



Mobile Phones as Computing Devices: The Viruses are Coming!

David Dagon, Tom Martin, and Thad Starner

Imagine this scenario: Paul, the CTO of WidgetCo, visits BadCo, a rival company. Paul attends a private dinner at BadCo's headquarters to discuss a possible cooperative venture. While there, BadCo's industrial espionage team uses Bluetooth to infect Paul's mobile phone with a program that turns it into a listening device. BadCo can call Paul's phone without it ringing, Paul's phone automatically answers, letting BadCo eavesdrop on what's occurring in Paul's environment through his phone's microphone. BadCo uses this ability to spy on Paul's later meetings at WidgetCo and steal the venture for themselves.

Although this story is fictitious, it's feasible (for other possible attack scenarios, see the sidebar). Security researchers have already demonstrated a way to wrest control of a remote phone for listening purposes, called bluebugging. However, we can illustrate the basic idea of turning a mobile phone into a listening device simply by using the hands-free interface on many phones. By setting the ringer to its lowest setting, turning off the vibrator, and turning on the "auto answer" mode, a phone will answer a call without any owner intervention. Although many phones won't let the phone be in "silent" mode while also in auto answer mode, you can set the volume and ringtone to be unnoticeable in most environments.

Even turning off a mobile phone might not be adequate protection. Most

mobile phones use a "soft" power switch, which doesn't physically disconnect power to the phone but instead turns off the screen and puts the phone in a lower power state. A malicious program running on the phone could imitate this "power off" state when the user presses the power button. It would keep the phone operating to monitor the microphone, steal information from the user's phone, or even record audio for later recovery in the phone's memory.

Understanding existing threats against mobile phones helps us better protect our information and prepare for future dangers. Merely enumerating known attacks doesn't help us understand all possible threats. Instead, a taxonomy of attacks against mobile phones will show known attacks as well as potential future attacks.

THE RISKS OF MOBILE PHONES

Mobile phones have evolved from their roots as analog walkie-talkies to full-scale Internet-enabled computers. Today, mobile phone handsets are arguably the dominant computer form factor consumers purchase (see Table 1). These devices have become powerful and sophisticated—many are even more powerful than desktop computers of the late 1990s. Mobile phones are also moving toward an "always on" form of networking, where users can get Internet data services continuously through the service providers network. Increasingly, these phones also incor-

porate IEEE 802-based networking technologies (for example, Wi-Fi and Bluetooth). But having such powerful networked computers leads to a new class of malware: viruses, worms, and trojans specifically designed for the mobile environment.

Most consumers think of Wi-Fi and Bluetooth as short-range communication standards. As such, most manufacturers consider the threat to mobile phones minimal because users would have to be physically near a malicious party to be attacked. However, a team at Flexilis was able to establish a Bluetooth connection with a standard mobile phone more than one mile away with a 19dbi panel antenna (see www.g4techtv.com/screensavers/features/48021/Bluetooth_Attack.html). In addition, because Bluetooth devices are often carried, an attacker can abuse even a truly short-range standard in areas of high-concentration, anonymous pedestrian traffic such as subways.

Threats against mobile devices are more acute than traditional malware. Mobile devices, such as phones and PDAs, are often more personal than "personal computers." Users might think that because their phones are constantly with them, they are more secure than PCs. But physical control of a computer doesn't automatically guarantee secure control. Users tend to have a false sense of security with handheld or portable consumer electronics, leading them to trust these devices with

more sensitive information. Mobile device attacks endanger a person's most private information: numbers, names, contacts, appointments, passwords, and even identities. Although such personal information is also present on PCs, it's more diluted, scattered, and less organized than it must be on limited mobile devices. Indeed, attacks on mobile devices often have an easier time finding private information.

A RESULT-CENTRIC TAXONOMY OF MOBILE MALWARE

An "important and sensible goal for an attack taxonomy... should be to help the defender."¹ Far from an academic exercise, a malware taxonomy not only classifies known attacks but also helps us anticipate what types of threats might come.

Attack taxonomies are most useful when they classify attacks in relation to some detection technology. However, detection and prevention systems for mobile attacks are in their infancy, so a defense-centric taxonomy would be difficult and speculative. It's not clear, for example, what types of monitoring efforts are feasible on all types of limited-computing devices and how attacks will manifest themselves with sensors monitoring mobile computing devices.

Not surprisingly, security research on mobile networks has therefore focused largely on routing issues,² and more recently on protocol security.³ But as attackers work their way up the protocol stack to exploit applications, our

ALTERNATIVE ATTACK SCENARIOS

A mid-level manager arrives at his office and finds the police waiting for him. His boss is also present, and she immediately hands him a termination letter. Stunned, the manager asks what has happened. The police begin asking him about the theft of files, and intimate that they know he secretly took proprietary files from work, and sold them on the internet. Although ultimately cleared in the criminal investigation, the manager finds it difficult to locate work. The real culprit in this story: the manager's mobile phone. Weeks before his termination, he picked up a virus on a subway, spread via Bluetooth. The virus in turn used the mobile phone as a launching point to steal corporate documents.

In another scenario, Bob enters a store and begins looking at a display of dress shirts. Suddenly, his phone alerts him to a message, sent wirelessly by some anonymous source: "The ties you looked at in the window are going on sale Thursday. Buy a shirt today and bring your receipt back for an additional 5% off." Bob looks around the store, surprised that a sales associate might have followed him from the window display to the racks. But the store is nearly empty and he can see no clerk. Distracted by the message, Bob starts to walk toward an exit when another message arrives: "Please wait. Before you go, look at our new display of dress slacks. A sales associate has been summoned." As Bob leaves the store, he passes another department store entrance. His phone goes off again: "If you want to browse some more, please see our sale items in housewares."

These scenarios are fictional, but the elements are based on fact. Viruses that can spread via cellular devices (see <http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html>), and mobile malware that can expose corporate networks (<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.brador.a.html>) do exist.

Additionally, by tracking Bluetooth-aware devices, companies can track, if not uniquely identify, individuals on the move. Using context information, they can also infer behavior (for example, browsing, making a purchase, lingering at a display). Individuals and organizations that remain ignorant of these threats compound their risk.

risk analysis of mobile threats should do the same. We build on the taxonomy of wireless routing attacks Yi-an Huang and Wenke Lee describe,² and classify attacks against mobile devices on the basis of the results attackers hope to achieve (see Table 2). In this article, we're primarily concerned with attacks against the phones themselves as opposed to threats to the service

provider infrastructure (for example, spoofing, jamming, and so on).

Information theft

People often attack mobile devices to obtain information. Two subcategories exist: attacks against *transient information* and against *static information*. Transient information includes the phone's location, its power usage, and other data

TABLE 1
Computing device sales for 2003

Device	2003 sales (in millions)
Mobile phones	> 500 (www.compoundsemiconductor.net/articles/news/8/2/8/1)
Desktops and servers	128
Laptops	36 (www.usatoday.com/tech/news/2003-11-17-gates_x.htm)
Portable compressed music players	24 (www.twice.com/article/CA412032.html?display=Breaking+News)
PDA's	10.4 (www.twice.com/article/CA380408.html?verticalid=820&industry=By+The+Numbers&industryid=23106&pubdate=02/09/2004)
Tablet PCs	0.6 (http://seattle.bizjournals.com/seattle/stories/2003/03/10/story2.html)

TABLE 2
Mobile malware taxonomy.

Compromised security goal	Attack examples
Confidentiality	Theft of data, bluebugging, bluesnarfing
Integrity	Phone hijacking
Availability	Protocol-based DoS attacks, battery draining

the device doesn't normally record. Using services such as Enhanced 911 (www.fcc.gov/911/enhanced), attackers can store a history of user movements through the city with some precision. Even without advanced location services, attacks can still locate phones with mobile regions (based on the tower that's providing service) even if the phones aren't in active use.

Attacks on static information target information that cellular devices store or send over the network. Thus, instead of targeting meta-information about the device (where it is, what state it's in, and so on), these attacks try to get data such as contact information, phone numbers, and programs stored on smart phones.

The BlueSnarfing attack is one example (see www.thebunker.net/release-bluestumbler.htm). A snarf attack works against particular mobile devices, letting attackers connect without alerting the owner. Attackers can access most data on the device, including phonebook entries, calendars, cards, and even the phone's International Mobile Equipment Identity, which uniquely identifies it on the mobile network.

At present, these attacks largely depend on misconfigured Bluetooth devices and other insecure default installations. They'll increase, however, as attackers learn ways to break IEEE 802.11 WEP protection schemes. For example, the 802.11 WEP protocol has demonstrated weaknesses that allow for both attacking message privacy⁴ and cipher key recovery.⁵ GSM-encrypted communications have also been vulnerable to ciphertext-only attacks.⁶

One particularly pernicious attack is

bluebugging (used in the scenario we presented in the introduction), whereby a targeted phone becomes a bugging device. The attack requires the target device to improperly offer a serial line service over Bluetooth. Most smart phones can record about an hour's worth of audio or more. The attacker can either record or broadcast the victim phone's audio, effectively turning it into a mobile bugging device.

Unsolicited information

Information attacks can also work in the opposite direction. For example, attackers can target mobile users with advertising, messaging, and other unsolicited information. Spam short message service messages are already quite common, particularly to US customers with unlimited SMS messaging plans (who are less likely to have service providers filter their messages). Spam over Internet Telephony (SPIT)—essentially, talking spam—is a variation that will likely grow as more users subscribe to voice-over-IP services.

Transferring unsolicited information isn't unique to spammers, of course. "Bluejacking," for example, lets users communicate using a simple discovery protocol. When discoverable Bluetooth devices query each other, they transfer a device name, such as "Nokia 7650" or "Palm OS handheld," and report this name to help with identification. For example, when a Nokia phone wants to send a document via Bluetooth to a Palm device, the Palm alerts the owner and prompts whether to connect to, for example, "Bob's Nokia 7650." Users can easily set the device names, and frequently change them to provide messages or statements. Bluejacking, while

ominous-sounding, is nothing more than setting a Bluetooth device name to advertise some message—for example, "Drink Coke"—and letting other users discover this. Although largely anonymous (a bluejacking target does learn a remote media access control address), most bluejacking instances have been limited to individuals exploring the technology.

Theft-of-service attacks

Some malware might attempt to use the victim's phone resources, effectively hijacking services. Possibilities include placing long-distance or 900-number calls, sending expensive SMS messages, and so on. The recent Mosquitos virus is one example (see www.symbian.com/press-office/2004/pr040810.html). Pirated copies of a computer game were infected with a virus that sent (potentially) expensive SMS messages when users played the illicit copy of the game. The Brador WinCE virus poses a similar threat to services because it opens a backdoor on the infected device. Hijacking phone resources isn't unexpected—malware authors have been using victims' resources for quite a while.⁷

Denial-of-service attacks

Two types of DoS attacks against mobile phones are possible—those that attempt to flood the device (for example, MAC Layer DoS attacks against 802.11 networks⁸) and attacks that attempt to drain power.

At present, it's extremely easy to crash or overwhelm most Bluetooth applications on mobile devices just by sending repeated pieces of information, corrupted packets, and incorrect file formats. In experimentations at the Georgia Tech Information Security Center, we've also found that many commercial and open source Bluetooth stacks are vulnerable to simple protocol attacks. The problems with these new, large, and complex protocol layer implementations are not unlike the vulnerabilities that plagued IPv4 implementations

years ago. If Bluetooth follows a similar development path, it will take years of experience and testing to identify and remove most bugs in the some 31,000 lines of code that make up the average Bluetooth stack implementation.

Power demands always constrain mobile devices, so this latter category is more serious. Attacks that exhaust a device's battery keep the device active all the time, preventing it from going into lower-power idle and sleep states (for more information, see the "Battery Exhaustion: A Threat to Mobility" sidebar). The impact of the attack depends on the device's ratio of active to sleep power. On a mobile phone, this would mean the user's battery life would last only as long as the talk time, not the standby time, even if he or she wasn't using the phone.

A carefully crafted battery exhaustion attack would lead the user to believe the battery had become defective. As batteries become older, they're less able to hold charge than when they were new, so users might believe their batteries were dying naturally. Having a dead battery would merely annoy an individual user. However, if battery exhaustion could rapidly spread from phone to phone, an attacker could disrupt mobile phone service on a wide scale or within a class of users. Another possibility would be to use battery exhaustion as a "secondary" attack to amplify the impact of another attack.

RECOMMENDATIONS

Some simple precautions will help prevent and diagnose threats to mobile devices.

Education

Customers, employers, and government agencies should know what types of attacks can be mounted against mobile phones.

Visualizations

Mobile phones should provide visualizations and logs of their most critical statistics, such as battery level, rate

BATTERY EXHAUSTION: A THREAT TO MOBILITY

Some attacks we've noted are annoyances, while others are more serious. One factor that distinguishes mobile computing devices from traditional desktop computing is their power limitation. Attacks that waste even small amounts of CPU time are therefore serious potential threats for mobile devices. Frank Stajano and Ross Anderson first described this form of attack, calling it a "battery exhaustion" or "sleep deprivation torture" attack.¹

Battery energy is extremely limited for mobile phones. Mobile phone hardware and software reduce energy consumption as much as possible, letting the phone have a longer battery life or use a smaller battery. Power-management systems have various states, such as active, idle, and sleep. A phone's expected battery life is based on a mix of these states, with little time spent in the active state. The active state consumes much more power than the idle and sleep states, so if an attacker can keep a phone in the active state, the battery life will be much shorter than expected.

Battery exhaustion attacks can occur in several ways, which fall into three broad categories:²

- *Malignant power attacks*, in which an attacker creates a virus or Trojan horse whose purpose is to increase power consumption.
- *Benign power attacks*, in which an attacker exploits an execution path in an unmodified program, causing it to consume large amounts of energy by giving the program pathological data.
- *Network service request attacks*, in which the attacker repeatedly requests a network service from the target device. Even if the service request isn't granted, validating the request consumes precious energy.

An example of a malignant attack is a program that repeatedly performs a high-energy task, such as reading from memory, operating on the result, and then writing the result back. Malignant attacks are easy to catch—existing virus scanners should be able to find them because they're new or modified software.

Benign attacks, however, are difficult to catch and defend against. Because they involve an unmodified program, a virus scanner wouldn't catch them. An attacker can mount a simple benign attack by creating an animated GIF that consists of the same image repeated several times. To the user, the GIF will appear unanimated, but it will require more processing than a static GIF and will keep the device busy as long as the image is displayed. An attacker could embed this image in a Web page, thus attacking any user who visited the page. Network service request attacks, being a special form of benign attacks, are similarly difficult to catch and defend against.

REFERENCES

1. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," *Proc. 7th Int'l Workshop Security Protocols*, LNCS 1796, Springer-Verlag, 1999, pp. 172–194.
2. T. Martin et al., "Denial-of-Service Attacks on Battery-Powered Mobile Computers," *Proc. 2nd IEEE Int'l Conf. Pervasive Computing and Communications*, IEEE CS Press, 2004, pp. 309–318.

of battery consumption, data transmission, and CPU activity. Users can inspect these visualizations to determine potential problems, and investigating logs after an attack might be useful for containment and prevention. (However, such logs could be exploited against the user in a court of law or

used in investigations. In the absence of privacy legislation protecting these logs, users should consider appropriate log retention and disposal policies.)

Conservative defaults

Network applications should be shipped turned off or non-discoverable

WEARABLE COMPUTING

by default. To encourage use of these features, sales personnel might show users how to enable them and describe how to monitor phones for misuse.

Profiling

Service providers could profile a user's typical activity to detect malicious use of the user's phone. If they detect suspicious activity, service providers could call or send a user a message seeking to confirm that he or she knows about the activity. Credit card companies use similar profiling to reduce fraud.

Hard switches

By using power switches that physically disconnect the power to the phone, the users can be more confident that their phones are truly off. If a phone has a speakerphone mode, using a physical switch helps prevent the abuse of micro-

phones designed to capture ambient audio from the user's environment.

Heterogeneity

Diversity of platforms provides an inherent level of protection from viruses. Without a critical density level of vulnerable phones in the same physical area, malware tends to spread slower. Open standards and compliant but competing implementations help create a strong culture of diversity, survivability, and innovation.

Although malicious attacks on mobile phones are somewhat inevitable, service providers and mobile phone manufacturers shouldn't restrain innovation and exploration. Mobile phones represent a new frontier in computing. Third-party development and open standards will be key to creating

new markets, just as they were during the transitions from mainframes to minicomputers, minicomputers to desktop PCs, and isolated to networked systems. Stifling innovation due to the threat of malicious programming will hurt the field and eventually be a disadvantage to those who purport closed systems. **P**

ACKNOWLEDGMENTS

Some of this material is based on work supported by the National Science Foundation under grant number ANI-0219801. The work was sponsored in part by NIDRR's Wireless RERC.

REFERENCES

1. K. Killourhy, R. Maxion, and Kymie Tan, "A Defense-Centric Taxonomy Based on Attack Manifestations," *Proc. Int'l Conf. Dependable Systems and Networks (ICDS 04)*, IEEE Press, 2004, pp. 102–115.
2. Y. Huang and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," *Proc. Recent Advances in Intrusion Detection (RAID 04)*, Springer-Verlag, 2004, pp. 125–145.
3. J. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," *Proc. ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC)*, ACM Press, 2001, pp. 146–155.
4. D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, vol. 353, Kluwer, 1996, pp. 153–181.
5. A. Stubblefield, J. Ioannidis, and A.D. Rubin, "Using the Fluhrer, Mantin and Shamir Attack to Break WEP," *Proc. Network and Distributed System Security (NDSS)*, Internet Society, 2001, pp. 1–6.
6. E. Barkan, E. Biham, and N. Keller, *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*, tech. report CS-2003-05, Technion, Israel Institute of Technology, 2003.
7. S.E. Schechter and M.D. Smith, "Access for Sale," *Proc. 2003 ACM Workshop Rapid Malcode (WORM 03)*, ACM SIGSAC, 2003, pp. 19–23.
8. V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc," *Proc. IEEE Military Communications Conf. (MILCOM)*, 2002, pp. 1118–1123.