TOPIC: MOBILE COMPUTING AND SECURITY ISSUES.

Owodele Odukale

ABSTRACT

The past decade has seen a growth in the use of mobile computing. Its use can be found in areas such as social media, information exchange, online social gaming amongst others. However its use in the transmission of more sensitive data gives causes for concern due to its security vulnerabilities. Traditional computing systems make use of certain detection technologies and firewalls to prevent intrusion but such methods are difficult to apply with mobile computing thus making the security of data between mobile workstations and mobile unit a challenge. Challenges experienced in mobile communication include: forced de-authentication, disconnection and mimicry of the host mobile station or unit. The purpose of this research is to propose a secure mobile communication scheme that makes use of an asymmetric algorithm to encode the messages before transmission so as to provide secure communication over the channel. The mobile client will have a public key and a private key that will be used to encode messages sent over the communication channel while the server side decrypts the message using the private key.

INTRODUCTION

Mobile communication technology has a lot of benefits in today's world. The use of smart cellphones, laptop computers, personal digital assistants and tablets has become very popular at all user and application levels. Mobile computing can be defined as having access to computing resources from anywhere using mobile devices. Securing

these new devices is paramount as the use of such devices in such a platform comes with new security risks and challenges. Sensitive information can be stored in mobile devices which can be transferred in out of the boundaries of a networking environment. The users of mobile devices have flexibility in the sense that they can set up workstations anywhere without being bound to any networking system. This advantage of a mobile system to the user makes security management a difficult task to accomplish as the users cannot be tracked down to a single location (Leunga et al, 2007).

Traditional security technologies such as firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection, and VPNs are not enough to tackle security issues in mobile computing since such communication takes place mainly through the radio signals rather than wires, so it is easier to intercept or eavesdrop on the communication channels. Traditional computing systems are fixed (non-mobile) as such the database and other components can easily be protected by physically removing each part away from each other thereby creating distance to enable the system to operate on its own without interactions with the external environment. For such a system, a firewall technique can offer enough protection (Lampson et al, 1992).

LITERATURE REVIEW

The activities of mobile computing systems are dependent on its communication with the mobile support station as such it can not operate in isolation due to limited resources available to a mobile unit. User anonymity is another security issue faced

when using a mobile communication system as the trust level afforded by each node in the wireless network is difficult to maintain. Data transfer between databases at nodes which hold location data and other information or parameters in the user profile must be maintained secure and authentic. Another problem with mobile computing system is that an attacker may masquerade as a mobile support station and may use this medium to issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user profile containing the patterns and history of the user's movements. This type of interference may give room to information leakage. Securing data from attackers in this way will involve presentation of sufficient proof that the user approves of the queries submitted by the (foreign) mobile support station controlling the zone under which the user is currently roaming or passing through (Lampson et al, 1992).

Replication of sensitive data or replication of the environment surrounding the user can be used as an avenue for lowering security or opportunities for multiple attacks as such, degradation in the access and latency times must not be experienced by the user while roaming between zones. A mobile unit can be disconnected from a mobile station to conserve power (elective disconnection) or due to an unforeseen event, such as system crashes or total communications break-down when moving into certain geographic regions (non-elective disconnection). Disconnection of any kind introduces a number of lapses for security breach for attackers to mimic either the mobile unit or the mobile stations and gain access to the mobile user. This type of system interference can be

resolved if the mobile station and the mobile user establish some kind of secret key agreement before transition into an elective disconnection. Zero-knowledge protocols can be implemented in which the mobile unit and the mobile support station can convince each other that they hold the shared secret without having to transmit the full secret (Leighton and Micali, 1993).

Mobile devices are easily stolen, and theft of such devices is on the rise. In most theft cases the aim was the data stored on the device rather than the device itself. One such well known case that happened in Beirut-Lebanon on Oct, 27, 2010 was the attack on the investigation team of the UN created International Tribunal for Lebanon, set up in 2007 to bring to justice those involved in the assassination of then Prime Minister Rafiq Hariri. The result of the attack was the confiscating of the laptop computers, cell phones, notebooks and other materials that were in the possession of the investigation team. One of the main goals of the attack was the sensitive and crucial data stored on these mobile and portable devices (Naharnet, 2010). There is compelling evidence that mobile devices pose one of the fast growing areas of security concern. Since January 2008, Privacy Rights International's published Chronology of Data Breaches documents that 20 percent of the data breaches reported resulted from mobile device losses: Lost laptops, notebook computers, PDAs, portable drives, USBs, CDs, flash cards, SD cards, and disks (Nascio, 2009). As a result of these incidents, all of the major mobile devices makers have taken steps during the past few years to improve device security, such as by providing longer device unlock codes like the case of Apple iOS devices, and extending encryption support to SD cards and other mobile data storage devices.

However, many defense technology experts feel that protection measures remain insufficient for defense needs and therefore must be strengthen with additional safety measures (John, 2011).

AIM AND OBJECTIVE

The aim of this seminar is to propose a secured method for transmitting data through the mobile computing network using an asymmetric encryption algorithm. The objective is to provide a safe means of using the mobile technology as a viable communication channel.

PURPOSE OF THE STUDY

This study seeks to contribute to the furtherance of the safe use of the mobile computing technology over the internet. Currently this area of computing is venerable to attacks due to its many security loopholes that exist in the system

METHODOLOGY

The researcher's proposed method for providing security on the mobile communication interface involving the use of asymmetric encryption communication software that will be used to send messages across the communication channel. The communication software will make use of a secured version of RSA asymmetric algorithm which will be used to encode messages sent across the mobile based station and the mobile devices such that data intercepted cannot the accessed. The RSA algorithm will be used RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977 (Nigel, 2008)

The system architecture is illustrated in Figure 1 below.

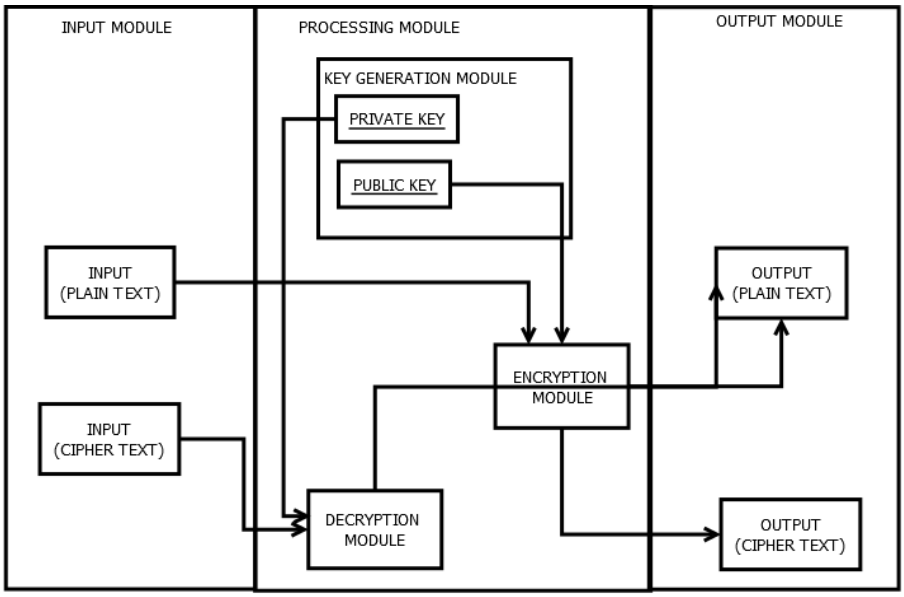

Figure 1. System Architecture for the Secured Mobile Communication System

From the diagram it can be seen that there are two input types.

a) The INPUT (Plain text): This input goes to the encryption module where the recipient's public key is provided. This module then encrypts the input and displays the output as OUTPUT (Cipher Text)

b) The INPUT (Cipher text): This input goes to the decryption module where the recipient's private key is provided. This module then decrypts the input and displays the output as OUTPUT (Plain Text)

Mode of Operation:

The mobile client will have a client version of the software installed on their system. Each client will have its own public key having a length of 1000 bytes.

When a message is delivered by the client software, it will be encoded using the mobile server's private key before it is sent over the communication channel.

The server side software that receives the message will decrypt the message using its own private key.

The same process is repeated when a message is to be sent back from the server to the client but using the client's public key to decrypt the message.

RSA Encryption Algorithm:

The RSA algorithm for the encryption of the message text to cipher text is shown below:

- Enter value of public key E,N
- Enter message, M
- Calculate the Cipher text using C= M ^ E mod (N)

Software Encryption Flowchart:

The flowchart showing the graphical sequence of activities for encrypting a message is illustrated in Figure 2 below:-

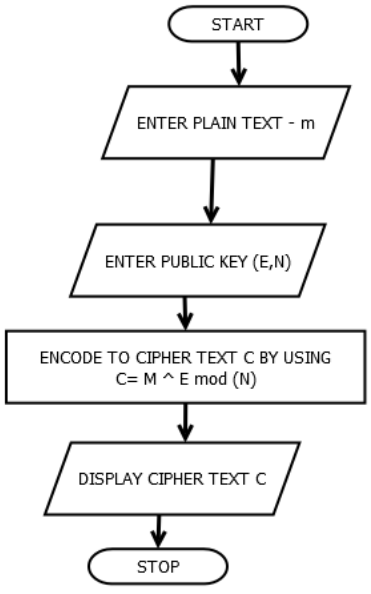

Figure 2 Software Encryption Flowchart

RSA Decryption Algorithm

The algorithm for the decryption of the cipher text to padded text is shown below:

- Enter value of private key D,N
- Enter cyper text, C
- Calculate the Padded Message using M = C ^ D mod (N)

Software Decryption Flowchart

The flowchart showing the graphical sequence of activities for decrypting a message is illustrated in Figure 3 below:-

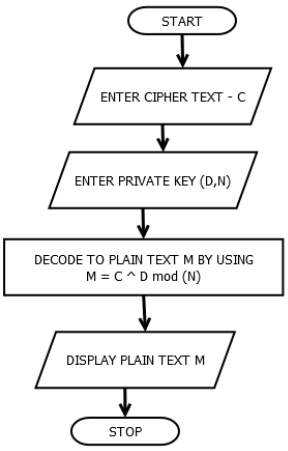

Figure 3 Software Encryption Flowchart

PERSONAL POSITION OF THE TOPIC

If implemented, this proposed secure mobile computing security communication system will ensure the safe use of the mobile platform for transfer of sensitive information between client and server systems. Sensitive operations such as e-commerce transactions for example, will be performed via mobile devices without the interference of a malicious third party.

SUMMARY AND CONCLUSION

The opportunities created with improvement in technologies are vast and endless but as with all things in life, every solution always comes with its own list of challenges. This is also the case with the use of mobile computing systems. Mobile computing denotes technologies that enable people to search, access and utilize network services and content from an array of Service/Content Providers. It offers a wide range of application to the users though with high security risks with the need to proffer security measures to combat the problems associated with this means of communication. In this paper, the researcher has introduced the concept of mobile computing and has analyzed the security challenges and proposed a possible method of solving these problems.

In conclusion, the potentials of the mobile computing technology cannot be over-emphasized. The only issue borders on security. With this proposed scheme of mobile communication, the reliability of secured information exchange will be assured.

REFERENCES

Smart, Nigel (February 19, 2008). "Dr Clifford Cocks CB". Bristol University. Retrieved August 14, 2011.

Adrian Leunga, Yingli Shengb, Haitham Cruickshankb, "The security challenges for mobile ubiquitous services" Information Security Group, Royal Holloway, University of London, Egham, UKbCentre for Communication Systems Research, University of Surrey, Guildford, Surrey, UK , 2007

B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," Technical Report 83, Digital Systems Research Center, February 1992.

T. Leighton and S. Micali, "Secret-key agreement without public-key cryptography,"in Advances in Cryptology — Proceedings of Crypto '93 (D. R. Stinson, ed.), vol. 773 of Lecture Notes in Computer Science, pp. 456—479, Springer-Verlag, 1993.

http://www.naharnet.com/stories/en/676.

Naharnet Newsdesk (28 October 2010). Men Disguised as Women Likely Involved in Attack on UN Investigators in Dahiyeh

http://www.nascio.org/publications/documents/NASCIO-securityAtTheEdge.pdf, july 2009.

John Edwards, DOD tackles security challenges of mobile computing, defense Systems, June 13, 2011