



Demystifying Data

Taking the Mystery
Out of Wireless Data

Cellular Security

by Steve Isaacson

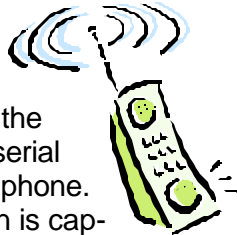
First Published in WirelessNOW

Introduction

With the popularity of the Internet, security has become a huge issue for computer users. Hackers have defaced popular web pages and created havoc for ISP (Internet Service Providers). Recently, the CIA's home page was attacked and spray painted with electronic graffiti. Some ISP's operations have been halted by hackers sending "SYN storms" to a host and thereby blocking connections for legitimate users. The host computer is fooled by an array of phony connection requests (SYNs) which quickly use up the maximum number of allowed users.

With cellular phone usage booming, the tapping of cellular phone conversations has reached the attention of the highest levels in government. Common frequency scanners can be easily modified to listen to any cellular phone call. By simply cutting a wire here or removing a resistor there, an inexpensive scanner becomes a cellular phone wire tap device.

The cloning of cellular phones is a multi-million dollar problem for cellular carriers. Cellular hackers simply drive along a busy roadway with a commercial device designed to capture the phone number and serial number of a cellular phone. Once the information is captured, any cellular phone can be programmed with the identical information.



Combine the security issues of the Internet with the transport medium of cellular and you have the potential of not only a security leak but a security flood.....or do you. Is a cellular data "conversation" as easy to listen to as a cellular voice call? Do Internet security issues affect the integrity of cellular data's Internet Protocol based Cellular Digital Packet Data? Can the cloning of cellular devices open up the corporate host to any cellular hacker?

Virtual Wire Tapping

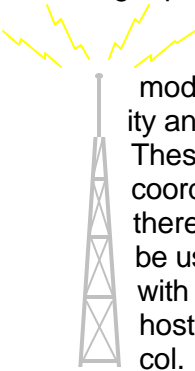
Wire tapping a phone line has been around as long as phones. Simply clip a device onto the two phone line wires and you can listen to the conversation. Wire tapping a cellular phone is similar except that you use virtual clips. Cellular phones use two radio frequencies instead of wires to talk and listen. Using a cellular scanner, simply tune in to the frequencies and you hear the conversation. However, these frequencies may change during the conversation. For example, a cellular phone user driving down a highway may change radio frequencies several times during a conversation. This is because the user is being handed off from one cell site to another. This hand-off sequence is difficult to track for a would-be hacker.

Circuit-Switched Data Security

Cellular Security

Demystifying Data

The sending of data over cellular frequencies has been around for several years now. Each year more sophisticated algorithms are developed to cope with the challenges of the harsh radio environment. A common technique used in these algorithms is to dynamically change the data transmission rates as the quality of the cellular signal changes. For example, a high quality signal allows the modem to send data at higher speeds. As the signal degrades, the modem detects the decreased quality and slows the transmission rate. These dynamic changes must be coordinated with the host modem, therefore matching protocols must be used. A laptop modem equipped with a cellular protocol must talk to a host modem with the same protocol.



hackers from decoding your valuable data.

For comparison, think of a baseball game where the pitcher and catcher exchange signals. The pitcher and catcher agree on the speed or type of pitch but the batter is out of the loop. The batter must guess at what the pitch will be. The batter gets several chances to guess and only the best can guess right 1/3 of the time. The hacker, like the batter, has the challenge of guessing the right signal. The decoding of data transmitted over cellular is not an easy task. But, like the batter, there is a slight chance the hacker guesses right. To strike out the hacker, use an encryption software package for all your cellular data transmissions.



Enter the hacker. A cellular data hacker, like the cellular phone hacker, must first find the frequencies the modem is using. The data hacker must then capture the modulated data and try to decode it to useful information. This decoding process is much more difficult than one might think, especially over cellular. The conversation between the laptop cellular modem and the host modem includes special algorithms telling each other when to change the transmission speed. Since the hacker's modem is a passive listener and "out of the loop" of the signal conditions, it is unaware of the varying transmission speeds. The algorithms designed for reliable cellular data delivery deter



Demystifying Data
7890 Tufton Court
Fishers, Indiana 46038
(317)576-0463
info@dataspynet.com



WirelessNow
1130 Connecticut Ave
Suite 325
Washington DC 20036
www.wirelessnow.com