

Corporate Defence Against Dynamic Attackers

Author: Fabio Ghioni

Company: Telecom Italia Group

Address: Via Torino, 2, Milan, Italy

Phone: +39 02 8595 5616

E-mail: fabio.ghioni@telecomitalia.it

Introduction

Pervasive technology is becoming fashionable as well as useful. Everything you buy seems to have a communicating computer in it. Even the latest running shoes. What the writers of Star Trek, forty years ago, prospected for the 23rd Century, has become reality in the 21st. Captain Kirk and Mr. Spock talked through wireless ear/mouthpieces (the communicators), looked at the Universe on mega-screens, accessed data at the touch of a button or with vocal commands. It has nearly all come true. We have Bluetooth earpieces, Smartphones, touch screens, plasma mega-screens and an infinite number of other electronic utilities that are all connectable to create an ubiquitous network.

Though all this technology can be considered helpful in the chaotic and stressful world we live in, the dangers of this technology trend have to be seriously considered. As it is well known, as soon as a new product is launched on the market, the hackers and crackers bend it until it breaks and they won't be happy until they find all its breaking points. Not satisfied, they will invent all kinds of remedies for the wounded toy and this

is where the real danger lies. If, for instance, they find a new way to hack into a company's new wireless network, they can do all kinds of damage. For this reason, it is necessary that any hardware that is implemented has to be secured and protected in a proactive and continuous manner.

New Technology and its Consequences

Technology keeps evolving and becoming more sophisticated. Nowadays you can find an "intelligent" microchip in just about anything you buy, from the key ring for your house keys (that rings if you can't find it in your bag) to the shoes on your feet (the latest running shoes from Adidas sense the vibrations from the ground, and adapt the sole of the shoe so as to absorb them). In the office everything is connected, you can make calls from your pc, using the address book in your mobile phone, you can track a courier package in real time, it has a RFID tags attached, from the moment it leaves your hand to the moment it reaches its destination.

All this technology is wonderful, even if it does sometimes seem a little invasive. One of the greatest apparent advantages of the latest innovations is the fact that they occupy less and less space. The first IBM mainframes occupied entire rooms and had very limited capabilities. The latest laptops can be carried in a hand bag and come with a minimum of about 40-60 Gb of memory, they connect to everything and anything (WiFi networks have allowed man to

take an enormous step forward in this respect). You can link up to your e-mail from the airport and in certain cities around the world (where the WiFi network is sufficiently disseminated), even from your taxi or supermarket.

One of the greatest issues related to this new technology is privacy in conjunction with security. Whenever an element is added to a corporate network or is adopted by a private individual, it must comply with either corporate policies or with the individual's concept of data protection and privacy. Furthermore, security managers must endeavour to do everything possible to ensure that the network *in toto* and the individual media are resilient to possible malicious attacks from the outside. With regards to new media, such as "Mobile Always On" computers and palm pc/phones (that allow you to receive SMS, e-mails IMs on your phone with all kinds of audio/video attachments), this means that every effort must be made to screen them from attacks when they connect to the network from remote locations. The users of these media must also be aware of the added risks of WiFi technology and must take precautions such as encrypting sensitive data stored on the media.

Corporate and Real Time Instant Messaging

Another ubiquitous technology is taking over corporate communication: Instant Messaging (IM). Instant Messaging is a communications service that enables you to create a kind of private chat room

with one or more individuals, in order to communicate in real time over the Internet. Until not so long ago IM was used at home but, over the last two years, it has gradually been adopted in the work environment, with or without companies' *placet*. This also means that corporate security policies may or may not be present.

This rapid adoption of corporate IM is changing the nature of communications at work. Corporate users find the interactive nature of IM communication particularly useful for open collaborative discussions. Yet, with all its benefits, IM offers a unique challenge to the corporate security manager. Initial attempts by corporate security departments to ban or limit its use have been met with user pushback. For many organizations, IM is now a low cost productivity and collaborative tool that is integral to the work environment. The reality is that corporate IM is here to stay and security managers must learn to deal with its implications.

There are a few noteworthy reasons for which IM in a corporate environment poses such a large security issue. Firstly, today's extended IM functionality opens the corporate to a wide variety of threats. Unlike the purely text-based IM transmissions of five years ago, IM users today may link audio, video and file attachments to message transmissions. As such, IM may be exploited as a means for launching and propagating malicious attacks such as worms or trojans. Many perpetrated attacks in the recent past have taken advantage of e-mail as

a means of launching malicious code. Infection is often initiated when the user clicks on an attachment or embedded URL. With IM's extended capability for attachments as well as embedding URLs, hackers can exploit IM in a similar fashion.

Secondly, corporate IT organizations are still playing catch up with regard to secure IM policies. Many security teams have been slow in responding to this proliferation of IM. The use of IM has thus far been unregulated in many organizations and hence poorly managed. Often, users may be running older versions of IM clients that could be vulnerable to exploits. In some cases, no patch management policy is in place for IM since it is not an "official" corporate application. Users are often uneducated with regard to the risks associated with IM. Besides the risks of malicious code attachments, uninitiated users may treat IM as a secure communication medium when in fact IM communication is primarily unencrypted and can be read off the wire.

Thirdly, until now, there have been relatively few tools available for monitoring and protecting IM communication. These tools need to be able to detect malicious attacks targeted toward IM clients and servers. As IM becomes more business critical and widely used, vulnerabilities are being discovered on a regular basis and the number of security infringements is increasing exponentially.

The increase in security threats can be attributed to three major areas:

1. greater interest from virus writers based on the continued rapid adoption of instant messaging by corporate employees for business communications, often without knowledge of, or management by, corporate IT organizations
2. increased perimeter security for other attack methods such as Web access and email systems being installed by IT departments
3. Increased sophistication of attacks, including published methods that encourage copycats, multiple mutations of initial attacks and migration of new threats, such as social engineering and phishing to IM systems.

Unmanaged and unauthorized use of IM within corporate networks presents an increasingly serious threat to corporate security and must be eradicated. Probably the easiest and most simple solution is to implement a corporate IM program and totally ban all the others that may have been used by the employees.

With regards to Real Time IM, new generation telephones with "Mobile Always On" technology allow a person to continuously send and receive messages in all kinds of formats (as discussed previously). On a corporate level, this can cause several problems, even if a company allows IM with a policy approved program, a person that has a new generation mobile phone that also links into to the corporate network, can inadvertently act as a bridge for malicious attacks to the network. It is, therefore, essential that employees and collaborators (ie. Consult-

ants) are aware of the risks that they themselves run as well as of the damage they can cause to the corporate network with the incautious use of technology media.

Conclusions

As technology develops and changes, we have to follow it at the same pace. Security measures that protect the users and the owners of the new media from malicious attacks by cyber criminals, that are almost as dynamic as the evolution of the technology they attack, have to be adopted. To do so, corporations have to invest time and money in security awareness and defence measures. The latter have to be resilient in so much that they have to withstand even the most brutal attack, but they must also be sufficiently flexible to be modified in time as the nature of the attacks morph and as the components of the network change and evolve.