Wireless Technology – Considering the Benefits and the Risks

Mike Lee, Security Specialist, BT

Every so often a technology or product comes along that captures the imagination of both the private and corporate sectors. To do so it has to be simple, effective, popular and inexpensive. It also has to have productivity and usability advantages over the technology or process that it will ultimately replace.

This is the case with wireless networking. It is cheap, available and so easy to implement that many semi-technical computer users can simply install it and be productive in minutes.

It means that home PC users and corporate home workers can configure their networks when and where they want them, and not be restricted to the location of the telephone point that comes into the house.

It also means that the new philosophy of "lifestyle" working, where using open areas and coffee shops is encouraged, can be adopted and fully exploited by employees using their laptops. The productivity and usability benefits are enormous.

That's the good news. We all know the bad news. Almost every periodical or technical paper published recently has made reference in some way to the massive security exposure that these wireless networks also deliver.

Simply put, a move towards a wireless environment is a move away from a controlled, well-understood method of delivery that uses hard wires installed in a building.

A hard wired environment is well managed and relatively easy to control access to. The perimeters are well known and even if the network is extended over a switched public network via direct lines it remains understood and secure. The service level of the wired network could be maintained with traffic levels monitored easily, and any service outage or denial could be minimised. Even extending this network over the internet is relatively secure and the risks understood.

Wireless networking relies on the broadcast method of communication. It sends out a signal and anyone with a suitably configured receiver will be able to access and understand the information. That information is processed by the receiver, which then broadcasts a signal back to the originator.

I make no apology for talking about this technology in these simple terms because I believe that we have to understand what we are dealing with here. At a basic level, wireless is an inherently open, insecure and unreliable method of communicating. (Remember the original mobile phone when compared to land lines?)

A lot of work has been done and even more words published on the various methods of securing wireless networks. This paper will not attempt to comment on the existing, proposed or even the theoretically possible methods of connecting these networks. History has taught us that it does not matter how technical or sophisticated the techniques become, there will always be an expert who will discover a vulnerability in the process. It is an ongoing game of catch-up – similar to the battle between car manufacturers and car thieves.

The bottom line is that any network can only claim to be secure in its current state. Whenever someone declares that they are secure and have never been hacked, I always add the word "YET" to their statement.

Even at the time of writing, some of the more accepted methods of securing or communicating data have been compromised. Consider two recent vulnerabilities. The first was the Webmail SSL protocol that was hacked by scientists at the Federal Institute for Technology in Lausanne. The second was when two Cambridge researchers published a paper detailing how a complex mathematical attack can yield an ATM PIN in an average of 15 guesses. Both of these exploits are well documented on security websites. Whether real-life attackers will ever use these vulnerabilities has yet to be seen, but the fact is that the game goes on!

There are however, very real issues to be considered by any business that wishes to use these technologies.

1. Be aware of the technical vulnerabilities.

Ensure that your security processes and managers are well aware of the exposure that these devices can cause. Even if you do not plan to use these devices in your own company you must plan to monitor any illegal or non-authorised deployment, either by misguided employees or by malicious insertion.

Remember, it would be easy for a visitor or cleaner to plug a wireless access point into a spare LAN socket that is configured for access, and then connect while sitting outside in the car.

2. Perform the Vulnerability and Risk Assessment

Any type of new process or technology should always be processed through a Business Continuity model. That is, to establish what the vulnerabilities and risk factors are when compared with the business value of that process.

A good example is when you deliver a business or mission critical process over a wireless connection. You may be able to ensure that this is totally secure (given the known vulnerabilities and methods of attack) but what happens if the wireless connection is interrupted, either by circumstantial or deliberate interruption in the airwave spectrum? The most common wireless technology uses the 2.4GHz wavelength, which is shared by many domestic and commercial devices.

An effective denial of service attack is simple to mount against a local wireless application. If it is essential that a connection be maintained, then consider a hard-wired contingency method.

See Appendix A for a vulnerability assessment check list.

3. How is the wireless network to be used?

There are many scenarios to consider when wireless-enabling an existing network. One rarely has the luxury of planning a “greenfield” network for a new office, but in that event many of these considerations are equally valid.

Any installation has to be carefully considered and audited, and some of the points below need to be considered.

a. Is the office stand-alone or in a tower block, and what other wireless installations are deployed locally?
b. Is the perimeter of the premises known and is it bigger than the wireless broadcast perimeter? (if the Wireless LAN is small and in a large complex that is secure, then the attack risk is lessened)
c. What service level of connection is guaranteed to users? (wireless broadcast speed diminishes over distance - therefore the location of Wireless Access Points (WAP) and how many users they serve is relevant)
d. Will the users have constant bandwidth requirements or will they fluctuate? (general office suite applications that have a maximum attachment or file swap size of several megabytes, internet access that maybe restricts downloads etc…)
e. As and when new video and audio products and applications arrive, what is their relevance?
f. Will the population move around according to time and needs? (a good example of this is that many users may move their laptops to a coffee area at 11:00 and expect to remain connected. This may overload a WAP)

The above list is by no means exhaustive but you will see that the considerations are very different to those in a wired environment.

Once installed there will be a bedding-in process and trust will grow in the facility. Your staff will very quickly become accustomed to using the mobile connected capability and any loss of a service, especially in critical meetings or when meeting tight deadlines, will become a big issue.

4. Wireless Networks on Mobile/Personal devices.

One important issue is the use of wireless networks by legitimate home workers. A company will go to great lengths to ensure that the remote access facility given to home workers will remain secure and maintain the integrity of the corporate data when their network perimeter is extended into the home. Generally, this means dialling-in through proprietary software that requires an authentication token or smartcard, plus a digital key or certificate on the PC to complete the secure authentication.

Many companies are going down the broadband route, which means having a PC permanently connected to the internet and then using a carrier mechanism over this to connect home workers' PCs to the corporate network.

A popular domestic solution is to have a home PC that runs the broadband connection and then network the corporate laptop to the home PC and use internet connection sharing to enable the laptop to connect to the internet. If this is hard-wired and the methods used are corporately authorised then it remains secure. However, the employee is now able to purchase the wireless components to connect the laptop and the home PC together to enable roaming within the home.

This introduces a very weak link into what may be a very secure corporate connection. It is very difficult for the IT monitoring facilities in a company to detect that this is in place and police the situation. It is for this reason that many companies are choosing to limit the type of software and hardware that can be installed on their employees' laptops in an effort to minimise the risk when new technologies are available on the market.

The final area to cover in this section is the use of laptop PCs when connecting via wireless networks. An attack exists that uses the laptop PC as an attack point. An attacker would connect to the laptop via the wireless facility and could insert a key logger or Trojan facility that could then be used to corrupt or attack the corporate network. The company security policy should cater for this but again it is difficult to police with personal mobile devices.

5. Security Considerations

Any organisation that takes its IT security seriously should invest in a security policy. This will cover many issues including the resilience and integrity of corporate networks. It is essential that any network is secure and impervious to attack from all known methods and vulnerabilities.

When installing a wireless network, it should be hardened and invulnerable according to its location and usage. This is covered above but a relevant scenario is one where a company installs a wireless LAN that uses all of the known and available security techniques and is hardened to a high degree. Once this is assessed and tested it can be released into production and used for very sensitive and maybe even mission critical applications.

It is important to remember that the surrounding wired network should be readdressed to ensure that it could not be used as a launch vehicle by which the wireless network can be attacked from within the secure environment to administer an unauthorised user onto the Wireless LAN and enable any kind of subversion. This includes ensuring that all existing wired access points are monitored and secure from illegal access.

Wireless technology in networks is certainly attractive, with mobility, productivity and in some cases cost effectiveness benefits. When correctly introduced, implemented and managed, wireless networks can greatly enhance the effectiveness of a business. There is also no doubt about their popularity and the way they can enhance customer-facing applications or retail effectiveness.

However, like any other technology, wireless technology must be correctly assessed, with its productivity benefits, security vulnerabilities and possible business continuity impacts, as well as its overall resilience being carefully considered.

Before you deploy wireless technology, first understand the risks and implications regarding: -

- The inherent vulnerabilities of broadcast technology.
- How it will be used and how quickly your business will start to rely on it.
- The benefits to personal and home use and the opposing risk to the corporate environment.
- The ever-complex war against illegal access and the way wireless technologies can introduce a weak link.

We have to choose the correct tools for the job with regard to cost, productivity and risk. To be driven solely by technological desires can hurt your business continuity and bottom line profitability.

In addition to the technical considerations regarding security, integrity and resilience, the implementation of a wireless network also includes many management and delivery issues. This paper has attempted to cover many of the issues that are covered in BT's solutions for delivering and implementing secure productive wireless networks.

See www.btglobalservices.com for more information.

Appendix A

An effective risk assessment would consider: -

The attack itself

Viability of the attack.

> This means the external knowledge of the process and the attack points.
> If it can be attacked, how easy it is to ascertain the location of the attack points and any schedules involved?

Value of the attack.

> This is the value to the attacker in terms of profit or publicity.
> Is there a benefit to anyone from attacking, apart from vandalism?
> What is the propaganda value of an attack in terms of brand damage or embarrassment to your company?

Cost of attack.

> How much would it cost to attack your site in financial and human terms?
> Will special equipment be needed and is it widely available?
> How long would it take?

Risk of the attack.

> Can the perpetrator be identified or caught while attacking?
> Are they at physical risk and does that matter?

Your possible losses

The cost of damage.

> What cost is associated with correcting the attack and resuming normal business?

Impact to your business.

> What business assets (financial and intellectual) can be lost, damaged, stolen or vandalized?
> How much business would you lose due to loss of confidence, customer loyalty, bad publicity and goodwill?

Audit and tracability

> Do you collect audit data that could be used in an investigation?
> Do you investigate 'small' incidents? If you do, this could make you a harder target.

Assess the likelihood of the attack and the cost to your business.

Then you can determine how well you want to defend the service and how much money should you spend on detection and protection.

The telecommunications services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard terms of contract. Nothing in this publication forms any part of any contract.

Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000