Attacks on Cellular Systems

Hai-Ping Ko
GTE Laboratories Incorporated
Waltham, MA 02254

The cellular industry is growing quickly but so is the fraud. For instance, based on the surveys conducted by the Cellular Telecommunications Industry Association (CTIA), the number of U.S. cellular subscribers, cell sites, and total revenue have grown 112, 27, and 36 times, respectively, over the past ten years. At least 38.2 million, 14.5% of the entire U.S. population, have subscribed to the wireless service and another subscriber is added approximately every 2.8 seconds. There are more than 300 cellular carriers in the States now, but only a small group of entrepreneurs ten years ago. Cellular fraud cost the cellular industry $365 millions in 1994 and at least $500 millions in 1995, consistently 2.56% and 2.62% over the total revenues, in respective years. [1,2,3]

GTE has a special responsibility to understand and to make recommendations on the security problems and solutions of the cellular systems. In 1993, GTE Laboratories was selected by CTIA as the industry's technical analysis laboratory for fraud detection, control, and prevention. Most cellular attack methods were understood. In 1994, the GTE Laboratories succeeded a tiger team attack to a cellular switch station. The switch station was severely compromised without detecting the attacks. The GTE Laboratories consequently was invited by CTIA to conduct a vulnerability study of the cellular industry in general and proposed security policy recommendations and standards to the cellular industry. [1,4,5,6]

I will briefly describe some known attacks on the cellular phone systems, based on years of work of C. Carroll and R.A. McKosky at the GTE Laboratories. I will also briefly describe my sense of computer security and intrusion detection at one of the largest telecommunication companies, GTE.

The attacks on the cellular systems can take place through air (wireless) or through wirelines. To understand this, it is important to know that every connection from a cellular phone to a regular telephone involves the following types of communication: (1) air communication between the cellular phone to a nearest cell base station, (2) wirelined communication between the cell base station and a cellular switch station, and (3) wirelined communication between the cellular switch and the destination through the conventional Public Switched Telephone Network (PSTN). The cellular switch stations are the brains of the cellular systems. With networked computers, they control and direct all the requested connections. These switch stations are connected with the cell base stations and the Public Switched Telephone Network under various protocols and agreements and make sure together that the requested cellular connection can be serviced without interruption when cellular phones move from one location to another. [1,7,8]

The most severe attack to the cellular systems through the air is phone cloning. Unlike a regular telephone which can be recognized by a uniquely distinguishable wire, a cellular

phone is only recognized by a pair of uniquely assigned numbers: ESN (Electronic Serial Number) and MIN (Mobile Identification Number). Such pairs of numbers are transmitted to a cell base station through the open air whenever the cellular phone is powered on. These numbers can be easily read by equipments at a price from $700 to $2000. With an equipment of $7000, one can even possibly find the physical location of any powered-on cellular phone. It is illegal to clone cellular phones with such ESN/MINs, but the cloning methods are freely available from the Internet and phone cloning has become a cottage industry. Some cellular phones are equipped with PINs (Personal Identification Numbers). In such cases, when placing a call, the PIN will need to be sent through the assigned voice channel after ESN and MIN are sent through a control channel. Such cellular phones are less likely to be cloned. However PINs are vulnerable to eavesdropping as well. In fact, there are equipments which can be used to trace the transmitted ESN/MIN/PINs in real-time. [1,3]

Another possible attack through the air is hijacking. Once a voice channel is established between a cellular phone and a cellular base station, a counterfeit cellular phone may seize the voice channel by increasing its power level above that of the legitimate cellular phone. A criminal could then make an illegal cellular call. [1]

The cellular switch stations need the tightest security against any electronic or physical attacks on the cellular systems. These switch stations not only control the cellular connections but also maintain all the registered ESN/MINs and the billing information. The cellular switch computers are vulnerable to all types of network attacks. They are accessible from the Public Switched Telephone Network, which was in turn accessible via the Internet. They are physically connected to modems, various computers, LANs, and WANs, directly or indirectly. Any loose security on the modems, computers, or links will make one or more cellular switch stations vulnerable.

In 1994, one of the cellular switch stations accepted the challenge of a tiger team attack. Only ordinary hacking techniques were used, such as looking for an open port access and cracking weak passwords. The tiger team easily gained the root privilege remotely, altered the password file, obtained the highly confidential information about ESN/MINs and customer billing. The tiger team intentionally left obvious footprints in the hope of being caught, but was not detected. The tiger team also used social engineering gaining physical access to the offices and the computer room, beating the SecureID mechanism, and placing a Trojan horse program on an office PC.

Switch stations of other cellular carriers are not too much different from the switch station under the tiger team attack. It was confirmed in 1995 that several other cellular switch stations of different cellular carriers were equally vulnerable. Even though the switch station under the controlled attack has tightened its computer and physical security since 1994, the overall cellular connections remain vulnerable.

The wirelined attacks are as real as phone cloning. As published in the New York Times of 9/12/95, among the arrested attackers, two actually broke into the computer systems of cellular phone companies.

There have been actions taken to combat the attacks on the cellular systems. For instance, for the phone cloning and hijacking problems, the following methods are being used or considered: voice verification, radio frequency fingerprint verification, dynamic PINs, call pattern analysis, authentication and voice encryption. Securing the cellular networks involves considerations of security ownership, security policy, personnel training, enhanced auditing, and again authentication and encryption on remote connections. More than 30 security issues were identified for the wireless systems and networks by the GTE Laboratories in 1996. Security guidelines were developed by the GTE Laboratories for the cellular industry shortly afterwards. I will not get into any further details here.

Since my employment with GTE beginning early 1995, I observed that GTE is sensitive to computer security problems. Secure architectures were carefully designed and reviewed for every development of company product. Audit records at application level were generated. Some part of GTE are sensitive to external penetrations only and other parts of GTE carefully keep a record of all attacks and observed 80% of them originated internally. In any case, the actual adoption of automated audit analysis and intrusion detection is relatively new and experimental. Well-tested intrusion detection tools have captured unexpected attacks after they are properly installed. GTE understood the existence of potentially fierce attacks and appreciated the value of automated intrusion detection. The cellular fraud problem is well understood and put in good hands at GTE.

References

[1] Cellular Fraud Training Manual for the United States Secret Service, prepared by Cellular Telecommunications Industry Association Technical Analysis Laboratory at GTE Laboratories Incorporated, April 11, 1995

[2] CTIA's Semi-Annual Data Survey, INFOFAX from CTIA (Cellular Telecommunications Industry Association), June, 1996

[3] Fraud and Countermeasures, Part II: Clones, Private Line #10, copyright by 1995 Cellular Networking perspectives, 1996

[4] McKosky, R.A., Security Guidelines, Prepared for CTIA, 1996

[5] McKosky, R.A., Vulnerability Assessment of the Wireless Industry, 1996 Security Seminar, CTIA Network Vulnerability Solutions Committee, June, 1995

[6] Summary of Security Recommendations for Wireless Systems and Networks, Prepared for CTIA by GTE Laboratories Incorporated, 1996

[7] Tanenbaum, A.S., Computer Networks, 3rd Ed, Prentice-Hall, Inc., 1996

[8] Telecommunications Engineer's Reference Book, edited by F. Mazda, Butterworth-Heinemann Ltd., 1993