CHAPTER

5

Don’t Do Secure Things from Insecure Places

Location, Location, Location…

Tom is a senior sales associate for Magnatec Inc. (MTec), a large, US-based business-to-business (B2B) electrical parts supplier. He has current customers in 42 of 50 states and the potential for customers in all 50. Not surprisingly, Tom spends a great deal of his time on the road making sales calls to potential customers and servicing current customers. MTec has assigned him the typical road warrior “tools of the trade”—a laptop, tablet, and smartphone. All of Tom’s gear is preconfigured by his corporate IT department. Tom takes advantage of Internet access wherever he happens to find himself: hotel rooms, coffee shops, customer conference rooms, fast-food restaurants, public restrooms, etc. He is totally indiscriminant and approaches the decision to use an available Wi-Fi based solely on convenience. When he finds a reliable and fast Internet connection, Tom often has four to six hours of work to catch up on. This can include entering new sales orders, sending queries to his sales team, requesting technical support, submitting receipts for per diem reimbursements, and the like. Tom is on the road roughly 150 days a year, so he’s often catching up on his personal to-do list as well. Paying bills, checking credit card statements, and sending receipts for tax purposes to his accountant are all on his list.

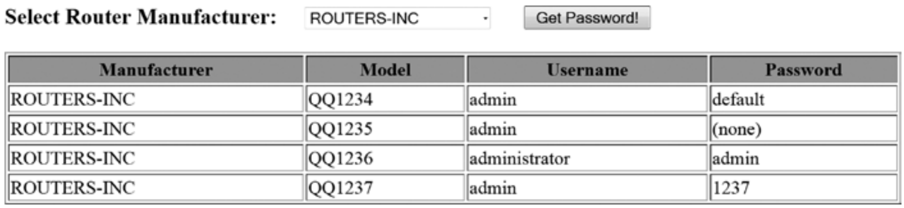
Tom spends little or no time considering the security of the wireless networks he uses. What's more, as readers are likely to have guessed from the description of his behavior, many of these networks are completely open, available to all of the customers at a coffee shop or the guests in a hotel at any given time. Recently, MTec introduced a virtual private network (VPN) service to more effectively protect company data in transit. MTec employees have been instructed to connect to the VPN when on the road and transmitting or receiving company data. Because connecting to the VPN requires a second (and separate) step, after connecting to Wi-Fi, Tom (along with many other MTec employees) often "forgets" or neglects that step. This puts employees' company data (and their personal data) at serious risk.

Background: Wireless Networking at Home, at Work, and on the Road

At this point, mid-way through 2014, most of us (even those who didn't grow up using the Internet in school or smartphones to surf the Web) are now extremely familiar with Wi-Fi, which has become very nearly ubiquitous in modern society. We use Wi-Fi at airports, train stations, universities, coffee shops, bars, hotels, restaurants, public parks, conference centers, public toilets, movie theaters, the stores where we shop, and in our homes and workplaces. We take it completely for granted. In our minds it is just there. We expect it to "just work," and most of the time it does. But even when it does "just work" how it's supposed to work in our minds, does it work for us in a safe, secure way?

Home Sweet Home…

At home, a wireless router or access point set up by a telecommunications provider (Comcast, AT&T, Charter, etc.) very likely uses a default username/password combination. Although the technician may or may not change these defaults at the time the system is installed, customers certainly should do exactly that! If not—if users just leave system settings unchanged—criminals can very easily take advantage of published and widely available default credentials to access users' home wireless network, and potentially their private data as well. Similarly, a router purchased through a retailer (from a manufacturer such as Linksys, Netgear, etc.) also has default factory-set credentials (see Figure 5-1). Customers who choose not to—or don't think to—change these credentials are putting themselves at risk.



Select Router Manufacturer: ROUTERS-INC Get Password!

Manufacturer	Model	Username	Password
ROUTERS-INC	QQ1234	admin	default
ROUTERS-INC	QQ1235	admin	(none)
ROUTERS-INC	QQ1236	administrator	admin
ROUTERS-INC	QQ1237	admin	1237

Figure 5-1. Default credentials for most brands of wireless access points and routers are freely available with a simple web search. This can be useful if a home user needs to reset a router, but it also means that users who don't reset these default passwords are vulnerable to attackers

In June 2014, Comcast ruffled some feathers with a project blurring the lines between "home" and "public" wireless networks. When subscribers to Comcast's Xfinity Internet service received new cable equipment in their home, many discovered that the device broadcasts a second, disparate wireless network called "XfinityWiFi." Comcast intends to create a nationwide network grid. This would allow Xfinity subscribers to log on to one of these wireless hotspots—though this so-called public hotspot may in reality be broadcasting from private users' homes!

Comcast allows customers to disable this feature, but the default is active. The telecom giant claims the two networks (private and public) are independent, with distinct antennas inside the hardware, and that outsiders would never have access to a customer's private devices or data. Comcast also maintains that because public Wi-Fi users have to sign in using Comcast credentials, the public users (and not the home subscribers) would be responsible for any crimes committed over the Wi-Fi network.

Despite these assurances, customers and analysts are uneasy with this arrangement. Any access, regardless of how limited it is, can be exploited. "If you're opening up another access point, it increases the likelihood that someone can tamper with your router," says Craig Young, a security researcher at Tripwire.[1]

(Using a ubiquitous public network such as "XfinityWiFi" or "ATT Wifi," so that your mobile device automatically connects to any network with that name, raises other security issues as attackers can "spoof" these network designations. We discuss this threat in greater detail in Chapter 7).

[1] CNN, Jose Pagliery, "Comcast Is Turning Your Home Router into a Public Wi-Fi Hotspot," http://money.cnn.com/2014/06/16/technology/security/comcast-wifi-hotspot/, June 16, 2014.

Back at the Office…

In the professional sphere, most large organizations maintain a default wireless policy and lock down their Wi-Fi networks. Organizations that do not maintain proper oversight can easily find employees setting up their own wireless routers, creating "rogue" Wi-Fi networks. These rogue networks may be set up by employees when the wireless signal is poor in certain parts of the plant or in an attempt to circumvent filtering (or other restrictions) often imposed on users of wireless networks. These hotspots—physical wireless access devices—can introduce vulnerabilities to the corporate network and allow outsiders (potentially criminals seeking access for financial gain or mischief) to gain entry to the system.

It is critical that corporate network administrators regularly "sniff" their network to seek out these rogue access points and remove them from the network. Administrators can use a "WIPS" (wireless intrusion protection system) to automatically detect unauthorized access points. It is also critical to encourage or incentivize employees to resist the temptation to install or to use unapproved networks. Ultimately, introducing additional points of system vulnerability isn't good for anyone except potential attackers.

On the Road Again…

Challenges to system vulnerability within the context of the actual physical plant where you work vs. when you work at a distance are quite disparate. End users on the road face an entirely different set of challenges. We are all grateful when we find an open, available wireless network with good performance—"Can I get a miracle please?" But, these networks carry risks. A network with an open login is just that—*open*. It's open to everyone. An open network might be okay for checking on baseball scores, or reading headlines. These aren't personal data with any kind of inherent value to users per se; they are public data. But an open login shouldn't be used for sensitive work or personal data because doing so makes these private data public. A secure network or VPN on top of an open network (see VPN section following) should always be used for sensitive data. Otherwise, anyone can see exactly what you'd like to keep private.

Because of the almost perpetual Wi-Fi in hotels, convention centers, airports, bars, and restaurants, modern travelers' wireless connections are the focus of this chapter. Nevertheless, the same cautions also apply with "old school" wired connections. Don't do online banking or sensitive work transactions from a desktop computer in a hotel's business center, for example. Don't assume that a wired connection in a hotel room is any more secure than a wireless connection. If improperly configured, your wired traffic can be visible to other hotel guests or employees monitoring the connection.

In July of 2014, the United States Secret Service (USSS) released an advisory to the hospitality industry concerning hotel business center devices, primarily focused on desktop computers.[2] The USSS, in conjunction with the Department of Homeland Security, warned hoteliers that attackers had been caught using "keyloggers" on the business center computers in several hotels in Texas. A keylogger is a piece of software (or more infrequently a hardware device) that captures every keystroke typed on a computer keyboard. With this software installed, a criminal can capture e-mail logins, banking information, corporate credentials, or any other information entered using the keyboard. As a basic law of survival in the cyber jungle, it is simply unsafe to use publicly accessible PCs for any purpose beyond checking the weather report or football scores. This includes machines in the public library, in university computer labs, at the airport, or anywhere else that end users don't maintain autonomous, exclusive physical control of the device(s) they're using to enter, send, or manipulate sensitive data.

Encryption Standards

In tandem with the increasing ubiquity of Wi-Fi in modern society, several sophisticated encryption methods have been developed to protect end users' data from criminals seeking to steal it. The most commonly used encryption methods are sanctioned by the Institute of Electrical and Electronics Engineers (IEEE) Standards Authorization. These methods are broadly referred to as the "802.1X" standards. The first, released in 1999, was called "Wired Equivalent Privacy (WEP)." This was by any current benchmark an extremely basic standard, employing a 40-bit key (which later was increased in size to 128-bit). By the early 2000s, serious concerns had emerged as to the protection offered through WEP, based on the relative ease with which its password (or key) could be cracked by criminals seeking unauthorized access.

Even though the IEEE officially declared WEP "deprecated" as of 2004, and the FBI demonstrated in 2005 that any WEP key could be cracked in less than three minutes using commonly available retail computers and tools available for free on the Internet, some organizations continued to use it! Users were consciously choosing to ignore evidence that their network protection was faulty. As in so many areas of our lives, including personal health, finance, and romantic spheres, denial can be a very powerful driver of dangerous behavior.

In January of 2007 the retailer T.J. Maxx—a department store chain operating more than 1,000 stores in the United States and throughout the United

[2] Krebs on Security, Brian Krebs, "Beware Keyloggers at Hotel Business Centers," http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/, July 14, 2014.

Kingdom and continental Europe—suffered a massive data breach exposing the credit card numbers of more than 45 million users to theft. A significant contributing factor underlying this breach was the attackers' access to the corporate network over the Wi-Fi in a particular store that had been using the WEP protocol. T.J. Maxx's parent corporation estimated that the breach cost over $250 million in damages.[3]

Despite substantial evidence of the inadequate protective screen offered by WEP, the Payment Card Industry (PCI), a consortium of leading banking and credit card companies, did not officially prohibit the use of the WEP protocol in financial data transmission until 2008. Perhaps most surprising here, in light of the massive security losses in which WEP had been directly complicit, existing WEP installations were "grandfathered in" until June 2010! Perhaps, to paraphrase Oscar Wilde, we really do have the power to deny anything we like.

In 2003, in response to the weakness uncovered in WEP, a "draft" version of the next IEEE 802.1X standard was released. This standard is commonly referred to as WPA, for "Wi-Fi Protected Access" (or sometimes WPA1). WPA represented a significant improvement over the older WEP protocol. WPA employed a new encryption key for each packet of data either being sent to or received by a network, rather than using a standard key for all data packets.

The new WPA protocol was embraced by savvy administrators and forward-thinking organizations aware of the weaknesses of the older WEP protocol, and applied to new web infrastructure. Older WEP routers and access points were not upgradeable to WPA technology, so organizations had to commit funds and other resources to transition their systems to WPA protection. As in the case of the widely publicized T.J. Maxx breach, many organizations delayed this upgrade in accord with the 2010 grandfather date to lower costs. The delayed transition did not go unnoticed by criminals.

In 2004, WPA2 was finalized as IEEE standard 802.11i. The emergence of WPA2 hastened the official depreciation of WEP. WPA2 used substantially stronger cryptographic keys for data encryption than previous encryption protocols. Fortunately, most WPA1 hardware was upgradeable via firmware (permanent read-only software programmed into memory) to the WPA2 standard, incurring no additional equipment costs and consequently increasing adoption rates.

In light of the widening private use of network infrastructure WPA2 was offered in two "flavors." The WPA2-Personal version was intended for home users, and employed a shared passphrase that all devices in a home or small business

[3] Boston.com, Ross Kerber, "Cost of Data Breach at TJX Soars to $256m," http://www.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/, August 15, 2007.

network could easily share across the network. The WPA2-Enterprise version was intended for much larger corporate-scale networks. In addition to a shared "encryption key" WPA2 could be configured to require an extra logon. For example, users on a corporate network using Microsoft Active Directory could be prompted for their AD (active directory) credentials to complete the Wi-Fi network logon.

In addition, modern wireless infrastructures can be configured to require "two-factor authentication," as discussed in Chapter 2. In this scenario, a password for the wireless network has to be used with a USB token, a smart card, a fingerprint scan, a code provided by a mobile app, or additional second factor.

VPN

Wireless networks can offer informed, professional users technical signals as to the level of security present in a given network, but, except in the case of home networks, the average end user can't tell what type of security a wireless network (train station, airport, hotel, coffee shop, etc.) is using. The absence of any prompt for a password, key, or other credential of course indicates that there is *no* security present in the network whatsoever! But beyond the absence of a security prompt, average users don't know if the Wi-Fi they're on is using the WEP, WPA, WPA2, or some other security protocol. In the absence of any assurances concerning wireless security, conscientious users really have only two choices.

One, don't transmit any personal, sensitive, or work-related data over that network. This isn't as easy to avoid doing as it sounds. Often times, our mobile devices are transmitting or receiving data in the "background" when they are connected to a wireless network, with no instruction from the user intentionally prompting such data transmission activity. E-mail clients check e-mail, Facebook looks for new messages, location-aware services may be using GPS, etc. Your mobile devices may be having ongoing conversations with numerous other mobile devices of which you are simply unaware—by design. We discuss "background" wireless activity in relation to mobile devices more deeply in Chapter 7.

If complete public abstinence isn't possible, a VPN (virtual private network) is the only viable option. In the universe of confusing 21st-century computing acronyms that have begun to proliferate in public discourse, VPN actually is perfectly named (see Figure 5-2). The network is "virtual." It does not require a physical connection to corporate headquarters, or a specific geographic location. The network also is "private." In a properly configured VPN, data are encrypted at both ends of the tunnel: at origin and destination. An attacker who intercepts the data stream somewhere in the middle can see only useless gibberish; nothing of value is revealed. It is also a "network." The VPN is a secure "channel" or "tunnel" that carves through the public Internet carrying private encrypted data from sender to receiver.

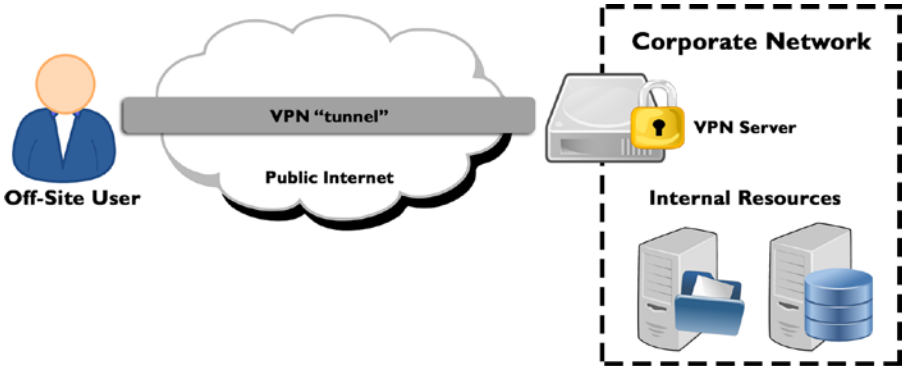


Figure 5-2. A VPN creates a private and secure "tunnel" through the public Internet

Workplace Security, on the Road

For all intents and purposes, users of a VPN should be able to do everything, with the same level of privacy and security, that they can do from their home or corporate network. Often, access to certain internal sites, databases, or file shares on a corporate network is restricted geographically, so that only devices within a certain physical distance to the server can access these resources. Universities often restrict access to online journals, or other contracted databases to users physically on campus, per the written terms of their agreements with publishers or other content providers. This kind of usage boundary often is accomplished using the Internet protocol (IP) address of the device seeking access. Here, from the standpoint of access to critical resources, an off-site device connecting via the VPN is assigned an IP address within the same range as those devices physically proximal to the university or corporate physical plant. The off-site device looks and functions via the network just as a device physically on the campus or in the building, and the user can access internal resources accordingly.

When a company mandates the use of a VPN to access corporate data or use corporate resources, the security of the user's wireless network (or even wired network, for that matter) is essentially irrelevant. If a digital resource is protected behind a VPN, users must connect to the VPN at all times whenever they are away from their physical workspace. The Internet connection type is immaterial from the standpoint of data security. VPN use isn't limited to remote users. Increasingly, organizations are beginning to use VPNs at their physical locations for certain core employees or certain critical services, as an extra step to protect their most sensitive data. Employees may not need to connect to the VPN to check their e-mail or send out a standard contract but would need to access the VPN to pull up the firm's HR database or invoice client records.

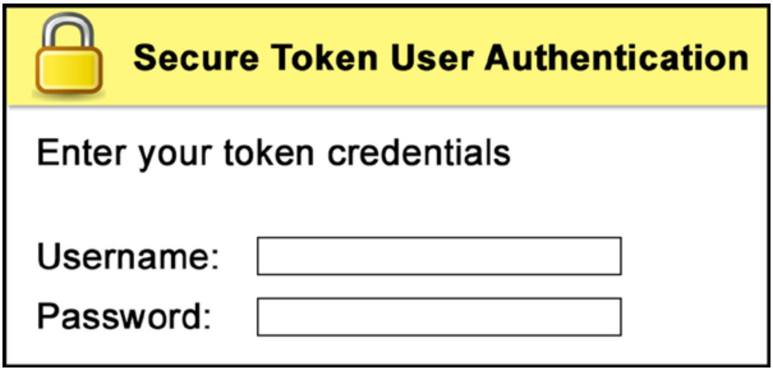
Although the use of a VPN can substantially diminish the external vulnerability associated with data sent through the pipe, interestingly, the use of a company VPN also has the potential to introduce security concerns for individual private users. An employee working away from the office connected to the VPN for work purposes may decide to send a personal non-work e-mail or execute personal financial transactions over the secure portal. In most conventional VPN configurations all of the user's traffic (work-related or other) is routed through the company's VPN server(s) while the user is connected to the network. In theory the company or other organization representatives can monitor employees' personal transactions and also access their personal credentials or other sensitive data. "Tom," from our chapter opener, didn't consistently use the VPN available to him more out of indifference or forgetfulness than anything else. But some users may approach this decision more systematically, purposefully using their employer's VPN for some but not all of their digital traffic.

This kind of inadvertent (on the user's side) internal vulnerability can emerge within what is called "full tunnel" VPN. Here, there is no mechanical segregation of data moving through the pipe. By contrast, split-tunnel VPN is designed to attempt to "intelligently" route data packets and requests. When the pipe is split, work-related packets go through the VPN server(s). Non-work-related data do not go through the protected channel, and instead are channeled through the public Internet only.

However, this kind of intelligent infrastructure is probably best thought of as being more organic in function than mechanical. Split-tunnel VPNs are at best an inexact science, and intelligent routing is far from perfect in practice. Given that both public and corporate conduits carry potential privacy liabilities, users have the option of leveraging their own VPN. Best practice in this context for end users—not withstanding issues of convenience—may be for them to connect to their corporate VPN for work-related tasks only and then reconnect to a private VPN before executing personal transactions. Yet, this can contribute to situations like Tom's, where transactions that "should" be performed over a VPN are made through vulnerable public channels. An alternative, more employer-driven approach would be for managers (or IT staff) to position all sensitive company resources behind a firewall or other infrastructure that is accessible only through the VPN. This approach simplifies the end-user decision process considerably. If someone like Tom "forgets" to connect his VPN, he won't be able to access any sensitive data!

Extra Layers of Protection

The security offered through a VPN can be enhanced when more sophisticated protocols are used to access network resources, which can include the incorporation of smart cards and tokens. As discussed in Chapter 2, increasingly, organizations are adopting a multilayered approach in what is broadly referred to as two-factor authentication. The adoption of layered protection also has become much more common for VPN connections, where users must employ a physical device (often a smart card—a credit card–sized device used to prove identity—or a USB token) in conjunction with a password to authenticate to the VPN (see Figure 5-3).


Secure Token User Authentication

Enter your token credentials

Username:

Password:

Figure 5-3. Many corporate VPN systems require two-factor authentication for login—a physical identity token or smart card and the associated PIN or password

Despite the obvious inconvenience factor associated with this more complex approach, a common rationale made for adopting a two-factor gate is that users most often connecting to firm resources through a VPN also are likely to be the "road warriors" or frequent travelers who are rarely in the office. Because of this, these also are the users most likely to lose a mobile device or have one stolen, as compared with users who work primarily in their at-work office. A stolen laptop, tablet, or smartphone, combined with a digitally stored VPN password, can allow a reasonably sophisticated thief unfettered access to sensitive company data or systems, which can have potentially lethal consequences.

Requiring employees to use a smart card or token (most of which do not allow for passwords to be saved) offers an additional line of defense that can help to thwart a potentially devastating attack. Organizations not using two-factor authentication for VPN access should be diligent in requiring employees (or other users) to immediately change their credentials in the event a device is lost or stolen.

Other Uses for VPNs

Although VPNs are most common in corporate, government, and academic environments, private end users also can benefit from the security they offer. One of the most common non-work-related applications is to disguise an end user's physical location.

For example, many live video streams, such as coverage of sporting events like the World Cup, are available only in certain countries. A stream that is just available in Germany isn't typically available to viewers in the United States. However, if an account is obtained with a German VPN provider, the sportscasting provider won't be aware of the user's true location. Game on!

Likewise, users in countries where the government filters Internet access can use a VPN to circumvent these restrictions. A user in China, for example, where Facebook is banned, may connect to a VPN to access the popular social media site. Users who leverage third-party providers (i.e., those not sponsored by their employer) should make the effort to learn their provider's privacy and security policies and not blindly trust the VPN provider with the flashiest advertising.

It's important here to remind readers what a VPN is for and what it is *not* for. A VPN can protect data in transit from snoops, and it can disguise users' physical location. While the connection between the user and the VPN is secured, the connection between the VPN provider and the user's destination may or may not be. A VPN is not designed to provide complete end-user anonymity, to prevent surveillance of browsing activities or location. We discuss methods to accomplish those goals in Chapter 6.

Additional Reading

For more on how to protect yourself in the world of Wi-Fi, see the following links, and visit our web site at `www.10donts.com/wireless`:

- ITWorld, "If Your Router Is Still Using the Default Password, Change It Now!" The author describes using published credentials to access several poorly protected routers: `www.itworld.com/consumerization-it/326421/if-your-router-still-using-default-password-change-it-now`
- WikiHow, "How to Change Your Wi Fi Password," with definitive instructions and screenshots for most common routers: `www.wikihow.com/Change-Your-Wi-Fi-Password`

- Seattle PI, "Comcast Is Turning Your Xfinity Router into a Public Wi-Fi Hotspot," describing the Comcast program and how subscribers can opt out: http://blog.seattlepi.com/techblog/2014/06/09/comcast-is-turning-your-xfinity-router-into-a-public-wi-fi-hotspot/
- Lifehacker, "Why You Should Start Using a VPN (and How to Choose the Best One for Your Needs)," a good overview of VPNs with some reviewed: http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs
- PC Magazine, "10 VPN Services You Should Know About," a comprehensive review of many leading VPN services: www.pcmag.com/article2/0,2817,2403388,00.asp