Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) – May 2015
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Security Controls and Measures in Mobile Computing

M.Sandhiya[#1], K.Saranya[*2]
[1,2]*Department of Computer Applications, S.A Engineering College, Chennai*
kalaimano55@gmail.com

***Abstract*—**In this paper of mobile communication environment lots of research is going on to improve performance of security issues. Security is one of the a key issue that needs to be considered. As more and more people enjoy the various services brought by the mobile computing, it is becoming a global trend in the upcoming technology. At the same time securing mobile has been paid increasing attention in the society. We concentrate our research on few authentication protocols that were proposed to provide security between the user and the network. Now we going to analyse the security risk confronted by mobile computing and the security mechanism.

Keywords—*-Mobile computing, mobile computing security, distributed systems security.*

1. Introduction

The radical evolution of computers, especially in hardware and communications between the Satellite networks, cellular telephony, WANs and INTERNET has introduced in the idea of mobile computing in 1992 by Imielinski and Badrinath. The decreasing size of computer components and the increasing availability of wireless communication technology make to possible ubiquitous on mobile computing. The networks turn stand-alone personal computers into distributed systems that allow users anywhere on the network to access the shared resources. Wireless networks should be used to provide access to the computers that have better performance and users should be able to have both mobility and performance instead of having to trade them against each other. As wireless communication takes place through the radio signals rather than wires, it is easier to intercept or eavesdrop in the communication channels. Therefore, it is very important to provide security from all these threats. The large area can be covered by installing sever without an assigned key is denied access. Presently many wireless technologies are being used with each having their own approaches to provide security. In this paper we will discuss about some of the current approaches and industry standards that are being followed

2. Security issues

Security is the prerequisite for every network, but mobile computing presents more security issues than traditional networks due to additional constraints imposed by the characteristics of wireless transmission and the demand for mobility and portability.

2.1 More vulnerabilities of networks

In ad hoc networks, mobile hosts are not bound to any centralized control like base stations or access points. They are roaming independently and are able to move freely with an arbitrary speed and directions. Besides these security risks, ad hoc networks are prone

3. Security Counter Measures

Secure mobile computing is critical in the development of any application of wireless networks.

3.1 Authentication

In a WLAN, an AP must authenticate a client before the client can associate with the AP or communicate with network. The IEEE 802.11 standard has defined two types of authentication methods. They are open system and shared key authentication. Open system authentication allows any device to join the network, assuming that the SSID matches the access pint SSID. In shared key authentication, only Pcs that possess the correct authentication key can join the network. both of these keys are one-way communication.

3.1.1 Security requirements

- Availability- Ensures that the intended network services are available to the intended parties when needed.
- Confidentiality- It ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.
- Integrity- guarantees that information is never corrupted during transmission. Only the authorized parties are able to modify it.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

- Non-repudiation- It ensures that an entity can prove the transmission or reception of information by another entity that is a sender /receiver cannot falsely deny having received or sent certain data..

3.2 WEP – Wired -Equivalent Privacy

WEP is a standard protocol which is tried to secure the wireless networks. It is one of the part of IEEE 802.11 standards. It was cracked almost a decade back and rarely seen these days.

This protocol encrypts the communication between the client and an AP. WEP specifies the use of a 40-bit encryption key. The encryption key is concatenated with a 24-bit "initialization vector" (IV), resulting in a 64-bit key. The resulting sequence is used to encrypt the data to be transmitted.

3.2.1 WEP implementation

Using WEP/WPA/WPA2 on the client side(e.g., from your smart phone or laptop: when you are trying to establish a connection to a security-enabled network for the first time, you will be prompted to enter connection to the network; that key or passphrase is the WEP/WPA code. It is provided by the network administrator or service provider.

WEP/WPA/WPA2 is using on the access pointer or router. Most wireless access point and routes today allow you to select during setup the security protocol to be used.

3.2.2 WEP Architecture

WEP to help overcome this security gap in wireless networks, IEEE 802.11 working group instituted Task Group has proposed significant modifications to the existing IEEE standard as a long-term solution for security, called Robust Security Network (RSN). TKIP primarily addresses the shortcomings of WEP and fixes the well-known problems with WEP, including small initialization vector and short encryption keys. Once the verification process completes, the authentication server sends a response message to the access point that the client has been authenticated and network access should be granted.

3.2.3 Algorithm

This algorithm is made used of RC4 stream, the main problem in RC4 is, if the same key eas used repeatedly then it becomes very easy to crack the key sniffing enough number of packets and carrying out a passive attack.

```
Void wepkey64 (char*passphrase, unsigned char k64[4][5])
{
Unsigned char pseed[4]={0};
Unsigned intrandNumber,tmp;
Int I, j;
For{i=0;i<strlen(passphrase;i++)
{
Pseed[i%4]^=(unsigned char),(passphrase[i];
}
randNumber=pseed[0]|(pseed[1]<<8)|(pseed[2]<<16)|(
psee          d[3]<<24);
for(i=0;i<4;i++)
{
For(j=0;j<5;j++)
{
randNumber={randNumber*0*343fd+0*269ec3)&0*ff
ffffff;
tmp=(randNumber>>16)&0*ff;
k64[i][j]=(unsigned char)tmp;
}
}
}
```

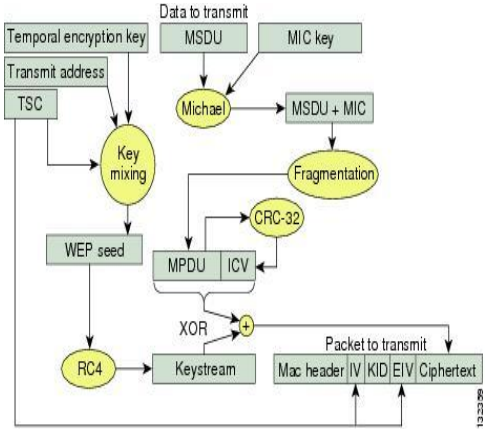

Fig.1: WEP-Architecture

Hence, not all users will be able to take advantage of it. A phase adoption process for this standard is anticipated because of the large amount of installed 802.11 devices.

3.2.4 Security controls

Our work on security issues in mobile computing has addresses the problems pertaining to its security of information within three sub-areas, they are:

- The security of information residing in the mobile units, considering device constraints.
- The security of information as it travels over the air between mobile units and mobile support agents. An important consideration in this area is power consumption of the algorithm that implements this secure area.
- The security of information within the rest network includes the security of database holding control data

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

used on the operations and management of mobile wireless network.

3.2.5 Graph

The Global Market for Wireless Network Connections in Industrial Automation Components (in Thousands of Units)

	2012	2013	2014	2015	2016	2017
Thousands of Units	2,067	2,265	2,509	2,784	3,103	3,445

Source: IHS Technology February 2014

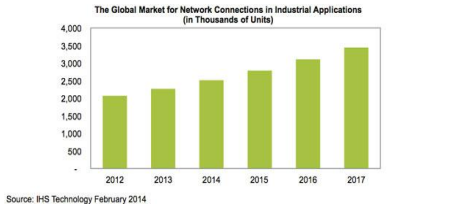

Fig.2: Graph result

3.2.6 Performance

The certificate-based security protocol is considered to be more secure than symmetric key protocol in terms of key management. Because of its computational complexity, public- key cryptosystem is considered to be a burden on a mobile user with limited resources.

The recently announced smart card chip contains 8-bit CPU as a standard smart card controller and an additional and arithmetic of the co-processor optimized for modular exponentiation of long operands. The table given below shows the performance of KSSL cryptographic primitives on PDAs

	PalmVx (20MHz)	Visor (33MHz)
RSA (1024-bit)		
Verify†	1433 ms	806 ms
Sign	80.91 sec	45.11 sec
RSA (768-bit)		
Verify†	886 ms	496 ms
Sign	36.22 sec	20.19 sec
MD5		
1024 bytes	292 Kbits/s	512 Kbits/s
4096 bytes	364 Kbits/s	655 Kbits/s
SHA-1		
1024 bytes	124 Kbits/s	227 Kbits/s
4096 bytes	140 Kbits/s	256 Kbits/s
RC4		
1024 bytes	117 Kbits/s	215 Kbits/s
4096 bytes	190 Kbits/s	351 Kbits/s

†With a public-key exponent of 65537

Fig.3: result

4. Conclusion

Mobile computing technological provide anywhere and anytime services to mobile users by combining wireless technology. The uses of mobile resources in environments provide important benefits and also the serious security problems are derived.

The future work includes the systematic definition of at least two different security policies that are used by different backbone networks. Securing mobile computing is critical to develop viable applications, hoping to keep security development in pace with other aspects of wireless technology.

Acknowledgement

This project is the result of dedicated effort. It gives us immense pleasure to prepare this project report on “S.A Engineering College”. I would like to thank our project guide for consultative help and constructive suggestions on making this project a successful one.

References

[1] D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole publisher, 2002.
[2] J. Walker, “Overview of IEEE 802.11b Security”, http://www. intel.com/technology/itj/q22000/pdf/art_5.pdf.
[3] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting Mobile Communications: the Insecurity of 802.11”, http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.
[4] B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A Secure Routing Protocol for Ad Hoc Networks,” Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.
[5] Chang-Seop Park, “ On Certificate-Based Security Protocols for Wireless Mobile Communication Systems.”IEEE Network 1997.
[6] Vipul Gupta and Sumit Gupta “Securing the Wireless Internet” IEEE Communications 2001.
[7] Bakre, A., Badrinath, B.R. Handoff and System Support for Indirect TCP/IP. In Proceedings of the Second Usenix Symposium on Mobile & Location-Independent Computing. Ann Arbor, MI, April, 1995.
[8] Rosemary Walsh. The Gold mailer.In 9th International Conference on Data Engineering, Vienna, April 1993.To appear.
[9] Daniel Barbara, Chris Clifton, Fred Douglis, Hector Garcia-Molina, Stephen Johnson, Ben Kao, Sharad Mehrotra, Jens Tellefsen, and
[10] John Howard, Michael Kazar, Sherri Menees, David Nichols, ahadevSatyanarayanan, Robert Sidebotham, and Michael West. Scale and Performance in a Distributed File System. ACM Transactions of Computer Systems, 6(1):51{81, February 1988.
[11] J. Ioannidis, D. Duchamp, and G. Maguire, Jr. IP-based Protocols for Mobile Internetworking. In Proceedings of SIGCOMM '91, pages 235{245, September 1991.Describes IPIP and IMCP.
[12] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[13] http://security.stackexchange.com/questions/35614/standard algorithm-for-wep-key-generator-64-bit

M.Sandhiya is holding Under Graduation Degree in BCA Computer Application from Anna Adarsh College for Women of arts and science and pursuvingPostb Graduation on Master of Computer Applications from S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar & Report Writing.

K.Saranya is holding under graduation degree in BCA Computer Application from Jaya College of arts and science and pursuvingPostb Graduation on Master of Computer Applications from S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar & Report Writing.