Krunal Murlidhar Kumbhare

19BCE1210

TARP

Faculty: Dr. Umity Srinivasa Rao

## Abstract

Over the years we have seen rising cases of cyber attacks like backdoor attacks, phishing, etc. This is of great concern as lots of money, time, hardware are exploited and several others are still vulnerable. Most powerful tool of a system which can access anything is the terminal. If it is vulnerable then anything could be exploited. My solution to this problem is an application terminal locker which has two parts- terminal application, mobile app. Using terminal locker users can be authenticated and authorized to get access to terminals in remote servers. This application enhances the security of servers and also reduces cases of loss of availability of servers.

## Introduction

A successful organization can be achieved if it has a good security in its core computers, it is through these their work is done and if these devices are vulnerable to small attacks, the whole organization might get affected. Our project “Terminal locker” aims to achieve a secure connection between the computers and the server and securing the terminal of each computers as well.

The Terminal, also known as the command line, is an essential component of any useful operating system. Linux has very powerful console ( terminal). One small command has power to format entire directory. So there can be big security issues if proper care is not taken. So this project focuses on preventing such situations by securing the terminal.

The research by Parikh and Patel [1] concluded that advancement in cybersecuriity technology would generally lead to reduced impact of attacks but also humans are important to reduce the impact. A big part of security lies on the user and their behavior, impulses, psychological predispositions and, decisions. So if people are educated in proper way the social engineering attacks can be reduced. [2] For confirming remote hosts, SSH1 uses the RSA open/ private key. The default design licenses clients to well-known new open keys of remote hosts without affirmation via testaments.

[4] The password-guessing attacks can be classified as non-stealthy attacks and stealthy attacks. In a non-stealthy password guessing attack, there are several login attempts in a short duration. These login attempts are detected and blocked by existing security tools. Those attacks that can't be detected via way of means of the prevailing protection equipment are known as stealthy password guessing attacks. Since they're now no longer detected, they're additionally now no longer blocked via way of means of security tools. Stealthy password guessing attacks may be initiated manually via way of means of a person (hacker) or automatic via a botnet (disbursed set of bots). In the guide mode, the attacker makes use of a single source (a pc with a selected IP address) with a password cracking tool to perform the attack.

It would take a lot of time to educate people about all the vulnerabilities, precautions, procedures, protocols, etc. So my solution is to introduce the concept of QR code which they would be scanning from their phone’s app and the connection would be established.

In general people in the industries use Yubikey, Zukey, passwords, RFID to configure, secure, authorize their personal devices and computers. Such devices are costly and also they need to be programmed. There are companies, labs, work places where there are less budget assigned to security. So they may not be able to equip themselves with authentication devices mentioned above. So they may lock their computer, shutdown, hibernate, or unplug their systems. This isn’t a good idea always as will increase the time cost for the company. My solution is to introduce a more handy application which would be installed in the computers and would require no other extra investment in buying new sophisticated devices for authentication and verification. A part of the software would be installed in the computer and the other part which is an app would be installed in a smartphone, tablet, or any other computer. Upon scanning the code there would be connection establishment based on the inputs received.

The algorithm which we are planning to use for encryption is HMAC algorithm.

[5] In 2003, a comparison between HMAC-SHA-1 and CBC-MAC-AES was performed. It was observed that the hardware performances differences weren’t that significant. And also there was no significant difference in software performances. But we must also note that the hardware implementations of HMAC had improved performances as the packets becomes larger.

## Literature Survey

[7][8] Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

[13] There are various vulnerabilities which are or could be exploited by hackers and crackers. Like session hijacking, phishing attacks, man in the middle attack, attacks using social engineering, etc. There are also wireless network threats. They are of two types- active, passive.

Attackers change the contents and information of the message put fake information to destroy the network security. Here integrity is disturbed. Examples of this are unauthorized access, active eavesdropping, man in the middle attack, session hijacking, DoS. Whereas the attacks where the attacker just listens and reads the packets and doesn’t alter its contents are passive attacks. These type of attacks are usually hard to detect.

There are phishing attacks where similar looking web pages are made with identical content. But the URL link differs and points to attacker’s site. If the user unknowingly/ knowingly proceeds to use the application then the attacker would e able to track and get the information of users. They may get to know their usernames, password, OTP, email id, phone number, date of birth, etc.

To overcome this problem we can replace the password, OTP, other confidential information with QR codes.

There are various algorithms, techniques, methods used for encryption. [6] Mainly they are classified into six types- cryptography key algorithm, hash function algorithm, digital signature algorithm, web security algorithm, email security algorithm and IP security algorithm.

Under cryptography key we have symmetric and asymmetric key algorithms. Most popular ones are DES, AES.

DES is a block cipher. The message is divied into blocks. Each block size of 64 bits and with 56 bits key length. It uses two attributes of cryptography- substitution and transportation. It involves 16 steps.

AES is a symmetric key algorithm. Here the block size is of 64 bits and the key length 128, 192 or 256 bits. The whole block of data is treated as a matrix. The message in the form of block is then passed through operations and we get the cipher. AES was introduced to overcome the drawbacks of DES.

In the study by Sujatha [11], they compared the time required for encryption using various algorithms. It was found that 3DES took more time than DES and DES took more time than AES. Also the speedup ratio of AES was decreasing for larger inputs.

Under the asymmetric key algorithm we have RSA as one of the popular algorithms which is currently in use. RSA stands for Rives-Shamir-Adleman. The encryption key is not secret here. Main iidea is based on product factorization of two large prime numbers. It has four steps namely key generation, key distribution, encryption and decryption.

For the hash function algorithm MD5, SHA-512, HMAC, etc. Algorithms are used. MD5 is used to save the integritiy of the message transferred. Here the user compares the checksum of the message received. The output is of a fixed length of 128 bits in MD5. And input block sizes are 512 bits.

SHA- 512 is another popular algorith,. SHA-2, SHA-256 are other algorithms that are famous in the SHA family. SHA-256 is used by Bitcoin. The output is of fized length. Hash function divides the output equally. The input is padded with padding bits. The input consists of original message, padding bits, padding size. There are default value considered to start with. 1024 bits block and the output of previous step is taken as an input in this method.

HMAC stands for hash message authentication code. It is used in IPSec, SSH, TLS and several other authentication systems. It also has application in JSON Web Tokens. Two keys- inner and outer- are derived from the secret key. Due to this the immunity towards attacks is increased.

The digital signature algorithms two keys- public, private. The private key can be verified using the public key. The signature helps to verify, authenticate messages, check for integration and non-repudiation. Four main operations involved are- key generation, distribution, signing and verification of signature.

SSL algorithm is widely used wev security algorithm. It stands for secure socket layer algorithm. It is designed to communicate between network and application layer of network topology. IT satistfies confidentiality of message triad of CIA triad. Also provides digital signature functionality. There are public, private key which play a big role in encryptioni, decryption.

SET algorithm is a web security algorithm. It stands for Secure Electronic Transaction. It is mainly used for online transactions like credit cards transactions. The key features are confidentiality, integrity, cardholder bank account approval, service provider merchant authentication.

Over the years the password and OTP are getting replaced with other methods like QR code scanning, biometrics, question answering, etc. My project is focused on using QR code for authentication. Few companies use RFIDs also which is another new technology. [12] QR codes are two dimensional ( 2D) matrix of bar codes which are usually scanned using smart phones, tablets, QR code reading device, or barcode scanner. QR code has better capability of holding information when compared to barcode. It also has error correcting capability- L ( low), M ( medium), Q ( quartile), H ( high).

[3] This paper proposes an asymmetric key based authentication framework, QRToken, for easy-to-use login to websites, SSH servers, etc., QRToken authentication use clientside locally stored RSA private key to encrypt identification information as well as other parameters, and present a QR code in the form of a small two-dimensional picture that encodes the encrypted information. User takes a picture of the QR code with the cell phone camera and sends it as a cryptographic response to the server to complete the authentication process. We believe the simple act of scanning QR code for authentication brings ease in management and enhances user experience.

Their framework supports QRToken both as a software application and as a hardware device. It can also be made available to every website with their SDK package installed, due to the use of asymmetric-key mechanism. We also illustrate how to combine both software and hardware based approach as a twofactor authentication mechanism to further strengthen security.

## System design

User terminal lock command

Notify user “locked”

Terminal locked

User QR code scan

Terminal unlocked

yes

no

Fig.: Flow diagram of terminal locker

Code generated

Mobile app scan over

Fig.: Mobile app flow diagram

## Implementation of System

We are securing the part of the system that has control over the PC, i.e., the terminal. With a single command anything can be removed, created, updated or read. My solution to secure terminal is an application that is to be installed in system and a mobile application to authenticate the user.

The system application is terminal locker. The flow of terminal locker is shown in the diagram above.

When the user executes the terminal locker command the terminal locker first checks if the terminal is already locked. If it is locked then it notifies user. Else it locks the terminal. And then it also notifies other terminals on PC about the “locked” state of the terminals.

Then whatever terminal is open/close/idle/working would be locked. Even the new terminals which would be opened would be locked already. This step is done using file system by changing the lock variable in the file to “Yes” or “No” based on the state of the terminal locker. The file content is set to “Yes” if the terminal is locked else it is “No”.

Now the terminal is locked and would be unlocked only when the user authenticates. For authenticatiion purpose the user has to use the mobile app.

For this the user has to open the app and grant the required utilities, accesssories access it ( for example camera). Then focus the camera towards the QR code and scan it.

In the backend of the app, a new URL would be generated and would be redirected to the browser. There the query would alter the contents of the file on the server by setting the content to “No”.

The server then reads the file and sets “unlock” if the content of the file is “No”. For unlocking all the terminals on the PC are notified. This is done using a bash script which is appended to .bashrc file.

References

[1] http://www.raijmr.com/ijrmeet/wp-content/uploads/2017/12/IJRMEET\_2017\_vol05\_issue\_06\_01.pdf

[2] https://acadpubl.eu/jsi/2017-116-13-22/articles/16/97.pdf

[3] Andrews, Ron & Hahn, Dalton & Bardas, Alexandru. (2020). Measuring the Prevalence of the Password Authentication Vulnerability in SSH. 1-7. 10.1109/ICC40277.2020.9148912.

[4] [http://link.springer.com.egateway.chennai.vit.ac.in/article/10.1007/s12530-020-09360-3#Sec1](http://link.springer.com.egateway.chennai.vit.ac.in/article/10.1007/s12530-020-09360-3" \l "Sec1)

[5] Deepakumara, Janaka & Heys, Howard & Venkatesan, R.. (2003). Performance comparison of message authentication code (MAC) algorithms for Internet protocol security (IPSEC).

[6] Patil, Chandrashekhar. (2020). Study on Network Security Algorithm.

[7] "What is Network Security? Poda myre". Forcepoint. 2018-08-09. Retrieved 2020-12-05.

[8] [https://en.wikipedia.org/wiki/Network\_security#cite\_note-1](https://en.wikipedia.org/wiki/Network_security" \l "cite_note-1)

[9] https://research.ijcaonline.org/icaet2016/number2/icaet036.pdf

[10] https://www.ijser.org/researchpaper/Implementation-of-Advanced-Encryption-Standard-Algorithm.pdf

[11] https://www.ijert.org/research/renowned-information-security-algorithms-a-comparative-study-IJERTV5IS020233.pdf

[12] Shettar, Iranna. (2016). Quick Response (QR) Codes in Libraries: Case study on the use of QR codes in the Central Library, NITK.

[13] Tariq, Muhammad. (2011). Wireless Security and Threats.

[14] Xu, F., Han, S., Wang, Y., Zhang, J., & Li, Y. (2015). QRToken: Unifying Authentication Framework to Protect User Online Identity. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing.