Visual Authentication And Security For Mobile Devices

M.Irish[#1], B.Dharani Manogran[*2]

[#] PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.
[1]irishmark15@gmail.com

[*] Assistant Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.
[2]dharani18@gmail.com

Abstract— **This paper focuses on developing an efficient key agreement protocols for two and three handheld devices over a temporal confidential and authenticated channels. It simplifies previous unnecessary complications and reduces the bottleneck associated with running time human's involvements. The Man-In-The-Middle (MITM) attack is the major threat for handheld devices to agree a session key in which they do not share any prior secret in advance, even if these devices are physically located in the same place. The Man-In-The-Middle (MITM) attack is the major threat for handheld devices to agree a session key in which they do not share any prior secret in advance, even if these devices are physically located in the same place. This work aims to improve the Bluetooth device transfer in pair devices using high security. Generates password in invisible patterns. To be used in the Visual Authentication protocol to implement and generate the selection random keys**.

.

Keywords— **MITM, Authentication protocol, Bipartite Tripartite.**

I. INTRODUCTION

The man-in-the-middle attack is a form of active cryptography and computer security in which the attacker relays messages between the victims by making independent connections with them, making them believe that they are talking directly to each other over a private connection, but in fact the entire conversation is controlled by the attacker**.** The man in the middle (MITM) attack can also be defined as an attack where monitoring is done when the communication occurs between two users and possibly modified by a third, unauthorized party. The third party may perform the attack in real time**.**

A sequence of messages are exchanged between principals that either distributes secrets among some other principals or allows the use of some secrets to be recognized which is called as an authentication protocol. The properties about the system are deduced by certain principals involved; for example, either only a few principals have access to particular Secret information (typically cryptographic keys) or a particular principal is operational. To verify claims about subsequent communication this information is used , for example, a received message encrypted with a newly distributed key must have been created after distribution of that key and so is timely. A countable number of authentication protocols have been specified and implemented**.**

They may employ existing authentication protocols that utilize passwords, long secret keys or public key as the proofs of identity. However, most of the above methods are impractical or insecure for the situation. Taking password based protocols used in Bluetooth for example, two users input the same password of four to eight digits in both handheld devices. Nevertheless, passwords are usually poorly chosen by human, so the probabilistic guard is not so strong. In addition, an adversary may oversee the device's screen and key pad using a hidden camera or a telescope while the user keying the password. After that the adversary can inject a Man-In- The-Middle (MITM) attack to intrude the protocol. Protocols that employ secret keys require the devices to share private information in advance, which is not feasible for the above scenario. It is also impractical to require every handheld device to register a public key from a certificate authority. Moreover, to avoid the MITM attack in directly sending public key to another device, the device owners need to assert the integrity of the public key. Comparing two long strings is also a difficult task for human beings therefore, it is advised to use public key

Based solutions are also not applicable to this environment. Owing to the unfeasibility in applying theoretical protocols to the practical world, constructing an efficient protocol for handheld devices is a hidden problem that should be solved by cryptographers**.**

The Man-In-The-Middle (MITM) attack is the major threat for handheld devices to agree a session key in which they do not share any prior secret in advance, even if these devices are physically located in the same place. Apart from insecurely typing passwords into handheld devices or comparing long hexadecimal keys displayed on the devices' screen, many other human-verifiable protocols have been proposed in the literature to solve the problem. Unfortunately, most of these schemes are unsalable to more users. Even when there are only three entities attempt to agree a session key, these protocols need to be reran for three times. There are several solutions [7]–[12] attempt to solve this problem. These solutions can be referred as human-verifiable authentication protocols where the security levels of these Protocols rely on human users to carefully carry out the protocol. One noticeable work from these protocol is by McCune *et al.* [10]. They proposed a scheme named seeing is- Believing (Sib) which uses the display of a mobile phone to demonstrate its identity to a handheld device equipped with a camera. The idea of their scheme is that a handheld device generates a temporal public key and sends it to another handheld device. To solve this Problem there exists different solutions attempt. Such solutions are referred to as human-verifiable authentication protocols where they rely on human users to execute the Protocol through the wireless channel, like Bluetooth. Here a handheld device generates a temporal public key and sends it to another handheld device through the wireless channel.

This device displays the code as a digital image on its display and also creates a public key in the form of a visual code [13]. The photographs this code is taken by handheld device's camera and verifies the public key using this public key commitment.

1. Security protocols:

Protocols such as secure authentication becomes challenging, when various kinds of root kits reside in PCs (Personal Computers) to observe the behavior of the user and to make PCs devices untrusted. Because of the limited capability of computation and memorization of authentication protocol involving humans in authentication protocols during promising is not easy. The attacker is capable of creating a fake server to launch phishing or pharming attacks. The attacks are Key Space and Brute-Force Attacker, Key loggers, Malicious Software (malware), Shoulder-Surfing Attacks. The objective of security protocols also known as cryptographic protocols, are to distribute different security services across a distributed system. These goals include: the authentication of agents or nodes, establishing session keys between nodes, ensuring secrecy, integrity, anonymity, non-repudiation and so on. As they require the participation of a trusted third party or session server, they involve the exchange of messages between nodes. Typically they make liberal use of various cryptographic mechanisms, such as symmetric and asymmetric encryption, hash functions, and digital signatures.

Timestamps can also be used.

2. Bipartite and tripartite protocol:

The scheme is a top-down recursive function, which is not user friendly for human users. Therefore the algorithm can be re-written as a bottom-up function in a distributed form. It provides explicit instructions for users to follow. Secondly, the functions Combine Two and Combine Three are replaced by bipartite and tripartite authentication protocols. To model the last properties, a corrupt query that allows the adversary to issue when all oracle has already been terminated is defined. This command returns all messages that are sent and received in visual channel during the execution of the protocol. Since multi-sessions protocol execution in a device is not allowed, this command will only retrieve the visual messages sent in one protocol instance. Besides, the protocols apply some cryptographic functions like symmetric encryption, message authentication code (MAC) or hash functions. These functions are denoted as some oracles that can be queried by the adversary for a polynomial time. Let's assume two handheld devices *A* and *B*, wants to authenticate each other such that *A* is equipped with a high resolutiondisplay2 and *B* is equipped with a camera. Tripartite authentication protocol consist of three entities *A*, *B*, and *C* such that *A* is equipped with a high resolution display, *C* is equipped with a camera, and *B* equipped with both display and camera.

3. Password-Authentication Protocols:

Traditional password protocols are susceptible to off-line dictionary attacks: Many users choose passwords of relatively low entropy, so it is possible for the adversary to compile a dictionary of likely passwords. Obviously, the adversary from trying the passwords On-line cannot be prevented, but such an attack can be made infeasible by simply placing a limit on the number of unsuccessful authentication attempts. On the other hand, an offline search through the dictionary is quite doable. SPEKE a simple password exponential key exchange method is described. SPEKE consists of an exclusive class of methods which provides key establishment and authentication over a channel which is not secure using only a small password, excluding the risk of offline dictionary attack. SPEKE and the Diffie-Hellman Encrypted Key Exchange (DHEKE) are inspected in terms of both known and recent attacks, together with the preventive constraints. Authentication and key establishment are provided over an insecure channel by this method, and are immune to offline dictionary attack. Faces delay during authentication. Remote user authentication protocol and a password change protocol are the components of each set. The Remote user authentication protocol is used to authenticate the users accessing to a server, while the password change protocol is employed to update the user's password once the user has been successfully authenticated.

4. Transitive authentication protocols

Transitive authentication is built upon the bipartite and the tripartite authentication protocols. In the Setup phase of the protocol, all participants, except the final representative, it has established a session key with a trust representative. In the Distribution phase, each participant distributes Agreed Key to its partners using the agreed session key. By using bipartite and tripartite protocol the establishment of the session is proven secure, the transitive authentication protocol should also be secure if every user faithfully executes the protocol. Some level of physical security of network wiring is given to a number of network applications operating in the existing wired network. As there are no physical protection in wireless medium, addition of a new wireless network makes this assumption false. Two other likely alternatives are considered inappropriate, end-to-end security at the application layer and end-to-end security at the transport layer, given the requirement for seamless integration. A large couple of existing nodes in the wired network should not be modified because it is an implication of seamless integration. Stipulating application or transport layer based end-to-end security requires modifying the software base of the entire fixed node network. The transitive authentication calls for mutual trust among each entity. But there is no way to stop it, if an insider intentionally harms the protocol by leaking the agreed key to other outsider, or inviting an outsider into the community.

5. Secure remote password protocol

A Secure remote password protocol is a new password authentication and key-exchange protocol which is suitable for exchanging keys and authenticating users over network which is untrusted. The new protocol allows weak phrases to be used safely by resisting dictionary attacks mounted by either passive or active intruders. Significantly it improves performance. A variety of tradeoffs offered by current authentication technology between security and performance is somewhat unsatisfying to implement.

6. Manual authentication for wireless devices

Manual authentication techniques enables wireless devices to authenticate one another via an insecure wireless channel with the help of manual transfer of data between the devices. Manual transfer refers to the operations performed by human operators of the devices performing one of the following procedures: copying data output from one device into the other device, comparing the output of the two devices, or entering the same data into both devices. The objective of enabling two wireless devices to securely authenticate one another and agree on a shared data string. Human involvement is required. Quite a number of applications operating in the existing wired network assume some level of security arising from the physical security of network wiring. Since the wireless medium are not physically protected, introduction of a wireless network makes this assumption false. To secure the wireless link the existing application base to function is made secure.Two other likely alternatives, end-to-end security at the application layer and end-to-end security at the transport layer, are considered inappropriate, given the requirement for seamless integration into the existing networks.

7. Multipartite Transitive Authentication

The algorithm used is a top-down recursive function that divides N entities recursively into three groups until each group contains less than three members. Two subroutines called Combine Two and Combine Three, which respectively establish a session for two and three members in a group are applied. Using Combine Two or Combine Three each group selects a representative and combines with other groups. Until all groups are merged together the process is repeated recursively. The modification includes the following. Firstly the scheme is a top-down recursive function, which is not user friendly for human users. Therefore the algorithm is rewritten as a bottom-up function in a distributed form. It provides explicit instructions for users to follow. Secondly, the functions Combine Two and Combine Three are replaced by our bipartite and tripartite authentication protocols. As stated earlier, scalability is a concern for SiB. To scale up the authentication a general algorithm that utilizes the bipartite and the tripartite protocol is proposed. There are N handheld devices that desires to establish a conference key such that all devices are equipped with cameras and high resolution displays.

CONCLUSION

This paper focuses on developing an efficient key agreement protocols for two and three handheld devices over a temporal confidential and authenticated channels. They simplify previous unnecessary complications and reduce the bottleneck of running time human's involvements. This paper also proposes a system for multiple handheld devices agreeing a conference key securely, by using the visual authentication protocols.

REFERENCES

1. GAnGS: Gather, Authenticate 'n Group Securely∗ Chia-Hsin Owen Chen†, Chung-Wei Chen‡, Cynthia Kuo§, Yan-Hao Lai∗, Jonathan M. McCuneces.
2. Provably Secure Password-Authenticated Key Exchange Using Di±e-Hellman Victor Boyko1, Philip MacKenzie2, and Sarvar Patel2
3.Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques Simon Blake-Wilson
4. Manual authentication for wireless devices Christian Gehrmann
5. Strong Password-Only Authenticated Key Exchange * David P. Jablon
6. Entity Authentication and Key Distribution Mihir Bellare & Phillip Rogawayy
7. Talking To Strangers: Authentication in Ad-Hoc Wireless Networks Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong
8. Seeing-Is-Believing: Using Camera Phones for Human-Veri_able Authentication Jonathan M. McCune Adrian Perrig Michael K. Reiter
9. Security Weaknesses in Bluetooth Markus Jakobsson and Susanne Wetzel
10.Hash Visualization: a New Technique to improve Real-World Security Adrian Perrig & Dawn Song
11. A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices Chien-Ming Chen, King-Hang Wang