SIM2K
Adapting Technology to Your Business Needs

3•17
Information you can use

SIMformation

Wireless Mistakes to Avoid

To keep private Wi-Fi networks secure, encryption is a must-have – and using strong passwords or passphrases is necessary to prevent the encryption from being cracked. But this is just part of the security that must be incorporated into a Wi-Fi network. Many other settings, features and situations can make your Wi-Fi network as much or even more insecure as when you use a weak password. Here are some of the pitfalls SIM2K has identified as potential weak spots in Wi-Fi installations:

1. Using a default SSID or password

Your Wi-Fi network's name, called the service set identifier (SSID), can make your network less secure. If you leave the default SSID for your router or wireless access point (AP) as it set at the factory, such as "linksys," it can increase the chances of someone successfully cracking the Wi-Fi password. This is because dictionary-based cracking depends upon the SSID, and a default or common SSID makes it a bit easier. So do not use any default SSID; instead, carefully choose your own.

Keep in mind that some wireless routers with a seemingly unique default SSID – such as those that include the router's model number or serial number – can be security risks as well. This is because they may have a default Wi-Fi password that's associated with some other attribute that someone could detect by snooping on your communications.

2. Not physically securing the APs and network hardware

You could implement the best Wi-Fi security protocols in the world, and they could still easily be bypassed if someone gets physical access to your wireless access points or other network components. For instance, if you have an access point sitting on a table in an unlocked room, someone could come in as a visitor and, with the touch of a button, quickly reset the AP to factory default settings, opening up unsecured access to the network. Or if there's an open network port in the lobby or waiting area, someone could quickly plug in a rogue AP, giving himself unsecured or even secured wireless access to the network. Ensure that the main network components, including the modem, router and switch, are secured in a locked room or closet, and that the rest of the network and components are physically secure and out of reach, especially in any public areas of the building. Furthermore, consider disabling any unused wall and switch ports in public areas.

3. Having a shared Wi-Fi network password

This is mostly an issue for networks using the personal or pre-shared key (PSK) mode of Wi-Fi Protected Access I or II (WPA or WPA2) security. In a PSK setup, everyone uses the same Wi-Fi password to connect to the wireless network, so there isn't a good way to control individual user access. For instance, if an employee leaves the company or if a wireless device configured with the Wi-Fi password is stolen, the ex-employee or device thief could easily access the network. Of course, you should change the Wi-Fi password after events like this, but that can be a real hassle for you and your users. Using your network login credentials is preferable over a "one size fits all" password.

4. Using WPS PIN authentication

A feature included in most wireless routers and some business APs, called Wi-Fi Protected Setup (WPS), is supposed to make securing networks easier, but it can actually pose some serious security risks. A vulnerability in the PIN authentication method makes it easy to crack the 8 digits used and thus retrieve the password, allowing someone on the network. This vulnerability is why SIM2K relies on the enterprise mode of WPA2 security, as the WPS feature doesn't work with that mode. If that's not possible, we will disable WPS on wireless routers or APs when possible. Since the WPS PIN vulnerability was discovered in late 2011, vendors have had time to update the WPS technology to help patch this security hole; however, it's best to err on the side of caution.

5. Allowing users to connect to neighboring Wi-Fi networks

One lesser-known vulnerability is users accidentally connecting to neighboring Wi-Fi networks while in the office. The problem with this is that laptops and other wireless devices that employees connect to other networks are then vulnerable, and their data could potentially be accessed by users on that other network. Employees or their wireless devices can also be tricked into connecting to other networks if someone sets up a rogue AP, evil-twin AP, or honeypot network to perform man-in-the-middle attacks. These types of attacks can be combated by having rogue AP detection on your network and employing server verification with the enterprise mode of WPA2, as discussed above.

6. Allowing unauthorized access via misconfigured VLANs

Most wireless routers have a guest feature designed to provide visitors with access to only the Internet and maybe select portions of the local network, protecting your private network and computers. On business-class routers, switches and APs, you can emulate this functionality by configuring virtual networks and/or multiple SSIDs to drive connections to a secure network. For either method, it's wise to verify that the private network is truly secure while on the guest access.

As Wi-Fi connectivity for employees and guests grows, it is important to properly install any Wi-Fi device on a network. SIM2K will help you properly configure your Wi-Fi to avoid these and other potential problems. Call us for details.

Wi-Fi, Meet WiGig

WiGig is a relatively new wireless technology that lives in a part of the radio spectrum (60GHz) where bandwidth is extraordinarily plentiful. The FCC has allocated 14GHz of spectrum for unlicensed use representing the largest allocation ever for consumer use. WiGig will relieve congestion in the traditional Wi-Fi bands at 2.4GHz and 5GHz by giving them an alternative with 20 times more spectrum. WiGig also offers extra-wide channels for bandwidth intensive applications such as super-fast file transfer, screen sharing and virtual reality.

WiGig still faces some challenges. Radio signals at 60GHz are like flashlight beams – the signals can't penetrate walls or other solid objects. Tiny, sophisticated antennas are required to point the signals in the right direction. The WiGig antenna (a little smaller than a postage stamp) should be installed on the surface of a mobile device in a location unlikely to be blocked by the user.

Whereas Wi-Fi products operating in the 2.4GHz and 5GHz bands can communicate over longer distances and through walls, WiGig products will normally be confined to applications within a room or large open area. WiGig can deliver the high speeds and low latency required by applications such as streaming a video from a smartphone to a nearby HDTV, using a cordless VR headset, and quickly transferring content from a server to a mobile device. Plus, WiGig will enable hotspots in crowded environments, such as airports, to serve more users simultaneously.

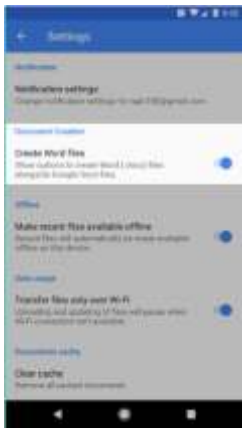
WiGig could be instrumental in the development of all-wireless environments. Office workers often use laptops, tablets, or 2-in-1 devices that they can take home or on the road. When at their desks, they want to use the larger display, local area network and various peripherals at their disposal. WiGig is the first wireless standard that can handle all of their communication needs. Dell is looking into incorporating WiGig into their docking stations eliminating the need to cable devices to it.

Conference rooms are an even more compelling use case. Users may want to connect to projectors, the office LAN and each other. WiGig would eliminate the need for cables and different types of connectors. WiGig has the bandwidth to handle all of the communication tasks simultaneously. There is one more compelling reason to use WiGig: privacy. WiGig is attractive for mission-critical applications (such as on the factory floor) because it offers exceptional bandwidth using signals that can't easily escape the building. As WiGig matures, it could even find use in smart homes. For instance, WiGig could be used within the home to remotely control smart locks, lamps and thermostats.

Given how much bandwidth WiGig offers, there is plenty of incentive to improve WiGig's performance and reduce its cost. This means we may see wide-spread adoption of WiGig as the faster speed and greater bandwidth offer exciting possibilities for IoT and traditional device communications.

Word Up, Google Docs

If you have ever looked through the settings of the Google Doc app for Android, you might find something interesting.Sitting amidst all of the app's everyday options is a quietly significant feature, disabled by default: the ability to create standard Word documents within the app with a single touch – to start a file that is in the DOCX format from the start, in other words, rather than in Google's own proprietary format.



This may not seem earthshattering, especially if your company is invested in Google Docs. But for those companies who still have ties to the Microsoft Office universe (as most business users do, at least to some extent), the presence of this option is actually pretty significant.

Google has increasingly been working to make its mobile office offering more compatible with the Microsoft Office standard. But even so, most of the previous efforts have been more like "Ok, we'll throw out a bone" and do a token compatibility with Office products. Now it appears they are finally providing a true word processing program that is Word – only on Android, not Windows.

Maybe it was just a matter of time. Or maybe it was Microsoft's offering of its own Office for Android app that forced Google into offering Word emulation in Google Docs. Either way, Google Docs for Android is clearly now aiming to exist as a non-myopic Word alternative – an app that supports the universally acceptable Word format not just as a tacked-on afterthought but as a core part of its functionality, for those who want it.

You can still create files in the native Docs format and then convert them to DOCX later, of course, but if and when you're in a position where DOCX is the expected norm, you no longer have to take that extra step.

To be sure, Google's Docs app is still nowhere near as fully featured as Microsoft's own Word app for Android. A reviewer for Computerworld tested these productivity apps and concluded that Microsoft's Android Office suite is the best overall choice for those needing desktop-level Office compatibility. As the reviewer put it, "... for those who prefer the Google productivity approach – an equally valid setup in which basic features are supplemented by outstanding systems for collaboration, sharing, and platform-agnostic interaction – interfacing with a Word-dominated world is becoming less of a hassle." So if you are a Google Docs company with Office clients, this is something to consider, especially now with many Android apps making a path over to Chromebooks, too.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Windows 7 Hangs Tough

Windows 7's decline in user share, driven for a year by desertions to Windows 10, has stalled for the last eight months, data published this month showed.

According to analytics vendor Net Applications, the user share of Windows 7 – an estimate of the proportion of the world's personal computer owners who ran that operating system – climbed by 1.2% last month to 48.4%, the highest mark since June 2016. And Windows 7 ran more Windows machines than any other edition, accounting for 52.8% of the personal computers powered by Microsoft's OS. (The difference between the user share of all PCs and only those running Windows stemmed from the fact that Windows ran on 91.8% of all personal computers, not 100%.)

Windows 7's user share dropped by almost a quarter – losing 13.7% – in the 12 months following Windows 10's mid-2015 launch. As with declines in other editions, notably Windows 8 and Windows 8.1, the beneficiary was Windows 10, whose growth rate was fueled by a free upgrade program for consumers and many businesses.

But since mid-2016, when Microsoft ended the free upgrade deal, Windows 7's user share, although fluctuating slightly month to month, ultimately stabilized. Its share of all Windows in February was 52.8% – more than July's 52.4%. During the same period, Windows 10's share increased by just 2 percentage points.

Windows 7 will be retired from support in January 2020, or just under three years from now. And while some industry analysts have contended that commercial customers are well along with plans to upgrade PCs to Windows 10, that isn't reflected in these numbers.

There was a glimmer of good news for Microsoft in the data, however. Six years ago, when Windows XP was a month shy of three years to retirement, the venerable OS boasted a user share of all Windows of 59.1%, or about 6 points higher than Windows 7's at the same distance from the end of support. Even so, unless Windows 7 marches toward retirement considerably faster than did XP – and again, there's no sign of that yet – the 2009 operating system will power a large chunk of PCs come January 2020. Windows XP ended April 2014, the month that its supported ended, on 29% of all Windows personal computers. Assuming the same closing pace as XP, Windows 7 will still be on almost one in four Windows PCs when Microsoft pulls the support plug.

SIM2K still supports Windows 7 and believes it has long life in the marketplace, as these figures show. We were never in the "upgrade now" mode when Windows 10 was released, as that made no economic sense at the time. As more and more new PCs are purchased with Windows 10 pre-installed, we have obviously moved to support this operating system as well, but for all our clients still on Windows 7, be assured we will continue to support this OS for some time now and into the future.

"Random Tid-Bytes"

Do You have a Yahoo! Account? Part 2

If your company believes it has had a data breach, it's probably a good idea to thoroughly investigate it promptly. Unfortunately, Yahoo didn't, according to a new internal investigation. Yahoo admits it knew it had an intrusion back in 2014 that affected 500 million user accounts – but botched its response. The findings were made in a Yahoo securities exchange filing, in which the company has blamed a "state-sponsored hacker" for this breach. Yahoo found that their security team and senior executives knew that a state-sponsored actor had hacked certain user accounts but even as the company took some remedial actions, such as adding new security features, some senior executives failed to comprehend or investigate the incident further. It was only about two years later when Yahoo publicly disclosed the breach. That came after a stolen database from the company allegedly went up for sale on the black market. However, after Yahoo disclosed the breach, a few months later, the company learned of an even bigger hack of 1 billion user accounts. That breach originally occurred in August 2013 but wasn't noticed until law enforcement provided Yahoo with a copy of the stolen data last November. To protect users, the company has forced password resets and invalidated forged cookies. Because of the breaches, Yahoo said the company is facing about 43 class action lawsuits.

Old School Malware Infects Google Apps

More than 130 Android apps on the Google Play store have been found to contain malicious coding, possibly because the developers were using infected computers, according to security researchers. The 132 apps were found generating hidden iframes, or an HTML document embedded inside a webpage, linking to two domains that have hosted malware, according to a security firm. Google has already removed the apps from its Play store. But what's interesting is the developers behind the apps probably aren't to blame for including the malicious code. Instead, the platforms the developers used to build these apps were probably infected with malware that looks for HTML pages and then injects the malicious coding. Some malware, such as the Window-based Ramnit, have been known to search for files on a computer and inject them with malicious coding. After infecting a Windows host, these viruses search the hard drive for HTML files and append iFrames to each document. If a developer was infected with one of these viruses, their app's HTML files could be infected. In another scenario, it's possible the app makers downloaded developer tools that were already tainted with the malicious coding. Because these 132 apps linked to two now defunct malicious domains, they actually don't pose much of a threat. It may be that whoever tampered with these apps did so accidentally. But it just goes to show that you can never be 100% safe from malware, even legacy infections.

5G Cellular Coming Up ... Fast

Today's cellular networks tout "4G" speed (for Fourth Generation) so is it a surprise that 5G is on the horizon. 4G has untethered us from our living rooms and offices, allowing us to navigate unfamiliar roads and streets using voice directions from Google Maps, stream movies on Netflix while commuting to work, and interview a prospective hire on FaceTime during a flight layover.

When Verizon Wireless rolled out 4G service in the U.S. in 2011, the term "mobile device" described handsets, tablets, and laptops. However, 6 years later the term "mobile device" has been eclipsed by "connected device" as we factor in the advances in technology including the Internet of Things (IoT). Cisco Systems estimates that by 2021 there will be 12 billion connected devices globally and approximately one-quarter of them will be cars, aerial drones, industrial robots, and other types of machines.

Industry experts believe that 5G promises to be even more transformative, because it will support communication among objects, as well as people. In a report released in January, IHS Markit, a London-based research firm, says the arrival of 5G, sometime around 2020, will elevate wireless to an elite category economists call general purpose technologies that includes the printing press and the steam engine. The study estimates that 5G will generate $3.5 trillion in economic output and 22 million jobs worldwide by 2035.

The leap will require giant increases in network capacity and data transmission speeds. Today, 4G speeds in the U.S. typically max out at about 1 gigabit per second under ideal conditions; 5G will dial that up to 10 gigabits per second. This will enable you to download a high-definition movie in less than a second, a task that takes several minutes nowadays.

Perhaps the biggest advance will be a vast reduction in latency – that is, communication lag times. Low latency is more or less a prerequisite for the commercialization of a slew of new technologies, including driverless cars, which need to ping one another multiple times per second to avoid collisions, as well as telesurgery and robotics. To shorten delays, 5G networks will have built-in processing power, store data closer to where it's needed, and run on a new swath of radio-frequency spectrum.

The changeover won't happen with the flip of a switch. An umbrella group of standard-setting agencies, 3GPP, is supposed to publish a set of draft specifications by late 2019. The U.S. and South Korea will probably launch prestandard 5G networks sooner than that.

This summer, AT&T and Verizon will each begin trials in select cities using 5G to beam movies and TV channels into homes wirelessly, competing with cable and satellite TV operators head-on. Australia and South Korea will demo their own 5G networks next year, the latter during the Winter Olympics. But the bulk of deployments will start in 2020, with carriers prioritizing cities.

In the transition, carriers, equipment makers, and others will invest a cumulative $200 billion a year, according to estimates.

Germany's luxury automakers announced in September that they were teaming up with Ericsson, Huawei Technologies, Intel, Nokia, and Qualcomm to form the 5G Automotive Association, whose mission is to help set standards and define uses for next-gen networks. Daimler, one of the association's founding members, envisions a future in which its car-sharing subsidiary, Car2go, could dispatch a driverless vehicle to pick up a customer at her home. "Connectivity is important, and we are looking forward to getting more and more information into the cars," says a spokesman for Daimler. He cautions that a network delivering consistently good coverage as you travel from one city to another "is unlikely to come into being for a long time."

In Aachen, Germany, Ericsson is testing 5G at a prototype factory where robots work at lightning speed. "You need a very fast control loop in order for the feedback of how the robot moves to be processed," says a company official.

The fast-growing drone industry is also eagerly awaiting the advent of 5G. Most unmanned craft store video-and-mapping data from their flights onboard, then download it after landing. With 5G, drones will be able to beam high-definition video while in flight. That would allow fire departments, for instance, to dispatch a drone to the scene of a blaze to gauge the situation. "We are moving from a world where there's thousands of aircraft with sensors on them to a world where there are millions of aircraft with data on them," says the CEO of drone maker American Aerospace Technologies. "And that data needs to be transmitted in real time or near real time."

For wireless carriers, many of which have seen annual revenue growth dip into the single digits, 5G can't come soon enough. Given the huge investments cellular companies worldwide will have to make to upgrade their networks, there are bound to be clashes over access. Wireless operators have been powerless to stop services such as Netflix and YouTube from building profitable businesses atop their infrastructure. Will they stand by as makers of driverless cars and drones do the same, or will they press for a cut of the revenue? No doubt, governments and consumer groups will weigh in with their own proposals.

New World Order

Share of the projected annual $200 billion investment in 5G by country

1 U.S.	28%
2 China	23%
3 Japan	11%
4 Germany	4%
5 U.K.	3%

GRAPHIC BY BLOOMBERG BUSINESSWEEK, DATA: IHS MARKIT

By 2030, wireless networks will need to handle up to 10,000 times more data traffic than they did in 2010. Operators need networks that can grow in line with traffic demand while using existing investments. 5G speeds will certainly open up new possibilities for data transfer on top of, hopefully, improved voice transmissions. How fast this new ... fast ... service is implemented remains to be seen, but development is certainly moving forward quickly.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com