Examining the Security of Wi-Fi 6 and 5G

Stephen Orr, Distinguished Architect,
Cisco Systems

Mark Grayson, Distinguished Consulting Engineer,
Cisco Systems

Andrew Myles, Manager – Enterprise Standards,
Cisco Systems

Contents

Abstract

Wi-Fi 6 and 5G both represent the very best of modern wireless networking technologies. Each has a variety of vital attributes that enable them to be used as part of wireless networking solutions satisfying a range of sometimes overlapping, but often different, use cases. For example:

- **Wi-Fi 6 is best for local area communications in the enterprise, industry, and the home, and increasingly in public spaces.**
- **5G is best for wide area, highly mobile applications, but increasingly for some local area use cases too.**

There are some misunderstandings about the security of both technologies, partially because of a marketing attempt to brand 5G as more secure. This is inaccurate and leads to unfortunate confusion for people who would like to make informed and accurate decisions about trade-offs between wireless systems. The reality is that Wi-Fi 6 and 5G both provide the security features necessary to serve as the basis of secure wireless communications, together and separately, well into the next decade.

To help better understand the security of both technologies, this paper takes a deeper dive into the security journey of 5G and Wi-Fi 6 since their birth over two decades ago. It concludes that, while the resulting security architectures of 5G and Wi-Fi 6 are slightly different, they are the result of a journey in which both technologies started with very limited security and ended with both incorporating many similar security advancements. That said, Wi-Fi 6 arguably has a slight advantage today due to its use of more advanced encryption mechanisms (and greater architectural flexibility), but the reality is that both 5G and Wi-Fi 6 encapsulate modern security practices, and both are prepared to meet the security challenges of the future . . . together.

5G and Wi-Fi 6 are complementary

With the launch of both 5G and Wi-Fi 6 in 2019, considerable comparison, criticism, and conjecture have arisen as to which is the best, or most secure, wireless communication technology. Opinions are usually biased, depending on one's technology preference, vendor status, or market alignment.

Comparing Wi-Fi 6 and 5G is akin to the classic comparison of trains, planes, and automobiles. All three are modes of transportation that have a common goal of moving people and goods from point A to point B. But each mode achieves its goals in a unique way, offering different capacities, speeds, comfort, costs, and models of control. So it's up to individual customers to determine which best suits their needs at a particular time. And for many, all three transportation modes are part of the answer.

The comparison of trains, planes, and automobiles provides the basis of an analogy that can be applied to any comparison between 5G and Wi-Fi 6. Instead of considering it as a **good vs. bad** choice, we should recognize that the two technologies have evolved over multiple generations to meet the varied communications needs of their users in a variety of situations, similar to how trains, planes, and automobiles satisfy a variety of transportation needs. Cellular technologies have a long history in wide-area communications, where providing coverage for the many users over a wide area was the primary goal, but 5G now aspires to also address more local-area use cases. In contrast, Wi-Fi has dominated local-area communications but is now starting to address more challenging higher-density public access use cases. Many aspects of 5G and Wi-Fi 6 are based on increasingly similar underlying technologies. Both technologies are phenomenal in multiple dimensions, and there is no doubt that both 5G and Wi-Fi 6 will continue providing the underpinnings of the fundamental socioeconomic changes that have been enabled by wireless communications over the last two decades.

Users should view 5G and Wi-Fi 6 as complementary because they can cover multiple use cases (with some distinctly better suited to each technology) while overlapping in other use cases. It's certain they will both be used as the basis of communications well into the next decade.

The answer is the same if we focus on the security-related aspects of 5G and Wi-Fi 6. Any security evaluation needs to transcend questions of which technology uses better ciphers or authentication mechanisms or has a better architecture. Instead, we need to focus on how both of these technologies can provide users confidence that their data will be transmitted with a level of security appropriate to the use case. Users and the organizations they are working with must be confident that their data is secure and their privacy protected, whether in an office or a home—or on a train, plane, or automobile—or, more likely, when working and learning remotely.

As our daily lives become more digitized, it's no surprise that users now genuinely desire excellent security when using modern wireless communications—and they should have it. Security and privacy must now be viewed as fundamental rights in our evolving technology-centered culture, and as such, they must be protected. Thankfully, 5G and Wi-Fi 6 can help meet this need now, and future generations of 5G and Wi-Fi 6 will be designed with appropriate security to meet the ever-changing threat landscape.

Think security before it's too late

"Water shapes its course according to the nature of the ground over which it flows."
—Sun-Tzu

One of the assumptions that many people make when attempting to evaluate 5G and Wi-Fi 6 security is that they must be compared against some absolute level of security "perfection." This isn't the case, because acceptable security is impacted by the reality of the world in which we implement and use the technology.

Over the years, six of these fundamental realities have become apparent. They give us context for how security has evolved in the cellular and Wi-Fi worlds. They also help explain current 5G and Wi-Fi 6 security offerings. The six fundamental realities are:

- Security is constrained by the threats we know about (including implementation bugs) or can imagine for the near future.
- Security is typically designed after the fact and is frequently sacrificed for "time to market" considerations (or the "if it ain't broke, don't fix it" model).
- Vendors and consumers often scramble for something faster, but not something more secure (until they've been hacked).
- Most users have limited knowledge of the security details of their network connectivity.
- Once a security vulnerability is exposed, the hype cycle reaches a crescendo, and after a mad dash to fix the problem, security is again pushed to the side.
- New and better security functionality is almost always compromised by the desire for legacy interoperability (and fewer help desk calls).

These realities highlight an important fact: most users don't like to think about the many nuances of security because it can be a bit abstract and complicated. But like most things in life, when something goes wrong, they must think about it, at least briefly.

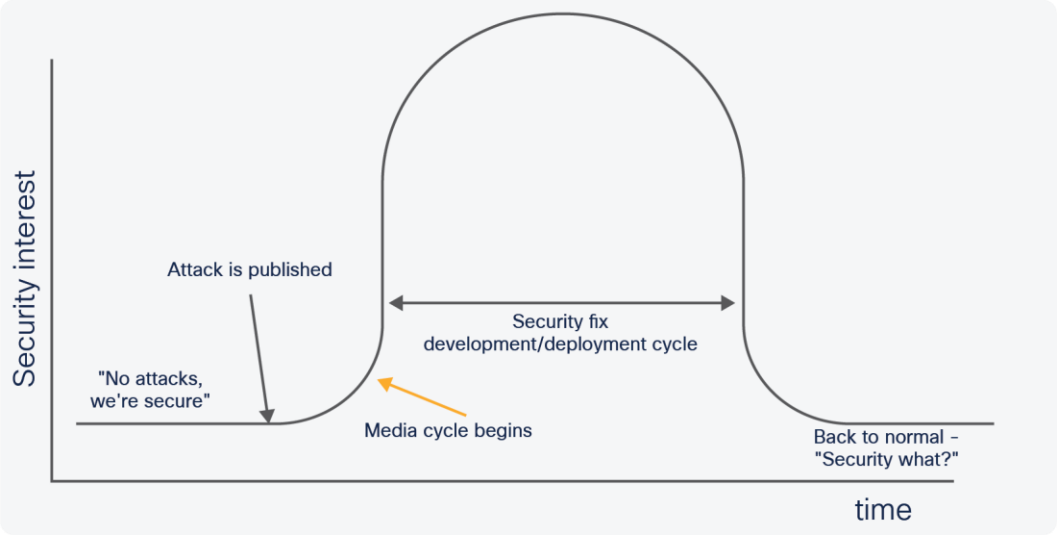

Figure 1.
Like a wave, interest in security crests and wanes over time

The good news is that both 5G and Wi-Fi 6 represent the culmination of multiple generations of development in which Cisco and other participants in 3GPP (the standards development organization for 5G) and the IEEE 802.11 Working Group/Wi-Fi Alliance (the standards development organization/international trade association for Wi-Fi 6) have responded to the evolving security requirements of their users and the threat landscape.

Wi-Fi security: An evolving response to user needs

Over the last two decades, Wi-Fi security has evolved through four main eras:

- The first era: Soon compromised (1997 to 2002)
- The second era: Fixed problems and recognized differing user needs (2002 to 2012)
- The third era: Did it "right" for over 15 years (2004 to 2020)
- The fourth era: Now in place and positioned for the future (2019 to ?).

This journey has helped Wi-Fi security meet the needs of today's users while positioning it to handle new security challenges that lie ahead.

The first era

The original purpose of Wi-Fi was to provide untethered access in enterprise networks. But there wasn't enough thought about security at the time because few people were authenticating users or encrypting traffic on a typical wired network.

However, it was soon realized that the physical security of a wired connection was greater than that of a wireless connection accessible to anyone within radio range. This led to the development of Wired Equivalent Privacy (WEP) in the IEEE 802.11 Working Group. WEP used a preshared key-based authentication/encryption mechanism that aimed for parity with the perceived security of wired networks.

Unfortunately, WEP was compromised within a few years. The resulting **WEP debacle** of the early 2000s (a life-or-death moment for Wi-Fi) actually proved beneficial for Wi-Fi because it emphasized the need for the technology to provide effective and evolving security mechanisms. The rethinking of security requirements at the time also revealed that home and enterprise users may have different security needs.

The second era

The second era of Wi-Fi security was called Wi-Fi Protected Access (WPA). It was specified by the Wi-Fi Alliance in 2002 in cooperation with the IEEE 802.11 Working Group and was a direct answer to the WEP debacle. The prestandard IEEE 802.11i amendment was used as the basis for Wi-Fi Certified WPA. This used the Temporal Key Integrity Protocol (TKIP) for encryption because "already shipping" hardware that supported WEP could readily support TKIP.

At the same time, the Wi-Fi Alliance defined two modes of operation to better align to the differing security and security management needs of Wi-Fi users:

- **WPA-Personal:** Required a passphrase (good for a typical home or small office user)
- **WPA-Enterprise:** Used an Extensible Authentication Protocol (EAP) method in conjunction with IEEE 802.1X to provide credential-based authentication (certificates, username/password, etc.) and dynamic encryption, and a network authentication server (typically RADIUS) to validate those credentials (good for the typical enterprise user)

Because WPA used TKIP, it was a security compromise, but it was intended to last only a few years, until the third era of Wi-Fi security was deployed. However, WPA turned out to be surprisingly robust, remaining effective in many use cases for far longer than anyone expected.

The third era

The third era of Wi-Fi security was called WPA2. It built upon the WPA architecture, but migrated from TKIP to the Advanced Encryption Standard with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) as defined by the IEEE 802.11i amendment. WPA2 required a hardware upgrade for most devices in order to use AES.

WPA2 proved to be very successful, maintaining a secure environment for a wide variety of use cases for over 15 years. The main problem during the WPA2 era of Wi-Fi security was the number of users who insisted on mixed modes of operation, with WPA2, WPA, and even WEP operating together. Any mixing of modes usually reduced security to the lowest common denominator. Only very recently have new attacks started to threaten some aspects of WPA2.

The WPA2 era introduced several security innovations, including:

- **IEEE 802.11r:** Enabled fast, secure roaming (certified by the Wi-Fi Alliance as part of Wi-Fi Certified Agile Multiband and Voice-Enterprise)
- **IEEE 802.11w:** Enabled protection of management frames (mandatory in all Wi-Fi Alliance certifications from July 2020)
- **IEEE 802.11u:** Enabled easy connection to networks using WPA2-Enterprise class security (certified by the Wi-Fi Alliance as Wi-Fi Certified Passpoint)

The fourth era

Recently, the Wi-Fi Alliance launched WPA3 and Wi-Fi Enhanced Open. This should position Wi-Fi for another decade of service. This period will likely span uses cases ranging from those with no security needs at all to those requiring “top secret” government-class security. Variations include:

- **Wi-Fi Certified Enhanced Open:** Addresses use cases in which open networks or networks with publicly available passwords are still being used and wireless privacy is of concern, but not authentication
- **Wi-Fi Certified WPA3-Personal:** Mitigates the known vulnerabilities when WPA2 is used with a preshared key, by using the IEEE 802.11 standardized Simultaneous Authentication of Equals (SAE) for authentication
- **Wi-Fi Certified WPA3-Enteprise:** Similar to WPA2-Enterprise, except the use of any mixed mode with TKIP is banned and the use of protected management frames is mandatory
- **Wi-Fi Certified WPA3-Enterprise-192:** So named because it provides a consistent cryptographic strength of 192 bits from EAP authentication (EAP-TLS) to over-the-air encryption using AES-GCMP (Advanced Encryption Standard with Galois Counter Mode Protocol)

Wi-Fi security will continue to address new challenges in the future

For the last twenty years, Wi-Fi security has continuously evolved to meet the needs of its users. It has allowed Wi-Fi to be safely used in homes, enterprises, public spaces, public hotspots, and high-density venues. It has also allowed a multitude of device types (smartphones, TVs, gaming consoles, laptops, etc.) and interfaces (headless, small keyboards, etc.). It achieves this goal by providing a set of tools that can be deployed flexibly in a diversity of architectures.

Secure Wi-Fi has been a powerful tool that has enabled a variety of uses, from spurring economic development and educational opportunities to helping gather a variety of data (environmental, transportation, infrastructure) to improve our quality of life. Secure Wi-Fi has also helped the various branches of the military and public safety personnel to better protect our communities. The list is endless yet not complete, as new applications continue to be created almost every day.

But there are challenges in Wi-Fi’s future. To overcome those, users must:

- **Avoid** supporting backward compatibility with previous security mechanisms for too long. Backward compatibility protects past investments, but it generally diminishes, rather than enhances, security.
- **Protect** personally identifiable information (PII) from being leaked or misused by setting client policies that prevent users from even connecting to untrusted, unsecured, and unauthenticated networks—especially for devices containing sensitive data.
- **Recognize** that Wi-Fi security is generally architecturally limited to over-the-air encryption and authentication, with the flexibility to meet varied user needs by adopting the best-in-class approach for any situation. However, this flexibility can also provide greater opportunity for successful attacks. One possibility is for the Wi-Fi community to recommend a limited number of end-to-end architectures.
- **Promote** greater ease of use for the highest levels of Wi-Fi security. Wi-Fi Passpoint is an excellent technological starting point, but it’s often difficult for network operators to deploy and for end users to use. Initiatives such as OpenRoaming (which was architected by Cisco to build on Wi-Fi Passpoint and is now being adopted by the Wireless Broadband Alliance) aims to accelerate the adoption of best-in-class security by making it easy by default.

Cellular security: A similar challenge

Like Wi-Fi security, cellular security has evolved over the last three decades:

- **1G** (analog cellular): Had no security
- **2G** (GSM): Introduced the SIM card (1991 to 1998)
- **3G**: Security shifted to mutual authentication (1998 to 2009)
- **4G** (LTE): Flattened the access network architecture (2009 to 2020)
- **5G**: Migrated away from monolithic SIM-based authentication (2020 to ?)

As a result, cellular security can serve many of the diverse needs of today's users and is in a good position to address future security challenges.

2G (GSM) security

1G provided analog-based telephony with no security. Fortunately, this fundamental flaw was recognized, and security became an integral element of 2G. The introduction of a SIM card for 2G was important for supporting critical authentication and key agreement (AKA) algorithms, as well as storing a high-entropy, secret authentication key.

2G defined only a challenge/response authentication of the SIM card and two stream ciphers:

- The **relatively** stronger A5/1 (which has been shown to have an effective key length of 54 bits).
- The **intentionally** weaker A5/2 (designed for export to certain regions). The details of A5 together with the AKA algorithms were originally confidential, an attempt at "security through obscurity."

While operators were free to use their own AKA algorithms, many used an example algorithm called COMP-128. Unfortunately, details of the example algorithm were exposed, and less than a year later an attack on COMP-128 was published that allowed derivation of the secret authentication key from a set of challenge/response pairs, enabling attackers to use the secret key to effectively clone the SIM card as well as decrypt over-the-air calls.

3G security

By 1999, the cellular community had completed the definition of its next-generation 3G system, significantly enhancing security mechanisms from 2G. With 3G, we saw the introduction of mutual authentication between the SIM card and the cellular network. It also shifted to peer review of security algorithms, including the MILENAGE algorithm set for authentication and key agreement and the KASUMI algorithm that provided 128 bits of key length for confidentiality and integrity protection.

The 3G architecture introduced a significant change: the Radio Network Controller (RNC). This was a centralized node that terminated the air interface encryption. This ensured that third parties could not eavesdrop on user communications by intercepting backhaul links from the distributed base stations, a weakness for 2G cellular voice calls.

4G (LTE) security

The advancement to 4G saw the flattening of the access network architecture. The location for terminating the air interface cipher that was centralized in the RNC in 3G was now distributed out to the LTE base station. This triggered the introduction of optional IP Security (IPsec) to protect the backhaul of base station traffic.

4G also saw the introduction of a keying hierarchy, in which a single authentication using the SIM generated a master key that was used to create a hierarchy of keys, including the keys used to protect the signaling between the handset and the core network. This master key was also used to generate the keys used by the base station (eNB) for protecting the user plane data, as well as for radio resource control signaling, and a set of keys for protecting subsequent "next hops." These keys are used to deliver so-called "forward security," in which knowledge of the current keys used between a base station and device cannot be used to guess the keys used between the same device and a future base station. In addition, 4G introduced the 128-bit AES security algorithm (in counter mode) that is mandatory for all equipment to support.

Earlier 2G and 3G systems were built on a foundation of SS7-based signaling. However, no security is integrated into SS7 because it was originally assumed that it would run only on "closed" networks, making the mobile network vulnerable to several attacks. Significantly, 4G saw the introduction of IP-based Diameter signaling used to transport authentication and authorization information between network elements.

5G security

As 5G comes on the scene, a 3rd Generation Partnership Project (3GPP) study[1] has already concluded that it may need to support 256-bit algorithms in the future, even though the current release has already adopted the same security algorithms as LTE (128-bit AES). A key positive of 5G is that it sees changes related to privacy; previous generations of cellular systems freely exposed a user's permanent identity, their International Mobile Subscriber Identity (IMSI), to any querying network. This has led to the development of so-called "IMSI catchers," devices that can be used to track mobile phones based on their IMSIs. 5G addresses this issue, defining the hashing of parts of the user's IMSI to generate a Subscription Concealed Identifier (SUCI) that is signaled to networks during authentication.

5G also sees a departure from the reliance on a single approach to authenticating all users onto the network based on SIM cards. This reliance on a single authentication type is now seen as a hindrance to 5G aspirations to address new use cases (such as the Industrial Internet of Things [IIoT] and wireless enterprise access). 3GPP has addressed such shortcomings, with 5G now integrating the EAP framework, first adopted by Wi-Fi into WPA-Enterprise back in 2002, into its architecture. The 5G standard now provides examples of how to use EAP-TLS certificate-based authentication in 5G, as well as other EAP methods that support mutual authentication.

[1] 3GPP 33.841.

5G security will continue to address new challenges in the future

For the last thirty years, cellular security has continuously evolved to meet the needs of its users, including those in the private sector. This has included accommodating the ever-increasing demands for faster data speeds as well as the broadening of service offerings from consumer-centric mobile broadband. Cellular security can also support the massive machine-type communications needed for the IIoT, as well as the ultra-high-reliability and ultra-low-latency services required to support production-critical industrial processes.

5G is now targeted at delivering a common, secure, and extensible architecture that can support many types of communications services, with significantly differing traffic characteristics. 5G security addresses a broad set of requirements and threats directly with an end-to-end architecture, covering not only aspects related to the radio access network, but also issues related to handling of sensitive material within the device. This includes credential provisioning, network slicing security, and securing of the signaling exchanges between network functions.

From a security interworking perspective, 5G deployments in the future will need to better accommodate roaming scenarios in which the service being delivered by a roaming partner may not align with the latest revision being used by the home operator. Moreover, irrespective of whether the system supports the latest revision, deployment scenarios may require the 5G system to support active-mode handover and idle-mode reselection to legacy systems. These requirements open the system to masqueraders that could facilitate attacks against devices by attempting to trigger the latest device to connect to older-generation cellular technology that uses weaker security.

Both 5G and Wi-Fi 6 will address the evolving threat landscape

5G and Wi-Fi 6 deliver a simple, flexible, scalable, secure, and extensible architecture. Both feature high overall efficiency that can support a myriad of communication services with significantly differing traffic characteristics. They have reached this point after a multidecade journey:

- Both cellular and Wi-Fi started many years ago, with no effective security.
- Wi-Fi focused on over-the-air security, with the flexibility to be deployed in a wide range of end-to-end security architectures.
- Cellular security tended to focus on end-to-end security, with a recent transition to increased flexibility, often based on mechanisms used by Wi-Fi.
- Both cellular and Wi-Fi have evolved to include many features that improve their overall security, including better encryption and authentication mechanisms.

In many respects, the evolution by both technologies means 5G and Wi-Fi 6 security is effectively equivalent. The main difference is that Wi-Fi 6 is slightly more flexible in how it can be incorporated into end-to-end architectures while 5G is more locked down. But even this difference is diminishing, as 5G has adopted some of the flexibility mechanisms inherent in Wi-Fi 6. The recent introduction of WPA3, including 192-bit encryption, arguably puts Wi-Fi 6 slightly ahead in the short term.

With the threat landscape continually evolving, it is accepted that further enhancements to the security capabilities of both 5G and Wi-Fi 6 will be regularly required. Both the 5G and Wi-Fi 6 security architectures are well positioned to respond to this evolving threat landscape without having to wait for a “forklift upgrade” during the next generation. Waiting would be an unacceptable price, given the typical generational cadence of 7 to 10 years.

In the nearer term, 5G and Wi-Fi 6 will soon need to address the security implications of transmitting messages such as beacons and other system information messages. Doing so allows over-the-air attackers who broadcast rogue beacon or system information (SI) messages, or replay previously recovered messages, to influence a device's operation. It's likely the necessary changes will be achievable in software.

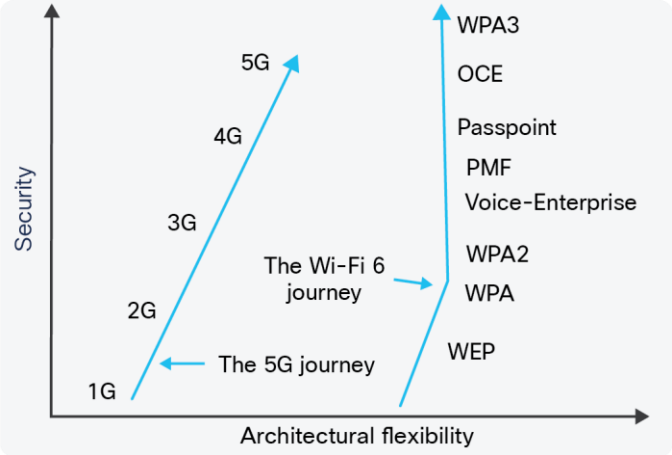

Figure 2.
The end points of the 5G and Wi-Fi 6 security journeys are similar

Network slicing and segmentation is seen as a critical new capability in 5G and Wi-Fi 6 networks, enabling slices/segments to be optimized for different requirements. Slicing is likely to introduce new threat vectors as common functions are shared between multiple stakeholders, especially if slices can be managed by third parties. Again, it's likely that 5G and Wi-Fi 6 are well architected to adapt as the threats from this mode of operation are better understood.

One of the more significant future threats to both 5G and Wi-Fi security is the possible arrival in the next twenty years of effective quantum computers that will enable fast and efficient code breaking. The ability to introduce new quantum-safe ciphers and key derivation algorithms with increased key lengths is now a baseline requirement for any security architecture.

Finally, whereas conventional cellular systems are primarily deployed using a limited number of outdoor macro-base stations, the advent of 5G is anticipated to see the introduction of a massive number of small 5G base stations (to a density that approaches that of Wi-Fi access points). This will expose 5G to the same types of attacks that Wi-Fi has experienced for many years, since deployment will be in areas where physical security cannot be guaranteed (rogue access point attacks). This might be another area where security for 5G can leverage the experiences of Wi-Fi.

5G and Wi-Fi 6: Partners in security

Our discussion has largely focused on the roughly parallel evolution of 5G and Wi-Fi 6 security over the last two decades. We've seen that both 5G and Wi-Fi 6 contain many similar security mechanisms, but with slightly different architectures. Also, we now understand that Wi-Fi 6 is more flexible and has slightly better encryption as of today, but that both 5G and Wi-Fi 6 can address current needs while being flexible in adapting to future threats.

Just as people use trains, planes, and automobiles in various combinations to reach an end goal, the complementary natures of 5G and Wi-Fi 6 will allow users to leverage the best attributes of both technologies. Unlike trains, planes, and automobiles, 5G and Wi-Fi 6 will be usable at the same time by a single user.

For users (or an automated path selection algorithm) that can choose between 5G or Wi-Fi 6, there will be no need to deal with abstract notions of **security** when deciding which technology to use (or which path to select). Instead, they can be confident that both wireless technologies encapsulate the best modern security practices and can work in partnership to overcome the challenges facing the future.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-743921-00 06/20