective service, the message becomes immediately encrypted with a particular key. This key would then be available to the consumer that initiated the OTP service system. When the user receives OTP via an SMS message through traditional methods, a specific application designed for end-to-end encryption which would have been installed on the phone would decrypt the SMS OTP message, thus making it available for use by the user.

To ensure the correct working of this process, a Key distribution centre is required. It would be responsible for authenticating users so that the system can ensure that the key is being delivered to the correct location and permissions to utilize a service. If the conditions are met, the users are provided with the appropriate key.

KDCs usually work using symmetric encryption and creates tickets depending on what the server key is. The ticket is then sent to the user/client who in turn sends it to an appropriate server. When the server has verified the ticket that is submitted by the client, then the client is granted access to their activities. Kerberos is a widely used protocol that implements KDC quite well.(Parmar *et al.*,2012)

6.3 Bluetooth Low Energy & iBeacon

Bluetooth Low Energy and iBeacon implements the same are a part of the latest version of the Bluetooth protocol, Bluetooth 4.0. Devices that can utilise the BLE feature can operate at a range of about 50m, which can be further altered by varying power for the transmission to decrease max distance.

BLE enabled devices advertise their presence at regular intervals (R. van Rijswijk-Deij.,2010) on 3 different bands across the spectrum in order to minimise the interference that it may cause with other signals in the vicinity, for instance, Wi-Fi. These advertisements are transmissions that can permit data transfer of up to 31 bytes. The iBeacon system is able to transfer 3 data elements that include the UUID (Universally Unique Identifier), and the "major" & "minor" location values. The OS permits apps on the device to scan and try to locate for beacons that are broadcasting a very specific UUID. The UUID is responsible for identifying one or multiple beacons of a group. What the "major" and "minor" location values do, is that they locate and pinpoint a specific beacon among the group of beacons identified by the UUID.

So, these major and minor values are capable of transmitting specific data, in our case OTP information, from the beacon to a particular device. The beacon's location is the restricting factor in this scenario, therefore, this type of system could be used in corporations or large scale industries where espionage is also a concern and the misappropriation of funds. This way, every online transaction can be monitored, and this is especially useful for when large amounts of money are being transferred and connections must be secure.

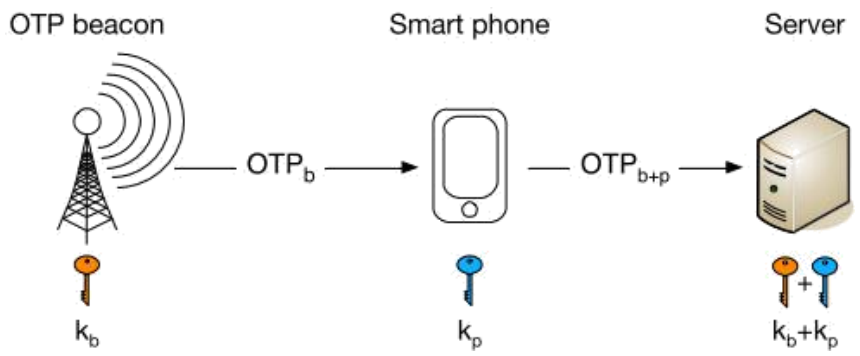

Fig. No. 9: iBeacon Method [2]

So, a user that would like to authenticate themselves on the server would initiate the OTP authentication application on their device. The application with its granted permissions would be able to scan for beacons in the vicinity to receive an OTP when detected through broadcast advertisements. The mobile device together with its secret key is able to generate the required OTP from the one received through the beacon. The OTP is sent to the server for authentication and grant transaction rights and access if successful.

Chapter 7: Image-Based Authentication

7.1 Introduction

There is another alternative solution which doesn't require tampering with the hardware elements of any authentication system. This image-based authentication technique would be done at the source itself, that is on the e-commerce website that requires an improvement in its security. The idea behind this system is as follows. The user will have to select particular images during the inception of his/her account. The images would be selected from an ideally endless library of images. When logging into the account and approving transactions, the user would then be asked to pick an image or a set of images from a grid of several images. The image the user would have to choose would have to represent the same image(s) that the user selected in set up.

The way this would occur is using advanced image recognition techniques that would be implemented by the e-commerce system. The image recognition would determine what the key aspects of the initially selected images were and utilise the keywords understood from the image to display a suitable grid of images on login or for transaction approval. The key words wouldn't be saved thus leaving attackers at a disadvantage.

7.2 Approach

The Image Identification Set (IIS) stores the images of users in the Authentication System.(Vision, A. P. I.,2017) So, when the user tries to log in to the website the IIS for a specific user is taken and used to authenticate the user. The images themselves cannot be stored into the IIS due to their size, so instead the category of the image is stored, or rather, the keywords associated with the images.

7.2.1 Google Cloud Vision API

The Google Cloud Vision API is widely known to be an advanced image analysis tool. This is the same API implemented in Google's image search engine. This API is quite suitable for image-based authentication as its analysis capabilities are required to understand those image(s) selected.

The API utilizing machine learning abilities to be able to thoroughly understand the contents of an image. It classifies images into several thousands of categories. For example: “Oak tree”, “cruise ship”, “Big Ben”, etc. Objects are scanned for within an image to obtain the different categories that could describe the image. This category detection feature is very useful for the working of the image authentication system. The images are not stored in the IIS, the categories are, and that can only be achieved through Google Cloud Vision.

This process does not end here. When the user tries to log in to their account and the categories are retrieved from the IIS, these categories must be matched to existing images. The Vision API utilises these existing categories to retrieve a bevy of images that match it. Now, from this list, only a few shall be chosen mixed with some bogus images unrelated to the categories specified and then displayed on a grid for the user to pick from.

Once the user has selected the appropriate category images from the grid, they will be verified successfully and can go about their transactions.

Chapter 8: Conclusion

OTP systems are a widely used multi-factor authentication technology that does not require extra inconvenient devices, such as proprietary tokens. The purpose of their creation and implementation on a wide scale after its inception was to fight replay and data delay attacks, which were common during the time. However, current OTP systems are lacking in the very field for which they were designed: security. This limitation can prove to be especially deleterious when it comes to E-commerce where transactions with credit or debit cards and other online means of payment occur. Over the years, attackers have become resourceful and have developed improved methods of gaining access to confidential information; Trojans being the most common and effective method of infiltration and retrieval of the OTP to hack into accounts. Yet, despite all of this and the attacks that have occurred on major e-commerce websites, as discussed, OTPs have barely changed.

Changes must be made. It could be through the physical devices that are involved in the authentication of accounts and transactions, by improving communication security among the devices using end-to-end encryption, or through existing technologies within these devices which are highly underutilized. Although, these techniques may be

expensive to implement, they may be well worth it if they are meant to prevent the potential loss of large amounts of money, and private information of consumers.

Changes can also be made on the front end through the website of the e-commerce retailers. A yet to be explored technique using image-based authentication can be implemented with the help of Google"s Cloud Vision API, to develop a system that utilize machine learning and image recognition. The technique could fend off attackers as well as a system such as this would be hard to breach through brute force. A user"s physical memory is used to authenticate themselves and that keeps attackers at a loss.

References

1. "5 Reasons to Replace Your Traditional One-Time Passwords,(2011)" *Enterprise Systems Journal*. Available: https://esj.com
2. "e-Authentication Methods - Public-Key Authentication," *web archive*. [Online]. Available:- www.e-authentication.gov.hk
3. "e-Authentication Methods - Symmetric-Key Authentication," *web archive*. [Online]. Available: https://web.archive.org
4. "e-Authentication Methods - Biometric Authentication," *web archive*. [Online]. Available: https://web.archive.org/
5. "e-Authentication Methods - Passwords and PINs," *web archive*. [Online]. Available: https://web.archive.org
6. "Kerberos Key Distribution Center," (*Microsoft*, 11-Dec-2016) [Online]. Available: https://technet.microsoft.com
7. "Storage Options | Android Developers."(10-Dec-2016).Available: https://developer.android.com
8. "The 10 Worst Security Incidents Of 2014 Breaches," *IT Security, Inc*.Available: http://www.it-security-inc.com
9. "WhatsApp - End-to-end Encryption," (*WhatsApp*, 2015),Available: https://www.whatsapp.com/
10. Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* (pp. 641-644). IEEE.
11. Barkan, E., & Biham, E. (2005, August). Conditional estimators: An effective attack on A5/1. In *International Workshop on Selected Areas in Cryptography* (pp. 1-19). Springer, Berlin, Heidelberg.
12. Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010, August). On the analysis of the zeus botnet crimeware toolkit. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on* (pp. 31-38). IEEE.
13. Bloomberg,(2014) "CurrentC"s Data Breach Adds to Awful Week for Apple Pay Rival," *Bloomberg.*
14. C. Cawley,(2014) "eBay Security Breach: Time To Reconsider Your Membership?," *makeuseof*, Available: http://www.makeuseof.com/
15. Dr. Igor Muttik, (2011),"Securing Mobile Devices: Present and Future," *McAfee Labs*.
16. Dubin, J. Are one-time password tokens susceptible to man-in-the-middle attacks.
17. Etaher, N., Weir, G. R., & Alazab, M. (2015, August). From zeus to zitmo: Trends in banking malware. In *Trustcom/BigDataSE/ISPA, 2015 IEEE* (Vol. 1, pp. 1386-1391). IEEE.
18. Felt, A. P., Greenwood, K., & Wagner, D. (2011, June). The effectiveness of application permissions. In *Proceedings of the 2nd USENIX conference on Web application development* (pp. 7-7).
19. Golde, N., Redon, K., & Borgaonkar, R. (2012, February). Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications. In *NDSS*.
20. Kalaikavitha, E., & Gnanaselvi, J. (2013). Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. *International Journal of Engineering and Science*, *2*(10), 14-17.
21. L. J. Iacone, "Lamport"s one-time password algorithm," *Javaworld*, 2009. [Online]. Available: http://www.javaworld.com/
22. Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770-772.
23. M. Y. Rhee, *Mobile Communication Systems and Security*.(2009),Singapore: John Wiley & Sons (Asia) Pte Ltd,
24. Maslennikov, D. (2011). ZeuS in the Mobile is back. *SecureList Blog*.
25. Mulliner, C., Borgaonkar, R., Stewin, P., & Seifert, J. P. (2013, July). SMS-based one-time passwords: attacks and defense. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 150-159). Springer, Berlin, Heidelberg.
26. Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. *Journal of Computer Science and Information Technology*, *7*, 195-206.
27. R. van Rijswijk-Deij,(2010), "Simple Location-Based One-time Passwords," *Utr. Tech. Pap*.
28. Vision, A. P. I. (2017). Image Content Analysis/Google Cloud Platform.
29. W. Morrison, "The Fundamental Problem With OTPs in Two-Factor Authentication," *LoginTC* (2014), Available: https://www.logintc.com