by Gary McGraw

Are Cell Phones the Next Target?

Cell phones and other mobile communications devices are ripe for attack. The number of wireless platforms is growing, market penetration on the consumer side is deep, and defenses are either weak or nonexistent. Wireless device manufacturers and network providers are understandably concerned and taking action to improve the security of their products.

DÉJÀ VU

The first real cell phone worm, called Cabir, was a proof-of-concept worm released in July 2004. It targeted phones running the Symbian OS and spread by sending an executable file via Bluetooth. Since then, a number of variants have been seen in the wild, with the latest surfacing in January. None of these variants include malicious payloads, though phones infected with Cabir tend to have power consumption problems.

Non-propagating but nonetheless sophisticated attacks against Bluetooth phones appeared before Cabir in late 2003. Discovered and discussed by brothers Ben and Adam Laurie, these exploits allow an attacker to silently connect and gain access to particular target phones (see www.thebunker.net/security/bluetooth.htm). Given a successful exploit, an attacker can carry out a number of potentially malicious actions, such as disrupting a phone call or initiating a voice, data, or fax call.

Just as in the computer security world, we're likely to face both nuisance attacks from script kiddies and financially motivated attacks undertaken by criminals. (Don't be at all surprised when phishing makes its way to Web-enabled cell phones.) The opportunities for such nefarious behavior are enormous.

For example, most modern mobile wireless devices accept SMS messages. These messages can originate from another phone or any one of the many free SMS Internet gateways out there. That means anyone can send an SMS to a device, provided they have the target phone number. Clearly one worst-case scenario would involve using SMS as a propagation vector, with a payload that attacks a weakness somewhere on the receiving device. An attack that could disable a target would cause no end of trouble for infected consumers. In turn, these consumers would flood the help lines of affected providers, as well as the retail stores where the phones are sold. Suffice it to say that patching millions of phones via flash cables would present a physical challenge beyond current capabilities.

RESPONDING TO THE RISKS

The security community is beginning to pay more attention to the wireless device space. A full-disclosure mailing list called MobileBugTraq (since renamed MobiBug) was launched this April. The list is devoted entirely to the security of mobile devices and terminal systems. These kinds of forums have existed for years on the Internet, but have only just crossed the wireless divide.

Providers are beginning to consider an automated updating approach to phones. Current approaches to patching involve major software releases or updating a phone in a store. Automated updates can be used to counter threats as they emerge, but great care must be taken to design a system that's immune to attack in the first place.

> In my opinion, it's time to think about a CERT for the wireless world.

Providers are also beginning to talk about incident response plans. The Morris worm resulted in the formation of CERT in 1989 as a central security coordination center for the Internet. Perhaps it's time to think about a CERT for the wireless world.

Most wireless platform vendors understand what they're facing, and they're working hard to build security into their systems. If we're lucky, wireless vendors will get in front of the problem before Mayday problems such as Code Red, Nimda, and Slammer occur. If we're complacent, we may be in for a world of hurt.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.