Providing the proper privacy and authentication for the PCS phone

Privacy and Authentication Needs of PCS

JOSEPH E. WILKES

Although radio has existed for almost 100 years, most of the population uses wired phones. Only over the last 10 years have large numbers of people been exposed to the use of wireless or cordless phones. With this exposure, peoples' concepts of privacy as well as their confidence in the telecommunication industry to bill a call to the correct person have been challenged.

The current concepts of privacy of communications and correctness of billing are based on the telephone companies' ability to route an individual pair of wires to each residence and office in the country. Thus, when a call is placed on a pair of wires, the telephone company can correctly associate the call on a wire with the correct billing account. Similarly, since there is pair of wires from my home to the telephone company central office, no one can listen to my call.

Although anyone in the telephone industry could easily refute these claims with examples of wiretaps, for most people, a wiretap is an abstract concept that only someone who is involved in illegal activities has to worry about.

When communications are moved to a shared media,[1] more than one person can transmit and listen on the media. When the media is shared, anyone with access to the media can listen to or transmit on the media. Thus, communications are no longer private. In shared media, the presence of a communication request does not uniquely identify the originator, as it does in a single pair of wires per subscriber. In addition, any information that an originator sends to the network can be overheard by all users of the network and could later be sent by someone else attempting to place a fraudulent call. The participants of phone calls shown in Fig. 1 may not know that their privacy is compromised.

When the media is shared, privacy and authentication are lost unless some method is established to regain it. Cryptography provides the means to regain control over privacy and authentication.

There have been attempts to control privacy and authentication though non-cryptographic means. These have failed thus far. When the original cellular service was conceived, the authentication of the telephone placing the call was implemented through a Number Assignment Module (NAM) and an Electronic Serial Number (ESN). The NAM would be implemented in a Programmable Read Only Memory (PROM) for easy replacement when the phone number changed and the ESN would be implemented in a "Tamper resistant module" that could not be changed without damaging the cellular telephone. In practice, many manufacturers implement the NAM and the ESN in battery backed RAM (or EEPROM) with external programming from either the keypad on the phone or a set of programming leads associated with the battery/feature connector on the phone.

Similarly, privacy of cellular communications was assumed to occur because 900 MHz scanners would be too difficult and too expensive to build. When those scanners became easily available, the Electronic Communications Privacy Act was passed in 1986 and in 1992, the FCC banned the importation and manufacturing of scanners covering cellular phone bands. In practice, the laws will not help since the are millions of scanners in existence today. Furthermore, cellular test equipment is easy to build or buy and most cellular phones can be placed in a maintenance mode that allows them to monitor any channel. Any cellular phone can be easily converted to a cellular scanner.

Today, as PCS is being designed, many people think that the TDMA and CDMA modulation schemes are too difficult to decode, and thus are inherently secure. Unfortunately, history shows us that what is difficult today is easy tomorrow. As manufacturers race to build low-cost phones, the parts to build low-cost scanners will become available. Even if PCS scanners are banned, PCS telephones will need maintenance modes that can be used to monitor calls.

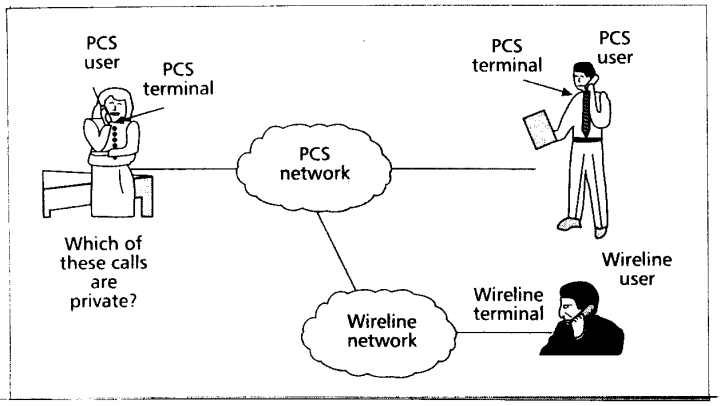
To provide the proper privacy and authentication for a PCS phone (also known as a Portable Terminal), some cryptographic system will be necessary. This article defines requirements that a cryptographic system used for PCS would need to meet. It does not attempt to define the cryptographic system. It does provide a template for examining cryptographic systems to choose between cryptographic alternatives.

Some of the cryptographic requirements are in the air interface between the Personal Terminal and the radio port. Other requirements are on data bases stored in the network and on information shared between systems in the process of handovers or giving service for roaming units.

The paper first discussions four levels of privacy (including defining two new levels). Then, requirements are identified

[1] *Examples of shared media are: party line telephone service, radio communications, cable TV, local area networks, wide area networks, and the Internet. Only radio communications are discussed here, but the concepts apply equally well to the other media.*

1070-9916/95/$04.00



■ **Figure 1.** *PCS privacy.*

and discussed in the areas of privacy, theft resistance, radio system performance,system lifetime, physical requirements as implemented in portable/mobile Personal Terminals, and Law Enforcement needs.

Privacy Definitions

When most people think of privacy, they think of either of two levels: 1) none, or 2) privacy good enough for military users.

However, as I describe here, there are really four levels of privacy that need to be considered.

Level 0: None – With no privacy enabled, anyone with a digital scanner could monitor a call.[2, 3]

Since not all participants in a call to a Personal Terminal with no privacy would be aware that their conversation could be monitored, a lack of privacy indicator should be required any call that lacks privacy.[4]

This lack of privacy indicator would be needed when a wireline user is communicating with a PCS user that lacks privacy. It would also be needed when a PCS user with privacy communicates with a PCS user that doesn't have privacy.

The designers of the PCS system must, as a matter of public trust, provide in all systems either a level 0 system with a mandatory lack of privacy indicator or a level 1 secure system.

Level 1: Equivalent to Wireline – As discussed in the introduction, most people think wireline communications are secure. Anyone in the industry knows that they aren't, but the actions to tap a line often show the existence of the tap. With wireless communications, the tap can occur without the knowledge of anyone. Therefore, the actions to tap a wireline call must be translated into a different requirement for a wireless system.

The types of conversations that would be protected with this level of security are the routine everyday conversations of most people. These types of communications would be discussion of a personal nature that most people would not want exposed to the general public. For example, details of a recent operation or other medical procedure, family financial matters, mail orders using a credit card, family discussions, requests for emergency services (911), and discussion of vacations plans (thus showing when a home is vacant).

The cryptographic system must be designed so that information about one conversation does not compromise any other conversations from the same or different participants. Thus, a cryptographic system designed that individual conversations might take a year or more to break with current technology would provide a secure enough system for most people. Once a particular conversation was broken, the same effort would be needed to break other conversations.

Level 2: Commercially Secure – This level would be useful for conversations where proprietary information is discussed. For examples, stock transactions, lawyer-client discussions, mergers and acquisitions, contact negotiations, etc.

A cryptographic system that allows industrial activities to be secure for 10 to 25 years would be good enough. Once a particular conversation was broken, the same effort would be needed to break other conversations.

Level 3: Military/Government Secure – This is the level that most people think of when cryptography is discussed. This would be used for the military activities of a country and the non-military government communications. The requirements for this level would be defined by the appropriate government agencies.

Privacy Requirements

Users of wireline telephones have come to expect some level of privacy in their communications. Although telephone taps are easy to do, they are most times easy to discover. As we move to a nation of wireless telephone users, we may giving up our right to privacy in communications unless, the PCS system design is done in a way to maintain privacy. This section discusses the various privacy needs of a wireless telephone user.

Figure 2 is a high level diagram of a PCS system showing areas where privacy could be compromised and therefore attention must be made to each of these areas to ensure privacy. A user of a PCS needs privacy in the following areas:

Privacy of Call Setup Information — During call setup, the portable terminal will communicate information to the network. Some of the information that could be sent is: calling number, calling card number, type of service requested, etc. All this information must be sent in a secure way.

Privacy of Speech — All spoken communications must be encoded so that they are not capable of being intercepted by some listening on the air waves. See "Privacy Definitions" for details.

Privacy of Data — All user data communications must be encoded so that they are not capable of being intercepted by someone listening on the air waves. See "Privacy Definitions" for details.

Privacy of User Location — When the PCS portable terminal communicates with the land network, via a radio port, the communication must be encoded so that the location of the portable terminal is not disclosed. The usual method to meet this need is to encrypt the user id.

Additionally, the user location data base in home and roaming systems must not be subject to attack from either unauthorized insiders or from external sources.

[2] Although these scanners do not exist today, they would be built as PCS services become available. Cellular scanners did not exist in the '70s but were built when the use of the 800 MHz band increased. Even if the FCC bans the manufacturing and importing of the scanners, as they have for cellular capable scanners, there are enough electronics magazines (Radio Electronics, Popular Electronics, Nuts and Volts, etc.) published each month, that plans for the digital scanner would soon appear.

[3] Also Personal Terminals placed in the maintenance mode could be used to monitor calls. Manufacturer's need maintenance modes to test Personal Terminals as they are manufactured or repaired. The literature to determine the maintenance modes is difficult, if not impossible, to keep out of the hands of people without the need to know yet at the same time be readily available for legitimate purposes.

[4] The lack of privacy indicator could be as simple as a beep tone every 15 seconds to remind the participants of the call that the call could be monitored. This is similar to the tone used on recorded conversations.

Privacy of User ID — When a user interacts with the network, the user id is sent in a way that does not show the user id. This prevents analysis of user calling patterns based on user id.

Privacy of Calling Patterns — No information must be sent from a Personal Terminal that enables a listener of the radio interface to do traffic analysis on the PCS user. Typical traffic analysis information is: calling number; frequency of use of the personal terminals; and caller identity.

Financial Transactions — If the user transmits credit card information over any channel, it must be protected. Users may order items from mail order houses via a telephone that is wireless. Users may chose to speak their credit card numbers rather than punching them in via a key pad.

Users may access bank voice response systems, where account data is sent via DTMF. Users may access calling card services of carriers and may speak or use DTMF to send the card number.

All these communications need to be private.

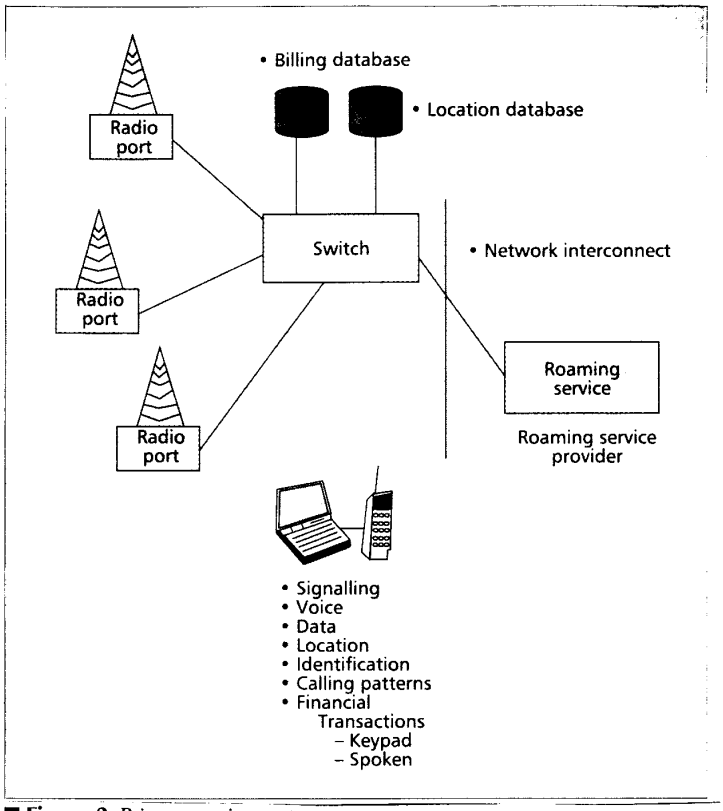
Theft Resistance Requirements

The system operator may or may not care if a call is placed from a stolen personal terminal as long as the call is billed to the correct account. The owner of a personal terminal will care if the terminal is stolen.

The cryptographic design should reduce theft of the Personal Terminal by making reuse of a stolen Personal Terminal difficult. Even if the Personal Terminal is registered to a new legitimate account, the use of the stolen terminal should be stopped. The cryptographic design should also reduce theft of services by making reuse of a stolen Personal Terminal unique information difficult. Requirements needed to accomplish the reduction in theft are as follows.

Clone Resistant Design – In the current wireless systems, cloning of Personal Terminals is a serious problem; methods must be put in place to reduce or eliminate fraud from cloning. To accomplish the fraud reduction, Personal Terminal unique information must not be compromised by any of the following means:

- Over the Air: someone listening to the radio channel should not be able to determine information about the Personal Terminal that can then be programmed into a different Personal Terminal.
- From the Network: the data bases in the network must be secure. No unauthorized people should be able to obtain information from those data bases.
- From Network Interconnect: systems will need to communicate with each other to verify the identity of roaming Personal Terminals. A fraudulent system operator could perpetrate fraud by using the security information about roaming Personal Terminals to make cloned Personal Terminals. The communications scheme used between systems to validate roaming Personal Terminals should be designed so that theft of information by a fraudulent system does not compromise the security of the Personal Terminal. Thus, any information, passed between systems for security checking of roaming Personal Terminals, must have enough information to authenticate the roaming Personal Terminal, and at the same time, it must have insufficient information to clone the roaming Personal Terminal.
- From Users cloning their own Personal Terminal: users can perpetrate fraud on the system. Multiple users could use one account by cloning Personal Terminals. The requirements for reducing/eliminating this fraud are the same as those to reduce repair and installation fraud described below.



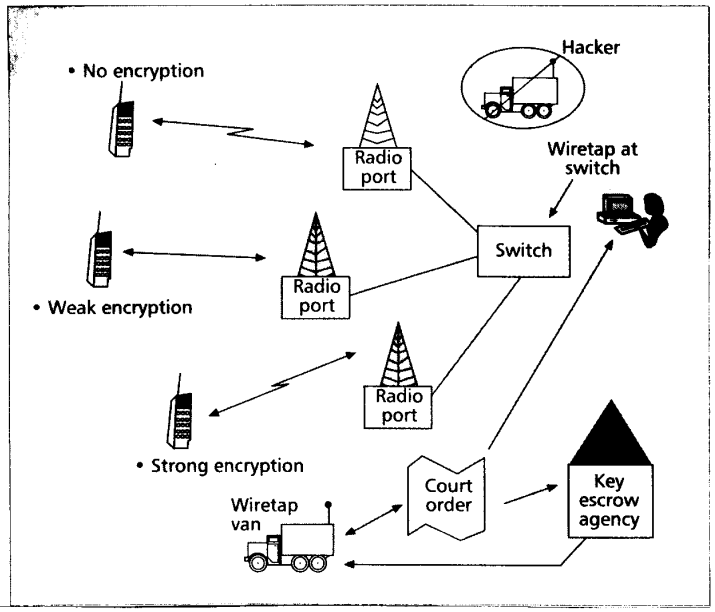
■ **Figure 2.** *Privacy requirements.*

Installation Fraud — Theft of service can occur at the time of installation of the service. Multiple Personal Terminals can be programmed with the same information (cloning). The cryptographic system must be designed so that installation cloning is reduced or eliminated.

Repair Fraud — Theft of service can occur at the time of repair of a Personal Terminal. Multiple Personal Terminals can be programmed with the same information (cloning). The cryptographic system must be designed so that repair cloning is reduced or eliminated.

Unique User ID — Handsets may be used by more than one person. It is necessary to identify the correct person for billing and other accounting information. Therefore, the user of the system must be uniquely identified to the system. (Note: this may require a separate security module that plugs into the Personal Terminal.)

Unique Personal Terminal ID — When all security information is contained in a separate module (smart card or PCMCIA card) the identi-



■ **Figure 3.** *Law enforcement requirements.*

ty of the user is separate from the identity of the Personal Terminal. Stolen Personal Terminals can then be valuable for obtaining service without purchasing a new (full-price) Personal Terminal. Therefore, the Personal Terminal should have unique information contained within it that reduces or eliminates the potential for stolen Personal Terminals to be re-registered with a new user.

Radio System Requirements

When a cryptographic system is designed, it must function in a hostile radio environment characterized by bit errors caused by:

Multipath Fading — The radio signals will take multiple diverse routes from the Personal Terminal to the base station site. The effect of the multiple diverse routes is to cause fading that can be severe and cause burst errors.

Thermal Noise — Although the system may be interference limited, there may be conditions when the limiting factor on performance is thermal noise.

Interference — The PCS systems may initially share radio spectrum with other users. The modulation scheme and the cryptographic system must be designed so that interference with shared users of the spectrum does not compromise the security of the system.

Jamming — Although usually thought about only in the context of military communications, civilian systems can also be jammed. As wireless communications becomes ubiquitous, jamming of the service may be a useful means of social protest. It can also be a method to break the security of the system. Therefore, the cryptographic system must work in the face of jamming.

Support for Handovers — When the call handover occurs to another radio port, in the same or adjacent PCS system, the cryptographic system must maintain synchronization.

[5] *The original cellular security model was developed in 1974 by AT&T. It is just now in the process of being upgraded and cellular phones using it will exist for several more years.*

System Lifetime Requirements

It has been estimated that computing power doubles every three years. An algorithm that is secure today may be breakable in five to ten years.[5] Since any system being designed today must work for many years after design, a reasonable requirement is that the algorithm must last at least 20 years. As part of meeting this requirement, the algorithm must have provisions for being upgraded in the field.

Physical Requirements

Any cryptographic system used in a Personal Terminal must work in the practical environment of a mass produced consumer product. Therefore, the cryptographic system must meet the following requirements:

Mass Production — It can be produced in mass quantities (millions per year).

Exported and/or Imported — The algorithm must be capable of being exported and imported. Two problems are solved with export and import restrictions lifted:

- It can be manufactured anywhere in the world.
- It can be carried on trips outside the United States.

As an alternative, if an import/export license for the algorithm can not be obtained, the following restrictions must be done.

- Either only U.S. Manufacturing or Two-Stage Manufacturing: All Personal Terminals must be made in the United States or, All Personal Terminals made outside the United States will have final assembly in the United States.
- All Personal Terminals must be impounded on leaving the United States.

Basic Handset Requirements — Any cryptographic system must have minimal impact on the following Personal Terminal requirements: size; weight; power drain; heat dissipation; microprocessor speed; reliability; cost.

Low-cost Level 1 Implementation — The level 1 Implementation would be the expected baseline for most PCS systems. Therefore, the level 1 implementation must especially be low-cost. Low-cost solutions are obtained by either implementations that be done in software or by low-cost hardware implementations. Software solutions are especially attractive, since often there is spare ROM, RAM, and CPU cycles in the microprocessors used in Personal Terminals.

Law Enforcement Requirements

When a valid court order is obtained, current analog telephones (either wired or wireless) are relatively easy to tap by the law enforcement community. The same requirements described in this article to ensure privacy and authentication of wireless PCS communications make it more difficult to execute legitimate court wire-tap orders.

The law enforcement community has needs to wiretap Personal Terminals after properly obtaining court orders. When an order is obtained,

there are several ways a PCS system operator can meet the needs of the order. Any method used must not compromise the security of the system.

Figure 3 shows possible approaches to tapping the call. The tap can be done over the air or can be done at the central switch.

Over the Air Tap

When the tap is done over the air, a wiretap van will be needed. Since PCS is a cellular type of system, the van must be driven to inside the cell where the call is placed. A centrally located base station would receive interference from portable terminals in many cells or would not be able to receive at all a low-power portable terminal.

In a large-cell PCS system, wiretap stations could be deployed in each cell, but in a small cell system, the number of tap points would be too high. Therefore, a wiretap van would be needed and would have to be driven to the correct cell where the call is placed.

After the van is driven to the correct cell, the van needs to be close to the portable terminal. A van might have an antenna at a maximum of 6-10 feet high vs. a base station antenna height of 25 to 100 feet or more. Thus, the van must be closer to the portable terminal than a cell radius. A quick rule of thumb for the wiretap van is that if the portable terminal is visually observable, then the wiretap van can receive the portable terminals transmission.

If a wiretap van is used, then the transmissions of the portable terminal must be decrypted. The following options are possible:

No Encryption — This approach makes tapping the easiest; if no encryption is used, anyone can listen in to a call over the airwaves. Thus, law enforcement personnel can listen to and record a call. Unfortunately, so can anyone else.

Breakable Algorithms — If the algorithm is weak enough, law enforcement agencies can break the algorithm when permitted to do so by an appropriate court order. Unfortunately, given the proliferation of desktop Personal Computers, any algorithm that can easily be broken by the law enforcement community will also be quickly broken by anyone else.

Strong Encryption — With strong encryption, then it is difficult if not impossible for the wiretap van to decrypt the transmission. One method to resolve this dilemma is to use a key escrow system where all cryptographic keys would be available from an appropriate key escrow agency. With a court order, the information could be obtained by law enforcement agencies so that they could listen to and record a call.

Unfortunately, given the proliferation of desktop personal computers, any algorithm that can easily be broken by the law enforcement community will also be quickly broken by anyone else.

Procedures must be in place and a set of trusted key escrow agencies chosen so that the key could not be obtained through fraud.

Wiretap at Switch

Since all PCS calls must be routed through a central switch, the calls could be decrypted at the central switch under a court order.

This is the preferred method for low power wireless calls. This method leaves it to the user and the system provider to have appropriate levels of security in the wireless portion of the call.

Summary

This article sets standards that any cryptographic system must meet to be suitable for use in a ubiquitous wireless network. Before any cryptographic system is chosen for use in PCS, the ability to meet or not meet these requirements must be examined, discussed, and understood.

Biography

JOSEPH E. WILKES studied Communications Theory at the Polytechnic Institute of Brooklyn (now Polytechnic University) where he received the degrees of MSEE and Ph.D.EE. He joined AT&T Bell Laboratories in 1972. From 1974 to 1981, he was part of the team the designed the world's first cellular system. He represented AT&T at the first cellular standards meetings and he is the principal author of the original EIA compatibility specification for cellular telephones. Besides cellular telephony, he has worked on personal computers, OSI protocols, information services and video services. Since 1992, he has been active in a variety of wireless projects at AT&T and has represented AT&T at standards committees: T1P1, TR-46, and the Joint Technical Committee on Air Interfaces (of T1P1 and TR-46). He is a distinguished member of technical Staff at AT&T Bell Laboratories, Holmdel, New Jersey, and is a licensed Professional Engineer in the state of New Jersey.