Software Defined Radio Forum

Security & Architecture Working Group

SDR System Security

S&A-SEC

Document No. SDRF-02-P-0006-V1.0.0

(Formerly SDRF-02-A-0006-V0.00)

Index

1 Overview

This document provides a brief introduction to some of the security aspects related to the introduction of Software Defined Radio Technology to wireless personal communication systems (PCS). To do that, we establish a taxonomy of security elements, and examine the more important ones. The element structure enables development of a *Threat Vector*, and facilitates examination of new security considerations. It can be extended or modified to accommodate new insight into communications security.

The subject of security for SDR systems is quite broad and covers many issues. The intent of this document is to introduce these issues briefly. Detailed discussions of these issues are not presented here and will be developed in future versions of this document.

1.1 Definition

We will define security in a broad sense as that system attribute that maintains the privacy and integrity of the system and the information distributed across it. It includes mechanisms to ensure accurate content delivery to intended recipients, denial of interception by intruders, rejection of attempts to gain unauthorized access, mechanisms for configuration management of software download, and record-keeping with non-repudiation of actions taken by all participants.

1.2 History of PCS security

PCS systems originally evolved from the public service telephone network (PSTN) where the Bell System in the US and GPO agencies in much of the rest of the world maintained tight control over physical access to system elements. Although little attempt was made to provide link encryption, the use of switched circuits in the architecture and the large number of potential routes for a call meant that the core network provided adequate security. When needed, end-to-end encryption protected the vulnerable end points of a call.

The security requirements of military systems, because their extreme need for security, have led to a sophisticated set of organizations to define, maintain, and refine security measures. Much of that technology is also applicable to PCS, and can be used to implement commercial security measures, but detailed consideration of military security is beyond the scope of this document.

When the first generation (1G) cellular systems were fielded, the exposure of an unencrypted analog air interface was underestimated. A radio link is inherently insecure, and initial 1G designs did not reflect the great reduction in physical security that came from introduction of a wireless link. The result was lack of privacy for users, with a number of famous incidents where over-the-air conversations were recorded. There was also considerable loss of revenue by service providers through cloned mobile terminals.

Second generation (2G) system architectures were designed to have substantially better security. But as they were deployed, they encountered increasingly sophisticated attacks. Future generations of systems will need increasingly sophisticated security measures to outpace developments in subversion techniques.

PCS services have received wide acceptance as a means to have a voice conversation without the constraint of a wired telephone. Another widely accepted contemporary service is access to the internet, and the use of internet protocol (IP) for transmission of all kinds of information using personal computers (PCs) as terminals. Unfortunately the predominant developers of PC operating systems were much more concerned with feature enhancement than security. The result is that IP based systems are currently much more susceptible to malicious penetration, viruses, and random failure than is desirable. As IP bases services become available over wireless links, their security shortcomings must not be allowed to disrupt system operation.

1.3 A note on probability

The only inherently secure cryptographic system is a truly random "one time pad," effectively a symmetric key of indefinite length used by each end of a communication link. Anything less has some probability of being cracked by application of enough computation. And even the one time pad is subject to traffic analysis.

So the design of communication system security must consider the potential threats, and trade off the cost of meeting threats with the probability of encountering them and the loss if they are successful. It is also necessary to evaluate the cost of a successful penetration. Interception of a cryptographic key, for example has more far-reaching consequences than retrieving transitory data, such as the current selling price of a stock.

From the perspective of a rational perpetrator, the benefit derived from penetrating the system must be balanced against its cost. (Of course, protection from damage by irrational perpetrators must also be considered.) These considerations can be very complex, but are essential to effective system security. SDR technology has a significant benefit in this area, as system security can be upgraded or new security strategies introduced when necessary.

1.4 Threat structure

In this document we review security objectives for commercial systems with a view to understand the need and to build a basis for its cost justification. We then examine different operating modes of the system to understand the exposures that exist in different types of operation. Then we look at the different players in security considerations, and discuss their motivations and means to threatening system operation. There are a number of different activities that present a threat to the system, many of them deriving from the inherent exposure of radio transmissions to interception. 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 user expectations for system security.

Participants in the PCS market expect that a system will:

- Protect operating information
- Protect Content

- Protect Billing and Payment
- Provide regulatory conformance

2.1 Protect operating information

Operating information is information used by the system as differentiated from content. The following are types of operating information.

2.1.1 Radio parameters

Radio parameters are data that can affect 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.

2.1.2 Signaling/control

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.

2.1.3 Keys and passwords

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.

2.1.4 Traffic volumes

Part of the inherent insecurity of an RF link is that perpetrators can intercept the radiated energy without detection. There are occasions when the very presence of traffic on a channel provides information that something is happening, even though the message content cannot be understood. The only effective deterrent to traffic analysis is dummy traffic to hide the real information. Under some system architectures, that may have the unfortunate effect of denying access to real users to whom the channel appears busy.

2.1.5 User identity and location

It is a violation of user privacy if the user's 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.

2.2.1 Privacy

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. We can safely assume that a perpetrator with a supercomputer is not trying to obtain the weather information in Seattle, even though that topic initiates much of the wireless traffic in the northwest. As we have seen, threat analysis is essential to determining the security mechanisms to be invoked.

2.2.2 Funds transfer

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.

2.2.3 Intellectual Property Rights

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 is 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 Protect 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 billing and payment.

2.3.1 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.

2.3.2 Credit card transactions

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. I 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.

There are three ways that credit card information can be supplied with a wireless system. One is to have it part of the users record in the home location record (HLR), and transmitted from their in a separate message to the seller. Alternately, the user can speak the number in a phone call, or key it in to the telephone keypad. As the number goes over the air interface in the latter cases, protecting it becomes a security issue.

2.3.3 Prepaid funds control

Smart cards area form of credit card with an embedded chip. One use of the resulting capability is to store money in the card so it can be used in lieu of cash. There is no reason a wireless mobile terminal cannot provide the same capability, particularly as personal area net (PAN) wireless ability is provided. 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 his handheld device.

Most of the security concerns for these transactions have been developed by the smart card industry, and can be applied to wireless terminals.

2.4 Provide 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.

2.4.1 Initial certification

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.

2.4.2 Delivery/download

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 Authorization Agency (CAA) and be carefully certified. Rogue software in a terminal is a major point of vulnerability.

2.4.3 Verification

Software download can be described as an open-loop process. 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 the analog to digital converter (ADC) capability to test the emissions from other units in the vicinity the base station can perform as an ongoing test facility to identify units that arenot performing correctly or are attacking the system.

2.5 Summary

These dimensions describe the areas in need of protection in order to make the system meet the expectations of participants in the PCS marketplace. They represent areas where threats may be directed, and which must be considered by security architectures.

3 Security Threat Vector

The Security and Architecture Working Group of the SDR Forum is proposing a new construct as a means of addressing the broad field of wireless system security. It is called the SDRF Security Threat Vector (STV). The vector has three components:

STV = f(System Operating Mode, Perpetrator, Security Violations)

In the sections that follow, we describe the different cases that constitute each of these elements. Combining them, there are 48 different combinations to describe specific threats, as indicated in Appendix A.

Consideration of these threats is the means by which susceptibility to security violations can be developed, and examined for weaknesses.

3.1 System Operating Modes

Threats to a system are dependent on what the system does. Transfer of funds, for example, is subject to very different attempted violations than is software download.

3.1.1 Voice communication

Wireless telephone calls.

3.1.2 Data transfer

Transmission of digital data. Money is a specific case.

3.1.3 Software download

Loading a program into the mobile terminal, consisting of physical transfer, validation, and installation.

3.1.4 Application execution

Running a program in the terminal that performs a function or interacts with an application somewhere on the network.

3.2 Perpetrators

A perpetrator is an individual who takes some action that may result in a security violation. The intent of the perpetrator is an important consideration in analyzing threats.

3.2.1 Negligent

Negligent individuals are not intent on penetrating the system or causing damage. Better design on instructional materials, training, and improved user interface design come into play to reduce negligent interference with system operation.

3.2.1.1 Normal User

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.

3.2.1.2 Accidental Interferer

A person who misuses equipment in a way that inadvertently interferes with other users of communication systems.

3.2.2 Unauthorized

The existence of a system attracts certain kinds of people who attempt to access the system beyond their normal access rights. Their intent is usually just to obtain access or intercept traffic, but they may disrupt operations in the process.

3.2.2.1 Interceptor

A person that 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.

3.2.2.2 Prober

An individual who tests the system for weak points, just to see how it works. Probes the system using either standard or specially built equipment trying to find loopholes or access points where they can gain access.

3.2.2.3 Impersonator

A person who attempts to accesses the network using normal procedures, but 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.

3.2.3 Malicious

These individuals intend to steal service or information, or to disrupt system operation.

3.2.3.1 Thief

Someone who wants to avail themselves of services or content that are offered for a fee without paying.

3.2.3.2 Intentional Interferer

A person with intent to disrupt or deny other users' communications. An intentional jammer. This could also involve physical destruction of stations or equipment.

3.2.3.3 Insider

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 violations

These are categories of action taken by a perpetrator.

3.3.1 Impersonation

Pretending to make the system think that access is being attempted by a legitimate user.

3.3.1.1 Impersonating a user

Accessing the system with an illicit terminal by offering false credentials and pretending to be a legitimate authorized user.

3.3.1.2 Impersonating a network

Setting up a false base station and enticing legitimate users to log on.

3.3.1.3 Man-in the middle

Using a false terminal and base station combination, relay the attempts of a legitimate user to log onto the system and monitor or change the data stream as it passes through.

3.3.2 Unauthorized Access

Extracting data from the system or injection data into the system by means other than impersonation. These attacks are attempts to get around the normal barriers to unauthorized access rather than dupe them.

3.3.2.1 Interception

Extraction of the content of a transmission by someone other than the legitimate recipient.

3.3.2.2 Unauthorized access to control

Provides the opportunity to make unauthorized changes to system operation.

3.3.2.3 Unauthorized access to data

Data capture by someone not authorized to have it

3.3.2.4 Unauthorized access to cryptomaterial

Stealing keys or passwords to use them illegitimately.

3.3.3 Denial of Access

3.3.3.1 Denial of service

Performing an operation or a series of operations that consume system resources to the extent that performance is reduced. One example is the use of a large number of "ping", or status request messages to cause a given system element to divert a substantial part of its processing power from normal operations.

3.3.3.2 Subversion

Finding a way to alter system parameters so that one or more users are wrongfully denied access. An example would be resetting flags in the home location register (HLR) to indicate that the user was delinquent in payment.

3.3.4 Physical

A direct attack on system hardware. Entering the premises where system equipment is operating and turning it off or damaging it.

4 Security Measures

There are a number of measures involved in making a wireless system secure against the various threats to system dimensions.. They must be carefully considered in the architecture of the system and its initial design. These are the tools available to the system designer.

4.1 Central Authorization Agency (CAA) and authorization dissemination

The core element of any security structure is a CAA. This agency determines what individuals or organizations have access to various aspects of the system. The CAA delegates portions of its authority to subordinate elements in order to meet the operational needs of the system, including provision for issuance of certificates by one or more certification authorities (CA), also referred to as trusted authority (TA). 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. Certificates are provided by a Certification Agency (CA), which may be operated by the CAA or may be a third party service.

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 system element. The system design should be carefully checked prior to implementation and in final testing for its ability to remain robust under high load conditions and in the presence of multiple errors.

When in operation, system elements with error conditions must be isolated and removed from service.

5 Scenarios

Each of the STVs can be considered with one or more scenarios. These are examples:

STV6 (Voice, Negligent, Unauthorized access)

Normal users will not ordinarily represent a threat to the system. However, mobile terminals generally have an "engineering mode" which makes available much information that the user usually sees. If there are any combinations of button pushes that can disrupt the system, it can be assumed that they will be accidentally activated at some point. Once discovered, it is likely they will published on the internet.

This threat is mitigated by determining that there is no state that can be activated by a normal user which will access control functions in the system and disrupt operations or provide detrimental access.

STV 10 (Voice, Malicious, Unauthorized access)

On early analog cellular systems, an interceptor could pick up enough information during a normal user's call setup to set up a counterfeit terminal. The perpetrator could then make long distance calls that would accrue to the original user. Substantial amounts of system resources were consumed and large amounts of revenue forfeited from this security threat.

6 Conclusions

The fundamental nature of wireless links provides both user terminal mobility and susceptibility to interception. We have described a number of considerations relating to system security, introduced a Security Threat Vector to aid in analysis of system threats, and presented some of the measures available to system designers and operator to deal with the threats. Consideration of system security should also take into account the economics of both the system operator and the would-be attacker.

Use of Software Defined Radio Technology is PCS systems opens a door to certain threats that were not possible in all-hardware systems, and the SDR Forum work in the area of software

download is addressed at this threat. SDR Technology also brings added flexibility to introduce new security features into existing systems to deal with new threats as they appear.

Future work will identify areas among the Dimensions, Threats, and Measures where more detailed consideration will benefit SDRF members. It will also involve model rectification and resolution between the publications of the Regulatory and Download Working Groups, who have developed documents with security implications. Although there is very few fundamental differences, the three working groups need to work together to arrive at a common position as the SDR Forum moves forward.

Appendix A
Threat Vector Table

Threat No.	Operating Mode	Perpetrator	Security Violations
1	Voice	Negligent	Impersonation
2	Voice	Negligent	Unauthorized Access
3	Voice	Negligent	Denial of Service
4	Voice	Negligent	Physical
5	Voice	Unauthorized	Impersonation
6	Voice	Unauthorized	Unauthorized Access
7	Voice	Unauthorized	Denial of Service
8	Voice	Unauthorized	Physical
9	Voice	Malicious	Impersonation
10	Voice	Malicious	Unauthorized Access
11	Voice	Malicious	Denial of Service
12	Voice	Malicious	Physical
13	Data	Negligent	Impersonation
14	Data	Negligent	Unauthorized Access
15	Data	Negligent	Denial of Service
16	Data	Negligent	Physical
17	Data	Unauthorized	Impersonation
18	Data	Unauthorized	Unauthorized Access
19	Data	Unauthorized	Denial of Service
20	Data	Unauthorized	Physical
21	Data	Malicious	Impersonation
22	Data	Malicious	Unauthorized Access
23	Data	Malicious	Denial of Service
24	Data	Malicious	Physical
25	SW Download	Negligent	Impersonation
26	SW Download	Negligent	Unauthorized Access
27	SW Download	Negligent	Denial of Service
28	SW Download	Negligent	Physical
29	SW Download	Unauthorized	Impersonation
30	SW Download	Unauthorized	Unauthorized Access
31	SW Download	Unauthorized	Denial of Service
32	SW Download	Unauthorized	Physical
33	SW Download	Malicious	Impersonation
34	SW Download	Malicious	Unauthorized Access
35	SW Download	Malicious	Denial of Service
36	SW Download	Malicious	Physical
37	Application Execution	Negligent	Impersonation
38	Application Execution	Negligent	Unauthorized Access
39	Application Execution	Negligent	Denial of Service
40	Application Execution	Negligent	Physical
41	Application Execution	Unauthorized	Impersonation
42	Application Execution	Unauthorized	Unauthorized Access
43	Application Execution	Unauthorized	Denial of Service
44	Application Execution	Unauthorized	Physical
45	Application Execution	Malicious	Impersonation
46	Application Execution	Malicious	Unauthorized Access
47	Application Execution	Malicious	Denial of Service
48	Application Execution	Malicious	Physical