

Viral convergence



Mobile telephony has revolutionized our lives. From 1947, when the first experiments were carried out, through Motorola's DynaTAC 8000X 'brick' in 1983, until today, there have been many changes, all aimed at improving communication, usability and services.

One of the problems that arose when mobile telephony started to become popular in the 90s was the need to establish a system that could guarantee the confidentiality of calls made from mobile phones. The old telephone devices only consisted of a radio system, which although complex, still allowed communication to be easily heard just by intercepting the signal.

Digital technology tried to solve these flaws, establishing an encryption system in the calls, which was easier because it was based on a digital system instead of an analogical one. The terminals establish encrypted communication with the base station; therefore an interception attempt should not be successful. GSM technology in Europe and CDMA in America and Asia, implemented the improvements that were thought necessary regarding call confidentiality.

Nevertheless, these encryption systems have been breakable for some time, and it is not very difficult for an attacker to break the code and in little time (just a few minutes) the theoretically 'private' conversation can be heard. What we are talking about is a hacking technique aimed at listening to a conversation between two people without their consent, and this is considered a crime in practically all legislation worldwide.

In recent years we have seen that cell phone handsets are no longer just telephones. They are complex mini-computers, with an amazing array of functions if compared not just to the DynaTAC 800X, but even to the models available only a couple of years ago. The similarity between PCs and cell phones is constantly increasing, and cell phone handsets will soon be (if they aren't already) PC terminals offering all the same features as their desktop counterparts.

However, there are two sides to this convergence. Just as PCs are flooded with junk mail, SMS message spam is now becoming the blight of cell phones, in addition to 'traditional' spam on phones capable of receiving emails.

When this convergence reaches the point where it is difficult to differentiate between a desktop computer and a cell phone, we will find ourselves at a very significant crossroads regarding security. Current telephone systems operate with GSM (from the mid-80s), GPRS or in the best case, UMTS (from the beginning of 2000) specification networks, but the functions on the devices are latest generation, designed 10 years later than the network.

Apart from the security of conversations (which we have seen is quite weak), cell phone terminals are also facing the problem of malware convergence. If desktop systems are flooded with huge amounts of malware, mobile systems will have to tackle these threats as directly as their larger counterparts.

Viral convergence



I'm not talking about the half-hearted attempts like Cabir or Skull which have caused more media impact than damage, but of malicious code aimed at identity or password theft or stealing any other information that could benefit hackers financially. If phishing has been successful among desktop computers, then there is no doubt that when users start to bank using cell phones, phishers will also target them. The same applies to banker Trojans, which hidden in the phone's memory, will wait until a user connects to a banking website to capture their data.

In a possible future malware scenario, there is no end to the problems that could affect latest generation cell phones with permanent broadband connections operating at several megabytes per second. The size of the malicious code could cease to be a problem, since storage cards are practically standard in new phones. Imagine a code that spreads by Bluetooth. Once installed on a phone, it could cause numerous problems:

- Access and modification of the phone directory. Perhaps just to annoy, but it could also change phone numbers, for example, an online banking number, or redirect phone calls to a premium-rate number in another country.
- Modification of connection data. Once again talking about banking phone connections... this could be just like phishing but adapted to cell phones.
- Interaction with other Bluetooth devices. Some time back, the possibility of cars being infected by Bluetooth connections was mentioned, although it was never verified. But what about printers with Bluetooth connections? Couldn't they be flooded with hundreds of sheets printed with unknown, senseless characters sent by a malicious code to the printer?
- Disruption of the cell phone's additional functions. It could be as simple and annoying as making a GPS included in the handset lead you in the wrong direction or leave you stranded in the middle of nowhere.
- Adware. A malicious code that interrupts telephone conversations to show the speakers an advert. Annoying and effective.
- Telephone Zombies. The installation of a bot on a phone, leaving the infected device under the control of the bot herder, to send spam, denial of service attacks...
- Spoofing payment and authentication systems. Cell phone payment systems, such as Mobipay, already exist. These could be affected by malware, or at least their data could be spoofed, and the same applies to credit card transaction authentication systems via mobile phones.

How far do we want to go? A code exploiting the GPS system (or simply the GSM localization functions), could be used to pinpoint the user's geographical location. We are therefore talking about a different kind of personal security issue, in which not only communication privacy is at stake, but where the phone owner's

Viral convergence



movements can be monitored. With all that data in the hands of crooks, the implications go beyond the realm of IT attacks.

Telephone operators will be able to do little in these cases. Any attempt to try to find malicious code would fail since communication would be encrypted. To try and break that encryption would be illegal, worse still; it would be futile as the danger would reside in the terminal, not in the communication.

The only way of entering malicious code in old handsets (theoretically, at least) would have been a call, a message or directly through the keyboard, all of which proved to be impossible. The phones around now can connect to personal computers via cable, infrared or Bluetooth systems, where entering code is possible and very easy.

Just go to an airport, for example (near the VIP lounge would be ideal; there will be more expensive and modern telephones) and search for Bluetooth devices. The moment I found least telephones willing to connect to my computer was during the night, when there were still no less than ten. Just imagine rush hour or at the beginning or end of vacation periods.

It is clear that threat protection is going to be a key element in cell phone terminals. And not only against viruses, but against threats that can endanger user data. And I am not talking about SD card MP3s, but of bank details. Protection will have to focus on two basic points:

- Protection of incoming files and email and multimedia messages against all kinds of malware.
- Protection of non-telephonic communications, like infrared and Bluetooth systems.

The system will have to have a very high security level, to which we will have to add the need to understand the telephone and its functions, what it does and how it does it. But in systems where the size of the documentation is bigger than the device itself, very few compulsive technology buyers are going to read the user guide apart from looking at how to change the melodies or download games.

At the end of the 80s, when the first problems due to viruses in PCs started to arise, solutions were implemented which are hardly useful nowadays. Companies that develop telephone systems and security must make a common effort so that errors committed during the 20 years of malware history are not repeated in the coming 20 months of cell phone history.

Fernando de la Cuadra
International Technical Editor
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com