Taking the Teeth Out of Bluetooth Phracking

THE CRYPTOPHONE PSTN/1, GSMK'S SECURE LANDLINE PHONE THAT IS FULLY INTEROPERABLE WITH GSMK'S SECURE CELLULAR AND SATELLITE PHONES.

Paris Hilton's hijacked phone notes, hot pics and movies, and celebrity contact info got her unwanted and undeserved notoriety. The incident also brought broad visibility to a blossoming dilemma: like computer data, our increasingly computer-like mobile phones' contents can be hacked. by David Geer

To be correct, your data can be phracked. Phracked, phracking, or phracker are the correct terms for a phone cracker or phone cracking. Cracking is the correct term for malicious hacking.

Following the classic security mantra of using layered protection, we present several counter-hacks that untethered communicators can use to foil the would-be phracker.

BLUETOOTH SECURITY — BLUETOOTH BACKGROUND

Bluetooth is a fairly recent technology that has faced its share of invasions. Notable attacks have included Blue Stumbling, Blue Snarfing, and Blue Jacking.

Blue Stumbling is the Bluetooth equivalent to War Driving*. By using Blue Stumbling, phrackers (phone

crackers) can pinpoint Bluetooth gadgets (PDAs, Mobile Phones) within a small radius.

*(*With War Driving, a cracker drives around with a laptop and a special antenna engineered from a potato chip cylinder discovering unprotected Wi-Fi networks. Wi-Fi crackers do this so they can use your connection for free, crack another system through your connection while masquerading as you to steal data or deface websites, or simply mess with your head. Blue Stumbling is also referred to as War Walking.)*

Blue Snarfing is a technique that permits a phracker to rob data from your Bluetooth device without pairing (making a direct connection) with it. Phrackers cannot only surreptitiously retrieve information from your Bluetooth device, but also send information to it without exposing themselves or having to be acknowledged by the recipient.

With Blue Jacking, phrackers can send information to the Bluetooth device without pairing with it so that you wouldn't know who it was from. It's a kind of Bluetooth-based version of spamming.

BOUNCING BLUETOOTH BREAK-INS

For most all the above, protection is as easy as downloading and installing the latest firmware update for your phone. Other fundamental precautions include turning off the Bluetooth service when you're not using it. If it's not running, it can't be hacked.

Insure that your phone has encryption abilities and use them. Some brands offer seamless encryption that's always on to protect your Bluetooth connections so you never have to set it (check the manual for your hardware). Nokia is such a vendor.

With Nokia Bluetooth enabled phones, the encryption is transparent to the user, always on, automatically protecting authenticated Bluetooth connections, including voice communications between a headset and phone.

Use the phone in non-discoverable mode (see your manual). When any Bluetooth device is in non-discoverable mode, it can't enter into a state where it can respond to inquiries. You can loosely think of it like not having your wireless 802.11 router set in broadcast mode.

Create new link keys for pairing with other devices. With Nokia phones, you can create a new link key for pairing devices by deleting the existing pairing from the paired devices menu. This keeps the passkey new and unique, harder to crack.

You can also audit your phone — test its security — using Bluetooth network discovery tools like BlueSniff and RedFang. With these software downloads

LEFT: The GSMK CryptoPhone 200, the world's first secure PDA-based cellular phone.

BELOW: The CryptoPhone 200T, GSMK's secure phone for both cellular and satellite connections.

and most any Bluetooth adapter, you can use a simple interface to check for the availability of Bluetooth networks and devices (including your own).

OTHER SECURITY MEASURES – AV AND FIREWALLING

Bluetooth is by far the only phone protocol or the only phone vulnerability. For advanced devices, firewalls and antivirus protection are recommended. Using Nokia as an example, you can use products such as Symantec's integrated firewall and AV product for Nokia's 9500 Communicator and the 9300.

Both F-Secure and Symantec offer AV for the Symbian OS-based Nokia smart phones, i.e., Symantec Mobile Security 4.0 for Symbian protects Symbian operating system based smart phones (series 60 and 80) like the 9300 and 9500 from not only viruses, but also Trojans and worms. Comparable information should be available from your vendor.

MORE FROM NOKIA

Don't accept unidentified Bluetooth applications or MMS attachments. These may include phone-based malware that is harmful to your phone. Don't download content to your mobile phone from an unknown, obscure, or unreliable source. Download from your operator's (carrier's) portals or other well-known brands, where you should assume good protection against potentially harmful malware (viruses and the like).

Nokia has a VPN solution for many of its smart phones at **www.nokia.com/nokia/0,,43117,00.html** A wallet feature available in many Nokia models secures sensitive e-commerce and other data. Data inside the wallet is encrypted and protected with a special access code that the phone user can define. See more at: **www.nokia.com/nokia/0,8764,43153,00.html**

THE CRYPTOPHONE G10, THE WORLD'S SMALLEST, LIGHTWEIGHT TRI-BAND SECURE GSM PHONE.

>>>RESOURCES

■ RAZORPOINT SECURITY TECHNOLOGIES **www.razorpointsecurity.com** Thanks to Gary Morse, president of Razorpoint, for his input on Bluetooth.	■ BLUESNIFF **http://bluesniff.shmoo.com** A Bluetooth network discovery tool
■ NOKIA **www.nokia.com** Thanks to Nokia for its input on Nokia mobile phone security.	■ REDFANG **www.securiteam.com/tools/5JP0I1FAAE.html** Another discovery tool
■ GIZMODO, THE GADGETS WEBLOG **www.gizmodo.com**	■ MISC. BLUETOOTH SECURITY RESOURCES **http://wiki.mediaculture.org.au/index.php/Bluetooth-_Security**
■ BLUETOOTH WEBLOG **http://bluetooth.weblogsinc.com**	■ BLUEZ.ORG **www.bluez.org** The Linux Bluetooth Protocol Stack

OR, JUST GET A PHONE BUILT AROUND SECURITY

The new CryptoPhones from Germany in four models are all about cryptography and security. The devices use AES256 (Advanced Encryption Standard) and Twofish algorithms for security and the 4096 bit Diffie-Helman key exchange technology.

The US Government has approved AES encryption for up to and including classified top-secret information. The 256 stands for 256 bits, the largest number of bits available to encrypt data. Twofish encryption was a top finalist for selection as the AES standard, beat out by Rijndael encryption.

The Diffie-Helman is based on RSA (the RSA algorithm invented by Ron Rivest, Adi Shamir, and Leonard Adleman, the achronym being formed by the first letters of their last names) math and enables secure key exchanges where the encryption and decryption key is the same exact key.

The CryptoPhone destroys its encryption key automatically the second the call ends. Standby time is a competitive 180 hours. Talk time using security is up to 3.25 hours on a single charge. The CryptoPhone supports GSM networks.

The CryptoPhone offers a hard line defense in the face of IMSI-catchers (IMSI stands for International Mobile Subscriber Identity) and network-based interception threats. An IMSI Catcher is a device for finding mobile phones (short range) and recording telephone calls. The device appears to the mobile phone to be just another base station.

DON'T ACCEPT UNIDENTIFIED BLUETOOTH APPLICATIONS OR MMS ATTACHMENTS. THESE MAY INCLUDE PHONE-BASED MALWARE THAT IS HARMFUL TO YOUR PHONE.

The phone provides CELP (the Code Excited Linear Prediction algorithm) voice quality and you can use a free GSMK CryptoPhone for Windows client to set up secure telephony between a landline user or users and the mobile GSM CryptoPhone 200 using a computer and modem. The format and form factor resemble PDA-phones with a large display and easily maneuvered interface.

Because the phone software is based on open source code, there is no proprietary control that might create its own security issues, i.e., there is nothing concealed from the user –there are no backdoors, no operator (carrier) key generation, or registration.

The CryptoPhone is the only mobile phone on the market with the full source code published. This enables engineers and programmers to assess its security independently. If you're a developer, you can develop your own CryptoPhone compatible products using the published source code and the public, standards-based communication protocols. **NV**