International Journal of Computer Applications Technology and Research
Volume 3– Issue 10, 645 - 647, 2014, ISSN: 2319–8656

A Review Study on Secure Authentication in Mobile System

Ahitha.H.S
Ponjesly College of Engineering
Nagercoil, TamilNadu
India

Deepa.A.J
Ponjesly College of Engineering
Nagercoil, TamilNadu
India

Abstract:In mobile environment, the users communicate with each other about location based information and services with the help of network nodes. But providing security to data has become a difficult task. Currently available network security mechanisms are insufficient, but there is a greater demand for flexible, scalable security mechanisms. Mobile security is of vital importance but can't be inbuilt. In this work, proposing two techniques for authenticating short encrypted messages that helps to preserve the confidentiality and integrity of the communicated messages. The messages to be authenticated must also be encrypted using the secure authentication codes that are more efficient than message authentication codes. The key idea in this technique is to provide the security using Encryption Algorithm. Security model should adjust with various capability requirements and security requirements of a mobile system This paper provides a survey on security in mobile systems

Keywords: Authentication, Message Authentication code, Computational security, Unconditional Security.

1. INTRODUCTION

Mobile computing is human-computer interaction by which a computer is expected to be transported during usual usage. It includes mobile communication that leads to several communication issues. To resolve this issue the proposed work has two techniques, in the first technique message to be authenticated is also encrypted with any secure encryption algorithm to attach a short random string in the authentication process. Since the random strings are independent for different operations the authentication algorithm will be faster and more efficient without the difficulty to manage one-time keys. In the second technique we make more assumption to use an encryption algorithm in block cipher based to improve the computational efficiency.

As networking technology become common place and essential to everyday life, companies, organizations and individuals are increasingly depending on electronic means to process information and provide important services in order to take advantage of ambient brainpower in PCEsPervasive computing environments. PCEs with their interconnected devices and abundant services promise great combination of digital infrastructure into many aspects of our life.Traditional authentication which focuses on identity authentication may fail to work in PCEs, to a certain extent because it conflicts with the goal of user privacy protection because the assurance achieved by entity authentication will be of diminishing value [10].

Preserving the integrity of the messages that are exchanged over the public channels is the traditional goal in cryptography that is mainly done using message authentication codes (MAC) for the only purpose of preserving message integrity. Based on security, message can be classified into two as unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with the unlimited computational power. But computationally secure MACs are only secure when forgers have limited computational power. Computationally secure MACs are further classified as block cipher, cryptographic hash function, or universal hash function. Phillip Rogaway [9] suggested a Block-Cipher Mode of Operation for Efficient Authenticated Encryption

More security issues are to be concerned with the fast transmission of digital information over wireless channels, the security issues include the spread of viruses and malicious software. There are about 200 mobile viruses or a malware program that causes problems to the systems based on F-Secure [1]. One of the major issues in mobile system is the low computational power. Many organizations are interested in deploying mobile application to improve efficiency and allow the capabilities. Further, the sections are preplanned as follows, Section 2 explains several cryptographic terms, Section 3 includes several Authentication methods, Section 4 Security Model that describes an application about deploying of (Radio Frequency Identification) RFID system and a cryptography based security model Section 5 Benefits of secure authentication, Section 6 Conclusion.

2. CRYPTOGRAPHIC TERMS

Basic security terms used in cryptography is the plaintext, cipher text, Encryption and Decryption. Plaintext is an ordinary form of message that is known to a viewer. Cipher text is the result obtained after performing Encryption on the plaintext. Encryption is done to hide the meaning of the message from everyone than the legal users. Decryption is inverse of Encryption. Strength of the scheme depends on the secrecy of the keys used. William Stallings [2] described in detail about the commonly used security terminologies. Security protocols identify the security objectives with the use of cryptographic algorithm. The main security objectives are as follows:

2.1 Authentication: The process by which the system checks the identity of the user who wish to access the information.

2.2 Confidentiality: The secrecy of the communicated data should be maintained. No one other than the legitimate user should know the content of the data.

2.3 Integrity: This is to check the originality of the message. It allows the receiver to verify that the message received was not altered during transfer.

The security objectives help us to provide trust on web. Trust is another feature of security coin that is related with both authentication and authorization. The algorithms are of two types as Symmetric algorithms and Asymmetric algorithms. Symmetric algorithms uses same key for both encryption and decryption. It is mainly used for providing confidentiality. An asymmetric algorithm uses different keys for encryption and decryption as public key and private key respectively. It is mainly used for authentication and non-repudiation [2].

3. AUTHENTICATION TYPES

Authentication is a process by which the system checks the identity of the user who needs to access it. It is one of the most essential security primitive. Authentication mainly based on the three factors as knowledge, possession and Attribute. The most common authentication methods are as follows:

3.1Passwords: The most popular authentication scheme is password that is used for multiple services. This is a straight forward method that provides sufficient security. Subjects should be aware about the length of their password and security. The drawback is that multiple password is hard to remember.

3.1.1 Single Factor Authentication: In single factor authentication user can use only one factor for authentication as the basic user name/password. The password may be textual, graphical Password or PIN. Harsh Kumar Sarohi et al [3] proposed graphical authentication method here a password consist of sequence of one or more images, with the help of mouse events like click, drag etc the user can input their password.

3.1.2 Multiple Factor Authentication:ShindeSwapnil et al [4] proposed multiple factor authentication user that can use multiple factors for authentication such as what the user knows (password or PIN), what the user has (smart card), what the user is (Biometric authentication). Multi-factor authentication is a type of strong authentication.

3.2 Tokens: Tokens are supposed to have high security and usability. To many service are grouped into the device and hence the token generators are included in the device. Every subject should use tokens in any of the form either as paper tables or key generators.

3.3Biometrics: Fingerprint is the most chosen biometric authentication method. Users like the feature of quick learning, but it may lead to the risk of data loss. Biometric factors are unable to change and the loss of private data is bad and it should be avoided.

4. SECURITY MODEL IN MOBILE SYSTEM

4.1 RFID (Radio frequency Identification)

RFID is the wireless non-contact use of radio frequency with electromagnetic fields to transfer data. The main use is to automatically identify and track the tags that are attached to objects. The tags contain information that are stored electronically. RFID in (figure 1) is similar to barcodes,it uses an electronic chip that is fixed on a product or an artifact. The information could be read, recorded or rewritten.

RFID System can be classified by the type of tag and Readers. A radio frequency identification system use tags that are attached to the objects that are to be identified. Tags are similar to labels. Two-way radio transmitter-receivers are called as readers. The readers send the signal to the tag and read its response. RFID tags contain two parts as an integrated circuit and an antenna used for storing and processing information and for receiving and transmitting the signals respectively. Tag receives the message and then responds with its identification and other information. The Tag information is stored in a non-volatile memory. Readers are also known as interrogators. Reader transmits an programmed radio signal to interview the tags.

RFID tags are of two types Passive and Active tags. Active tag has a battery attached on-board and it transmits its ID signal periodically. It is also known as Battery assisted passive tags that are activated in the presence of an RFID reader. But passive tags are cheaper and smaller because it has no battery.

Figure 1: RFID SYSTEM ARCHITECTURE

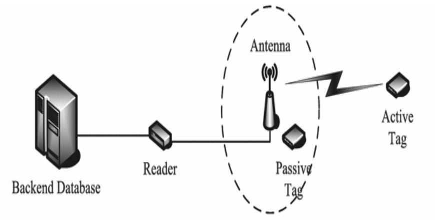

Fig. 1 RFID system architecture

RFID Authentication protocols used for secure and low cost RFID Systems [5]. To solve the security problem the low cost RFID system with the authentication protocols were proposed.

- **SRAC** (Semi-Randomized Access Control)
- **ASRAC** (Advanced Semi-Randomized Access Control)

4.1.1 SRAC (Semi-Randomized Access Control)

SRAC is designed using a hash function in tags as the security primitives. It resolves not only the security properties such as the tracking problem, cloning problem and denial of service attack but also solves the operational properties as scalability and rareness of IDs. In the randomized access control the tag replies to the reader by sending a message back as response that varies each time. Communication between the Server and Reader is done using strong keys with sufficient resources so they will be secure. But we have to concern more about the communication between reader and tags. The reader will pass the arrived messages to the server.

4.1.2 ASRAC (Advanced Semi-Randomized Access Control)

ASRAC is used mainly for preventing replay attack. Replay attack is a kind of active attack. The ASRAC is designed using a hash function and a random producer for security primitives. SRAC helps on reducing 75% of tag transmission. The advantage is that since both reader and tag confirms the received message using hashed outputs which internally has the generated random numbers, attackers cannot use the past messages.

4.2 Public key Cryptography based security model

Key management is an important issue in public key cryptography. The shared wireless network faces the problem of eavesdropping. R. Shanmugalakshmi [6] proposed that ECC's provide high security with smaller key size than RSA. ECC used in the security development in the field of information security and mobile devices with low computational power. When compared with RSA, hardware implemented ECC has less operating cost. ECC is a talented cryptosystem for next generation and widespread use in devices.

Public key Cryptography is mainly based on the intractability of certain mathematical problems. Elliptic curves have several discrete logarithm based protocol. ECC used for digital signature generation and key exchange mainly used for protecting classified as well as unclassified national security systems and information. In most of the applications the RSA is replaced by ECC.

5. BENEFITS OF SECURE AUTHENTICATION

Most organizations have a major portion of their workers accessing their network from outside the office via mobile devices. Yet user names and passwords are not enough to adequately protect devices against unauthorized access.So Today's enterprise needs an efficient, user-friendly solution to address the security challenges that exist in today's mobile business. Secure authentication that offers a smarter, more flexible alternative to meet the unique needs of business today, including all the economic and business benefits of a hosted solution:

Protection: Validation and Protection Service cuts the risk of unauthorized access, data breaches, and other security problems.An enterprise class security solution and a cloud-based application that meets their cost and reliability needs.

Scalability: Service security is delivered in the cloud, justifying the need for underlying hardware and software resources, enterprises can dial up or dial down their use of the service as their needs change.

Speed: Many times success is defined by being able to move as swiftly as business requires. There is no lag time while new servers, operating systems, and applications are provisioned and installed. Everything is ready to go on demand.

Availability: Validation and ID Protection Service offers carrier-class reliability within the highly secure Symantec global infrastructure, featuring military-grade tier-4 data centers. The Symantec Internet infrastructure enables and protects up to 30 billion interactions a day, with unmatched scale, interoperability, and security

6. CONCLUSION

As more of their users go mobile and they move critical data and applications into the cloud to achieve cost savings, flexibility, and scalability, enterprises must emphasize security more than ever.Since the numbers of operations are greater for encryption than authentication both in 2G and 3G, throughput for encryption is low compared to authentication as encryption consumes significantly more processing resources compared to authentication. To reduce computational overheads encryption should be used in critical user information only and not for regular traffic flow. Encryption if needed should be combined with authentication. In this case if the message fails authentication, decryption process is saved (not performed).Further the performance analysis determines the cost (in terms of time complexity and throughput). Quantifying the security overhead makes mobile users and mobile network operators aware of the price of added security features and further helps in making optimized security policy configurations. Finally, except for the transformation complexity and the processor capabilities, the real time required for a packet to be protected depends on the overall system load and traffic conditions as well.

7. REFERENCES

[1] F-secure, "New Century in Mobile Malware", 2006[online].

[2] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", 2006

[3] ShindeSwapnil K et al, "Secure Web Authentication by Multifactor Password a New Approach", International Journal of Software and Web Sciences, 2013.

[4] Harsh Kumar Sarohi et al, "Graphical Password Authentication Schemes: Current Status and Key Issues", International Journal of Computer Science Issues, March 2013

[5] Yong ki lee et al, "Secure and Low-cost RFID Authentication Protocols"

[6] R.Shanmugalakshmi, "Research Issues on Elliptic Curve Cryptography and its Applications", International Journal of Computer Science and Network, June 2009.

[7] Caimu Tang et al, "An Efficient Mobile Authentication Scheme for wireless networks" IEEE transactions on wireless communications, April 2008

[8] KuiRen et al, "A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments"

[9] Phillip Rogawayet al, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption", August 3 2001.

[10] S. Creese et al, "Authentication for Pervasive Computing, Security in Pervasive Computing" 2003.

.