

Wireless Devices and a New Generation of Viruses

Josh Ryder 2001-06-27

Wireless Devices and a New Generation of Viruses

by Josh Ryder

last updated June 27, 2001

Recently, NTT DoCoMo, a Japanese telecommunications company, released an advisory to all users of their popular I-mode phones warning that malicious e-mails had been circulating. These e-mails exploited certain cell phone features to perform actions such as automatically dialing an emergency number, making unsolicited calls to large groups of people, or freezing the display screen. According to sources at DoCoMo, no users had complained about damages caused by these messages; however, the company is considering legal action against the senders of these messages due to "inconveniences caused to its customers and harm to the popularity of mobile Internet" and, by extension, potential damage to the companies business. Unfortunately, if you received a message from a user whose phone was afflicted, then the next time you dialed, your phone would also become tainted, not only by suffering from the effects of the malicious message, but also by acting as a carrier.

While the spreading mechanism used in this malicious action may seem a bit archaic, text messaging between people using their telephones is becoming commonplace in Japan, and as such the problem spread like an out of control fire. With a little more work, it would be theoretically possible for such a threat to be self-propagating, acting like the now infamous "I Love You" Outlook virus whose presence was felt internationally.

The DoCoMo incident set off little warning bells in my head. Just how vulnerable *are* our wireless devices to actual virus incidents? While North America does not yet have the market penetration of standardized hardware that Japan does (NTT DoCoMo has a government-sanctioned monopoly), the question remains: what steps are being taken to ensure that our wireless devices are safe from sabotage?

Securing Wireless Networking Protocols

The first step in making electronic communication secure is to make sure that the pipe in which information is exchanged is reasonably tamper-proof. This, coupled with the need to standardize protocols for compatibility and ease of deployment, has brought about the

formation of two major wireless standards: 802.11 and Bluetooth. Other network protocols have been discussed (standard TCP/IP and fax/modem protocols of days past among them), but have been discarded either due to their inherent insecurity, or due to the high data overhead associated with transfers performed using them.

802.11 and Bluetooth are both methods that allow users to connect their portable devices - such as cellular telephones and PDAs - to access the network and communicate with one another without the hassle of cables. While Bluetooth is targeted at low-power, low-cost wireless devices (toasters, washing machines, home security systems etc.) and 802.11 (and 802.11b) are intended more for wireless users with higher bandwidth needs such as laptops, desktops and PDAs, both are faced with essentially the same security problems and concerns.

In the 802.11 standard, an optional security compliance level, Wired Equivalent Privacy (WEP), allows vendors to make the protocol at least as snoop-proof as a conventional wired network. Many vendors have also chosen to implement their own layer of encryption and authentication over and above the standard in order to further ensure that the end-user's information can be transferred safely. Bluetooth, for instance, has built-in authentication and encryption methods. Authentication is a combination of a Personal Identification Number (PIN) and a Bluetooth address, which creates a unique authentication key for each device/user. These mechanisms are especially important since the Bluetooth standard was developed with ad hoc connectivity in mind.

The driving idea behind ad hoc connectivity is that each person will have his or her own personal network, in which devices that he or she owns will communicate with one another. When the user is in transit, the devices continue communicating by establishing a connection to another close Bluetooth device. For example, let's say that your Personal Area Network (PAN) is largely centered about your cubicle at work. As you move from office to office, you may want your organizer to stay in communication with your other devices (such as your desktop). Your organizer will stay connected by communicating and negotiating with other Bluetooth-compliant devices as you walk around. Obviously, in order to prevent "strangers" from accessing and utilizing your PAN, a high level of protocol-level security is necessary. To further ensure data safety Bluetooth calls for frequency hopping at a rate of 1600 hops per second (the signal will jump from one frequency to another at a rate of 1600 changes per second).

Secure Wireless Protocols and Viruses

Once we are confident that the communication protocols are reasonably secure (meaning that it is computationally difficult to decrypt the data stream in a reasonable amount of time using normal hardware), we can begin to think about the risks facing individual devices and how to prevent them from being compromised. Protocols are considered secure if they can pass a stringent peer-review process that usually includes public releases of the actual encryption/decryption algorithm. When the domain experts (mathematicians and encryption gurus) have approved the underlying algorithm of a protocol, it is generally accepted as being secure.

If the protocols are insecure, it is theoretically possible for someone to change or even completely substitute information being sent to a user. For example, if you were being sent a shell script that contained the line "touch *", the attacker could replace it with the line "rm * -rf", replacing your innocuous document with one capable of deleting all of your files. A worm or other form of malicious code could be written to exploit the insecure protocols, allowing for proliferation among the users' networked wireless devices. By ensuring that the protocol is secure we remove a method for virus writers to attack us.

Wireless Devices Today

In North America, we are just beginning to see wireless devices that are not directly based on cellular technology. Some of the most ubiquitous devices are the WaveLAN wireless networks sold with Apple's iMacs and Powerbooks. The Apple Airport has finally brought wireless LANs to the masses, and while this device is little more than a glorified WaveLAN card with a big antennae and a pretty case, it has demonstrated that there is a huge public demand for wireless networks.

In a way, wireless technologies are currently protected by the emergent nature of the technologies. This is true for a couple of reasons. First of all, there are currently numerous devices on the market, and almost none of them contain similar hardware or software. Secondly, a virus creator generally decides to write a new worm or virus for one of two reasons: a) they want notoriety from peers, and thus will go after large targets (as evidenced by the Outlook e-mail worms), or b) they are bored. The fact that wireless is still an emergent technology deters virus writers from targeting the smaller fish in the security pond.

Because there is so much non-standard hardware present in the North American market, even the most cleverly crafted wireless device-targeted virus would have a minimal impact on the wireless network as a whole. For example, infecting 100 I-mode phones and causing them to

reboot is far less damaging than having the main boot records removed from tens of thousands of PC's. As the technology driving wireless devices grows, and as the storage capacity of these devices grows (and subsequently, more data is stored in them), the threat of a more serious virus with a more destructive payload also increases.

Note that I have carefully avoided discussing virus writers who may be motivated by the "I did it because it hadn't been done before, or to show that it could be done" mentality. This is primarily because people demonstrating this characteristic tend to be more ethical in how they deal with vulnerabilities [Gordon, Sarah: "The Generic Virus Writer"] and are thus less likely to write viruses for malicious or destructive purposes.

The current precautions made by hardware manufacturers are inadequate. (Both NTT DoCoMo and Telefonica, which is discussed briefly below, use I-mode phones, which are based on Java technology, a technology that was thought to be sufficiently sandboxed to prevent the spread and execution of undesirable code.) If there are a sufficient number of devices in the marketplace, virus writers who are interested in notoriety will concentrate their efforts on discovering and exploiting vulnerabilities within those devices. For example, the latest WinCE PDA's all include Outlook and Internet Explorer, two programs that are now rather notorious for containing security holes. It is entirely conceivable that these applications contain the same, if not more, security holes found in their desktop versions, they just haven't been exploited yet because there are not enough of these devices actively connected to make a noticeable impact.

Wireless Incidents So Far

As mentioned earlier, targeted attacks have been mounted against wireless devices. So why, given the previous discussion, did these attacks occur? The DoCoMo incident occurred mainly because NTT DoCoMo has a 60 percent market share of cellular devices in Japan. This stranglehold on the market, coupled with the ravenous appetite displayed by the Japanese population for the newest and greatest hardware, meant that the majority of DoCoMo customers likely had the most recent telephones, the I-Modes. Since the user base was large enough, and the profile of the network was sufficiently high, someone decided to make an example of them by exploiting a vulnerability in the I-Mode phones.

Today, even with the least advanced telephones, service providers and customers are still exposed to malicious attacks. Even if the devices are not advanced enough to allow for a "real" virus, the wireless networks are still vulnerable. In June of 2000, a virus originating on a PC

targeted the wireless network of Telefonica in Spain. The virus, called VBS/Timofonica, was written to cause an infected PC to spam random telephone numbers (via an SMS gateway designed to relay text messages to the phones) on the Telefonica network with a message critical of the service provider. While this virus did not actually spread between the telephones, it did flood the Spanish provider's bandwidth, effectively causing a Denial of Service.

Wireless Devices and Viruses: the Future

As the average consumer becomes more accustomed to wireless technology, the demand for wireless-enabled devices will likewise increase. Inevitably, as has happened in most telecommunications industries, a market leader will emerge, and their platform will become the defacto standard (Intel and the Palm devices are both good example of this). Once the hardware becomes more standardized and the user base increases, the chances that someone will a virus for them will increase significantly, as the impact of a well-written virus would be much greater than one targeting a few hundred devices. As a result, it is likely that we will see an increase in the type and number of viruses/worms/exploits for wireless devices increase dramatically as these technologies become more mainstream.

The cell phone sabotage issue raises an interesting question: who should be responsible for protecting consumers from this sort of malicious attack? It is entirely conceivable that other forms of attacks (as demonstrated with the DoCoMo exploit) including viruses and worms could be launched against a great many wireless devices. Historically, the onus has been placed on the user. If a home computer system gets infected with a virus, it is the user, not the service provider, who is expected to remove it or to prevent an incident by scanning incoming files for viruses, etc. This method is unfortunately not sustainable for the current generation of wireless devices, as most do not contain enough memory to store an up-to-date virus database, or even to have a simple mail filter setup. What of the safe protocols, you ask? Well, you can rest assured that no one is swapping your packets as you receive your untampered-with virus payload from some malicious user.

It would seem that as technology marches forward, and the demand for ever smaller portable devices continue, the service providers out there are going to have to take more responsibility for protecting their customers from the evils of the general networks. As wireless devices increase in capacity to store information, things may change again, but at least for the short term we probably should be asking our telecom and wireless service providers what steps they are taking to ensure that our precious wireless devices are sufficiently protected from the cold,

dark world.

Different companies are currently taking different approaches to preventing viral infection in their handhelds. For example, Symbol (a producer of handhelds) has chosen to pre-install Computer Associate's InoculateIT antivirus software in some of their new WindowsCE-based handhelds. Symbol realized that the WinCE platform is just as susceptible (if not more so) to macro viruses, applet bombs and exploit code, and are, at press time, the only WinCE device manufacturer that currently includes protection from these potential problems. F-Secure has also announced that they now have a service-provider-based solution to the virus problem. Called F-Secure Anti-Virus for WAP Gateways the product purportedly scans for and removes all manner of viruses from the data stream before it even reaches the handheld.

Conclusion

Wireless technology is currently in a state of early infancy. No one really knows how it will develop, or what it will become. Assuming that this technology does become mainstream, I believe it to be a safe bet that we will see several of the major anti-virus companies writing generic software for wireless platforms, or perhaps even working behind the scenes with wireless manufacturers to transparently protect without the consumer ever having to lift a finger. One thing is certain, wireless technologies are currently wide open to numerous types of attack: denial of service, viruses, worms and Trojans. As the use of these technologies becomes more widespread, as more users become reliant upon them, and as more crucial information is channelled through them, this will have to change.

Relevant Links

[NTT DoCoMo release](#)

NTT DoCoMo

[IEEE 802.11 FAQ](#)

Intermec

[BlueTooth FAQ](#)

BlueTooth

[The Generic Virus Writer](#)

Sarah Gordon

The Generic Virus Writer II

Sarah Gordon

Timfonica VBS/Timofonica worm

Timfonica

WAP Antivirus Products

Internet.com

Handhelds Ship with AV software

Internet.com

[Privacy Statement](#)

Copyright 2006, SecurityFocus