Security in Mobile Communications: Challenges and Opportunities

Chandan Varma.G[1]
[1]Department of Computer Science and Engineering
[1]Saveetha University Chennai 602105

Abstract— The nature of mobile communication, characterized for example by terminals having poor user interface and limited processing capacity, as well as complex combination of network protocols, makes the design of security solutions particularly challenging. This paper discusses some of the difficulties system architects are faced with as well as some advantages mobile networks offer when designing security solutions for mobile communication.

Keywords: mobile communication, network protocols, security.

I. INTRODUCTION

Over the last few years, a number of mobile communication systems have been developed and numerous service providers and equipment vendors are bringing to market steady stream of new innovations. When looking at traditional e-commerce, the lack of security and a high level of fraud are seen as the major obstacle to people embracing the possibilities and advantages e-commerce can offer. . According to Andersen the current insecurity of commercial systems on the Internet is thus perfectly rational from the economists' viewpoint, however undesirable from the users'. For m-commerce, there is a risk that a similar development will take place, but not necessarily so. In e-commerce the limited size and poor user interface of mobile devices pose particular problems for implementing user friendly applications in general and even more so for security.

II. REQUIREMENTS FOR COMMUNICATION SECURITY

Communication security is often described in terms of confidentiality, integrity, authentication and non repudiation of transmitted data. These security services are in turn implemented by various mechanisms that are usually cryptographic in nature. Ensuring system security at both the client and the server end must not be ignored. On the client side, the poor platform integrity, the multitude of default CA certificates and the arcane user interface pose severe security threats. System security can be addressed by installing firewalls and intrusion detection systems, by monitoring security alerts and prompt implementation of security patches. However this requires skilled system administrators to continuously look after systems, which is relatively labor intensive compared to communication security. Labor intensive compared to communication security. Due to poor management and operation and not by weaknesses in the cryptographic algorithms themselves.Confidentiality of transmitted data can be provided by encrypting the information flow between the communicating parties, and the encryption can take place end-toned between the communicating parties or alternatively on separate legs in the communication path. In GSM networks for example, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is totally transparent from the user's point of view. Non-repudiation is similar to authentication in that it is an asymmetric security service. A simple way to describe the difference between authentication and non-repudiation is that with authentication the recipient himself is confidence about the origin of a message but would not necessarily be able to convince anybody else about it, whereas for non-repudiation the recipient is also able to convince
third parties.

III. THE NETWORK OPERATOR AS TRUSTED THIRD PARTY

Public-key cryptography is the basis of several important security services such as non-repudiation and authentication and is an essential element for SSL that is used for securing .Web communication. One public/private key pair issued for authenticating one party by the other, and mutual authentication requires two key pairs. This requires the secure generation and distribution of potentially hundreds of millions of public/private key pairs, which poses a formidable key management challenge. A PKI refers to an infrastructure for distributing public keys where the authenticity of public keys is certified by Certification Authorities. If the certificate owner's identity is one of the attributes, then the certificate is called an identity certificate, and the purpose of the certificate is to link the public key and the identity together in an unambiguous way. The CA is a Trusted Third Party because it is trusted to correctly verify and certify the identity of the public-key owner before issuing the certificate. This is difficult to achieve with a handful of global CAs serving the whole Internet community as the case is for the Web PKI. In case of subscription based mobile networks there exists a formal relationship between users/subscribers on one hand and the network operator on the other. The user's private key as well as the root CA public key can be distributed in a secure way based on the distribution of subscription tokens e.g. in the form of the GSM SIM card. This will require a relationship between vendors and network operators similar to the relationship between vendors and credit card companies.

IV. SECURITY ACROSS HETEROGENEOUS NETWORKS

Network architectures are based on protocol layers which represent an abstract way of modeling and implementing data transmission between communicating parties. No data are directly transferred between adjacent layers on opposite sides. Instead, data and control information are passed down through the interfaces between the protocol layers on one side and up through the interfaces between the protocols layers on the other side. The network architecture and the security goal together indicate the most appropriate protocol layer where a security service is to be located. Authentication and non repudiation are for example only meaningful when implemented end-to-end between the parties that needs to authenticate each other. It could also have been to facilitate legal government interception of Traffic contents from the WAP gateway clear text gap. With

an end-to-end security architecture this would change, and in fact become similar to the existing security architecture on the Internet. Because of the deficiencies in the original WTLS protocol the WAP forum has defined a new standard for end-end SSL using tunneling through the WAP gateway. This is achieved by implementing a wireless enhanced version of the Internet TCP transport protocol layer in the mobile devices and run SSL on top of that. However, because the origin server will probably not support wireless enhanced TCP, there will be a proxy that acts as the termination point of two TCP sessions, one w-TCP to the client mobile terminal and one TCP to the server. It will just move packets across transparently from one connection to the other.

V. USABILITY OF SECURITY

Details of the security services and mechanisms are of-ten complex and users would quickly be overloaded with information if the details were presented to them. A common design philosophy is therefore to make security services and mechanisms as transparent as possible. How-ever there is a danger that users receive too little security information. If security is totally hidden from the user he or she would not be able to tell whether it is working the way it was intended, which in turn could allow successful attacks to remain undetected. Obviously, the security evidence provided cannot be more than the user can understand and handle but it must be sufficient for the required security level of the application. The challenge is to determine what type of evidence is really necessary and present it to the user in an intuitive and intelligible way. In the computer network jargon it is sometimes forgotten that communication ultimately goes between human users and organizations, and that some security services. The integrity of the evidence presented to the user can be assured by having a reserved area for certified content on the interface which is never used for other types of content. Because of limited size of visual displays this might seem to be an expensive sacrifice. We therefore recommend using the normal display for displaying security information, but in a special security mode, and instead to reserve a small exclusive area to indicate that the display is in security mode. The exclusive security display area and the security display mode should not be accessible by content applications. This security mode should be easy to invoke and be distinguishable from the other display modes. only are meaningful if they are designed to suit human users. The interpretation of communication in the human brain can conceptually be described as a semantic protocol.

VI. SECURING ACTIVE CONTENTS

Before active content was available Web pages were mainly static displays of information coded in the Hyper sound and image animation and provides the user with the ability to interact with the server side during a Web session. Active content exists in many forms. Java applets and ActiveX controls are some of the best known but there are also JavaScript's, VBScripts, MSWord Macros and even images. All these basically consist of mobile code that is sent from the Web server and loaded into the client machine for execution there.

All this is very appealing from a functionality and flexibility point of view but it poses a formidable threat to the integrity of the client machine. Active content can cause damage by intent or by simply being poorly designed. A discussion of threats and risks posed by active contents applets are described in Firewalls offer little protection because they are usually configured to let http Traffic and active content through. Unless the active content can be controlled, all files and network connections can be accessed and used, making it impossible to operate any secure applications on the client machine. Sandboxing and certification can be used to counter threats from active content.

Sandboxing basically means that the active content is constrained in what resources it can access on the host system. The advantage is that it is always active and completely transparent to the user. The disadvantage is that it severely limits the capabilities of active contents. Certification means that a trusted party has validated and digitally signed the active content and that the platform verifies the digital signature before it can execute. The advantage is that the active content can access all system resources. The disadvantage is that certification is not equivalent with trustworthiness. A Web browser can for be tuned so that any piece of certified active content is accepted by default or alternatively so that only active content certified by certain parties is accepted by default and that any other trigger a dialog box. The dialog box basically asks the user whether he or she wants the active content to be executed. Experience shows that users almost always accept active content when asked by a dialog box simply because they want the functionality and because most active content is benign anyway. This means that should the user receive a piece of malicious active content he or she will almost certainly make the wrong decision and accept it. The user simply does not have sufficient evidence to make an informed decision.

VII. CONCLUSIONS

We have seen that the aspects of mobile networks can make it both harder and easier to implement communication security as compared to for example the Internet. Communication between mobile and fixed networks create particular problems regarding security protocol design.

REFERENCES

[1] Hoshizawa, Y. (2002), Are Java-Enabled Mobile Phones Secured?, in . Gattiker, ed., 'EICAR Conference.
[2] Netscape Communications Corp. Open Wave Systems (2002), 'Download Fun FAQ', URL:http://developer.openwave.com/prod tech/faqdf.html
[3] IETF PKIX Working Group INTERNET-DRAFT. URL:http://www.ietf.org/internet-drafts/draft-ietfpkix-logotypes-00.txt.
[4] International Organisation for Standardization.ITU (1997), Recommendation X.509, The Directory: Authentication Framework (also ISO/IEC 95948, 1995), International Telecommunications Union.

