SDR SYSTEM SECURITY

Peter G. Cook (HYPRES, Inc. Elmsford, NY USA, pgcook@hypres.com)

ABSTRACT

As the PCS market moves from its origins in wireline voice connections to mobile wireless, legacy security provisions have proved to be inadequate. In particular the security risks associated with a wireless link that can be intercepted must be addressed.

This paper looks at the needs for system security in different operating modes. It then examines the threats presented by a number of different categories of perpetrators and modes of service misuse or disruption. Finally it looks at the measures available to reduce the risk of security compromise.

The result is a structure that can be used to develop scenarios that establish the degree of risk associated with various security threats, and evaluate the cost of reducing them.

1. INTRODUCTION

The security objectives for commercial systems must be based on an understanding the need and consideration of the cost justification. Security dimensions reflect the concerns of differing participants with divergent perspectives. We propose a threat vector as a means to structure threats to the system. It is composed of operating modes of the system, the different perpetrators and their motivations and means to threatening system operation. Finally we discuss some of the measures that can be taken to raise system security.

2. DIMENSIONS OF SYSTEM SECURITY

All participants in the field of PCS mobile wireless systems need assurance that the system will perform the tasks allocated to it without compromise. In this section we review individual aspects of system performance and functions that are requirements of the security architecture.

2.1 Protect operating information

Operating information is traffic used by the system or about its operation as differentiated from content.

Radio parameters are data that can effect radio link behavior. Effective system operation requires close control over such variables as radiated power and operating frequency. Regulatory authorities are also concerned with this data as it has a potential to cause the radio to operate outside its authorized limits.

Any PCS has a substantial amount of internal traffic dealing with call setup, teardown, billing, handoff, and link maintenance during the call. The system design must ensure that the user interface cannot be used to gain access to control of the system, because such access could be used to delete billing information, disrupt traffic flow, and many other undesirable actions.

Keys are used to disguise information during transfer. Passwords are used to permit access to parts of the system by individuals who have a need to do so. Interception of either of these items by unauthorized individuals compromises the system, and opens a particularly dangerous threat because it is very difficult to detect. Actions taken with stolen keys or passwords appear very much like normal operations, delaying corrective action.

It is a violation of user privacy if the users identity and location can be determined by intercepting a transmission, particularly if the content of the communication can also be determined. This was unfortunately the case with early analog cellular systems. On the other hand, there is now a requirement that the originators of PCS calls to 911 are geolocated, and knowledge of user identity is necessary to perform billing. One mechanism to protect identity is to encrypt the initial contact, and assign a random user ID for the duration of the call. Then all records of the call can be maintained under the temporary number, with translation to the actual individual available only at a central site.

2.2 Protect content

Most users of communications systems do so because they are interested in the content of the traffic. Different types of content are subject to different threats, and have different values that impact the probabilistic threat-cost model.

Much of the information content of PCS systems has little or no inherent value – a perpetrator intercepting it would find it of no value. Some data transferred, however, can be very important in a specific context, such as a project bid amount, potential sale of a company, or insider information that could be used on the stock market. As the system designer has no way of knowing what information will be conveyed, all user content must be treated as private and protected from interception to the extent practical.

The system design is, however, still subject to cost and probability trade-offs, and potential threats weighed with the cost of preventing them. The sheer volume of traffic means that valuable information traffic content has a low density. Threat analysis is essential to determining the security mechanisms to be invoked.

One very specific type of content is a funds transfer transaction, used to replace a banknote or a check with an electronic message. The use of a wireless link for this type of transaction requires a very high level of security to ensure that no funds are diverted or duplicated.

In the past, broadcast of music or video content has presented little concern because most listeners did not record the content, and available recording techniques had low fidelity. With digital representation, however, there is now a great deal of controversy about what constitutes fair use of purchased material. I can play a CD that I have purchased as many times as I care to on a CD player or a PC. And I can put it into your PC disk drive and let both of us listen to it. But if you retain the content as a file on your computer, that may be considered illegal copying.

This issue is potentially an interesting extension of the scope of wireless system security. Not only is the system designer being asked to protect the content of the traffic from unauthorized interception, but for the first time a requirement to prevent free use of message content is placed on the authorized recipient.

2.3 Payment and billing

The mobile terminal carried by PCS system users has a potential for use in making payment for goods and services. The system security mechanisms must be adequate for accurate biling and payment.

2.4 Reliable payment for services

Users of mobile systems have access to a variety of services. The essence of the business case for PCS systems is that users will find these services helpful and beneficial, and will be willing to pay for their use. It is a security requirement of these systems that users be billed for all the services they use and only the services they use. Non-repudiation is the security provision that restricts users from claiming they did not make use of a service when, in fact, they did.

The cash stream originating from the user is the primary source of funds for the entire wireless communications industry. It pays for operation of the network, for services provided by the company holding the users contract, for use of third party applications, and a number of other participants. Accurate billing and ability to support a number of billing plans and arrangements are essential.

Credit cards are an important way to shop over the phone or on the internet. Buying something involves providing the vendor with the credit card number, and other identifying information. A well designed wireless system can assist in this process by confirming the user’s identity as established in a subscriber identity module (SIM) or equivalent facility. Such confirmation must be subject to privacy concerns mentioned in Section 2.1.5. .

Use of a credit card on a wireless link is a significant potential exposure, so credit card information must be kept secure The number may be part of the users record in the home location record (HLR), and transmitted from their in a separate message to the seller. .If card information is spoken on a voice link, keyed in, or extracted from a user identity module (UIM) it must be protected.

A wireless mobile terminal can be used to store funds in the same manner as a smart card. The user can walk up to a vending machine, talk to it over a short range wireless link, and have the funds to buy merchandise subtracted from the balance in the terminal. Most of the security concerns for these transactions have been developed by the smart card industry, and can be applied to wireless terminals.

2.5 Regulatory conformance

Because there is a great deal of contention for use of the electromagnetic spectrum regulators are interested in maintaining control of how it is used, and for certifying that radio equipment meets their emission specifications.

Equipment to be used in commercial service must pass a set of qualification tests to receive a regulatory certification. Procedures for doing so in the US have recently been changed by the FCC to accommodate SDRs. The current requirement is that each combination of hardware and software must be certified together. In the future this will give rise to combinatorial difficulties, and other provisions will be needed. For the present, however, it is in effect.

Once a set of software has been certified, it must be delivered to the thousands of users who purchase it. In the past each phone had just one set, so there was no problem. With SDR, however, new software can be installed to upgrade a phone, or to give it additional capabilities.

Software can be installed into a terminal by adding a chip, using a cable connection, or an over-the-air transfer. Procedures for doing so have been described by the SDR Forum. Key requirements are to establish that the terminal is authorized for that specific software, and that the software has not been compromised in the delivery process. There are well-established authentication and certification procedures for doing so. When everything is complete, the new software load can go into service.

Because software download has such a potential for problems, it must be subject to intense scrutiny and protection. Authorization to operate must be derived from an appropriate Central Authority and be carefully certified. Rogue software in a terminal is a major potential vulnerability.

Software download is often treated as an open-loop process, with emphasis on structuring the path from developer to user to preserve integrity of the code. With advances in SDR and basestation technology, however, there is an opportunity to close the loop. Base stations can monitor the RF spectrum not only to service their assigned operating channels, but to look for inappropriate terminal operation in their proximity. By using the output from a very high-performance analog to digital converter (ADC), the base station can perform digital processing on a wide range of spectrum to test the emissions from other emitters in the vicinity. The base station can perform as a permanently installed test facility to identify units that are not performing correctly or are attacking the system.

3. SECURITY THREAT VECTOR

The Security and Architecture Working Group of the SDR Forum is working on a structure called a Security Threat Vector (STV). The vector has three components:

System Operating Mode
Perpetrator
Security Violation Mode

In the sections that follow, we describe the different cases that constitute each of these elements. There are 60 different combinations to provide a taxonomy of specific threats.

3.1 System Operating Modes

The model identifies five system operating modes:

Voice communication
Data transfer
Software download
Application execution
Money handling

3.2 Perpetrators

This model identifies three different categories of individuals who may violate system security, based on their motive.

3.2.1 Negligent

With no pejorative intent, users can put a system into abnormal operational mode. They can locally overload a system, such as at completion of a sporting event, or by demanding more data bandwidth than is available. They can put a terminal into an abnormal operating mode by keying in an incorrect sequence of commands.

Accidental interference can arise from improper operation of equipment, such as with shielding removed or connected to a high-gain antenna. Attempting to access system services while delinquent in payment is a security issue.

3.2.2 Unauthorized

This category includes individuals who attempt to access the system to intercept information or probe to test its security provisions.

3.2.3 Malicious

There are a number of different kinds of individual who approach the system with malicious intent. A thief is someone who wants to avail themselves of services that are offered for a fee without paying. An interceptor is a person who wants access to information they have no right to. This can be the content of message traffic, analysis of traffic patterns, or simply knowledge that communications are being conducted.

Intentional interferers intend to disrupt or deny other users' communications, committing a denial of service. Impersonators accesses the network with false credentials. This person may communicate with the intent to deceive the message recipient or attempt to gain access to unauthorized services or data. Of special concern is an individual authorized access to some part of the system who misuses their access to commit unauthorized acts, steal content or services, or disrupt system operation.

3.3 Security violation modes

These modes describe the consequences of an attack on the system.

3.3.1 Impersonation

An impersonator attempts to access the system with an illicit terminal by offering false credentials and pretending to be a legitimate authorized user, or posing as a base station to attract legitimate users to attach to the illicit station. A combination, the “Man-in the Middle” attack occurs when, using a false terminal and base station combination, they relay the communication of a legitimate user to log onto the system, enabling them to monitor or change the data stream as it passes through. Any of these mechanism which enables extraction of the content of a transmission by someone other than the legitimate recipient is considered interception.

3.3.2 Unauthorized access

Unauthorized access to control provides the opportunity to make unauthorized changes to system operation. Unauthorized access to data involves data capture by someone not authorized to have it. A severe problem occurs if an individual is able to steal keys or passwords as they can obtain access to a variety of system functions.

3.3.3 Denial of service

Any action involving performing an operation or a series of operations that consume system resources to the extent that performance is reduced. This situation may be very difficult to recognize as it has the same appearance as a normal system overload.

3.3.4 Physical damage

Entering the premises where system equipment is operating and turning it off or damaging it.

4. SECURITY MEASURES

The entire subject of security for wireless systems is a complex one, but experience has shown that neglecting it has severe financial and legal consequences. Early cellular systems followed the wireline model based on physical security of switching equipment with disastrous results. Substantial amounts unpaid service were stolen due to the inherent lack of security on the air interface.

The following are some of the aspects of securing wireless systems.

4.1 Central Authority and authorization dissemination

The core element of any security structure is a central authority, and the flow of authorization is a major aspect of a security architectuere. This agency determines what individuals or organizations have access to various aspects of the system. It delegates portions of its authority to subordinate elements in order to meet the operational needs of the system. The mechanisms for delegation must have the highest level of security in the system avoid an attack that diverts the flow of authority.

4.2 Encryption

Modification of the transmitted material in such a way that the authorized recipient can conveniently extract the original message, while anyone else, although they obtain the cyphertext, cannot extract the cleartext at reasonable cost.

4.3 Certification

A certificate attached to a message provides proof of the sender's identity and that the content has not been modified.

4.4 Non-repudiation

The system maintains an audit trail of activity, and makes it impossible for an individual to deny attribution for specific actions.

4.5 Fault management

Errors in system operation can put the system in a state where security can be compromised, particularly when multiple errors occur in the same locale. System elements with error conditions must be isolated and removed from service.

4.6 Monitoring

Base stations designs, in the past, have been pressed to provide the performance needed for effective operation. With development of very high performance RF front ends, such as that provided by Digital RF circuits, the opportunity for improvement in system architectures to strengthen security is opened. One such means is provision for monitoring the local RF environment. With improved base station performance, a monitoring system routinely monitor ambient RF activity, and establish a baseline of normal operations. It can then detect anomalous transmissions, and report them. Working with other monitors in the vicinity, it can determine signal characteristics, and determine location of the source.

5. WIRELESS SYSTEM SECURITY CONSIDERATIONS

The security architecture for a wireless system must be developed with some general considerations in mind. The first is that the wireless interface itself is inherently vulnerable. Anyone can present a signal to the system, and the receiver cannot determine the validity of any incoming signal until it has been processed. Further, anyone can intercept the normal transmissions of the system in operation, with some probability of interpreting them. There is some probability of occurrence for each specific threat, and a cost associated with measure to defeat it.

The result is a massive set of trade-offs to balance the weighted cost of occurrence against the cost of deterrence on a case by case basis. We have presented a threat taxonomy to assist in dealing with that trade space.

The ultimate requirement is that a user of the wireless system have an authorization derived from a common source with the system infrastructure. A legitimate user should have quick and easy access to system services, while the system accurately collects payment for providing them. An intruder should not only be denied access with minimum impact on system load levels and resources, the system should have provisions for identification of the individual and prosecution of corrective measures.

6. CONCLUSIONS

The Security and Architecture Working Group of the SDR Forum is working on analyzing and describing the structure of wireless system security. can be analyzed and structured. Use of that structure can assist in the complex effort involved in establishing a system security architecture within the overall system architecture.

A model, called the Security Threat Vector is proposed. Be categorizing threats into its components, System Operating Mode, Perpetrator, and Security Violation Mode, the system architect is better positioned to evaluate the threat-probability-cost relationship and incorporate appropriate countermeasures.

As new technologies emerge that can be used to strengthen system security, it is imperative that system architects understand them and how they impact the engineering trade-offs, risks, and costs associated with their designs. Use of SDR technology and high-performance hardware introduces many new capabilities, but also changes the risk structure.

7. REFERENCES

[1] SDR Forum document SDRF-02-W-0010-V1.01 SDR System Security, June 9, 2002