VULNERABILITIES OF NON-BIOMETRIC AUTHENTICATION SYSTEMS.

FINAL PROJECT FOR COURSE

<<05/05/2018>>

CCSER @ IIIT-B

IMT2015037

LAKSHMI PRIYA RAMISETTY.

PREFACE:-

Most of my work was complete research on the Concept rather than implementation of the project. I have looked through a lot of articles and a lot of reviews on Biometric authentication and then looked up for Non-Biometric Two factor authentication and looked up for some case studies online(Citations written). Then i came to a conclusion on OTP type of 2FA. And i wrote my views on how to prevent your bank account from being hacked and what to do when it gets hacked.

TABLE OF CONTENTS:-

INTRODUCTION:-

MAIN TEXT:-

Lets have a look at what Biometric authentication system is ,

Biometric is a security mechanism used for authentication and providing access to an individual based on verification of one's physical characteristics which are pre-stored in a biometric security system or scanner.They include fingerprint recognition(our finger print), iris and retina recognition(scanning eye), face recognition, voice recognition(recording our voice and recognising it) and latest technologies like behavioural recognition. It has very high accuracy and high speed.

Pros and Cons of Biometric Authentication Systems:-

Pros of Biometric Authentication Systems:-

1. Hard to Fake. Every person has a different finger print as already known.So, it is hard to manipulate the finger print or the retina until and unless some mishap happens which leads to a change in them.

2. They are stable and enduring. They wont change over ur lifetime inspite a little variation over time.

3. Easy to use. It is easy for people to use their finger print or voice for scanning or any other means rather than using hard core systems.

4. They are non-transferrable.As in they don't change over time.

5. They are less time consuming. It hardly takes more than 5 seconds to use them.

Cons of Biometric Authentication Systems:-

1. Accuracy. It is very less accurate when we capture the data partially and leads to a failure.

2. Privacy. It is easy to hack for people these days. What if the server in which you are storing the data gets hacked? It has very bad consequences when this happens.An example of the breach is the U.S. Office of Personnel Management (OPM), which was hacked resulting in the theft of 5.6 million fingerprints.

3. Error in devices. They start accepting false users and rejects users as well. So it is hard to differentiate the true one among others.

4. High Cost. Its quite a big amount to invest in the devices and its not upto mark.

So, as we have seen the Biometric authentication Systems and its pros and cons, lets add something to it.

If we add MFA(Multi-Factor Authentication) to Biometric Authentication System, it might be safer comparatively.

What are Non-Biometric Authentication Systems?

As we have seen Biometric Authentication systems, we come to a conclusion that it uses Physical body as in it need you to be involved in it. Coming to Non-Biometric Authentication Systems, it doesn't involve you as in your body, all it does is through computer. For Eg, OTP(One-Time Password).

OTP is one of the most popular Authentication Systems.It is widely used during login and transactions as a part of Two-factor Authentication(2FA) process, it is very vulnerable to cyber criminals.

CASE STUDIES:-

17th March 2016.

In Australia, things have gone from bad to worse in just a few weeks. Early in February, the Australian Communications and Media Authority (ACMA) reported that banking customers in Australia and New Zealand are being targeted with fraudulent SMS messages containing URLs that direct them to fake mobile banking sites. Fraudsters harvest their login credentials by means of a man-in-the-middle (MITM) attack – essentially hijacking the messages between the user and the bank.

If a mobile phone is compromised because its user unwittingly downloaded a malicious app (malware) onto it, the fraudster can simply command the malware to monitor text messages – including those containing OTPs – on that phone. Despite a decade of warnings over the vulnerabilities of SMS-based 2FA systems, many financial institutions still use them. Australian telcos urged banks not to use SMS for authentication back in 2012, with seemingly little effect. Now, after the discovery of an industrial-scale malware attack last week, perceptions should start changing quickly.

On 9 March, antivirus software company ESET warned that twenty banks in Australia, New Zealand, and Turkey are being targeted in a single, sophisticated attack. The weapon, catchily named Android/Spy.Agent.SI, is disguised as a version of the Adobe Flash Player app, which users are tricked into downloading from infected websites or illegitimate app stores (a reminder never to stray from the Google Play Store and Apple's App Store). The trojan lurks in the background until the user opens their mobile banking app. It then creates a fake login screen to access the user's login credentials. Designed specifically to bypass SMS-based 2FA, it then redirects all incoming OTPs to the hacker, and neither the user nor the bank will be any the wiser. Until the user checks their bank balance, that is.

Also attacking the banking customers of at least six banks in Australia, as well as one in Russia, is Xbot. Discovered by Paulo Alto Networks trojan has several very nasty tricks up its sleeve, including cloning the login pages of mobile banking apps and intercepting SMS OTPs. The same approach is used by the SlemBunk trojan, so named by FireEye late last year. It currently imitates the legitimate banking apps of 33 banking institutions in

North America, Europe, and Asia-Pacific. Not to be left out, Kaspersky Labs continues to track the emergence of Asacub, which seems to focus on banks in Russia and Europe and spreads through SMS spam.

Meanwhile, Symantec reports that Android.Bankosy has evolved beyond accessing SMS OTPs and is now capable of stealing OTPs delivered via voice messaging through call forwarding.

By all of the above case studies, i can say that it is easy for hackers to get into your system by just spamming people a malicious software, i.e.; just by sending u fake links which divert to various sites and thereby they can hack your system from the software in your device. So, from then , they get your OTP, and all the information about your bank details and they withdraw money without even you knowing unless you checked it online.

What to do when your Bank account gets Hacked?

1. Contact your bank and first block your bank credit/debit card.

2. If the bank account is hacked immediately after you have done some online transaction from some PC, then first scan and clean your PC with latest anti-virus scanner. This is to get rid of any rootkit or key logger that may have been installed on the PC and which would have compromised your login details and sent it to the hacker.

3. Reset your login password, pin, security questions answers.

4. Verify your contact details like address, phone number are not changed by the hacker.

5. Report the scam to right authority in the bank.

6. Report a fraud to local police station.

CONCLUSION:-

Monetary losses resulting from these attacks are not yet known, but one loss is certain and permanent.People have lost confidence in SMS OTP as a security technique. It's time for banks to step up their user protection with out-of-band solutions that are impervious to this kind of exploit.It is easy for people to get into your system, so its better to have some preventive measures in your system like antivirus installed and running continuous scan tests regularly.

REFERENCES:-

1. * <<Dennis McCafferty>>, << CRN >>,<< May 29, 2002>> https://www.crn.com/features/security/18837938/non-biometric-security-solutions.htm
2. https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/01/05/15-important-pros-and-cons-biometric-authentication
3. Case Study - https://www.entersekt.com/blog/2016-an-annus-horribilis-for-sms-otp (I didn't change anything in the case study

just to provide the accurate and exact information written in the article.)