Key Logging Resistant Using Visual Authentication

Sushan Poojary[1] Nitin Patil[2] Ganesh Rane[3] Aruna Pavate[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Atharva College of Engineering, Mumbai, India

Abstract— Now a days, the design of secure authentication process is challenging, as various kinds of keyloggers can be installed in personal computers to capture each and every keystroke made by the user and to make PC's untrusted devices. There are many legitimate keyloggers are present in the market, however, any legitimate keylogger can still be used with malicious software. Also, intervention of human in an authentication process, while promising better security, is not easy because of the limited capability of computation and memorization of human. Therefore, depending on users to enhance security ultimately degrades the usability. In this proposed work, we demonstrate how a careful design of an authentication process can enhance not only the security but also the usability of authentication. The proposed system uses two visual authentication protocols: one is a password (i.e. login credentials) based protocol, and the other one is a QR code based authentication protocol. The aim of this work is to prevent Keylogging without compromising with the usability.

Key words: Authentication, Malicious software, Keylogger, QR code

I. Introduction

The credential stealing and channel breaking attacks are the two major threats in electronic and financial services. The credential information such as users' identifiers, passwords and keys can be easily stolen by the attacker from the target computers if they are less secured. On the other hand, channel breaking attacks allow eavesdropping of communication between the user and the financial institution. The recent channel breaking attacks are more challenging like keylogging which utilizes session hijacking, pharming, phishing and visual fraudulence. It is difficult to prevent these attacks by simply encryption. For example, if a personal computer is infected with malicious software, then it is an easy target for credential attackers [1].

A. Keyloggers

Keyloggers, or keystroke loggers, are ingenious software programs or hardware attachments, used mainly for identity theft. Very simply, they record all the keystrokes a user inputs. The data is then either sent across to a person on the other end, or stored for later retrieval. However, like everything else, keyloggers have evolved greatly and are now capable of recording almost anything on the computer – right from voice conversations to clipboard contents [2].

B. Types Of Keyloggers

1) Hardware Keyloggers

The other large category is hardware-based keyloggers, which serve the same purpose, but are fundamentally different in the way of achieving their goal. They are fully self-contained hardware units that are attached to the computer, most usually as a plug between the keyboard and the computer, and they require no software to be set up. Different to software keyloggers, all the data is stored on the piece of hardware, and it never appears on the computer that is being monitored. Consequently, the only way to retrieve the stored data is by retrieving the hardware unit itself. As the data is not stored on the computer, it can't be accessed while the keylogger is working, nor is it vulnerable to anti-spyware software or hard drive crashes, which would usually erase software keylogger data[2].

Hardware keylogger is inserted between the keyboard and the USB (or PS/2) port. It also contains its own CPU to avoid drawing on the resources of your computer. Some of the USB keylogger devices are equipped with WiFi so you can access the data by logging into your email account.

2) Software Keyloggers

Keylogger software is a program that you download and install on your PC. It is often downloaded from reputable websites for the purpose of monitoring the computing activity of your child, employee, or as a means of retrieving your data in the event your PC crashes.

When you download keylogger software it runs in stealth mode which means it is invisible to the PC user. Although the software is installed on the hard drive it is not visible if you look for it in any files or folders. Instead it takes a password in order to make it visible.

Keylogger software is capable of sending logs of recorded data to your email account or a File Transfer Protocol address on a local server where you can access it. With some programs that are used for parental control you can also block questionable websites and applications that you do not want your child to access.

Regardless of whether your use a hardware keylogger or a keylogger software it is important to be aware that it can be used for positive purposes or negative purposes. The proper way to use keyloggers is for the good and the positive [3].

C. SCOPE

Besides the security of an authentication protocol, both usability and deploy ability are equally important and critical for the acceptance of any protocol in modern computing settings.

In our proposed work, we demonstrate how visualization can enhance not only security but also usability by proposing two visual authentication protocols: one for password-based authentication, and the other for one-time-password. Moreover, using an extensive case study on a prototype of our protocols, we highlight the potential of our protocols in real-world deployment addressing users shortcomings and limits [4]. Also our proposed system will provide security against keylogging without compromising with the user experience. Thus we aim to provide a highly efficient security system with good usability by removing excessive overhead.

D. Organisation

The rest of this paper is organised as follows. In section II gives brief overview of literature survey. Section III includes Proposed System with working and protocols used in the system. Section IV describes the conclusion and future work that can be implemented.

II. REVIEW OF LITERATURE

DaeHun Nyang, proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. They have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Proposed protocols utilize simple technologies available in most out-of-the-box smart phone devices. Author developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world [5].

M. Mannan, has implemented a simple approach of Mobile Password Authentication. While PC's tend to dominate transaction processes they are vulnerable to various forms of attacks so they have used an intermediate device in the form of mobile and hence security is not entirely dependent on PC's [6].

Haichang Gao, have put forth the idea of including graphical password strategy for authentication. Their paper presents the idea that long alphanumeric passwords are hard for people to remember while shorter is easy to crack so a conclusion is to include graphical password [7].

R Divya, proposed system consisting of two protocols for authentication which resisted keylogging. The two authentication protocols are Time based One-Time-Password protocol and Password-based authentication protocol. Their proposed system shows how visualization can enhance usability and security[8].

III. PROPOSED SYSTEM

Existing Authentication Systems discussed in the above section take more than enough amounts of details from the user. Also, the user has to remember considerable amount of login details and large passwords which are difficult to remember. The usability of the system gets deteriorated as provision for high security is made available. The User Experience has to be efficient and understandable. No overhead should be caused at user's side. Remembering of long passwords every time should be avoided. Also not much of user's time should be taken for authentication. Our aim is to prevent Keylogging without compromising with the usability. Fig. 1 describes the details of the proposed system. It includes following blocks.

A. System Model

The system is basically divided in three modules:

1) Terminal
2) Server
3) Smartphone

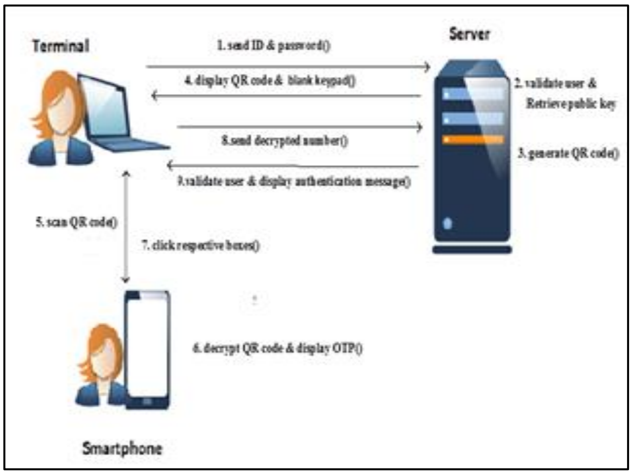
Terminal
Server
1. send ID & password()
4. display QR code & blank keypad()
2. validate user & Retrieve public key
8.send decrypted number()
3. generate QR code()
9.validate user & display authentication message()
5. scan QR code()
7. click respective boxes()
6. decrypt QR code & display OTP()
Smartphone

Fig. 1: Proposed System

1. Terminal

A user terminal is a desktop computer or a laptop using which user connects to the server. When server generates QR code, it is displayed on the terminal prompting the user to scan it with respective smartphone.

1) Server

Server is the system entity, which performs back-end operations. Server accepts and responds to the requests made by terminal interacting with the user. Using encryption, Server generates QR code when a valid user tries to connect it and display them on the terminal.

2) Smartphone

The user has a smartphone with an android application installed on it. Smartphone acts as a bridge between server and the terminal. First user has to register and login into that android application. Smartphone captures QR code displayed on the terminal and decrypts randomized OTP. It also stores a public key certificate of the server for digital signature verification which avoids request from an anonymous server.

B. Assumptions

In our system, for all trusted system entities, we assume following:

First, we assume that the connection between user's terminal and the server is secured with an SSL (Secure Sockets Layer) connection which is a very realistic assumption in most electronic banking systems. Second, we assume that the server is fully secured and immune to every attack performed by the attacker. Hence, the attacker's only concern is to attack user's terminal. Finally, we assume that the keylogger always resides at user's terminal not at server side. Hence, the attacker has a full control over the terminal.

C. Quick-Response (QR) code

A barcode is an optical machine-readable representation of data. It is widely used in our day-to-day life since it is attached to numerous amounts of products for identification. Barcode is mainly of two types: Linear barcode and Matrix or two-dimensional (also known as 2D) barcode. While linear barcodes shown in Fig.(2) have a limited capacity, which can range from 10 to 22 characters depends on the coding technique used. 2D barcodes shown in Fig.(3) have higher capacity than linear barcodes. These 2D barcodes can store more than 7000 characters. For example, the QR code is a widely used 2D barcode which can store 7,089 numeric, 4,296 alphanumeric, or 2,953 binary characters [2] making it a very good high-capacity candidate for storing plain and encrypted contents alike.

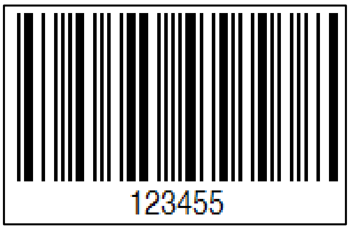

Fig. 2:

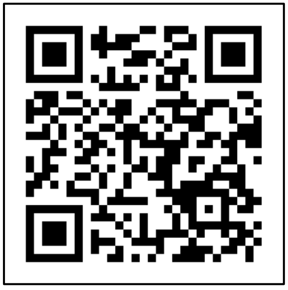

Fig. 3:

IV. Conclusion and Future Scope

In this proposed work, two visual authentication protocols which can be used to improve security and user-friendliness of the system. Moreover, we have analyzed both the protocols which not only improve the user experience but also immune to various challenging attacks, such as the keylogger and malware attacks. These protocols utilize simple technologies available in most of the smartphone devices. Therefore, our authentication protocols are feasible and can be deployed in real world as it runs with minimum hardware requirements. This work indeed opens the door for several other directions that would like to investigate as a future work. First, plan to investigate the design of other protocols with more stringent performance requirements using the same tools provided in this work. Second, there will be scope of randomly implementing arranged numerical keyboard on top of QR code and furthermost use google glasses to prevent shoulder surfing.

References

[1] R Divya, S Muthukumarasamy, " Visual Authentication Using QR Code to Prevent Keylogging", IJETT – Volume 20 Number 3 , Feb 2015

[2] http://www.brighthub.com/computing/smb-security/articles/68543.aspx on 4th April, 2017

[3] https://www.refog.com/comparison-of-hardware-and-software-keyloggers.html on 4th April, 2017

[4] DaeHun Nyang, Aziz Mohaisen, Jeonil Kang., "Keylogging-resistant visual authentication protocols", in IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 1, NO. 8, AUGUST 2014

[5] DaeHun Nyang, Aziz Mohaisen, Jeonil Kang., "Keylogging-resistant visual authentication protocols", in IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 1, NO. 8, AUGUST 2014

[6] Mohammad Mannan, P.C. van Oorschot., "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers", in Journal of Computer Security, 19(4):703–750, 2011.

[7] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, Xiyang Liu., "Yagp: Yet another graphical password strategy", in ACSAC '08 Proceedings of the 2008 Annual Computer Security Applications Conference, pages 121–129, 2008.

[8] R Divya , S Muthukumarasamy, "Visual Authentication Using QR Code to Prevent Keylogging", in International Journal of Engineering Trends and Technology (IJETT) – Volume 20 Number 3 – Feb 2015.