pentest
security assurance

Wireless Security Considerations

By John Denneny

Introduction

There have been many articles written in the popular press about wireless networks recently. The vast majority of these stories have been of a sensationalist nature, proclaiming this technology to be a security nightmare, and the users of it, totally irresponsible. In the past three months, the stories in the UK have been getting progressively bolder, naming individual companies, and providing addresses and other details to make a hackers job all the easier. Maps and co-ordinates of "low security" wireless networks are now freely available via the Internet. These progressively revealing stories are hardly surprising as each publication tries to out-do its competitors with a new angle. While the press has been getting bolder, no legal action (to my knowledge) has been brought against any of the publishers or writers of such material (internet or printed).

Even less surprising is the insistence by the manufacturers of this new technology that *their* wireless solutions are completely secure and represent no new threat to data security or integrity. I attended an IT conference last month in Harrogate (UK) aimed at Hospitals and health-care in general. Virtually every vendor had incorporated Wireless technologies as part of their solutions. Some had embraced the technology making wireless the central theme of their solution and it's easy to see why. Getting the right information to the right people in a timely and accurate fashion has always been important to the efficiency of hospitals and organisations that deal with saving peoples lives. When wireless networks are combined with increasingly smart PDAs, good application software and efficient databases, it is easy to see that the building blocks are available to help provide better patient care systems across the world. The benefits to hospitals that this technology brings are endless, and yet some hospitals and other organisations are reluctant to take the wireless step for security reasons. Of course the decision to use this technology, as is so often the case in matters such as this, has to be based on risk/benefit analysis. One thing that everyone can agree on is that this technology is here to stay.

The brief article that follows is aimed at giving a straightforward management overview of the benefits and risks of this technology, helping management to make a more informed decision about the suitability of wireless solutions.

The size of the problem today

According to IDC (November 2001) the shipments of wireless units (Access Points, desktop pc cards and laptop cards) in the US alone reached a million units per month late in 2001. In March 2002, one major manufacturer of this technology reduced its list prices by nearly 50%. The reduced cost of implementation and the flexibility that they offer combined with a list of other less obvious benefits make them an attractive proposition. The scene is set for a massive explosion in wireless technology.

As for the stories in the press, I have to say with little hesitation "It's all pretty much true". Wireless audits performed by our own consultants over the past 9 months confirm every security mangers worst nightmares. We found that more than 70% of wireless networks installed were "out of the box" with no security (not even the basic security features) turned on. The best analogy that we could come up with was to compare this to DECT cordless phones. The customer picks up the phone, takes it out of the box, plugs in his new cordless unit and reaps the immediate benefit of wireless technology. These DECT phones are widely available from the same kind of high street store (probably on shelves not too far apart) that you would expect to buy wireless network products. The point here is that the technology is so readily available, cheap and extremely easy to set up that small networks of wireless LANs are springing up within corporations without the knowledge of the IT department. Since the default installation for most manufacturers is "minimum security" (to give customers the most satisfying, works first time out of the box, experience), all of these "rogue" access points are an open invitation to the potential hacker. The situation is compounded by the fact that with limited knowledge of IT, rogue "installers" can place an access point behind the corporate firewall where little or no monitoring is turned on.

Turning our attention to the hacker for a moment we discover a whole new set of problems not previously encountered by security managers. The issue here is anonymity. In the past hackers were attacking from fixed, wired locations. Even an experienced hacker on the other side of the world has a nagging concern that the security guys protecting the system are smarter than he is. There is always a worry in the back of the hackers mind that he might be traced and brought to book over his actions. With wireless it's a whole new ball game. Imagine buying a second hand laptop from a computer fair, buying a wireless network card from a high street retailer (for cash), making a high gain aerial from a Pringle can and picking up a copy of Netstumbler or AirSnort from a fair or a friend. Now imagine that same person sitting in the centre of London surfing the web and then attempting access to "interesting files" on your servers. Lets face it he has little to loose, since the chances of identifying the hacker and then pin pointing his location are close to zero. It is this issue of anonymity which poses the greatest threat to IT security. The risk of getting caught will always be the best weapon against hackers; the same logic has applied to burglars, car thieves and tax dodgers for many years.

It isn't just the hacker that we need to analyse here. Corporations are potentially leaving themselves wide open for legal action based on a lack of due diligence leaving sensitive data open to the public. Some solicitors are convinced that legal action could be brought against corporations for failing to secure such data under guidelines set out in the Data Protection Act.

And the flip side of the coin is..

The simple message is that it doesn't have to be as bad as this. While it is certainly true that wireless networks introduce security problems, there are steps that can be taken to reduce (but not eliminate) the risk.

Newspapers seeking the latest sensationalist stories seem to promote the idea that wireless networks were created by the devil and should be shut down immediately. They fall way short of providing a balanced story since that wouldn't sell papers quite so well, and lets face it, if the paper ended the story with "And this is how to fix it…" the story would lack some of the initial impact. With the widespread use of this technology and the many benefits that it brings to workers around the world, the "turn it off" stance doesn't really help, and anyone who maintains this view will eventually be ignored.

Some of the information available to help fix some of the security threats introduced by wireless technology is widely available on the Internet. There is little point in going into the details here. A good starting point for anyone interested in the technicalities can be found at ewa-canada.com. This document by EWA in Canada (Hardening IEEE 802.11 wireless networks) provides a comprehensive and easily understood guide to managing wireless security threats and covers everything from placement of Access Points (i.e. not in your window overlooking the street) to denial of service attacks.

From a corporate point of view, the benefits of a wireless audit should not be overlooked. Wireless audits can assist with the identification of rogue access points, help to justify amendments to security policy, provide good sensible advice (much of which can be performed internally) and add to the weight of any due diligence case which might be brought against the company. If an external body is employed to provide expert assistance with matters relating to wireless networks, the corporation can legitimately reply to accusations of neglect in respect of the Data Protection Act by demonstrating that all sensible precautions were taken to protect the data.

One of the most difficult questions that organisations face once they have decided that they need expert assistance, is who to call! Wireless Security

About Pentest Ltd.

Established in 2001, Pentest Limited is a leading international provider of IT security, specialising in Web Application Security and Penetration Testing services. Pentest provides independent, practical advice to a wide range of clients across the UK, Europe, USA and Asia. For more information, or for further details about Pentest's services, please visit www.pentest.co.uk or call +44 (0) 161 233 0100.