By Alfred Loo

THE MYTHS AND TRUTHS OF WIRELESS SECURITY

Technology will never cure all wireless security ills. It will take a coordinated effort involving corporations, manufacturers, employers, and end users to fight the fight.

The recent security breach at a U.S. credit-card processing center put over 40 million accounts at risk of fraud [11]. This event was quite shocking to many of us—the day-to-day users of credit cards. We expect a financial institution of this stature to be aware of security threats and their serious consequences as it processes very sensitive and important data. An organization of such a size should be able to employ a team of security experts. Indeed, researchers in IT security are very active [5, 9], and research papers in this area are abundant. We tend to believe that security experts in consumer finance

THE STRENGTH OF A COMPUTER SYSTEM'S SECURITY IS ALWAYS MEASURED BY ITS WEAKEST COMPONENT.

In most systems, the weakest components are the end users, particularly when they are accessing the corporation's databases with wireless facilities at home.

organizations have adopted all possible measures and such breaches are highly unlikely. However, this event once again proved Murphy's Law—whatever can go wrong, will go wrong.

Organizations with fewer resources are even more vulnerable than the above-mentioned processing center. The incident is a wake-up call for every company to review its security measures. The strength of a computer system's security is always measured by its weakest component. In most systems, the weakest components are the end users, particularly when they are accessing the corporation's databases with wireless facilities at home. The reasons are simple.

- Wireless facilities for computers are fairly new for end users and there is a great deal of misunderstanding over their security features.
- Although computer facilities within the organization are protected by computer experts, connections from employees' homes are not.
- Research papers and books on wireless security are written for technical people. Most users, including some computer professionals, are not able to understand these materials.

Wireless routers have been available for several years, are extremely ease to install, and are inexpensive—most cost less than $100. A single router provides users with the following conveniences:

- It is quite common for families to have several computers, usually situated in different rooms. To share broadband communication, the installation of network cables would be a time-consuming and expensive task, depending on the distances between rooms. Wireless routers solve this problem easily.
- Users can move their computers easily around the home, as long as they remain within the coverage of the wireless signal. The computer is still able to access the Internet via the wireless facility and save hours of cable reconnection.

The Myths

A seasoned application programmer with a master's degree who uses a wireless router at home recently expressed his belief that his connection was secure. It is not. If an application programmer puts his faith in myths, we cannot expect anyone with less computer knowledge to be aware of the security problems.

In theory, nothing can be 100% safe. Indeed, even if an owner tries to protect his/her house from burglary by installing good locks, determined thieves can still break in provided they have the right equipment and enough time. If they cannot break the lock, they can break the door, or a window, or drill a hole in the wall, dig a tunnel, use explosives, and so on. However, all of these methods will take more time and make more noise. Carrying more equipment will increase the chance the thieves will be detected or even arrested before or after the task. Rational thieves will compare the costs of these methods with the estimated valuables in the house. They might decide it is not worthwhile to break into the house provided the owner has the right degree of security.

Wireless communication is very similar to this scenario. However, while many users believe their "doors," at least, are locked, the truth of wireless communication is the doors are not even closed and are actually wide open [3, 10]. Intruders can simply walk in. A wireless router user might believe the following:

- Wireless routers have been in the consumer market for several years. Many people are using them so they must be safe. There are enough security features in routers, so communications through them are automatically protected.
- It is time-consuming to hack a computer, so attackers go after corporate computers. There is nothing valuable enough in home communications to attract hackers. Users have little to lose. There will not be any serious consequences even if their transmissions are intercepted by hackers.

The Truths

Most wireless routers have some security features.

However, these features are optional and usually turned off. The installation of a router is quite easy, and the user can complete it within minutes. During the initialization process, a small installation program will ask them to type in the account name and password they use for their ISP. Users might believe they are protected by the password afterward; indeed, the account name and password are stored in the router. When the user turns on their computer, the router logs into the ISP automatically. The computer then communicates with the router directly and accesses the Internet through it. The router does not ask the computer to supply the account name and password again. As a result a hacker's computer can connect to the router without any knowledge of the account.

Hackers do not require specific hacking tools, as operating systems can find nearby routers and connect to them almost automatically. Hackers can then perform illegal operations such as hacking other computers, spreading viruses, organizing terrorist activities, and so on. They do not need to get into users' houses or plug in any cables. They might be sitting inside a car [1, 2, 6] parked on the road near a user's house. A hacker might also live next door with nothing more than a notebook computer and wireless LAN card. It is extremely difficult for users to detect this hacking process, as hackers do not need account names, passwords, IP addresses, or any identification to the ISP. It is impossible to trace them afterward.

Hacking can take place automatically if proper software is installed on the computer. For example, a hacker could leave a computer on in a van while masquerading as technicians from telephone or electricity companies. They do not need to stay in the van during the hacking processes. Antennas and amplifiers can extend the area of wireless coverage. A study [7] shows it is possible to attack a target from 20 miles away. This kind of hacking is more difficult to detect.

As the router is actually sending/receiving messages for the computers, it is impossible for the ISP to detect the number of users. This will create headaches for the users and governments. When the police come to the doors of the legitimate users, they will have a difficult time explaining what is going on. Governments will also have problems in identifying hackers from ISP records.

There is another illusion in the initiation process. Many routers have a default administrator account "admin" (with the same default password "admin"). Users can change the password or create a new account. They might believe this is another level of protection. Actually, this account is used only when users want to view or revise the settings in the router. Hackers do not need this piece of information to access the Internet through the router. This illusion only gives users a false sense of security.

As the security features are usually turned off, communications between computers and routers are transmitted in plain text. Messages can be intercepted easily. The hacker only needs an ordinary computer with a wireless LAN card to intercept the signal.

The Consequences

Many companies have developed applications that use Internet technologies as they offer many advantages. Employees can access the databases of the company with an Internet browser. Naturally, employees can also access the systems with their home computers so they can continue to work at home.

Such advantages are accompanied by additional risks. Many systems rely on only account names and passwords to authenticate users. If a hacker can obtain this information while a user is accessing corporate databases, every security feature installed by the corporation will fail and the unauthorized intrusion will go undetected.

Some corporations protect their log-in pages with SSL or similar techniques. Such traditional methods for wired communication can also be effective for wireless networks. The transmissions are encrypted if the corporation is using such techniques. Users might believe that further encryption is not necessary. However, they will also access Web sites that do not require high levels of security, and a patient hacker can obtain hints from these non-secured communications. For example, a user might use their favorite car model as a password. This word could be found in their communications as they frequently search for information about this model from the Internet.

It is common for users to have multiple accounts. Many Web sites providing free information also ask their readers to create new accounts. As these Web pages do not involve any money or confidential information, encryption techniques might not be used.

In theory, users should use different passwords (and account names) for different accounts. In practice, many people use the same password for multiple purposes as it is extremely difficult to remember all accounts and passwords. If account names and passwords are intercepted in unsecured transmissions, hackers can spoof users and break into company databases.

Even if users do use different passwords, it is still dangerous not to protect passwords for non-secured

SECURITY WILL NEVER BE PERFECT as hackers can always find new methods to crack systems.

Web sites. By analyzing user communications, hackers can detect patterns in the composition of passwords. It is difficult for people to remember a combination of characters and numbers that have no meaning. A common practice is to take words and numbers that are familiar and combine them.

For instance, a user might choose the first four characters of his son's name (for example, "davi" from "David"), combined with the year of his son's birthday (say, 1992). To make it a little more difficult to crack, the user reverses the order so the final password is 2991ivad. This password is not bad because it is easy to remember and it does not use a complete word from a dictionary. However, an assiduous hacker will find out the pattern if the password can be intercepted. The hacker can then try the user's corporate account with his daughter's name and year of birth (by adding or subtracting a small number from the 1992 in the example). If this does not succeed, the hacker can try the name of the user's wife, or something similar. Hackers can obtain these pieces of personal information by monitoring the communications of the user and his family members. In other words, such information could help to minimize the number of trials needed to break into a computer system.

By eavesdropping on user communications, hackers can find out the users' favorite or frequently used words and Web sites. This kind of information can also speed up the hacking process. Thus, it is important to encrypt all communications even when there is no confidential information in Web pages.

Finding the executives of a target corporation is also easy. The names of executives can be found on their company Web sites. Sometimes there are even photos and brief biographies on the same page. Hackers can follow the executives' cars and find their residences easily. Armed with this knowledge, hackers are ready to carry out their jobs.

Corporate Responsibilities

Parents do not leave their babies in the jungle and expect them to protect themselves. Nevertheless, many organizations do not take care of the home Internet connections of their employees. The widespread use of wireless routers by employees is a threat to many computer systems.

There are many ways to attack wireless communication, so it is almost impossible to make it absolutely safe. There are also basic weaknesses in the technologies that are currently being used in most routers (for example, WEP [4, 5, 8]). However, we should force the hacker to invest more time and install more hardware/software for each attack. This will increase the hacker's risk of being caught. Corporations should urgently review their security, with the following measures easy to implement.

- Corporations should educate their employees to the risks and appropriate countermeasures. From time to time, they could offer brief seminars with materials explained in laymen's terms.
- Corporations should remind users to be vigilant and report suspected intruders to the authorities as soon as possible.
- Users should be taught to turn on the easy and common security features of their routers. These features can be deployed in a few minutes provided that the router manufacturer builds software with a good human-computer interface. It is not possible to discuss all features in this article, but the following examples should suffice.
  > Every LAN card has a MAC address. Users can store the MAC address in the router and ask it only to accept computers with the right MAC address.
  > Users should turn on the encryption feature in the router.
  > Wireless routers broadcast their Service Set Identifier (SSID) to surrounding computers. Computers need this name for proper connection to the router. The user should change this name often and disable router broadcasting. This measure will mean that hacking is more time-consuming.

> Every router comes with an administrator account that has a default password. Some users do not bother to change this password. Once hackers log into routers, they can modify the settings and/or turn off all security mechanisms. Users should change the password (and account name) to protect the settings.

- Most router installations are easy. However, some routers come with poor human-computer interfaces in the parts that activate the security features. It is difficult for users to select a good router on their own. Corporations should evaluate routers and recommend only products with good security features and human-computer interfaces. If enough corporations are offering these kinds of recommendations, it will force manufactures to pay more attention to developing these areas.
- Digital certificates and VPN should be adopted as they provide higher levels of security in the long run.

Manufacturer Responsibilities

There are flaws [5] in the current security technologies of wireless routers. Security experts are proposing new standards [4, 5] to overcome these problems, but manufacturers can improve security in the meantime. Security will never be perfect as hackers can always find new methods to crack systems. Nevertheless, the following measures could be implemented quickly and easily.

- Router manufacturers should make their products safer by turning on security features as default settings. Users should be forced to turn them off if they do not need the facilities, and they should be warned of the risks.
- Manufacturers should incorporate small resident programs that allow the checking of the number of users at a particular time. Log files should be maintained so that users can check whether there are any intruders. These programs could be executed in the user's computer or the router (if the router has enough memory).
- Once a new hacking method is discovered, it should be announced on the manufacturer's Website or through email. Updated software and/or firmware (if any) that can combat the new attack should be available for downloading from the manufacturer's Web site.

User Responsibilities

- Users must follow the security procedures of their employers. It is their duty to safeguard the system by using computers properly.
- Users should invest their time in learning how to use wireless communication safely, such as by attending seminars offered by their employers.
- Users should be vigilant at all times. For example, many computer systems display the last log-in time when users log in. These records should be checked to detect intruders.

Conclusion

Technology alone will never be able to solve all security problems. Enhancement of the coordination between employers, end users, and wireless facilities manufacturers is constantly required. Users should understand it is their obligation to protect their employers' computer systems by understanding the risks and appropriate countermeasures, and that it would be worthwhile investing their time in updating their knowledge. Employers and manufacturers should make this process as easy as possible. Indeed, common sense, constant vigilance, and up-to-date knowledge are the best weapons in the fight against hacking. C

References

1. Associate Press. Florida man charged with stealing Wi-Fi: Practice is common, but arrests are unusual. MSN, July 6, 2005; www.msnbc.msn.com/id/8489534.
2. Bangeman, G. Illinois WiFi freeloader fined US$250. *Arc Technica*. Mar. 2006; http://arstechnica.com/news.ars/post/20060323-6447.html.
3. Berghel, H. Wireless infidelity I: War driving. *Commun. ACM 47*, 9 (Sept. 2004), 21–26.
4. Chen, J., Jiang, M. and Liu, Y. Wireless LAN security and IEEE802.11i. *IEEE Wireless Commun. 12*, 1 (2005), 27–36.
5. Edney, J. and Arbaugh, W. *Real 802.11* Security. Addison Wesley, Reading, PA, 2004.
6. Leary, A. Wi-Fi cloaks a new breed of intruder. *St. Petersburg Times*, July 4, 2005.
7. Maxim, M. and Pllio, *D. Wireless Security*. McGraw Hill, 2002.
8. McCullough, J. *Caution! Wireless Networking*. Wiley, 2004.
9. Pfleeger, *C. Security in Computing*. Prentice Hall, Englewood, NJ, 2006.
10. Reuters News. *Wireless Networks Easy to Hack*. Aug. 8, 2005; www.itweb.co.za/sections/internet/2005/0508081002.asp?S=Reuters&A=REU&O=FPW).
11. Schneier, B. CardSystems exposes 40 million identities. *Schneier on Security* (June 2005); www.schneier.com/blog/archives/2005/06/cardsystems_exp.html).

Alfred Loo (alfred@ln.edu.hk) is an associate professor in the Department of Computing and Decision Sciences at Lingnan University, Hong Kong.

DOI: 10.1145/1314215.1314227