Securing Wi-Fi Networks

Hackers can decrypt and read data on a wireless link protected by built-in WEP encryption, and may even be able to access the data on a wired network through a Wi-Fi access point. The authors assess Wi-Fi network security in one city, analyze alternative security techniques, and suggest ways to secure such networks.

Kjell J. Hole
University of Bergen

Erlend Dyrnes
Ernst & Young—Bergen

Per Thorsheim
EDB Business Partner

Wi-Fi networks,[1] based on the IEEE 802.11b/g standards, have become very popular in recent years. Many users have installed Wi-Fi networks at home, and numerous corporations have added Wi-Fi access points to their wired networks, giving employees easier access to corporate data and services.

The scenario in which an employee connects to the corporate network from a home network is of particular interest. Although IT personnel control Wi-Fi access points in the corporate network, they cannot control, and are not necessarily even aware of, access points in home networks. These networks have thus given hackers new opportunities to gain unauthorized access to corporate computer systems and their data.

A review of the results of an investigation conducted to assess the security level in Wi-Fi networks in the city of Bergen, Norway, provides a context for analyzing some popular wireless security techniques and for offering suggestions on how to better protect these networks from hacking.

WIRELESS HACKING

Strictly speaking, a *hacker* is a software or hardware enthusiast who likes to explore the limits of programming code or computer hardware. However, the term more commonly refers to a person who breaks into or disrupts computer systems or networks to steal data or create havoc by uploading malicious code.

Wireless hackers specialize in Wi-Fi networks and employ a number of techniques to locate local area network nodes or *hotspots*. For example, *war-driving* involves driving through an inhabited area and mapping houses and businesses with Wi-Fi networks, usually using software on a wireless-enabled laptop.

War-walking, or walk-by hacking, involves walking through a neighborhood with a Wi-Fi-enabled personal digital assistant. PDA owners whose devices have a Wi-Fi client card can unintentionally war-walk if the operating system automatically connects the device to a Wi-Fi access point when the user passes by.

A war-walker with mischievous designs may engage in *war-chalking*—marking special symbols on sidewalks or walls to indicate the security status of nearby Wi-Fi access points. Our study indicated that war-chalking does not seem to be a widespread phenomenon in Bergen.

Wireless hackers pose a security threat because the encryption mechanism originally developed for Wi-Fi networks, known as Wired Equivalent Privacy, has been broken. In fact, it is possible to download programs to crack the encryption key on any WEP-encrypted link, as long as enough traffic is transmitted over the link. As the "Wireless Hacking Tools" sidebar illustrates, these programs are available for various platforms.

In addition, a number of books describe ways to attack Wi-Fi networks.[2-4] These books outline how to use different software tools to map wireless net-

Published by the IEEE Computer Society

works, analyze the traffic on wireless links, crack WEP keys, and determine whether other security techniques have been implemented.

If WEP is the only encryption mechanism, wireless hackers can use one of the available cracker programs to decrypt the information. They can also obtain an IP address from the Wi-Fi network and gain Internet access to upload spam, viruses, worms, or Trojan horses or to download illegal material. Many freely available hacker tools also make it possible to access data on the wired network attached to the Wi-Fi access point.

Wireless Hacking Tools

The Internet is the perfect medium for distributing wireless hacking software. Some of these programs only list the names—known as service set identities—of the discovered networks, the channels they use, and whether or not WEP is active; other programs also crack WEP keys and support packet capturing as well as packet reinjection.

Wireless hacking tools are available for different platforms. Mac OS X tools for finding IEEE 802.11b/g wireless networks include KisMAC (http://kismac.com), which passively detects networks (promiscuous mode) and cracks WEP keys, and iStumbler (www.istumbler.net) and MacStumbler (www.macstumbler.com), both of which broadcast probe requests.

Linux and BSD tools include Kismet (www.kismetwireless.net), which provides passive network detection, and AirSnort (http://airsnort.shmoo.com), which passively detects networks as well as cracks WEP keys. NetStumbler (www.netstumbler.com) is a Microsoft Windows tool that broadcasts probe requests.

WI-FI SECURITY IN BERGEN

Bergen is Norway's second largest city with 235,000 inhabitants. Before our investigation, we knew little about the security of Bergen's Wi-Fi networks or the threat from wireless hackers. However, based on earlier research in Oslo, the capital, we anticipated that there would be many such networks.

Some results

To assess the security risks, we engaged in both war-walking and war-driving in three areas of interest: the city center, which contains many shops and small businesses; Kokstad/Sandsli, an area close to the airport with large businesses; and Fyllingsdalen, a location outside the city center with many large office buildings. We used these tools only to collect research data; we did not reveal the exact locations of any discovered Wi-Fi networks, nor did we break any encryption.

We found no less than 706 wireless networks in Bergen. More than 500 were in the city center. Only 244 of the 706 networks used WEP. Of course, we cannot conclude that the remaining 462 transmit in the clear, but random spot checks strongly indicated that many networks in Bergen do not utilize any form of encryption.

Figure 1 depicts our war-driving results (including a few smaller areas not discussed here). We found that a wireless network's service set identity, as shown in the map, is often the name of the owner, a street address, or the name of the company owning the network. Of the 706 networks found, 166 had default names assigned by the manufacturer.

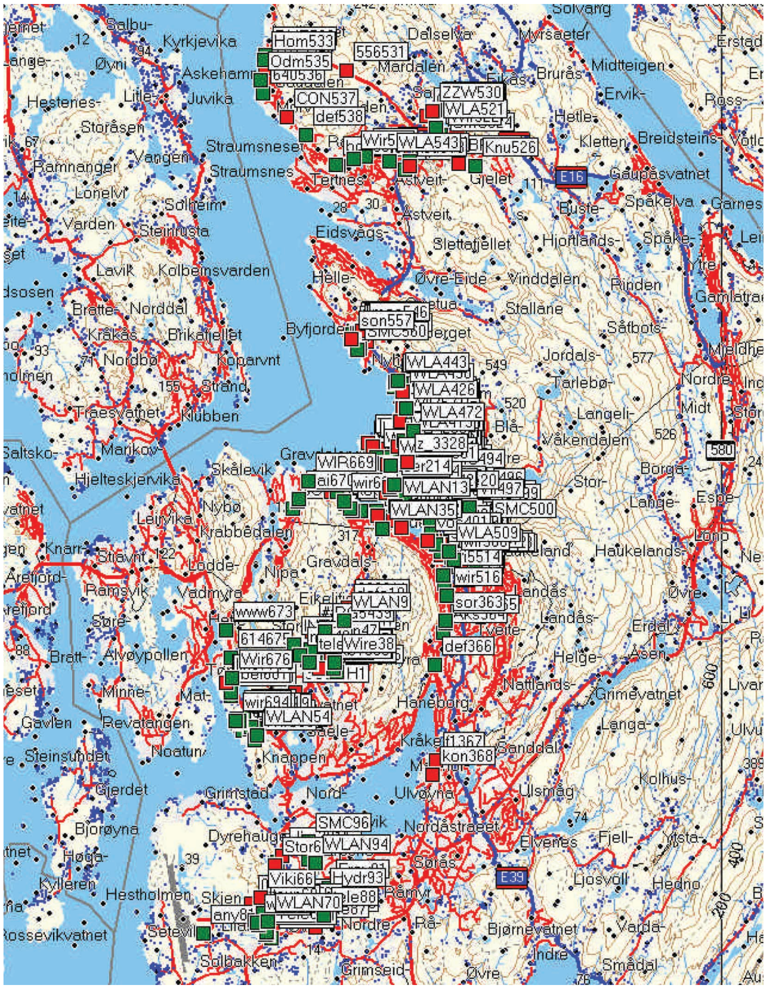

Figure 1. Wi-Fi networks in Bergen, Norway. Most of the 706 wireless networks revealed by war-driving did not use encryption.

Implications

Due to their high complexity, inevitable bugs, emergent properties unanticipated by designers, and ever-changing technologies, few people appreciate the difficulty of securing computer networks.[5] In this context, Wi-Fi is just another new technology that makes it even harder to secure a large network. From a hacker's point of view, adding a wireless extension to a wired network could make it easier to access network resources.

Cracking two packet keys should not enable an attacker to determine the session key.

Our investigation revealed not only insecure wireless networks owned by private citizens, but also company-owned wireless networks with only WEP encryption or no security at all. Many users apparently fail to recognize that radio signals from Wi-Fi devices penetrate walls, ceilings, floors, and other obstacles and that hackers can easily pick them up using standard hardware and a sniffer program.

Since numerous Web sites and readily available books detail how to crack WEP keys and extract data from Wi-Fi networks, wireless links protected by WEP alone can no longer be considered safe. Casual home users who generate little packet traffic arguably can continue using WEP for a limited time, as it can take several days to capture the one to six million packets needed to break a WEP key. Companies, however, generate considerably more traffic on wireless links and should therefore implement additional security as soon as possible.[6]

WIRELESS SECURITY OPTIONS

Several alternative security solutions to WEP are available, the most popular and useful being Wi-Fi protected access, virtual private networks, and captive portals.

Wi-Fi protected access

The Wi-Fi Alliance (www.wi-fi.org) created the interim WPA standard, which specifies security enhancements for authentication, access control, replay prevention, message integrity, message privacy, and key distribution in existing Wi-Fi systems. Applicable to home as well as enterprise users, the standard is designed to run on existing hardware as a software upgrade and is forward-compatible with the new IEEE 802.11i standard.

Features. To improve message protection, WPA utilizes the Temporal Key Integrity Protocol, which is designed to address all known attacks against, and deficiencies in, the WEP algorithm. TKIP defends against replay and weak key attacks, detects message modification, and avoids key reuse.

To improve user authentication and access control, WPA implements the Extensible Authentication Protocol (EAP) and the IEEE 802.1x standard for port-based access control. This framework uses Radius (Remote Authentication Dial-in User Service), a central authentication server, to authenticate each user on the network.

Rather than being an authentication protocol, EAP is a transport protocol tailored to the needs of upper-layer authentication protocols. It provides a plug-in architecture for numerous popular ULA protocols in use today.[3] These protocols facilitate a mutual authentication exchange between a mobile station and the Radius server residing on the network. They also generate keys for use on the wireless link between the mobile station and access point.

In a home or small office/home office (SOHO) environment, where there is no central Radius server or EAP framework, WPA runs in a special home mode, called *preshared key*, for which a user must enter a password before a mobile station can join the network. ULA is not supported in preshared key mode.

Key-scheduling flaw. WPA obtains the 128-bit *temporal key* from the EAP framework during authentication and inputs it into a key hash function together with the 48-bit *transmitter address* and a 48-bit *initialization vector*. The hash function outputs a 128-bit WEP key, or packet key. This key is used for only one WEP frame since the initialization vector is implemented as a counter that increases with each new package.

Because each package contains the initialization vector in cleartext, an attacker can obtain all utilized initialization vectors.[7] For example, let IV32 denote the most significant 32 bits of the 48-bit initialization vector. Given two WEP keys based on the same IV32, an attacker can use software to determine the temporal key. It typically takes about 30 hours to run such a program on a 2.53-GHz Intel Pentium 4, but the processing time is only six or seven minutes when four or more WEP keys based on the same IV32 are available.

WPA security relies wholly on the secrecy of all WEP (packet) keys. The attacker can determine the WEP keys based on the temporal key and decrypt all packets generated during the complete session. The attack does not imply that WPA is broken, but it underlines the importance of keeping every WEP key secret. In a well-designed system, cracking two packet keys should not enable an attacker to determine the session key. Thus, it can be said that WPA has a serious design weakness.

Interoperability problems. The Transport Layer Security protocol is the default ULA method for WPA. TLS (also denoted as EAP-TLS) is based on the Secure Socket Layer 3.0 protocol specification. SSL is a public-key, cryptography-based confidentiality mechanism.

While the Wi-Fi Alliance has recommended that all WPA products should support TLS, manufacturers can choose another ULA method. Although TLS will likely be the most popular method, using different ULA protocols creates interoperability problems between different systems. If most enterprise WPA systems use TLS, it could become the most popular ULA protocol in systems implementing the new 802.11i security standard.

Denial-of-service attacks. The goal of a DoS attack is to deny legitimate users access to a resource by disrupting or attacking the resource itself. For example, an attacker could generate numerous connection requests to a server, effectively blocking access to this server for many hours.

DoS attacks carried out at layer 2—the media access control (MAC) layer—of Wi-Fi networks exploit a management frame's lack of encryption and integrity protection even when WPA or 802.11i is utilized. An attacker can easily forge management packets and send disassociation or deauthentication packets to the mobile station or access point, thereby denying or delaying legitimate packets. Radio-frequency-based DoS attacks at a Wi-Fi network's physical layer are also possible. There are no efficient countermeasures against DoS attacks.[3]

Virtual private networks

A *virtual private network* is a security mechanism that superimposes a private network on top of a public network, such as the Internet. Most VPNs create point-to-point connections between a user and server that serve as tunnels through the public network. Various encryption techniques ensure that only the entities at each end of the tunnels can read the transmitted messages.

VPN tunnels are often used to connect employees to their company's intranet. One end of the tunnel is a VPN software client on the employee's laptop, while the other end is the VPN server software running on the company's computer. A VPN tunnel is particularly useful to an employee connecting from a Wi-Fi hotspot whose access points and wired network are outside the company firewall. After authentication, the VPN server opens a port in the firewall to give the employee intranet access through the VPN tunnel.

While WEP and WPA encrypt data only on the wireless link, VPNs keep the data encrypted all the way from the wireless-enabled laptop to the VPN server. Hence, the hotspot owner cannot read the transmitted messages.

VPN limitations. A VPN tunnel is ideal if a laptop client wants to communicate with only one server. If the client must communicate with multiple servers, however, it is necessary to establish a VPN tunnel to each server.

Another limitation is that a user who wants to browse Web sites must often turn off the VPN because most Web servers do not support it. This problem can be solved by letting all traffic from a laptop client go through a company's VPN server. To enable Web browsing, the traffic must first go through the VPN tunnel and the company intranet, before going back out on the Internet. This solution, however, might not be very efficient.

VPNs keep data encrypted all the way from the wireless-enabled laptop to the VPN server.

Incompatible implementations. The main problem with VPNs is different, incompatible implementations. Some are based on the Layer 2 Tunneling Protocol and Internet Protocol security. L2TP extends the Point-to-Point Protocol by facilitating the tunneling of PPP packets across an intervening network. IPsec provides privacy protection, integrity checking, and replay protection as well as mutual authentication through the use of client and server certificates. There also are many VPN implementations that are based on IPsec alone (without L2TP).

Other implementations are based on Microsoft's Point-to-Point Tunneling Protocol (PPTP) and one of two authentication protocols: the Microsoft Challenge Authentication Protocol (MSCHAP2) or TLS. PPTP also utilizes Microsoft Point-to-Point Encryption based on the stream cipher RC4, but it is not considered very secure.[8] Security experts maintain that IPsec-based VPN implementations offer the best security,[9] although some are vulnerable to man-in-the-middle attacks.

Many observers claim that IPsec VPNs will prevail in the long run. Others claim that IPsec is simply too complicated to install, and that simpler solutions are needed. Currently, it is not even possible to guarantee that two different implementations of IPsec VPNs will be able to communicate. Also, users having to install their own VPN clients often have problems configuring the clients.

Captive portals

A *captive portal* is a router or a gateway host that will not allow traffic to pass before user authentication.[10]

Consider the scenario in which a user with a mobile station wants to connect to a wired network through a Wi-Fi access point and the network has a Dynamic Host Configuration Protocol server. The following steps then define a portal's operation:

- let the mobile station receive an IP address from the DHCP server via a Wi-Fi link;
- block traffic, except to the captive portal server on the wired network;

- redirect any Web traffic from the mobile station to the captive portal;
- return a Web page displaying terms of use, billing information, or a login screen;
- once the user has accepted the terms, or logged in, allow access.

There are at least three different ways to use a captive portal. The first limits access to a set of known users defined by usernames and passwords, the second requires payment before service is established, and the third simply displays the terms of use before granting access.

Many portals only encrypt usernames and passwords during the authentication phase, and thus transmit all user data in the clear. Some portals do not even encrypt usernames and passwords. Many hotspot operators only use portals to obtain payment and leave it to users to protect their own data, sometimes without informing them.

Some portals only display the terms of use, and users often can access the Internet after simply entering their name. In this case, the name and unique MAC address of the user's mobile station—typically a laptop—serve as identifiers. Because all MAC addresses transmit in the clear, it is possible to determine another mobile station's MAC address and change it using a driver GUI in Microsoft Windows or the ifconfig command in Linux and BSD. Thus, a wireless hacker can get anonymous Internet access and shift the blame for any wrongdoing to others.

RECOMMENDATIONS

Unfortunately, no universal solution to Wi-Fi security problems is presently available. Both WPA and VPNs have potential, but their use often creates configuration and interoperability problems for users. It is possible, however, to draw some conclusions and offer a few recommendations.

WPA

We strongly urge both SOHO users and corporations to stop using WEP. SOHO users should upgrade to WPA in preshared key mode, as running it does not require any infrastructure. Corporations could upgrade to full WPA including use of a Radius server for authentication, but should only deploy if they plan to implement the new IEEE 802.11i security standard once it becomes available. It is therefore important to buy Wi-Fi equipment that can be upgraded from WPA to the 802.11i standard. Because WPA has some documented weaknesses, a corporation using WPA as an interim solution must keep up with WPA research.

Companies should avoid connecting access points using only WEP directly to their internal networks. Instead, they should connect all Wi-Fi access points in a wireless network to a separate wired network segment outside a firewall, and they should consider this network segment to be insecure. Companies should maintain this practice when updating to WPA. In the future, when an 802.11i security solution is available, it may be possible to connect the access points directly to the company's internal network.

The "Rogue Access Points" sidebar describes the serious security risk posed by users who buy their own access points and connect them to their company's intranet without permission.

Rogue Access Points

Because small Wi-Fi networks with only a few access points are relatively easy to install, many users have Wi-Fi networks at home. Many of these wireless network owners want to have the same wireless access at work, and the more adventurous ones buy access points on their own and connect them to their corporation's intranet without permission.

Most of these *rogue access points* are consumer grade with user-friendly default configurations and security features turned off. Unlike enterprise-class access points, which include management interfaces to the wired network and broadcast themselves when installed, rogue access points may not identify themselves on the wired network—in fact, they can be totally silent and transparent to the network administrator.

A rogue access point allows just about anyone, including a wireless hacker, to access the corporate network. Even though VPNs and firewalls control access through the authorized access points, the rogue access point can be wide open with WEP or WPA disabled.

Most employees are unaware of the risks that installing rogue access points pose. They may make no or only minimal changes to the access points' default settings. Consequently, some rogue access points can even be hidden to wired-side sniffers because they duplicate the MAC address of the employee's laptop. This duplication is the result of the mandatory configuration for some consumer-grade access points when installed on a home cable or digital-subscriber-line modem.

Consumer-grade access points often contain a DHCP server that is turned on by default. Installing a rogue access point can result in two DHCP servers on the same network segment, creating havoc. This event is likely to be discovered quickly, but discovering a rogue access point is more difficult if its DHCP server is turned off.

There are no standard techniques for finding rogue access points, but commercial tools are available for this purpose. Often, the software for detecting rogue access points is part of the platform used to manage large Wi-Fi networks. All network administrators should war-walk on a regular basis to detect rogue access points.

VPNs

A VPN can be a good security solution for a large company, especially since its IT department can preinstall VPN clients on the employees' laptops. The VPN secures the network connections from the laptops all the way to the VPN server on the company network.

It is more difficult to implement a VPN in a university or other environment where users must install their own VPN clients. Users are likely to employ multiple operating systems and OS configurations, requiring numerous VPN clients. Even if it were possible to find clients that are stable on all platforms, many users would have trouble installing and configuring them.

Captive portals

Captive portals are very useful—many hotels, for example, use them to ensure that their customers pay for wireless Internet access. However, the lack of independent analysis and quality documentation makes it hard to assess a particular solution's level of security. Because some portals offer only authentication without any encryption of passwords or user data, it is important to verify that a portal offers the required security services as well as to obtain information about its cryptographic techniques and protocols.

Hotspots

Because Wi-Fi networks make it easy for users to connect to the Internet while on the road, hotspots continue to pop up everywhere. However, as our study revealed, many of these hotspots do not support WPA. Therefore, users who want to connect to their company should use a VPN. In fact, regardless of the security a hotspot offers, a VPN is the most secure way to communicate because it keeps the data encrypted on the wired network, denying the hotspot owner any access to the transmitted information.

SSL and SSH. Wi-Fi users can use SSL and the Secure Shell protocols in a hotspot employing a captive portal with no encryption of user data. HTTPS uses SSL to enable secure access to Web pages. Some mail protocols, such as version 3 of the Post Office Protocol and the Internet Message Access Protocol, also employ SSL.

SSH authenticates and encrypts remote command-line connections; it is thus a secure alternative to rlogin. The protocol utilizes public-key cryptography like SSL but does not rely on a trusted authority to issue certificates. An SSH tunnel between a laptop and a server on the wired Internet can be used to encrypt all types of incoming and outgoing traffic. While SSL only works from program to program, SSH can connect two arbitrary ports through a tunnel. However, only users with access to a server that runs SSH can employ an SSH tunnel.

The main problem with the SSL/SSH solution is that it requires configuration of application software and SSH clients. It may not be difficult to encrypt all e-mail and Web traffic. Advanced users might be able to configure an SSH tunnel, but this is nontrivial for the average user, at least on some platforms. Of course, a corporation distributing fully configured laptops to its employees can use SSL and SSH.

Personal firewall. All Wi-Fi users should install a personal firewall on their laptops, not only to help prevent others at nearby hotspots from accessing their devices but also as part of a broad-based defense against hackers residing on other parts of the Internet.

Researchers continue to develop more robust security solutions for Wi-Fi networks. In the meantime, because IT personnel do not control access points in home networks, a wireless hacker can steal company data or upload malicious software through local machines. Companies should carefully consider this scenario before allowing employees to access corporate data through wireless devices at home or on the road. ■

References

1. M.S. Gast, *802.11 Wireless Networks: The Definitive Guide,* O'Reilly, 2002.
2. S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed: Network Security Secrets & Solutions*, 4th ed., McGraw-Hill/Osborne, 2003.
3. J. Edney and W.A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i,* Addison-Wesley, 2004.
4. L. Barken, *How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN,* Prentice Hall PTR, 2004.
5. B. Schneier, *Secrets & Lies: Digital Security in a Networked World,* John Wiley & Sons, 2000.
6. A. Engst and G. Fleishman, *The Wireless Networking Starter Kit: The Practical Guide to Wi-Fi Networks for Windows and Macintosh,* 2nd ed., Peachpit Press, 2004.
7. V. Moen, H. Raddum, and K.J. Hole, "Weaknesses in the Temporal Key Hash of WPA," *ACM Sig-*

Mobile Mobile Computing and Comm. Rev., vol. 8, no. 2, 2004, pp. 76-83.

8. B. Schneier, "Analysis of Microsoft PPTP Version 2"; www.schneier.com/pptp.html.
9. N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPsec"; www.schneier.com/paper-ipsec.html.
10. B. Potter and B. Fleck, *802.11 Security*, O'Reilly, 2003.

Kjell J. Hole *is a professor in the Department of Informatics and a member of the Selmer Center at the University of Bergen, Norway. His research interests include network security and resource management in wireless networks. Hole received a PhD in computer science from the University of Bergen. He is a member of the IEEE and the IEEE Computer Society. Contact him at kjell.hole@ii.uib.no.*

Erlend Dyrnes *is a senior manager with Ernst & Young, Bergen, Norway, where he is responsible for all IT-audit and information security advisory services. His research focuses on the technical vulnerabilities of computing platforms, operating environments, and information systems. Dyrnes holds CISA and CISM certifications from the Information Systems Audit and Control Association (ISACA). Contact him at erlend.dyrnes@no.ey.com.*

Per Thorsheim *is a security coordinator with EDB Business Partner in Bergen, Norway. He holds CISA and CISM certifications from ISACA, and CISSP certification from the International Information Systems Security Certification Consortium. Contact him at per.thorsheim@edb.com.*