ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# A Survey for Solving Security Issues in Mobile Computing

**Sreenubabu Dasari**
**Assistant Professor**
**Department of CSE**
**AITAM, Tekkali.**

**P.Ramkishore**
**M.Tech Student**
**Department of CSE**
**AITAM, Tekkali.**

*Abstract*

***The idea of mobile computing plays a major role in today's world, where the user doesn't need to bound to any physical location. The benefits of on-demand connectivity are not properly utilized because of the lack of proper security measures. In this paper, the main focus is on security problems arising from the technological advances in mobile computing as well as their solution using cryptographic techniques. Encryption of data takes place using symmetric or asymmetric cryptography algorithms depending on the area of application and level of security required. The paper presents a comparative survey on AES, DES, IDEA, RC2, BLOWFISH, RSA encrypting algorithms with their advantages and disadvantages over different parameters. Finally, we derive conclusion over security solutions through these algorithms that may be worked upon to enhance the information and network security in future.***

*Keywords—**Mobile computing; Security issues; Cryptography; IDEA; AES; DES; RC-2; BLOWFISH; RSA; DSA.***

## INTRODUCTION

Mobile computing can be referred to as a technology that permits the sending of data without being connected to any fixed physical network. The computing devices involved wirelessly connect themselves to the centralized information system to trade information. The technology enables its users the right to use and store information without being confined to a fixed location. Since the communication transpires primarily through the radio waves or pulsing infrared light rather than wires, it is easier to intrude into the communication channel, resulting in a number of possible threats for which security is demanded. Security issues like confidentiality, integrity, availability, overview and accountability require individual attention. The authentication protocol checks the integrity of other users on the network before granting them access to the private data on the user's side. Wireless networks are often outlined by serious limitations such as the low computational power and bandwidth availability. Since these resources are not readily available, the system cannot provide assured quality of services. Also, since the users are mobile they may dissociate from the network repeatedly or may intentionally turn off to save power. Apart from this, the solutions built for mobile devices must also be independent of the alliance because the users may move from one zone to another and this should not hinder their work. The aim of mobile computing is to provide users, access to information through any device, any network at any time. In this paper, we discuss a few security enhancing protocols and cryptographic algorithms as a solution to these problems with the aim of strengthening the security amidst the users and the network.

## SECURITY ISSUES AND ATTACKS IN MOBILE COMPUTING

### A. Security Issues

The security issues are:

- Confidentiality: Inhibiting users to access vital information.
- Availability: Guaranteeing that all the legitimate users can use the intended network services
- Integrity: Preventing illegitimate creation, deletion and modification of data. It assures that the information is never spoiled during transmission and only the authorized users can modify it.
- Legitimate: Guaranteeing that only the legitimate users can use the services.
- Accountability: Guaranteeing that the users are answerable for their security related actions. Wireless networks require more security specifications than wired networks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Several approaches have been advised and also the use of encryption techniques has been recommended.

### B. Possible Attacks

**Possible attacks are:**

- Impersonation: The user impersonates as another to get access to a system component to which he/she is not authorized.
- Unauthorized resource usage: The user attempts to access a system component without authorization. This situation may lead to filch or improper use of computing resources.
- Interception: The rival gets access to the information being conveyed through a communication channel. Types of interception are: Leakage of information, and Message pattern Analysis.
- Reforming resources and information: The rival modifies the message being transmitted, changes their sequence or delays them.
- Fabrication: The rival inserts irrelevant information into the communication channel. An example could be: The intruder repeats old messages to deceive the interacting parties.
- Disapproval of activities: A sender/receiver falsely denies having received or sent certain data.

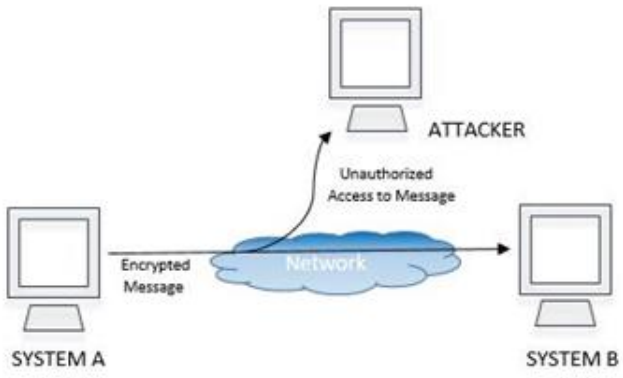


Fig. 1. Possible Attack during Message communication

## SECURITY FAULTS IN MOBILE UNIT EXTENSIONS

### A. Security And Mobility

Components of mobile computing comprises of users as well as the data that they carry, giving rise to a number of security problems that are far different from traditional computing. In static computing, physical shields were easily managed by simply detaching the system and the database from other components in the environment. Hence, making the system self-sustained without any requirement of communication with the other systems. The problem with mobile computing is the limited availability of resources owing to which it becomes necessary for it to communicate with the mobile support station. The main reason of security predicament arises due to constant change in the location of the users and thus the privacy of the data is hampered on being exchanged between users or between users and a fixed host. A user may want to maintain its privacy by existing for only those selected contacts with whom it often interacts. The nodes used in mobile computing must provide the user with a trust level of non-identification as well as the security of data when data is being transferred from one database to another located in different domains. Another security risk comes with the possibility of information leakage, through an invader spying a mobile support station. He may duplicate the environment around the user so that he may not experience any change in the way he accesses data and the invader could easily steal the useful information.

### B. Security and Disconnections

The level of disconnection could range from place to place. Some areas may operate at low bandwidth and some at normal. The active disconnections when the user moves between zones results in several reliability and integrity problems. The move between these levels of disconnection might give the intruder a chance to spy either the mobile device or the mobile station. To prevent this, the mobile device and the mobile station could settle upon some secret key to be exchanged before there is any change in the level of disconnection.

### C. Security And Location Information

A mobile unit must be able change from infrared mode to radio mode as it comes in contact with the networks with different features. This movement also results in the updating of location dependent information resulting in the risk of disconnection and the latency time being increased. In that case, the mobile unit has to be serviced by the nearest server.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## AUTHENTICATION PROTOCOLS

Comparing wireless and wired mobile communication systems, the probability of message intrusion is apparently more in wireless systems. By making a fake identity the confidentiality of the information can be disrupted as the attacker can access the communicating system. These limitations can be overcome by using cryptographic techniques which aims to provide security to an insecure wireless network.

Cryptography is the technique of protecting information from undesirable third parties by changing it into a form which is non-recognizable and secure, during transmission over an untrusted network. Data cryptography mainly involves messing up the contents of a message, like text or media files rendering the data incomprehensible and unreadable during transmission by the process of Encryption. The primary aim of cryptography is to keep information secure form unauthorized people or burglars.

Cryptosystem consist of two techniques of encryption- the symmetric-key cryptography and asymmetric -key cryptography. This system is used to share a common key between the communicating units before the start of session and later to encrypt the message. Table I presents a comparison between symmetric-key and asymmetric-key cryptography.

### A. Cryptography Techniques

1) Private Key cryptography here, same key is used to encrypt the message at sender's end and to decrypt the message at receiver's end. It is called symmetric key cryptography. Some commonly used algorithms are- AES, DES, IDEA, RC2, and BLOWFISH. Symmetric cryptosystems substitution techiniques include- Caeser cipher, Mono alphabetic ciphers, Multiple-letter encryption(Playfair cipher), Polealphabetic Ciphers and Rotor machines

2) Public key cryptography- Here, different keys are used for encryption and decryption mechanisms. A public key is used to encrypt the message at sender's end and a private key is used to decrypt the message at receiver's end. For the same message, two different keys will generate two different cipher texts. It is called asymmetric key cryptography. Some techniques used for encrypting or digitally signing data are RSA, Diffie- Hellman Key agreement and Digital Signature Algorithm.

**TABLE I. COMPARISON BETWEEN SYMMETRIC-KEY AND ASYMMETRIC-KEY ALGORITHMS OF CRYPTOGRAPHY**

| | Symmetric | Asymmetric |
|---|---|---|
| 1. | It uses a single secret key. | It uses a pair of keys- a public key and a private key. |
| 2. | It is an age old technique. | It is relatively new. |
| 3. | Are randomly generated k-bit strings. | Have special structure (e.g., large prime numbers) |
| 4. | Are simple to generate. | Are expensive to generate. |
| 5. | Commonly used for long messages. | Not Efficient for long messages. |
| 6. | These are faster and require less computational power and execution time. | These are slow and require high computational power and execution time. |

### B. Cryptosystem Working

The principle, on which cryptography is based, was proposed by Kerckhoff. The level of concealment of the encryption and decryption key and not the encrypting algorithm itself determines the security of the cryptographic system. The time required to crack the algorithm is directly associated to the length of key used to make the communication secure.

### Cryptographic Systems can be characterized along three dimensions:

1) The kind of operations involved in converting plaintext to cipher text- Encryption algorithms are based on two principles techniques: substitution, which aims to map each element of the plaintext into another element, and transposition, which reshuffle elements of the plaintext.

2) The keys used- symmetric, when both sender and receiver use the same key, or asymmetric, when the sender and receiver use different keys.

3) The processing of plaintext- A block cipher can process one input block at a time, and produce an output block for each input block. A stream cipher can process the input elements continuously, while producing one output element at a time.

There are 2 general approaches by which a conventional encryption scheme can be attacked:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1) Cryptanalysis: The nature of the algorithm as well as some knowledge of the properties of plaintext or samples of pair of plaintext and cipher text determine a cryptanalytic attck. These kinds of attacks uses the characteristics of algorithms to understand a specific plaintext or comprehend the key which is being used.

2) Brute-force attack: The attacker tries all possible combinations of key on a piece of cipher text until it gets translation into plaintext. On an average, half of all possible keys must be tested to gain success.

### C.Vulnerability Issues and Advantages of Symmetric Key Algorithms

AES is a 128-bit block cipher, which is a mathematically proficient cryptographic algorithm for data encryption whose main potency rests in the choice for various key lengths. AES encryption is fast and flexible; it can be made to run on various platforms especially on small devices, been tested for many security applications.

RC2, on the other hand is a 64-bits block cipher and can be attacked using chosen 234 plaintexts being susceptible to related-key attack.

DES is also a block-cipher with key length of 56 bits. DES Encryption relies on two attributes of cryptography:
Substitution and transportation. Due to the small key size of 56-bits, DES is now considered to be unsafe and insecure from point of view of many applications. It suffers from the problem of Simple Relations in its keys due to complementary relations between keys resulting in a complementary relationship between the resulting cipher text. The DES algorithm is susceptible to Linear Cryptanalysis attacks. This vulnerability raises a significant risk during encryption of bulk data that is likely probable with constant keys.

Blowfish is a 64 -bit block cipher which can be replaced with DES algorithm. Blowfish is unpatented, license-free, and is available free of cost for all uses. It was devised with the objective of providing high speed compactness, security and simplicity.

The rate of encryption is given to be 26 cycles per byte on a 32-bit microprocessor requiring less than 5kb of memory space. It makes use of a variable size key of up to 448 bits long and perform primitive operations like addition, lookup tables and XOR for the purpose of design and implementation.

IDEA stands for International Data Encryption Algorithm. It is a block cipher with key length of 128-bits, and is generally regarded as very secure algorithm. No practical attacks on it have come into light despite of a number of attempts made to find some. It is invulnerable to differential cryptanalysis in certain conditions. No fruitful linear or algebraic drawbacks have been reported. Its simple key arrangement makes it subject to a set of weak keys; some keys which contain a significant number of 0 bits produce weak encryption.

### D. Vulnerability Issues and Advantages of Asymmetric Key Algorithms

Since they do not require a shared key and has a simple security architecture it had the advantage over Symmetric Encryption techniques.
Diffie- Hellman key agreement is a an algorithm for exchange of keys permitting two associated users to create a shared secret key, over an unprotected communication medium, which only the two concerned parties are aware of, without even sharing . It is susceptible to man-in-the-middle attacks since it fails to authenticate either party exchanging the keys, which makes it advisable to use it in combination with a supplementary validation protocol, generally digital signatures. When using RSA, a 1,024-bit key is assumed good for bulk encryption to generate digital signatures and to exchange key, while a 2048- bit key size is recommended to keep digital signature secure for a prolonged period of time, for example a certificate authority's key.

Rivest-Shamir-Adleman (RSA) is an asymmetric algorithm which is often used for both encryption as well as for digital signatures. Both encryption and signing tasks are performed through a sequence of modular multiplications. It uses large integers (1024 bits). Its security is due to the cost of factoring large numbers. Keys of size (2048) bits should allow security for decades.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Digital Signature Algorithm (DSA) can be used only for signing data. Though effective, it is not as effectual as the RSA algorithm for verifying signatures. Signature generation uses a private; verification uses public key resembling private key. Every signing entity retains a pair of private and public keys. Public keys are accessible to public and private keys are hidden and kept secret. Verification can be done only by those who possess the public key whereas users having the private key can perform signature generation. A significant problem faced by DSA is the size of its fixed subgroup, which restrains the security to only 80 bits. DSA being widely used is an acknowledged algorithm. Table II presents a comparison of IDEA, AES, DES, RC2, BLOWFISH and RSA algorithms.

## V. CONCLUSION

The paper presents the advantages as well as drawbacks of some symmetric and asymmetric encryption algorithms on the basis of theoretical performance. Symmetric algorithms like AES perform encryption and decryption in comparatively less amount of time enhancing the safety of information while transferring the data 'over the air'. Asymmetric algorithms like RSA and Diffie- Hellman are secure with respect to their size of the keys. RSA rectifies the problem of the key agreement and key exchange issue in secret key cryptography. Hence the feature of public and private keys can be integrated from RSA algorithm in AES which can simultaneously provide the benefit of fast encryption/decryption as well as more security than symmetric- key algorithms. The cryptographic algorithms provide security but it cannot guarantee 100 percent safety. Hence, not only the encryption but also secure transmission of data over the network is mandatory. Firstly, if anyone attempts to make connection with the sender or receiver during the process of encryption and decryption, firewall can be provided to inhibit the intruder from attacking. Secondly, during transmission of encrypted message, the message can be broken into parts and be sent to different mobile stations from where onwards it can be delivered to receiver and only after authenticating the receiver it is unified to the original message. It will preserve the confidentiality of the message. Moreover, the message and key which is sent can be made similar in form to confuse the attacker between key and message.

## REFERENCES

[1]Deepak G., and Pradeep B. S., "Challenging Issues and Limitations of Mobile Computing", International Journal of Computer Techology and Applications, vol. 3, no. 1, pp. 177-181, 2012.

[2]S. Pullela, "Security Issues in Mobile Computing" , Department of Computer Science, University of Texas at Arlington, http://crystal.uta.edu/~kumar/cse6392/termpapers/Srikanth_paper.pdf .

[3]K. Kumari, "Challenging Issues and Limitations of Mobile Computing", COMPUSOFT- An International Journal of Advanced Computer Technology, vol. 3, no. 2, February-2014..

[4]I. Mavridis , and G. Pangalos, "Security Issues in a Mobile Computing Paradigm", in Proc. of CMS'97, Communications and Multimedia Security, Vol.3, pp.60-76, 1997.

[5]T. Hardjono, and J. Seberry, "Information Security Issues In Mobile Computing", Eleventh International Information Processing Conference-Security'95.

[6]D. Goswami, "Mobile Computing", International Journal of Advanced Research in Computer Science and Software Engineering", vol. 3, no. 9, September 2013.

[7]O.A. Hamdan, and B.B. Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, vol. 2, no. 3, March 2010

[8]S.P. Singh, and R. Maini,"Comparison Of Data Encryption Algorithms", International Journal of Computer Science and Communication, vol. 2, no. 1, January-June 2011, pp. 125-127

[9]Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures",

International Journal of Computer Science and Management Studies, vol. 11, no. 3, Oct 2011.

[10]U. Pandey, M. Manoria, and J. Jain, "A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation ", International Journal of Computer Applications, vol. 42, no. 1, pp. 0975 – 8887, March 2012.

[11]P. Mahajan, and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 15, version 1.0, 2013.