International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 3; Issue 3; March 2016; Page No. 240-243

Security issues in mobile computing

Manish

Department of Computer Applications, Chandigarh Group of Colleges Landran, Punjab, India

Abstract
Mobile platforms have become extremely popular among users and hence become an important platform for developers. New privacy and security issues arise with the prevalence of mobile computing due to the fact that mobile devices often store tremendous amount of personal, financial and commercial data, and therefore attract both targeted and mass-scale attacks. To meet the society's growing demand for mobile computing and security professionals, it is vitally important to provide various cryptographic techniques, so that we can secure our data and other important information from malicious users sitting on the Internet.

Keywords: Mobile Computing, Cryptography, SSL, Hash, Encryption, Checksum

1. Introduction

Mobile Computing has totally changed the way of communication. By removing the restriction of place, people world-wide have found new and rewarding ways of connecting with others- both privately and for business. The possibility of anytime, anywhere communication brings unprecedented choice and freedom. By virtue of being the most cost effective form of communication, mobile technologies have in mere decade, surpassed the number of users that it has taken the fixed network more than a century to reach.

Recent advancements in mobile network technologies have brought about a significant increase in available bandwidth, providing a solid basis for the transition from voice-only mobile services to web-based content services. These new services will also broaden the communication modes from one-to-one to one-to-many and many-to-many. With almost 2 billion subscribers in the early 2010's, mobility will be the common denominator for all communications.

In this era of technological evolution, we should not to lose sight of what made mobile communications successful in the first place- low cost, ease of use and user control. The user requirements and development trends call for an easy method to connect service and content providers to mobile networks and the end-user.

The next few years there will be further convergence of mobile communications and the internet, resulting in various new technologies and new pervasive products. This mobile Internet will not be simply the Internet of today accessed from a mobile device. As users, we will not be browsing Internet pages for content as we do today. Instead, we will be witnessing Artificial Intelligence, which will be beyond the imagination of the user and we will be using tailored applications and services profiled according to our personal preferences, time and place. Users will be able to download applications and content that fit their personal profile and lifestyle. The true challenge for the Mobile Internet's technical architecture is to provide this seamless user experience.

2. Security

Security is an integral part of every mobile e-commerce solution. The explanation of background of security and the cryptographic techniques used to secure Pervasive (ubiquitous) Computing and give an overview of the different standards, algorithms, and protocols used.

Security issues in Pervasive Computing are the critical aspect for its success. Because Pervasive Computing and mobile e-business may provide millions of people with the power to move trillions of dollars in goods or money by a few mouse clicks, the security of e-business transactions is a top priority.

Cryptography can be used to assure security in a lot of e-business scenarios. It can used to enable the secure spending of money on the net, for secure authentication of users, or for generating digital signatures for electronic contracts, just to name a few examples.

Here, we first give an overview of the various needs for security. We start by explaining some of the new challenges that appear when business is moved from traditional stores to mobile devices connected to the Internet. Then we present you the basic concepts and technologies of cryptography which provides detail coverage of all major security mechanisms used to protect communication in the Internet.

3. The importance of Security

In recent past, the Internet was discovered as a huge market with billions of customers around the world. The Internet already enables companies to sell to customers around the world with minimal investment. This is frequently called e-commerce. As more and more devices and appliances getting connected to the internet with Pervasive Computing, security becomes more and more important. Together with the advantages, Pervasive Computing brings new challenges that didn't exist before.

A merchant must know the identity of the customer and a recipient of a message, a command, or an order should know the identity of the sender. For some kinds of business, it is not sufficient that the customer authenticates himself by the use of a password.

Or imagine you can control heating at home over the Internet, in this case you better make sure that only you, or the other authorized persons, can turn on or off the heat and not anybody else surfing around in the Internet. In these cases, an electronic version of today's identity or credit card is required. This challenge is met using cryptography methods to authenticate persons or messages.
Cryptography can help to get secure access to data or services, and to protect the privacy of communication.

4. Cryptographic Patterns and Methods
For encrypting any information the Cryptographic algorithms are used in a form that cannot be read or altered by third parties. The sender of the information encrypts the data using a key; the recipient of the data decrypts the data back into a usable form by applying a second cryptographic operation also using a key. Cryptographic algorithms can be divided into two groups:
1. Symmetric algorithms and
2. Asymmetric algorithms.

4.1 Symmetric Cryptographic Algorithms
Symmetric cryptographic algorithms, also known as secret key algorithms, are characterized by the fact that the sender and the receiver use the same key to encrypt and decrypt the data. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet.
In Comparison with asymmetric algorithms, symmetric cryptography is fast and it can be used to encrypt and decrypt the large amount of data. To keep the communication secret, only the sender and the receiver of the information should know the key that was used to encrypt the data. If someone is exchanging data with a lot of other parties, he should maintain a separate key for each of them. This could become a complicated task if the network is quite large.

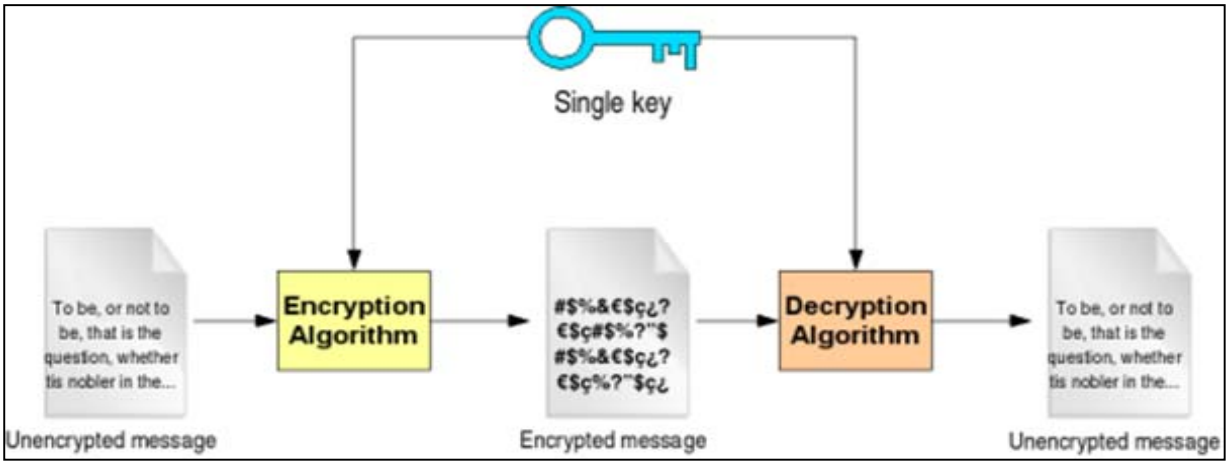

Fig 1: Symmetric cryptography

Symmetric cryptographic algorithms can be divided into two groups, based on the way the data is processed:
- Block-cipher and
- Stream-cipher algorithms

Cipher is another word for encrypt. Block-cipher algorithms split the data into fixed length blocks. The last block is padded, if necessary. Today, a block length of 64 bit is usually used. Systems based on stream-cipher algorithms encrypt each byte separately.
Today, only block-cipher algorithms are standardized in the industry, thus they are the one that are used in most situations.

4.2 Asymmetric Cryptographic Algorithms
Asymmetric cryptographic algorithms, also known as public key algorithms, were developed to solve the key distribution problem that every user of asymmetric cryptographic has. The main areas to use for asymmetric cryptography are:
- Distribution of keys
- Generation of digital signatures, and
- Encryption and decryption of information.

In public-key cryptography, for each person has a pair of keys (digital codes); one, the public key is accessed widely, and the other, the private key, is known only to the owner. Using the public key, any person can encrypt a message for the owner, and such messages can be decrypted only using the owner's private key. Thus a message intended for Alice can be encrypted and hosted safely on public servers without anyone but Alice being able to read it. This system of using two different paired keys is called an asymmetric key encryption algorithm.

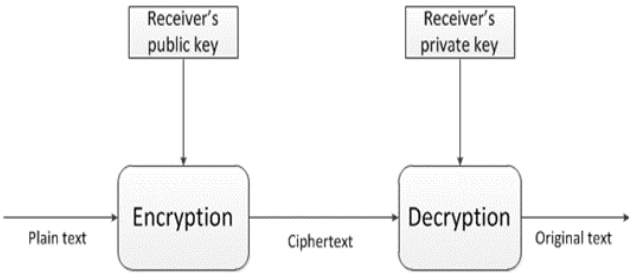

Fig 2: Asymmetric cryptography

5. Cryptographic Tools
There are several ways cryptography is used to secure operations and data. The followings are the most important ones.

5.1 Hash

A cryptographic hash function is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string, which is called the hash value (sometimes called a message digest, a digital fingerprint, a digest or a checksum). The ideal hash function has three main properties:

1. It is relatively fast to compute the hash value of any given message.
2. It is computationally difficult to calculate an alphanumeric text that has a given hash.
3. It is unlikely that two slightly different messages will have the same hash.

Hash functions are used in practical applications include message integrity checks, digital signatures, authentication, and various information security applications.

It takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the "hash value" is unable to know the original message, but only the person who knows the original message can prove the "hash value" is created from that message.

5.2 Message Authentication Code (MAC)

A MAC is an authentication tag or checksum computed by applying a secret key to a message. The MAC is always verified using the same key. The generation of a MAC can be based on hash function, on a stream-cipher or on a block-cipher algorithm.

5.3 Digital Signature

Digital signature enables the recipient to verify the identity of the sender and the origin as well as integrity of the document. It is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

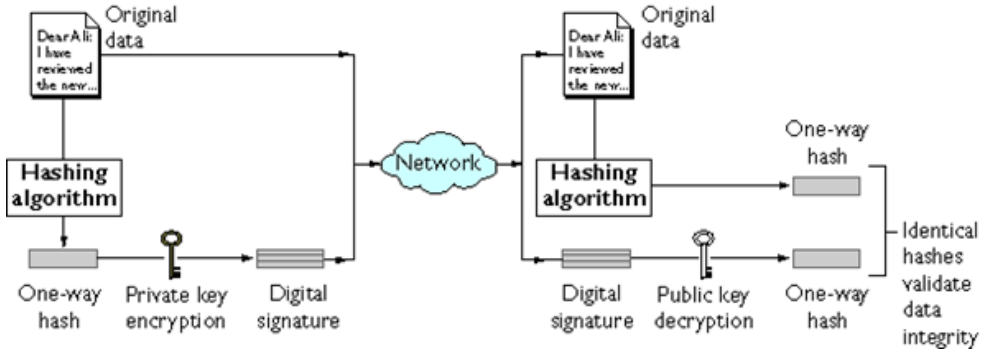

Fig 3: Digital Signature

5.4 Certificate

A certificate is a document that binds a public key to a specific person. The Trusted Third Party guarantees that the information contained in the certificate is valid and correct.

The certificates should contain the following information:

- Digital signature of the Trusted Third party,
- Name of the person owing the public key, and
- Public key itself.

5.5 Secure Socket layer (SSL)

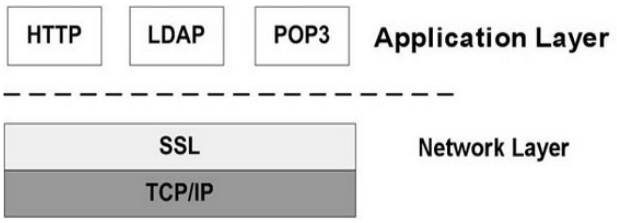

Fig 4: Secure Socket layer

Netscape developed SSL in 1995 to provide security and privacy on the Internet. Today, most web servers and browsers support SSL. A user recognizes an SSL-session at the "https://" instead of "http://"before the URL.

SSL sits on top of TCP/IP and below the application layer. By this, SSL is not only able to secure an HTTP connection, it can also be used for other services on the internet, like telnet or ftp.

6. Conclusions

There is still a long way for research to proceed before mobile computing will become a daily reality in society. Although considerable effort is being focused towards research in mobile computing, much of it is concentrating on the performance and availability of mobile computing, with comparatively little attention being given to the security issues in such an environment.

In this paper we have proposed security to be a major category for future developments in mobile computing. We have discussed briefly the issues of security in the context of mobility, various cryptographic techniques, presenting a number of potential problems in the security of a mobile computing environment.

The mobile computing environment and its security presents a new ground for further research, with some problems which are non-existent in the traditional non-mobile computing environment. Future work on the security of mobile computing must address the problems pertaining to the security of information with the three sub-areas of the mobile environment:

- The security of information residing in the mobile units, and the correctness and integrity of data in these mobile units.
- The security of information as it travels" over the air" between mobile units and mobile support stations.
- The security of information within the mobile wireless network. This includes the security of database holding control data used for the operations and management of the mobile wireless network.

These three sub-areas of research will be crucial if mobile computing is to be a reality in the future.

7. **References**

1. Uwe Hansmann, Lothar Merk, Martin S. Nicklous, Thomas Stober. Principles of Mobile Computing, Second Edition. Springer.
2. https://simple.wikipedia.org/wiki/Cryptographic_hash_function
3. http://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm
4. http://www.faqs.org/faqs/cryptography-faq
5. http://www.rsa.com
6. https://en.wikipedia.org/wiki/Cryptographic_hash_function