The Security Challenges of Mobile Devices

In the last couple of years we have witness a silent revolution in computing and in our daily life style. Computing and electronics have gone *mobile* without us changing our security approach. Moreover, thanks to the new communication standards, mostly wireless, each piece of equipment is usually able to communicate with each other device. So how can we balance security with mobile communicating, sometimes even embedded, devices?
As we can understand from reading the news headlines, we are not doing very well. There are often news of information lost, stolen or divulged, identities stolen, break-ins etc. We do not have a comprehensive approach to this new computing architecture, which on top is massive in the sense that it is common to the consumer and business markets but obviously with different issues, numbers and consequences. Moreover we do not even have a clear idea of where we are heading and what will be the scenario in a few years since technologies and products are changing so rapidly that we have serious problems in catching up with them.

In this article we will consider various aspects of the latest mobile and embedded computing, discuss the challenges we are up to and some of the possible approaches to at least reduce the risks.

Classical Mobile Computing

We start from the oldest technology to which we are all used: laptop or portable personal computers. Laptops are not a novelty, and for example I bought my first personal laptop in 1993, so we should be used to them and we should have learned to use them in a secure way. But in the last few years two developments have changed completely the scenario of laptop security:

1. mass distribution of laptops
2. wireless communication.

Until laptops were more expensive than desktop personal computers, few people had them both in the business and consumer markets. So people who had a laptop had also special needs, and usually it was possible to adopt ad-hoc security policies for business users of portable PCs, whereas private users were often good enough to be able to deal by themselves with the security issues related to their use of the laptops. Moreover, connection to the network was wired as a desktop PC, or through dialup to the company network. The main issue was the possibility for a laptop to connect to different networks, and thus carry information and viruses from one network to the other.

Compare this situation, which at that time we already considered quite risky, to the current situation were laptops are the most common personal computers (who has today a desktop PC even just as his backup PC?) and have automatic wireless connection to the best available local network. Laptops today are the main personal computing instrument, which implies that all information, both business and personal, is stored in them. It was not like this ten years ago and this implies that the risks associated with the use of the laptops have increased just by the increase of the sensitiveness of the information stored in them. In practice, the main risks with the current use of laptops are

1. loss or theft of the laptop
2. leak of information
3. distribution of unwanted or dangerous (viral) software.

The number of laptops which are lost or stolen is, quite frankly, unbelievable: just check for the number of them lying at the deposits of airports and train stations. Often the information stored in the lost or stolen laptops is quite sensitive, either for business, personal use or even national security. If you store in your laptop all your personal information like addresses, telephone numbers, bank account numbers and PIN codes, credit card numbers etc., it becomes extremely easy to steal your money and your identity. The same applies if in your laptop are stored similar information about your company or your nation if you are a public employee.

The current approach to mitigate this risk is to encrypt the information stored on the hard-disk of the laptop. This should prevent a third person to access the information stored in the PC. Even if the cryptography used is almost always practically unbreakable, there are other issues which make this approach not as secure as we expect. First of all, often people leave their PC not turned off but in some kind of sleeping mode, which means that even if the data is encrypted on the disk, as far as one is able to access the PC without turning it off, all data can be decrypted using the key which is stored in memory, usually in a transparent way. That is, if one is able to access the PC for example as administrator without turining it off first, automatically he will be able to access all the information stored in it.

This is often not as difficult as it could seem, since passwords are always the weakest point in ICT security. (Some laptops allow authentication with fingerprint scanning which in principle should give a much higher level of security but comes with many other well known problems.)

It would be then better, each time the user stops to work on the laptop for some time, and always when he is travelling, that the laptop is actually really turned off, deleting in this way the encryption key from memory. This is of course very difficult to achieve, since turning off and on the laptop

takes always some time, while resuming from and going to sleeping mode is much faster. Indeed it is very difficult to convince users of the need, for security reasons, not to use the sleeping mode.

Moreover there have been demonstrated physical attacks on PCs where it has been possible to recover the key used for encrypting the hard-disk by a hardware analysis of the RAM. Of course these are limited, extreme and expensive techniques, but they show that disk-encryption is not the bullet proof solution to the problem of laptop loss and theft.

The fact if it is best to encrypt the full hard-disk, usually with the same password as the user or administrator of the laptop, has been discussed many times. Another approach is to encrypt only the information which are considered sensitive in a dedicated folder, with a different password than the one used to access the PC. The practical problem is that the information can be stored or copied in other areas of the PC, from temporary files used by applications, to swap files used by the operating system, to copies done by the user, so that it is usually possible to find on the PC other copies not encrypted of the same information. Keeping the sensitive information encrypted in a separated area of the hard-disk requires a substantial effort by the user, which is often impossible to ask, so full hard-disk encryption is usually adopted.

Another approach is to manage and protect sensitive information at the application level; we will discuss this in the next sections.

But loss or theft of a laptop, even if dramatic, is not the highest threat. Every day our laptop connect to many different other devices and networks, and even if by now everybody has a personal firewall on the laptop, data has to be exchanged with these devices and networks. Here you should consider not only line and wireless network connections, typically tcp/ip, but also USB and Bluetooth connection to other devices from USB disks to cameras, telephones, PDAs and whatever else. Which data is exchanged the user been willing or unwilling, between the laptop and these devices and networks? Which sensitive information leaves the laptop (even just the fact that it exists) and what enters the laptop?

This is today security endpoint nightmare and the consequences from a security point of view of having portable personal computers with sensitive information connecting automatically to a myriad of different devices, can be devastating.

Indeed some companies have decided that the management and security issues associated with laptops are at the moment too risky and expensive, and they limit as much as possible the adoption and use of laptop within the company.

Removable Devices and Storage

As we have seen, one of the new development is the fact that most electronic devices now can store information and can be used as removable storage. Up to a few years ago, a generic electronic device was usually completely embedded, which implies that its own memory was used only to store internal data for its own processing.

Today instead most electronic devices, thanks to the standardization and use of cheap off-the-shelves components, use as memory standard hard-disks, often built with solid state technology. This means that it is quite easy to offer to the user the possibility to directly use the storage in the device for other uses independent from the device itself. From this point of view it is not any more completely correct to call these devices '*embedded*' and we should probably more appropriately call them just mini-computers.

Today we can store files, document and more generically information in USB disks, cameras, telephones, technical instrument used in medical, construction, engineering etc. applications. As of today it is possible to store a file in most electronic devices, even heavy duty or micro hand-held devices for constructions, gas, electricity, measurements and so on. Most of these devices can connect to other devices using USB cables, Bluetooth, wireless LAN, Ethernet tcp/ip etc. So from a security point of view, we should assume that every possible electronic device is equivalent for example to a USB (wired) or Bluetooth (wireless) disk.

What happens when we loose a USB disk or the disk is stolen? Usually these disks are not encrypted, so all information contained can be easily retrieved by whoever has the disk. Encryption of USB disk can be mandated in some situation, but it often makes the disk unusable since its main purpose is to transfer data from one device to another, and encryption prevents exactly that. Moreover, most embedded devices do not offer the possibility of encrypting the full disk as we can do on a laptop, so we should resort to the encryption of each single file, that is protecting information at the application level.

Protecting Information at the Application Level

Some companies are trying to implement the protection of information at the application level. There are tools, usually included or as add-on to the standard document processors, which allow to encrypt the documents at the application level and to introduce granular ad-hoc policies which allow to have a very detailed control on what users can do with the document: from no access at all, to only read access, to write access subject to approval, etc. to full access.

Apart from the complexity of introducing and using such infrastructures and applications, the main problems are that often they do not solve the issues, not for technical reasons (actually they are usually very well implemented) but because users cheat them quite easily. For example it is not unusual that a document is first written in draft as a normal non-protected file, and only when almost finished is uploaded to the secure application. The final version of the document is protected, but its earlier drafts are unprotected and there have been many cases of such leaks. Similarly it is very difficult to prevent an authorized user to extract a document from the system for example to work on it off-line, again defeating the security offered by the application.

There are other approaches to the protection of documents. For example there are systems which protect information by checking that it does not leave the perimeter of the company. They usually work as follows: there is a central database in which the security manager records all documents which have to be protected and should not leave the perimeter of the company. Then on all firewalls, email servers, web servers etc. are installed components which check all data leaving the network to prevent that the documents registered in the database or documents similar to those are sent out. Since 'sending out' now means also been copied on an external disk of any kind, this means that all company desktops, laptops, telephones, PDAs etc. must be managed by this application. In today business world, this is usually almost impossible both technically and practically.

We also have to remember that information is not only stored in documents, but actually is more often stored in emails, internal web servers (wiki etc.), databases and so on, and that there are many different ways, often individual to each company, in which it can be accessed. This of course raises still more the problem of protecting it.

Preventing Intrusions from Mobile Devices

Up to here we have mostly considered mobile devices as means to obtain information, but they can be as well means of inserting information, mostly unwanted. As far as we have a disk where we can store a file, we can also store a virus. So we can infect the entire network of our company by showing our last pictures to our fellow workers. Or someone can enter in the offices of our company with a mobile phone and just faking to make a phone call, upload a trojan to a PC which allows a wireless connection.

It sounds like science fiction, but it is actually not difficult at all if there is an unprotected or not patched PC, situation which is usually normal within all companies. Indeed, as we very well know,

today most of our defences are towards connections coming on wired networks from internet, very little if nothing is done to prevent or secure local wired or wireless connections from mobile devices.

The situation is serious and we still have to understand where to draw the line between usage and security. Since we cannot prevent the use of mobile devices, we should understand how, when and what can be used and which protective measures should be implemented.

Intrinsic Security of Mobile Devices

From an overall point of view, the main problem we face is that the few security measures we can apply to laptop cannot usually be applied to mobile devices. Indeed mobile devices have often very little if no computing power. Even if they have an operating system, this is often very limited in features and power and cannot offer the security we need. In other words, we cannot apply to mobile devices in part or in full the security policies that we can apply to desktops and laptops.

Instead, to be able to manage the security of our complex ICT environments, we need to be able to deploy our security policies to all IT devices, small and large, mobile and fixed. This is today impossible and it is also difficult to see how it could be possible in the next future. We have too many different objects which interact and which we should manage in different ways. The only way out probably is to rationalize, adopt some standard and allow to connect to our ICT networks only devices which are authenticated and which satisfy our security policies.

This of course is not what we see happening today, or at least nothing is happening fast enough to give us hope for a fast solution of the problem. Consider for example smart-phones, one of the biggest nightmare of a security manager. Features overweight by far security, different protocols and network automatic connectivities are big pluses, but this means that the user cannot even be sure to which network is connected to at a certain moment and which protocol is using. Encrypting data on the hard-disk is often impossible or difficult to implement, as it is the possibility of limiting functions depending on the network to which the phone is connected and so on (of course there are very well known exceptions to this situation). On the other side, being mini-computers they are liable to bugs, which means also the possibility of viruses and all what we know it can follow.

For example, one of the biggest complains, and probably the only one real complain, on the iPhone when it has been launched, it has been its lack of security features for enterprises like disk encryption, security policies etc. (These features have been added in subsequent releases.) It should be noted that the iPhone comes from Apple which is usually believed to be a company sensitive to

IT security issues. Still time-to-market and feature-loaded are much bigger selling points than security.

Fortunately things are changing and security features are added to mobile devices, but still a long, too long way lies in front of us.

Finally, if we want to look at it from the opposite point of view, the bottom point is that today it is up to the user to protect his data in and out of mobile devices. We could say that it is the user that must be careful never to put any unprotected sensitive data on a mobile device, nor to connect a mobile device to an unknown network.

But we cannot expect that each human on the face of earth is a ICT security expert, so we definitively have some very hard times in front of us. Technology and security solutions will catch up but for the moment the biggest burden unfortunately remains not only on the security managers but also on the final users.

Andrea Pasquinucci

PhD CISA CISSP
http://www.ucci.it/