Implementation of Non-Vulnerable Messaging System

Gaurav Lalwani, Rohit Wadhwani,
Pradeep Jethani,
Department of Computer Science and Engineering,
Jhulelal Institute of Technology,
Nagpur, India

***Abstract* — There are certain domains wherein the confidentiality of information is of at most importance and needs to be protected from unauthorized usage. This information may be stored in mobiles computers etc where this information is processed. The security in such cases is critical since these devices are prone to illicit physical access. Hence, encryption is used for protection of this information. The usage of cryptographic techniques has been persistent in the domain of security. However, older techniques are now more vulnerable and fail to provide the same level of protection as they once did. Hence, there is an arising need for the advent of new techniques that make use of encryption at increased complexity so that level of security is enhanced.**

Index Terms:Cryptography, Data Security, Mobile security.

INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication using encryption and decryption techniques. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers Cryptography is mainly used as a means of protecting the data during the course of its transmission from one device to another device. That is, cryptography can be seen as a security technique for transfer of data. This leaves the end devices, where the data is in the original format, vulnerable to an attack by a hacker. The situation worsens when there is a possibility of a physical access to the end device. This is probable in those cases where the device is portable and does not perform actual processing of the data stored. In such cases the device itself could get stolen and the possibly sensitive contents of its memory are physically available. Hence, in such situations it gets important to protect the data that is stored.

SYMMETRIC ENCRYPTION

Symmetric encryption is the oldest and best-known technique. 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. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

ASYMMETRIC ENCRYPTION

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key

can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message. The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

Secure Hash Algorithm (SHA) is a hashing algorithm. It is used for password (and other important info) hashing. SHA is used to create digital signatures of the data. By running the algorithm on the data, we produce the hash value (also known as signature). If the data changes in any way, the signature will not match and thus we would know that the data has been compromised/tampered with.

Advanced Encryption Standard (AES) is an encryption standard (symmetric key encryption). Encryption algorithms have a a way of getting back the original data (in case of public/private key pair, the public key encrypts data and private key decrypts it). With symmetric keys, the same key can encrypt and decrypt. But hashing algorithms are one-way processes. Once you hash data and get the hash value, you cannot run it backwards on the hash value to get the original data

LITERATURE SURVEY

Message security is the practice of encrypting messages on your device so that they can be read only by the intended recipient. Although Network Security and Device Security are important, this kind of message encryption is necessary in many situations:

Confidentiality: Message encryption is the only way to ensure that only the indented recipients are reading your messages.

Authenticity: Message encryption is the only way to ensure the identity of the people you are communicating with.

CONFIDENTIALITY

Agencies collecting data often rely on the trust and goodwill. Maintaining public trust helps to achieve better quality data and a higher response to data collections. Protecting confidentiality is a key element in maintaining the trust of data providers.

This leads to reliable data to inform governments, researchers and the community. Confidentiality and therefore trust can be broken when a person or organization can be identified in a disseminated dataset, either directly or indirectly. For example, a person could be directly identified in a dataset if that dataset contains their name and address. However, a person or an organization could also be indirectly identified if there is a combination of information in the dataset from which their identity can be deduced.

Confidentiality is an important principle in health and social care because it functions to impose a boundary on the amount of personal information and data that can be disclosed without consent. Confidentiality arises where a person disclosing personal information reasonably expects his or her privacy to be protected, such as in a relationship of trust.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991 while working at PKWARE.

COBIT 5 for Information Security

The publication provides guidance to help IT and Security professionals understand, utilize, implement and direct important information- security related activities and make more informed decisions. COBIT 5 for Information Security is a major strategic evolution of COBIT 5—the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thin king in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

IDENTIFYING VULNERABILITIES

Propose paper includes the analysis of the Global System for Mobile communication (GSM) so as to quantify the necessary bandwidth to perform such attacks. This technology was selected because, with over 1 billion GSM subscribers, these networks are by far the most widespread on the planet. As we discus later, our analysis of GSM does not preclude other technologies from similar vulnerabilities.

We encourage readers interested in the specific details of the mechanisms used in this attack to read section 2 of the paper. We offer a non-technical explanation of this material below.

Cellular networks can be broken into two chief components -the radio, or "air interface" and the wired backbone. We are chiefly interested in how traffic injected from the internet can be used to congest the air interface as it is the more constrained of the two.

We divide the air interface into two general components - Control Channels and Traffic Channels. It helps to think of control channels as a very small portion of radio frequency that allow cellular towers to send information pertaining to call setup, SMS delivery and network conditions (such as the availability of traffic channels) to mobile phones. Traffic channels are instead used to carry actual voice conversations after they have been established via the control channels. Figure 1, below, gives an intuitive representation of this setup.

SMS/CELLULAR NETWORK VULNERABILITY ANALYSIS

The majority of legitimate users for SMS can often be characterized as non essential, ranging from social they can typically be accomplished through a number of a other, albeit potentially less convenient channels. during the terrorist attacks of September 11,2001, however, the nature of text messaging proved to be far more utilitarian.

Text messaging allowed the lines of communication to remain open for many individuals in need inspite of their inability to complete voice calls. accordingly, SMS messaging is now viewed by many as a reliable method of communication when all other means appear unavailable.

Our project provides network security in Smartphone's. We used the cryptography technique for message security. The AES technique is used for encryption and decryption of data.

- ***Proposed System***

The system that is hereby proposed aims at providing security for network in mobile devices. The system uses symmetric encryption techniques. Thus, this provides ease of symmetric encryption for the bulk of data.

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively.

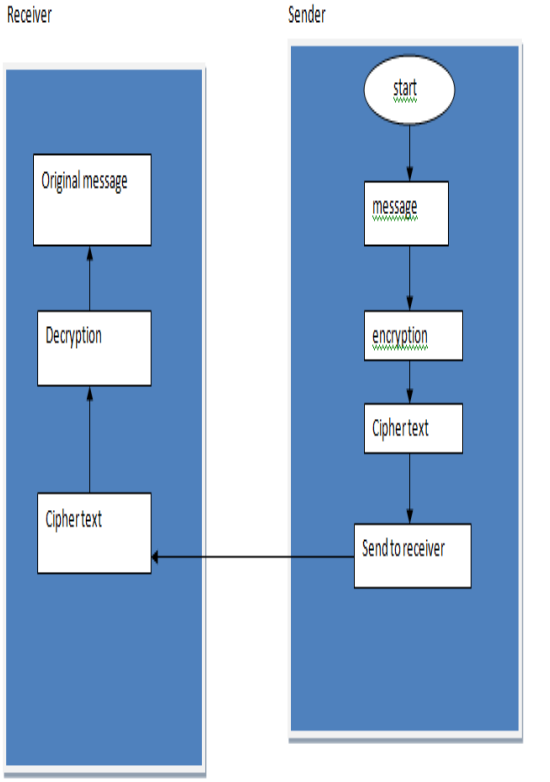
The four stages are as follows:
1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage.

FLOWCHART:



-

CONCLUSION

Thus, a pertinent solution is made available for all android mobile devices for providing security to network. This AES encryption provides a higher level of security and reliability provided by the simplicity of symmetric encryption. Even in the presence of these features, care must be taken as to where this type of encryption must be applied. by virtue of symmetric encryption, if a device can encrypt data, it can also decrypt it. Hence if the information that is stored is required in the device, then a symmetric encryption technique must be employed. Otherwise if the data is not to be accessed in the device, the proposed system is used to encrypt the information.

REFERENCES

[1] Thomas Martin, "Undecryptable Symmetric Encryption", Khalifa University, Dubai, United Arab Emirates, Feb.2011
[2] J. A. Halderman, S. D. Schoen, N. Heninger, W.Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest We Remember: Cold Boot Attacks on Encryption Keys" Proc. 17th USENIX Security Symposium (Sec '08), San Jose, CA, July 2008
[3] Nicholson A. J., Corner M. D. and Noble B. D., "Mobile Device Security Using Transient Authentication", *Mobile Computing, IEEE Transactions on,* vol. 5, pp 1486-1502, Nov. 2006
[4] John S. Thompson, Melinda M. Thompson, "Device security mechanism based on registered passwords", U.S. Patent 6 725 382, April 20. 2004
[5] Jeremy M. Isikoff, "Device Security System", U.S. Patent 5 748 084, May 5.
[6]en.wikipedia.org/wiki/advance_encryption_standard
[7]developer.android.com/reference/app/activity.html#activitylifecycle
[8] http://en.wikipedia.org/wiki/Messaging_security
[9] http://en.wikipedia.org/wiki/Cryptography