A SURVEY ON TRANSITIVE AUTHENTICATION IN MOBILE DEVICES

D.Angayarkanni
Department of Computer Science & Engineering
Vivekanandha Institute of Engineering & Technology for Women
Tiruchengode, India
angayarkannime@gmail.com

E.Menaka M.E.,(Ph.D)
Department of Computer Science & Engineering
Vivekanandha Institute of Engineering & Technology for Women
Tiruchengode, India
menakaparthi80@gmail.com

***Abstract* —In a Bluetooth scenario the man-in-the-middle (MITM) attack is the major threat for handheld devices to agree on a session key in which they do not share any prior secret in advance, Apart from insecurely typing passwords into handheld devices or comparing long hexadecimal keys displayed on the devices. Even when there are only three entities attempting to agree on a session key, these protocols need to be rerun three times. Here present a bipartite and a tripartite authentication protocol using a temporary confidential channel. To extend the system into a transitive authentication protocol that allows multiple handheld devices to establish a conference key securely and efficiently. To implement the prototype of the system on a mobile phone with satisfying performance using QR codes.**

***Keywords*—Human verifiable authentication protocol, mobile security. QR Codes**

I. INTRODUCTION

Using static passwords[1] for authentication, as it is commonly done, has quite a few security drawbacks, passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is the so called "two-factor" or "strong authentication" based on one time passwords. Fortunately mobile phones that are capable of running java applets are becoming more and more widely spread. It stands to reason to use your mobile phone as an authentication token.

II. PASSWORD AUTHENTICATION

Traditionally passwords[1][2] have been up to 8 bytes long. By today's standard 64 bits of entropy is about the minimum that can be considered marginally strong. 28 bytes is about the maximum that a skilled user can type reliably error free every time, this would be running text, and the limit for truly random bytes must be less. The major advantage of a password is that it costs nothing to create it and nothing beyond machine time to collect and verify it. Another problem is that users generally worry that they will forget the password, or have poor memorization skills.

Here presented a one-hop transitive authentication protocol for mobile devices. In their system, a device can be authenticated by another unmeet device if they have a shared “friend”. However, if the system is extended to multi users, one-hop transitive authentication may require too many redundant steps. This transitive authentication is built upon the bipartite and the tripartite authentication protocols. Idea of transitive authentication relies on the mutual trust among each entity. Bluetooth and MANA III are insecure if the password users entered are seen by the adversary. It is likely to happen when the key exchange is taken place in a public area. When there are three parties need to exchange keys, the above protocols need to execute three times. The tripartite protocol is more efficient such that it only requires two human involved Steps. This suggests that our protocols are very efficient comparing with the existing schemes. They proposed a scheme named Seeing-is-Believing[7](SiB) which uses the display of a mobile phone to demonstrate its identity to a handheld device equipped with a camera.

III. PASSWORD BASED AUTHENTICATION PROTOCOLS

A. EKE:

The encrypted key exchange (EKE) [3]protocol is augmented so that hosts do not store clear text passwords. Two parties sharing a password to communicate without exposing that password. That protocol, encrypted key exchange, or EKE, required that both parties have clear text versions of the shared password. The original EKE protocol protected passwords being sent over the network, but required a trusted key distribution center. Now extended EKE so that it may be used when talking to a single host. Local users' hashed passwords are protected by the operating system's file protection mechanisms remote users' passwords are protected by the new protocol. No third parties are necessary. It does not appear to be possible to protect passwords against an intruder who has captured the host's copy of the authentication data. An alternative implementation of the original EKE protocol relies on a public-key cryptosystem, instead of exponential key exchange. It has the drawback that the session key is chosen by one of the parties, as opposed to the exponential key exchange.

B. SPEKE:

A new simple password exponential key exchange method (SPEKE) [4] is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE[4] and the closely-related Diffie-Hellman Encrypted Key Exchange (DHEKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints are different. The class of strong password-only methods is compared to other authentication schemes. Benefits, limitations, and tradeoffs between efficiency and security are discussed. These methods are important for several uses, including replacement of obsolete systems, and building hybrid two-factor systems where independent password-only and key-based methods can survive a single event of either key theft or password compromise. a new password-only authentication protocol, SPEKE, which appears to be at least as strong as the closely related DH-EKE method about receiving unauthenticated DH parameters argue for the use of either a fixed huge modulus.

C. MANUAL AUTHENTICATION FOR WIRELESS DEVICES

Manual authentication [5] techniques have been designed to enable wireless devices to authenticate one another via an insecure wireless channel with the aid of a manual transfer of data between the devices. Manual transfer refers to the human operator 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. Techniques currently being standardized are described which achieve this, and which require only small amounts of data to be transferred between the two devices.

A user has two wireless-enabled devices, e.g. a mobile phone and a Personal Digital Assistant (PDA) suppose further that they wish the two devices to establish a secure association for their wireless communications. The problem is thus for the two devices to mutually authenticate one another and, where necessary, to establish a shared secret key, all using a wireless communications link.

D. QRP: AN IMPROVED SECURE AUTHENTICATION METHOD USING QR CODES:

The design and implementation of QRP[10], an open source, proof-of-concept authentication system that uses a two-factor authentication by combining a password and a camera-equipped mobile phone, acting as an authentication token. QRP is extremely secure as all the sensitive information stored and transmitted is encrypted, but it is also an easy to use and cost-efficient solution. In order to access to the mobile application need to input a personal password. This might be inconvenient for some people as per the small size of a keyboard in the phone. In this system, the server must have a copy of the user’s private key in order to generate the same pincode. A possible solution might be managing two different user keys, Another eventual drawback that want to avoid would be having a single point of failure in the server.

E. AUTOMATIC RECOGNITION ALGORITHM OF QR CODE BASED ON EMBEDDED SYSTEM:

The automatic recognition algorithm[10] of Quick Response Code is discussed. An image processing system based on embedded system is escribed to be able to binarization, location, segment, and decoding the QR Code. Barcode can be optimally recognized with the proposed algorithm. As the mobile phone with [12]camera device is getting more popular, recognition barcode based on embedded system is getting more important and practical. A new high-speed, high-accuracy automatic recognition method for recognizing QR Code in various illumination conditions is available. And there is no need the special scanner for barcode recognition in the proposed method. From the experiment, the proposed method produced better results than other method. The recognition test also showed the proposed method is effective for the QR Code[10] image recognition based on embedded system. The mobile QR code and barcode redemption market is estimated to cross $50 bn globally by 2017, according to Mind Commerce. Quick Response (QR) codes were initially designed for identifications of auto parts in the Japanese automotive industry. Automakers could keep track of parts, inventory, and quality check.. QR codes have found a great use in the marketing industry. Applications include product tracking, item identification, time tracking, document management, general marketing, and much more. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted; data is then extracted from patterns present in both horizontal and vertical components of the image.

F. A NOVEL USER AUTHENTICATION SCHEME BASED ON QR-CODE:

User authentication[11] is one of the fundamental procedures to ensure secure communications and share system resources over an insecure public network channel. Thus, a simple and efficient authentication mechanism is required for securing the network system in the real environment. In general, the password-based authentication mechanism provides the basic capability to prevent unauthorized access. Especially, the purpose of the one-time password is to make it more difficult to gain unauthorized access to restricted resources. service in order to reduce the risk of Instead of using the password file as conventional authentication systems, many researchers have devoted to implement various one-time password schemes using smart cards, time-synchronized token or short message tampering and maintenance cost. However, these schemes are impractical because of the far from ubiquitous hardware devices or the infrastructure requirements. To remedy these weaknesses, the attraction of the QR-code technique can be introduced into our one-time password authentication protocol.

The attraction of the QR-code[10] technique can be introduced into our one-time password authentication protocol. Not the same as before, the proposed scheme based on QR code not only eliminates the usage of the password verification table, but also is a cost effective solution since most internet users already have mobile phones.. Many cellular phones with embedded camera nowadays are natively equipped with the QR-code decoding software.

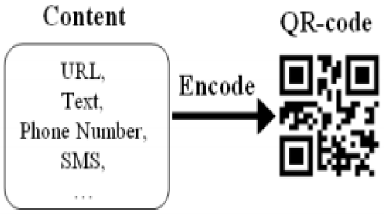


Figure 1 :QR-code Encoding diagram

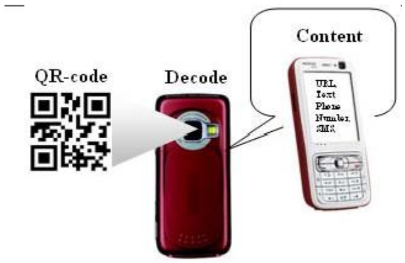


Figure 2 :QR-code Decoding diagram

1. *Security risk of the user's mobile phone*

Since the mobile phone has the user's long-term secret key, therefore, it needs to be well-protected. Fortunately, the mobile phones with embedded camera in our scheme only capture the QR-code and decode them with software running on the phone. Accordingly, the mobile device isn't directly exposed to other malicious users. Thus, under this reasonable assumption, the risks generated by the mobile phone will be significantly reduced.

2. *Security risk of the SP*

It is infeasible for an attacker to derive *SP*'s secret values *s* according equation because that the one-way hash function is unreversable. On the other hand, the attack of impersonating *CA* will also fail, because he still cannot derive x_A without the knowledge of *s*.

3. *Security risk of the remote user*

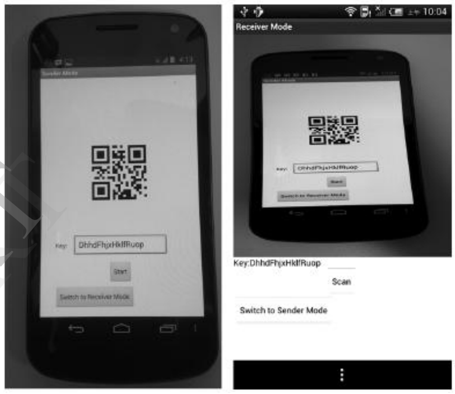
That it is infeasible to obtain the valid user's long-term secret key x_A without the knowledge of the corresponding random number *r*. On the other hand, if an adversary intercepts the information being transmitted over the public channel, it is still infeasible to derive *r* from $h(r, T_1, T_2)$ and $h(r, T_2, T_3)$, because that the one-way hash function is unreversable.

G. SEEING-IS-BELIEVING:USING CAMERA PHONES FOR HUMAN-VERIFIABLE AUTHENTICATION

To use the camera on a mobile phone as a new *visual channel* to achieve demonstrative identification of communicating devices formerly unattainable in an intuitive way. We term this approach Seeing-Is-Believing (SiB)[7]. In SiB, one device uses its camera to take a snapshot of a barcode encoding cryptographic material identifying, e.g., the public key of another device. We term this a *visual channel.* Barcodes can be pre configured and printed on labels attached to devices, or they can be generated on demand and shown on a device's display. To apply this visual channel to several problems in computer security. SiB[7] can be used to bootstrap authenticated key exchange between devices that share no prior context, including such devices as mobile phones, wireless access points, and public printers. To use SiB[7] to aid in the establishment of a trusted path for configuration of a TCG-compliant1 computin g platform, and to provide the user with assurance in the integrity of an application running on a TCG-compliant computing platform. It also use SiB to secure device configuration in the context of a smart home.

SiB[7] depends on a camera phone having the ability to use its camera to recognize two-dimensional (2D) barcodes. Several projects exist that seek to allow camera equipped mobile phones to interact with physical objects through the use of 2D barcodes. Rohs and Gfeller develop their own 2D code explicitly for use with mobile phones, emphasizing their ability to be read from electronic screens and printed paper. Woodside develops *semacodes*, which is an implementation of the Data Matrix barcode standard for mobile phones. Woodside considers the primary application of semacodes as containers for a URL which contains information about the physical location where the barcode was installed.

This device also creates a commitment of the public key in the form of a visual code, and displays the code as a digital image on its display. The other handheld device photographs this code using its camera and verifies the public key using this public key commitment. This public key allows the receiver to authenticate the sender after executing some simple confirmation steps. By rerunning SiB in the opposite direction, it allows the devices mutually authenticate each other. The rationale of this scheme is to provide data integrity via the visual channel. This method does not require preshared keys or preregistered public keys. It also limits the dangers brought by human errors; for instance, it does not need human to pick random passwords or input long keys. In the real world, many mobile phones and PDAs are equipped with cameras and pretty high resolution displays. Therefore, the scheme can be applied to practical world that is more convenient and more secure. Yet, there are also some disadvantages in SiB. The first problem is scalability. SiB protocol supports secure authentication for two handheld devices. When there are more than two devices that require building secure channels, they need to execute SiB in pairwise. That means if there are devices, each of them needs to take pictures from other mobile devices.



Key: DhhdFhjxHklfRuop

Key:DhhdFhjxHklfRuop

Figure 3. Implementation of two handheld devices

Seeing-Is-Believing, a system that uses barcodes and camera phones as a visual channel for human-verifiable authentication. This channel rules out man-in-the-middle attacks against public-key based key establishment protocols. The visual channel has the desirable property that it provides demonstrative identification of the communicating parties, providing the user assurance that her device is communicating with *that* other device. SiB enables establishment of a trusted path for configuration of the TPM in a TCG-compliant computing platform. Leveraging a TCG-compliant computing platform and SiB, one can verify the integrity of an application over multiple invocations.

Our 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, has established a session key with a trust representative. In the **Distribution** phase, each participant distributes **AgreedKey** to its partners using the agreed session key. Since the establishment of the session is proven secure in the bipartite and tripartite protocol, the transitive authentication protocol should also be secure if every user faithfully executes the protocol. The idea of transitive authentication relies on the mutual trust among each entity. If an insider intensionally harms the protocol by leaking the agreed key to other outsider, or inviting an outsider into the community, there is no way to stop it. To consider this is a trade off between efficiency and security when adopting transitive authentication protocol. However, it may happen that a human user wrongly executes the protocol. For example, one is not selected as a representative but they does not realize it. So keeps hanging around the room and finds other participants to execute bipartite or tripartite protocol. Its handheld device would not execute the authentication protocol. Then the user will find out she should sit down after she fails to pair up with other entity.

H. GANGS:

To establish secure communication among a group of physically collocated people (e.g. A group of people meeting at an airport and exchanging sensitive information using their mobile phones) Can be reduced to establishing authentic public keys among all participants

- Leverage Public Key Infrastructure (PKI) to exchange keys
- secure group password.

GAnGS[8] and this scheme support multiusers key agreement. That GAnGS has a different security perspective than our scheme. That GAnGS requires more human involved steps and may not resilient to human errors. The design of GAnGS is more complicate in order to defense against malicious insider attacks. Since this scope focus on key agreements, insider attacks can never be prevented since any insider may disclose the agreed secret key to outsider after executing the protocol legitimately. This scheme founded on transitive authentication which requires a higher level of trust among users. Our scheme is also insecure if the adversary can extract the visual code from our device's screen before the end of each bi- partite or tripartite protocol.

GAnGS requires users to take photos, to form a subgroup, to count the number of people in a subgroup, and to compare images. Although each task is regarded as a simply task, we found the accumulation of these tasks is cumbersome to perform. When there are three parties need to exchange keys, the above protocols need to execute three times. Our tripartite protocol is more efficient such that it only requires two human involved steps.When there are multiple users that need to exchange keys, the above protocol requires $O(n^2)$ operations. Only GAnGS and our multipartite protocol manage to be executed with lower complexities (O(n) operations). If we measure the complexity efficiency in terms of sequential O(log(n))operations, GAnGS and our multipartite protocol out perform other schemes with operations against $O(n^2)$ operations. On average, GAnGS requires each users to perform two SiB protocols, one photo takings, and one photo comparison. For our multipartite protocol, each user only needs one photo taking on averages. This suggests that our protocols are very efficient comparing with the existing schemes.

GAnGS is designed in the way to exchange users' public key authentically rather than agree a common shared key securely. Thus, the design of GAnGS is more complicate in order to defense against malicious insider attacks. Since our scope focus on key agreements, insider attacks can never be prevented since any insider may disclose the agreed secret key to outsider fter executing the protocol legitimately. Thus, our scheme founded on transitive authentication which requires a higher level of trust among users.

In addition, different users execute the protocol in different paces. In our protocol, fast users do not need to wait for all other participants to process the next round of protocol. As long as (n-1) photos are taken, n participants will be mutually authenticated. No matter how many rounds of protocol has a user executed, or how the graph has been constructed, the totally number of photo takings and the number of edges will still be(n-1)

The key is encoded using QR-code, implemented with an open source engine. QR-code supports several versions and error correcting levels. Since AES is used as the symmetric data encryption algorithm, require at least 256 bits of data capacity (two 128-bit keys). The sender spends less than one second on encoding key into QR-code, less than one second on sending packet through wireless network, and one second on AES encryption. On the other side, the receiver spends about three seconds on decoding key and less than one second on decrypting and verifying message. The computation cost for point multiplication and point selecting is less than one second, while the cost for bilinear pairing is less than three seconds.

IV. CONCLUSION

GAnGS [8], there are no practical group key agreement for ad-hoc gathering. And unfortunately, GAnGS are too complicated and inefficient when only group key agreement is needed. We have also proposed a transitive authentication system for multiple handheld devices agreeing a conference key securely, by using the bipartite and tripartite authentication protocols. QR-based authentication offers a very secure and fast authentication method that must be considered to securely and easily authenticate.

V. REFERENCES

[1] M.Bellare, “Authentication and ,” in Proc. Advances in Cryptology-CRYPTO, 1993, vol. 773, pp. 232–249

[2] MihirBellare,”Password authentication” vol. 17, no. 4, pp. 263–276, 2004.

[3] S.M.Bellovin and M.Merritt, “Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise” Proc. 1st ACM conf.comput.and communications security, pp. 244-250, 1993.

[4] D.P.Jablon, “strong password-only authenticated key exchange,” ACM SIG Comput. Commun.Rev., vol.26, no 5, pp. 5-26, 1996.

[5] C.Gehrman, C.Mitchell, and K.Nyberg, “Manual authentication for wireless devices,” RSA Cryptobytes, vol.7, no. 1, pp. 29-37, 2004.

[6] T.Wu, “The secure remote password protocol,” in Proc. Symp. Internet Soc. Network and Distributed Syst. Security, 1998, vol. 1, pp. 97–111.

[7] M.McCune, A. Perrig, andM. K. Reiter, “Seeing-is-believing: using camera phones for human-verifiable authentication,” in Proc. IEEE Symp. on Security and Privacy, 2005, pp. 110–124

[8] C.-H.O. Chen, “Gangs: Gather, authenticate’ n group securely,” in Proc. 4th ACM Int. Conf. Mobile Computing and Networking, ACM, New York, NY, USA, 2008, pp. 92–103.

[9] Yue Liu, “Automatic Recognition Algorithm of Quick Response Code Based on Embedded System” IEEE PAMI, 1995, Vol. 17. No. 12, pp.1191- 1201.

[10] David Pintor Maestre Universitat Oberta de Catalunya 08018, Barcelona, Spain “QRP: An improved secure authentication method using QR codes” June 8, 2012.

[11] Tasos Alexandridis, Paulos Charonyktakis, Antonis Makrogiannakis, “Forthroid on Android: A QR-code based Information Access System for Smart Phones” Mob. Netw. Appl., pp. 365–376, October 2002.

[12] M. Rohs and B. Gfeller, “Using camera-equipped mobile phones for interacting with real-world objects,” in Proc. Advances in Pervasive Computing, 2004, pp. 265–271