Security in Cellular Networks

Security has become the most serious problem facing North American cellular system operators and a major problem for cellular subscribers. Service providers need security against fraudulent use of their systems, while users of cellular phones need security against eavesdropping and false charges on their bills. This issue of Cellular Networking Perspectives will discuss the history of security in cellular networks, and explain how new technology such as digital cellular can help overcome the security challenges of today.

Security of cellular networks requires three concepts: Authorization, Authentication and Privacy. These concepts can be illustrated by imagining a withdrawal from a bank account. The bank will authorize a transaction by checking that the account exists and has adequate funds. The bank may also authenticate the customer by asking to see identification. Lastly, the bank will provide privacy by not releasing information about the transaction. Cellular systems must provide the same types of security, but in very different ways.

Authorization ...
Is Who I Say I Am Okay?

When a cellular phone is used to originate a call on a cellular system, the identity it presents is used to determine the services it is authorized for.

For cellular callers in their home system authorization is simplest. The subscriber database is searched for a record with the same phone number (MIN) and Electronic Serial Number (ESN) as the calling mobile. If no matching record is found, the mobile will be denied service. Further authorization proceeds based on the type of call. Some subscribers, for example, may not be allowed to make international calls, or may not be allowed to use certain features, such as call forwarding.

For roaming cell-phones, authorization was initially impossible because of lack of access to the roamer’s subscriber record. A network is required to connect all cellular systems and allow remote authorization of roamers. The amount of work to develop a real-time network to exchange subscriber authorization information is tremendous, and requires many legal, political and regulatory hurdles to be overcome. Early on in the development of the cellular industry, GTE TSI and EDS PCD (originally Appex Lunayach) realized that a network with custom interfaces to each cellular switch would temporarily fill the need, even with acknowledged deficiencies. The greatest deficiency of their networks was that they could not provide real-time access to subscriber records and had to rely to a great extent on validating from an internal list of bad ESNs. Although, in all fairness it must be said that the service these companies provided was a lot better than the alternative... nothing!

Fraud soon grew more sophisticated than the ad-hoc methods employed to prevent it. First, tumbling-ESN phones appeared, phones that continually generate different ESNs. By the time one ESN was found to be invalid, the call would be over and the mobile would be using yet another ESN. This type of fraud can only be tackled by industry-wide implementation of a real-time protocol and network to provide access to the subscriber database for each roamer. This standard is the TIA IS-41 cellular inter-system operations standard.

While IS-41, once fully deployed, can eliminate all fraud caused by presentation of an invalid MIN/ESN combination, it cannot provide adequate protection against cloning, the latest and most sophisticated type of fraud. Cloning involves the fraudulent use of a valid MIN/ESN combination. In its ultimate form, clone phones can read valid MIN/ESN combinations from other phones and use a different, but valid, combination in every call. Authorization is no longer enough, Authentication is now required.

Authentication ...
Am I Who I Say I Am?

Authentication determines whether a cellular phone is fraudulently assuming the identity of a legitimate phone. A solution to the challenge of detecting and preventing clones was designed during the development of the TIA digital cellular standard; IS-54, Revision B. The authentication part of this standard was produced by TIA subcommittee TR45.3 in its Ad-Hoc Authentication Group (AH AG).

TR45.3 AH AG chose to provide authentication through encryption, with the process occurring on the cellular control channel before a traffic channel is allocated. The encryption method is considered so sophisticated by the US government that its export is controlled by the State Department’s International Traffic in Arms Regulations. It cannot even be discussed in public. It was not published as part of the digital cellular air interface standard (IS-54, Rev. B), but as an appendix, with closely controlled distribution.

Encryption seems like an easy way to authenticate a mobile, but the architecture chosen by TR45.3 actually makes secure authentication quite difficult. Authentication using encryption in its simplest form involves an authenticating system (the Base Station in the case of cellular) transmitting a random number to a
suspect system (the mobile). Both systems execute an encryption algorithm using the random number and a secret key known to both systems, but hopefully not to anyone else. The output of the encryption algorithm is transmitted by the mobile to the base station. If the two outputs are the same, the mobile is accepted as authentic; otherwise it will be rejected as a clone.

The difficulty in the authentication method chosen by TR45.3 is that the control channel is used for transmission of the authentication random number. This channel is a shared resource, monitored by idle mobiles to determine system parameters and to obtain a traffic channel. Because it is shared, the random number transmitted by the system has to be the same for every mobile in a given cell. Therefore an easy way to appear as an imposter would be to just transmit the same response to the random number as a victim mobile. AHAG alleviated this problem by mixing 6 dialed digits with the secret key and random number into the encryption process. So it is only possible to emulate another mobile if the criminal happens to find a victim dialing a number with the same 6 digit suffix as the number that they want to.

---

**Voice Privacy ... Just Between You and Me**

Cellular phone calls are rapidly getting a reputation for being easily overheard by anyone with an FM scanner. The ease of eavesdropping on cellular phone calls can be overrated; the mobility of phones makes it difficult to locate and keep within range of a specific mobile. However, it is certainly possible to scan for interesting conversations. Digital cellular, by its nature, and especially by the inclusion of voice encryption methods, makes it difficult to locate and keep within range of a specific mobile. However, it is certainly possible to scan for interesting conversations. Digital cellular, by its nature, and especially by the inclusion of voice encryption methods, makes it difficult to locate and keep within range of a specific mobile.

All that can be said for sure is that digital cellular with encryption will provide much more protection against eavesdropping than analog cellular. While the security will not be absolute, it will certainly deter all but the most determined from eavesdropping.

---

**The Network Perspective**

A universal cellular network running the IS-41 inter-system protocol and voice privacy features from TR45.3 voice encryption methodology. This has led to criticism of the TIA. IS-41 is no longer an option; access to the subscriber database is required by the visitor cellular system, and the IS-41 network is required to transfer that information. This near-future network will be built almost exclusively upon SS7 to provide the needed performance.

---

**The Standards Perspective**

Authentication and Voice Privacy were developed by the TIA sub-committee TR45.3 in its AHAG group. The AHAG group has recently been moved up to the TR45.1 level, to better allow authentication and voice privacy concerns of the TR45.1 and TR45.5 committees to be addressed.

The encryption algorithm is in a controlled-access appendix. Inter-System authentication and voice privacy procedures were developed by the TR45.2 sub-committee in TSB-51 (soon to be published), which applies to IS-41 Revision B. TR45.1 is taking the AHAG encryption method and applying it to analog cellular in TIA-553, Revision A. TR45.5 is considering the inclusion of the AHAG authentication and voice privacy methods in the wideband cellular standard being developed.

---

**Glossary**

**AC** = Authentication Center. The location of the secret encryption keys for authentication and voice privacy.

**AHAG** = TIA Ad-Hoc Authentication Group.

**Authorization** the process of determining the services available to a subscriber.

**Identification** the process of verifying the identity of a subscriber [see IS-54].

**Control Channel** = A cellular frequency band set aside for broadcasting cellsite parameters and to allow access to cellular traffic channels.

**ESN** = Electronic Serial Number; the unique identifying number of a cellular phone.

**HLR** = Home Location Register. The location of all subscriber information, except for that at the AC.

**IS-3** = The identification of TIA-553 when it was an interim standard.

**IS-41** = The TIA standard defining protocols between M Scs.

**IS-54** = The digital cellular air interface standard. Revision B includes subscriber authentication and voice privacy. The details of the encryption algorithm are contained in a separate appendix, subject to ITAR regulations.

**ITAR** = International Traffic in Arms Regulations. The US State Department rules that control the export of technology considered to have military value.

**MIN** = Mobile Identification Number; the 10 digit phone number of a cellular subscriber.

**MSC** = Mobile Switching Center; a cellular switch. Also known as MTSO.

**NSA** = US National Security Agency.

**TIA-553** = The analog cellular air interface standard. Revision A includes subscriber authentication.

**TSB-51** = Inter-system procedures to support authentication and voice privacy.

**Traffic Channel** = Cellular channel that carries one cellular mobile conversation.

**Voice Privacy** = the process of encrypting digitized voice (see IS-54).