Communications Security, Reliability and Interoperability Council

CSRIC

February, 2017

WORKING GROUP 9
Wi-Fi Security

Final Report – Wi-Fi Security Best Practices

Table of Contents

1 Results in Brief

1.1 Executive Summary

Wi-Fi security is an important function and is the topic of investigation of several working groups in the industry and in the Federal government. It was the objective of the CSRIC Working Group 9 to propose recommendations on the best practices for Wi-Fi security.

In this report, the working group has proposed Wi-Fi security best practice recommendations that are supplementary and complimentary to the work of these other groups. The working group did not want to duplicate the efforts of these other groups and, especially, did not want to create best practices which conflict with the recommendations of the other groups.

Consequently, the working group has incorporated, at least by reference, the best practices from the documents of these other groups, including "Common Sense Rules for Public Venues" and best practices to deal with rogue access points.

In addition, CSRIC Working Group 9 makes the following recommendations:

- CSRIC Working Group 9 recommends that the FCC resolve the policy and legal issues regarding the ability of enterprise customers or network operators to use de-authentication to protect Wi-Fi users from legitimate cybersecurity threats.

- CSRIC Working Group 9 recommends that the business or wireless network provider implement an authenticatable network based on X.509 network identities or SIM cards, and provide a more robust registration method for short-term clients.

- CSRIC Working Group 9 recommends that a method and technology be developed that allows a client, during their registration to use a wireless network, be able to securely obtain and "pin" specific network authentication keys in their client device(s). This better protects the client from third-party trust store problems.

2 Introduction

2.1 CSRIC Structure

Table 1: CSRIC Working Group Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) V Working Groups			
Working Group 1 **Evolving 911 Services** **Co-Chairs:** Susan Sherwood & Jeff Cohen **FCC Liaisons:** Tim May & John Healy	**Working Group 2** **Wireless Emergency Alert** **Co-Chairs:** Francisco Sánchez & Farrokh Khatibi **FCC Liaisons:** Chris Anderson, James Wiley & Gregory Cooke	**Working Group 3** **Emergency Alert System** **Co-Chairs:** Steven Johnson & Kelly Williams **FCC Liaison:** Gregory Cooke	**Working Group 4A** **Communications Infrastructure Resiliency** **Co-Chairs:** Kent Bressie & Catherine Creese **FCC Liaison:** Jerry Stanshine & Michael Connelly
Working Group 4B **Network Timing Single Source Risk Reduction** **Chair:** Jennifer Manner **FCC Liaison:** Emil Cherian	**Working Group 5** **Cybersecurity Information Sharing** **Co-Chairs:** Rod Rasmussen, Christopher Boyer, Brian Allen **FCC Liaisons:** Greg Intoccia & Vern Mosely	**Working Group 6** **Secure Hardware & Software** **Co-Chairs:** Brian Scarpelli & Joel Molinoff **FCC Liaisons:** Steven McKinnon & Emily Talaga	**Working Group 7** **Cybersecurity Workforce** **Co-Chairs:** Bill Boni & Drew Morin **FCC Liaison:** Erika Olsen
Working Group 8 **Priority Services** **Co-Chairs:** William Reidway & Thomas Anderson **FCC Liaisons:** Tim Perrier & Ken Burnley	**Working Group 9** **Wi-Fi Security** **Chair:** Brian Daly **FCC Liaisons:** Peter Shroyer & Kurian Jacob	**Working Group 10** **Legacy Systems Risk Reduction** **Co-Chairs:** John Kimmins & Danny McPherson **FCC Liaison: Steven McKinnon**	

2.2 Working Group 9 Team Members

Working Group 9 consists of the members listed below:

Table 2 - List of Working Group 9 Members

Name	Company
Brian K. Daly – Chair	AT&T
Firdaus Aryana	CenturyLink
Craig Cowden	Charter Communications
Scott Craighead	International Association of Exhibitions & Events
Jon Green	Aruba, a Hewlett Packard Enterprise Company
Miles Green	Intersection (LinkNYC)

Name	Company
Mark Haley	Smart City Networks
Paul Hancock	AT&T
Jose Jiminez	Cox
Mohammad Khaled	Nokia
Sameer Khan	Sprint
Philip Levis	Stanford University
Ethan Lucarelli	Inmarsat
Robert Mayer	USTelecom Association
Brad Mayne, CFE	International Association of Venue Managers
Stephen Orr	Cisco
David E Savage	Boeing
Brian Scarpelli	ACT | The App Association
Mark S. Sims	Javits Convention Center
Jesse R. Walker	Intel Corporation
Pat Walsh	Gogo Inflight
Bing Wang	University of Connecticut

Also, DeWayne Sennett of AT&T served as Document Editor and Document Manager for the development of this CSRIC subgroup report.

3 Objective, Scope, and Methodology

3.1 Objective & Scope

This Working Group will develop, for CSRIC's consideration, recommended best practices for promoting security in networks and devices utilizing Wi-Fi spectrum bands. Security concerns threaten entities utilizing Wi-Fi devices and spectrum. Currently, enterprises utilizing Wi-Fi spectrum rely on numerous methods to secure their networks and connected devices from malicious attacks. Working Group 9 will identify, for CSRIC's consideration when, and under what circumstances, the use of a variety of advanced security techniques are appropriate. Specifically, the Working Group will identify, for CSRIC's consideration: 1) the threats most consistently facing Wi-Fi network operators and users; 2) the available security techniques to prevent and/or remediate the threats; 3) the extent to which each technique is effective against specific threats, avoids interference with legitimate activity, is easily deployed, and is currently deployed.

3.2 Methodology

The objective of the methodology utilized by the working group was to prevent any duplication of efforts with other groups that are investigating the topic of Wi-Fi security. Consequently, the working group examined the reports of other groups and incorporated, at least by reference, the best practices from the documents of these other groups. Based upon this information, the CSRIC Working Group 9 developed best practice recommendations that were supplementary and complimentary to the work of these other groups.

4 Background

This section provides background information about the security threats to Wi-Fi. Specifically, this section discusses the following topics:

- General discussion on Wi-Fi security threats.
- Identification of potential security threats toward Wi-Fi.
- Presentation of two example Use Cases – one Use Case on hotel Wi-Fi networks and a second Use Case on convention center/public venue Wi-Fi networks.

4.1 Discussion on Wi-Fi Threats

4.1.1 Background and Context

The only definition of a secure system we have ever had is one which exhibits only behavior explicitly defined by its specification. This is because attacks and compromises of cyber-systems work by attackers invoking unanticipated or unintended system behavior, not via some magical or supernatural powers.

As an example, the Wi-Fi specification calls for a Wi-Fi device to send messages to another by broadcasting over a radio channel, with the goal of emulating a point-to-point link between the two. However, any other radio receiver listening on the same broadcast channel can receive the message – behavior that is not intended by the Wi-Fi specification. An easy attack against unsecured Wi-Fi is to utilize this unintended behavior to eavesdrop on messages exchanged among devices.

It is useful to take a deeper look at what this means.

We build systems by decomposing problems into smaller, more easily solved sub-problems, build modules or components to solve each of the sub-problems, and then compose the modules and components together again to form the system. This approach to system development has two important consequences relevant here.

The first is that security is an emergent global property of the system. Security is a global property, because one vulnerability anywhere in the system can lead to a compromise of the entire system. This implies that security is an emergent property, because it can only come about by (a) all the components manifesting only behavior explicitly defined in their specifications and by (b) how the components are glued together to establish the behavior of the overall system. Being an emergent global property implies that security must be traded off against all the other emergent global system properties – performance, cost, energy consumption, usability, etc. That is, optimizing for all desirable emergent system properties simultaneously is rarely possible, and so it is usually necessary to trade off desirable system properties against each other to maximize the system's utility.

The second is that the system architecture provides the roadmap for attacks on the system. If under the standard definition of security, the attacker's goal is to exploit unanticipated behavior not explicitly in the functional specification, then the only ways the attacker can accomplish his goals are to attack the exposed communications channels connecting the components and to inject messages into the components via the interfaces they expose. What constitutes an exposed channel or component interface depends on the attacker's skills, and so we should expect adversaries with different kinds of skills are able to attack a system in different ways. As some examples of different kinds of adversarial skill sets that might be relevant to our discussion:

1. **Network adversary**. A network adversary can eavesdrop on any message sent over a communications channel, alter messages, inject messages, delay messages, reorder messages, miss-deliver messages, and delete messages.
2. **Software adversary**. A software adversary can read from and write to the memory of running software, both code and data, and can alter both program control flow and data in arbitrary ways. This includes the ability to observe program state changes, reverse engineer the software, thereby revealing all of its functionality to the attacker.
3. **Simple hardware adversary**. A simple hardware adversary can add, remove, or replace components on a motherboard, can monitor and inject data and control exchanged between components, control the electrical and thermal characteristics of system's environment, reflash BIOS and other firmware, and the like. A simple hardware adversary can, in short, transform an existing hardware platform into something with completely new capabilities and limitations.
4. **Sophisticated hardware adversary**. A sophisticated hardware adversary can monitor and reverse engineer operating silicon components, and can also cause the silicon components to operate outside of their specifications. Such an adversary can steal cryptographic keys from "secure" hardware and fundamentally alter the operation of any part.
5. **Supply chain adversary**. A supply chain adversary can inject backdoors and other weaknesses into components or software during design and manufacturing, and steal trade secrets and other proprietary information about how components and software are designed, manufactured, and function, information which other types of adversaries can consume to compromise deployed systems.
6. **Administrative adversary**. An administrative adversary consists of authorized personnel (aka "insiders") who abuse their position by deploying, operating, or maintaining a system in a way that is outside of established policy. They can thereby illegally obtain personal information about system users, proprietary information about the organization using the system, misuse the system for personal gain or revenge, etc.
7. **Social engineering adversary**. A social engineering adversary can exploit human relationships to gain unauthorized access to system resources. A classical social engineering attack is to simply ask a user for a password or some other access token, as a non-negligible percentage of user will comply with the request.

The first job for any cyber-security project is to select adversary models appropriate to its needs, as this is the only way we know to identify what security problem needs to be solved. The security goal then is to deter or otherwise mitigate an adversary with the assumed skills, so that it is no longer possible (or at least expensive) to uses these skills to expose unanticipated system behavior.

According to conventional security dogma, any one of our adversary models can inflict three types of damage against a system:

- **Confidentiality compromises**. The adversary can conduct unauthorized eavesdropping on data and control flows, to learn information about the system or its data which is not intended. As an illustration this corresponds to a network adversary's assumed ability to eavesdrop on communications.
- **Integrity compromises**. The adversary can inject unauthorized data and control into the system, and modify legitimate data and control flows, to make the system act contrary to its purpose. Continuing with our illustration, this corresponds to a network adversary's assumed ability to alter, inject, delay, reorder, and misdeliver messages.
- **Availability compromises**. The adversary can disrupt the services the system provides. This corresponds to a network adversary's assumed ability to delete messages from a communications channel.

4.1.2 Wi-Fi Threats

Let us now examine more specific threats to security that Wi-Fi introduces over more traditional link technologies, like Ethernet. Compared with link technologies based on a physical wire, Wi-Fi enhances a network adversary's ability to accomplish all three types of compromises:

1. Anyone with a radio receiver tuned to the right frequency and within about 100 meters of a Wi-Fi transmitter can capture messages sent over the channel.
2. Anyone with a radio transmitter and within about 100 meters of a Wi-Fi receiver can send messages on the channel.
3. Anyone with a radio transmitter can jam a Wi-Fi channel used by other devices within the radio transmitter's area of influence as determined by the ERP (Effective Radiated Power) of the transmitting device.

Many non-security professionals rank the threat against Wi-Fi's confidentiality as the one requiring the most urgent attention. This is in fact an invalid conclusion, as Wi-Fi uses encryption to provide confidentiality, but encryption provides no integrity protection, and is more easily compromised by active attackers who create message forgeries than by a passive listener. As an example, WEP, the original Wi-Fi encryption scheme, is subject to "bit-flipping" attacks, which results in completely valid forged Wi-Fi messages, even though the attacker lacks access to the WEP encryption key. Hence, as a practical matter, an integrity mechanism is needed to derive benefit from encrypting Wi-Fi messages.

It is worth noting that encryption does not mask all the information conveyed over any Wi-Fi channel. It is both easy and practical to identify particular applications and individual devices via traffic analysis of encrypted data, i.e., by analyzing the distributions of message timing and sizes. It is certainly possible to diminish the efficacy of traffic analysis by inserting dummy messages into the channel, but this kind of counter-measure sabotages Wi-Fi's ability to provide acceptable messaging performance. Accordingly, Wi-Fi security does nothing to defeat traffic analysis, and so its confidentiality claims cannot be absolute.

There also have been calls to make defense against denial-of-service attacks the highest priority. However, to date defending against denial-of-service has never been viewed as a practical problem, as launching a jamming attack has a low-cost, and the known message integrity mechanisms intentionally transform forgery attacks into denial-of-service attacks. Wi-Fi's security architecture has therefore delegated denial-of-service defense to non-technical means. Existing Wi-Fi devices are often mobile, and so can be moved away from a jamming source, and can then reconnect when they come within range of an access point whose signal strength is stronger than the jammer's. Also, it is reasonably easy to locate and then disable a jamming device. Neither the "flight" nor the "search-and-destroy" strategy may work with some types of Internet of Things applications, but these behaviors have proven more cost-effective thus far.

For these reasons, maintaining message integrity is the central design goal for Wi-Fi security, with confidentiality a secondary goal, and denial-of-service mitigation not a goal at all.

4.1.3 Discussion

Off-the-shelf, easy-to-use, and low-cost tools exist to launch attacks against Wi-Fi confidentiality, integrity, and availability. Given the relative ease of launching successful attack against a Wi-Fi network that has not been secured against integrity and confidentiality threats, it seems prudent to utilize Wi-Fi security mechanisms as much as possible.

However, it also seems that Wi-Fi attacks per se are somewhat less of a concern than network attacks from within the Internet. This is due to the short range of the Wi-Fi radio, normally around 100 meters. This means that an attacker must be near the Wi-Fi network targeted, and so, unlike an Internet-based malware attack, attacks against Wi-Fi per se cannot be launched from anywhere in the world. And since it is reasonably easy to locate the source of an active Wi-Fi attack, it also means a Wi-Fi attacker is at a significantly greater risk of being apprehended than for an Internet borne attack. Thus, the locality constraint on Wi-Fi attacks makes it difficult for a criminal enterprise to build a global business model based exclusively on Wi-Fi vulnerabilities, so we should expect attacks against Wi-Fi should be opportunistic and at most one tool inside a larger attacker tool set.

This discussion highlights that Wi-Fi security mechanisms are at best only a small part of a larger overall security story. The Wi-Fi security technologies WPA and WPA2 (IEEE 802.11i and ISO/IEC 8802-11i) were formulated assuming only the generic network adversary model. These security technologies are intended to mask Wi-Fi's unanticipated behavior which can be exploited by a local network adversary, but not the unanticipated behavior resulting from the rest of the system. If Alice and Bob communicate over any sort of communications channel – whether Wi-Fi or anything else – the communications channel cannot protect Alice from Bob's malicious behavior, or vice versa. Wi-Fi security cannot protect Wi-Fi devices from attacks originating in the Internet. Wi-Fi security cannot protect Wi-Fi devices from other devices whose software or hardware have been compromised. Wi-Fi security cannot protect Wi-Fi devices from corrupt administrators or users, or from hardware and software that has intentionally been weakened via supply chain attacks or from social engineering attacks. This set of technology therefore seeks to mitigate the ability of network attackers to exploit unintended Wi-Fi behavior only, but not to address broader security issues.

Even though software adversaries are outside the scope of Wi-Fi security per se, special scrutiny should be given to an attacker that possesses both the network adversary and software adversary skill sets. There are several scenarios in which this combination of skills can lead to successful attack, even when Wi-Fi security is being used correctly.

1. **Wi-Fi session establishment**. Wi-Fi security is layered on top of Wi-Fi association. Mobile clients constantly seek to discover access points and then associate and authenticate with them when one is found that offers significantly better communications characteristics than the current access point. The new access point is necessarily anonymous and hence potentially hostile to the client until after a successful authentication, which happens as a part of session establishment. Similarly, any client is anonymous and hence potentially hostile to the access point until after a successful authentication. Hence any Wi-Fi node must engage in unsecured communication in order to establish new sessions. While the Wi-Fi session establishment protocols have been engineered to mitigate this danger somewhat, weak authentication methods such as those based on passwords or PINs necessarily sensitive leak information, who can then be captured and then utilized to recover the password. There are also vulnerabilities present due to Wi-Fi's attempt to utilize legacy authentication methods never designed for use in this environment.
2. **Malformed datagrams injected into the Wi-Fi channel**. Another constant threat are malformed datagrams. Malformed datagrams are crafted to exploit "bugs" (i.e., unanticipated behavior) in the Wi-Fi device driver or hardware. An attacker possessing both network and software adversarial skills can empirically discover these bugs and then hand-craft messages that trigger them and transfer control to a script supplied by the malformed packet. When such unanticipated behavior is present, the malformed datagram can be sent and processed even when Wi-Fi security is enabled.

Both of these problems are special cases of the generic problem of context sensitivity. Like many real network protocols, the Wi-Fi protocol suite requires a context sensitive grammar for its description. A simpler grammar cannot capture the full range of expression. The theory of computing teaches us that context sensitivity implies two important properties. First, the protocol specification is necessarily ambiguous – it is in principle impossible to remove all ambiguity from languages based on context sensitive grammars. This implies that it is formally undecidable whether independent driver or hardware implementations (i.e., those from different vendors) provide equivalent semantics. Subtle differences in semantics can, however, be discovered by empirical observation and then exploited. Second, all languages based on context sensitive grammars admit what linguists call "novel but appropriate responses," which are new sentences never before uttered but which every native speaker of the language will instantly recognize as valid and meaningful. When it receives a novel message, therefore, there is no guarantee the receiver will handle it appropriately, because by definition it is a message never contemplated by the designers. This implies that no amount of testing, review, and analysis can identify the full range of behaviors which the receiver manifests, so we should always expect additional undiscovered vulnerabilities every Wi-Fi receiver.

Because of the security problems introduced by module composability on one hand and context sensitivity on the other, we have never built a system that meets the bar set by the generic definition of security, which is very compelling evidence that the notion of unconditional security assumed by many users (and marketers) is infeasible. Accordingly, a more practical goal than building secure systems is to make the risk of compromise at least fit into a predictable probability distribution, so the system's intended ecosystem can determine whether it can absorb the costs of compromise.

If it is not feasible to build a system that unconditionally defends against attacks by any of our adversary models, then some amount of adversarial penetration is the norm, and one common defect in many systems today is a lack of adequate monitoring, auditing, and analysis looking for these attacks. Part of this lack is due to cost – monitoring increases code size, validation, and time to market, and adversely affects performance, and auditing and analysis usually require rare expertise to be effective – but it is often due to ignorance and hubris. Most engineering teams mistakenly suffer from the illusion that they know more about their system than attackers. This belief is true when a technology first ships or is deployed, but our knowledge advantage over the attacker erodes each subsequent day. Today's hacker community is an ecosystem of highly skilled and professionally trained experimental scientists and engineers, who can and do reverse engineer products, but whose primary virtue is patience, as this allows them to eventually learn more about the behavior of the systems than those who built and operate it. Knowledge accumulates; attackers' skills and available resources improve over time; attacks only get better, never worse.

4.2 Potential Wi-Fi Security Threats

The following table identifies some of the potential security threats with an associated definition of the threat.

Table 3: Definition of Potential Wi-Fi Security Threats

Potential Security Threat	Definition	Mitigation
1. Ad-hocs and Soft APs	Ad-hoc Wi-Fi networks could be used as honeypots to collect user credentials.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g., using a VPN.
2. AP Security including software	Firmware and software updates can be tampered with, potentially installing malicious software.	The manufacturer of AP should have protection features that authenticate the software updates. Digital signatures may be one method to verify integrity of software and source authentication (the signer). However, these must be properly verified before installation using a secure process. Also, the process of how the software is quality controlled in the first place and signed by the author must be known and verified, or this is still a significant residual risk. Often code-signing keys and services are not well protected.

Potential Security Threat	Definition	Mitigation
3. Data Interception	The interception and capture of data sent over Wi-Fi by eavesdroppers.	Securely encrypted session protocols, between mutually authenticated and authorized (intended) endpoints. This mitigates both sniffing clear transmissions, and man-in-the-middle attacks.
4. Denial of Service	Block access to the network. RF interference to contend with the Wi-Fi signal to make it difficult to join the network. Sending disassociation packets to try to drop people from the network. TCP Resets may also be potential mechanism.	DoS, jamming, and de authentication can be extremely hard to mitigate. If clients are controlled, protocols available to help malicious de authentication.
5. Endpoint Attacks	Numerous exploits have been published to take advantage of buggy Wi-Fi drivers, using buffer overflows to execute arbitrary commands	Secure quality software development, software verification, change management, and configuration control of endpoints.
6. Evil Twin	Bad actor will set up an AP with an SSID that belongs to somebody else. A user will connect to that SSID thinking they are on a trusted network when they are not.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.
7. Hack into Other Systems via Wi-Fi	User uses Wi-Fi AP to probe or attack the back-end systems. Using a public Wi-Fi to launch attacks against the Internet.	Networks must authenticate and authorize clients, and monitor and control their usage as needed.
8. Malware Distribution	Use a public Wi-Fi network to distribute malware to the connected devices.	Networks must authenticate and authorize clients, and monitor and control their usage as needed. Clients must not allow installation of unauthorized software. Firewalls - It is possible to disallow Wi-Fi clients from communicating with one another, and only to the WLAN for example.
9. Man in the Middle	The Wi-Fi access point is between a legitimate AP and the user. The other could be the Evil Twin threat.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.

Potential Security Threat	Definition	Mitigation
10. Misbehaving Clients	Clients that form unauthorized Wi-Fi connections of any type, whether accidentally or intentionally, put themselves and server data at risk. Some Wi-Fi providers still depend on end-users to connect only to known, authorized wireless APs. Accidental or inappropriate Wi-Fi connections have never been easier.	Network must have established policy and controls. Networks should authenticate and authorize clients, and monitor and control their usage as needed. Clients must not allow installation of unauthorized software. Firewalls - It is possible to disallow Wi-Fi clients from communicating with one another, and only to the WLAN for example.
11. Misconfigured APs	Any configuration on AP that leaves network open to security vulnerabilities. For example, AP on public network that allows user to user communications. This also includes using obsolete protocols. For example, (WEP, SSL) instead of WPA2, and TLS v 1.2. Also, still relying on obsolete cryptographic algorithms (MD5, SHA-1) instead of SHA-256.	Network must have established policy and controls. Secure change controls and configuration management. PKI trust lists must be very secure from unauthorized changes. All certificates in the trust chains should use (at minimum) RSA 2048 bit keys, and SHA-256 message digests. These are specifically mentioned as they are on-going problems. ECC and other algorithms are newer and highly recommended as well.
12. Multiple Domain Issue	For example, devices are nomadic and different networks could have the same SSID. This could be an inadvertent duplication of an SSID.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.
13. Misuse of Wi-Fi networks for threatening or intimidation reasons	SSID naming could be a form of messaging to the users. E.g., the SSID could be something like “bomb attack”. This may be moved to a different part of the report.	Network must have established policy and controls. Networks should authenticate and authorize clients, and monitor and control their usage as needed. Clients must not allow installation of unauthorized software. Firewalls - It is possible to disallow Wi-Fi clients from communicating with one another, and only to the WLAN for example.
14. Privacy	To get PIN code to access AP, AP prompts for User Name, email, etc. and user does not know how this information will be used. They could also prompt for “like” on Facebook page to get the user’s social profile. If multiple APs, the APs could track the user location by signal strength for marketing and advertise purposes.	

Potential Security Threat	Definition	Mitigation
15. Rogue APs	Rogue APs may be defined as any Wi-Fi radio transmitter detected within the network operator's intentional coverage area that is not part of the network operator's system. Rogue APs may include benign devices making legitimate use of the Wi-Fi spectrum by third parties as well as malicious or harmful transmitters.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.
16. Malicious Rogue APs	Malicious Rogue APs are Wi-Fi radio transmitters operating within the network operator's intentional coverage area causing disruption to legitimate transmissions. Malicious Rogue APs may cause deliberate disruption through attack vectors defined in this table such as "Evil Twin," "Denial of Service," "Man-in-the-Middle," etc. or may include misconfigured access points.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.
17. Rogue APs on LAN	Unauthorized Wi-Fi radio transmitter connected to the network operator's wired infrastructure. This may provide unauthorized access onto the network operator's infrastructure both allowing possible attackers access to otherwise secure resources, or allowing unauthorized distribution of the network operator's services.	Network must have established policy and controls. Networks should authenticate and authorize clients, and monitor and control their usage as needed. Clients must not allow installation of unauthorized software. Firewalls - It is possible to disallow Wi-Fi clients from communicating with one another, and only to the WLAN for example. Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN.
18. Wireless Intruders	Malicious Wi-Fi clients operating in or near the airspace of a business.	Network must have established policy and controls. Networks should authenticate and authorize clients, and monitor and control their usage as needed. Clients must not allow installation of unauthorized software. Firewalls - It is possible to disallow Wi-Fi clients from communicating with one another, and only to the WLAN for example.

Potential Security Threat	Definition	Mitigation
19. Wireless Phishing	Hackers continue to develop new techniques to phish Wi-Fi users. One technique is to modify the Wi-Fi client web browser caches to redirect the clients to phishing sites.	Clients must verify they are connecting to the intended network. Technical control: Wi-Fi network (access point) authentication by the client. If the Wi-Fi network is not authenticated nor trusted, clients must connect through to a known trusted endpoint, e.g. using a VPN. Clients must have some form of configuration control.

4.3 Example Use Cases & Threats

This section contains the descriptions of some example Use Cases and Wi-Fi security threats facing Wi-Fi network operators and Wi-Fi users. The two Use Cases described in this section were included due to their unique characteristics relative to Wi-Fi security.

4.3.1 Hotel Wi-Fi Network Use Case

4.3.1.1 High Level Description

The hotel Wi-Fi usage is distinguished by its classes of users and the types of data each exchanges over the network. Among the classes of users for this usage are

1. Hotel guests, i.e., those who rent hotel rooms and who use Wi-Fi as a local attachment point to the Internet to exchange personal data.
2. Conference and workshop attendees, who use a hotel’s conferencing facilities and likewise use Wi-Fi to exchange personal data.
3. Casual or transient visitors to a hotel’s lobby, restaurants, shops, and the like, but who otherwise maintain no relationship with the hotel, who also use Wi-Fi for personal reasons.
4. Hotel staff, who operate and maintain the hotel per se and serve the needs of the hotel’s patrons. There is a range of different kinds of data exchanged by this category of users: business and customer data, information about the hotel supplies, telemetry on the hotel’s physical plant, training, and the hotel staff’s personal data.
5. The hotel’s IT staff, who are charged with operating and maintaining the hotel’s network and computing infrastructure, who configure the Wi-Fi network, and who collect and analyze network data.
6. Public safety personnel, such as fire and rescue, emergency medical, police, and the like, who access the network when their intervention is required.
7. A user may appear in different categories serially through time or simultaneously. An example of the former is someone who visits the hotel’s restaurant on one occasion and then rents a room as a guest later. An example of the latter is a member of the hotel’s housekeeping staff, who may aid remote IT personnel to install new equipment or trouble-shoot network failures.

4.3.1.2 Potential Security Threats

If the user classes and their data distinguish this usage from others, then this suggests there are several unique aspects to the hotel Wi-Fi case:

a. How users are registered – i.e., how they obtain log-in credentials – deregistered, and how the various user accounts are managed;

b. How the different classes of users and their data are isolated from one another; and

c. How access is prioritized among the different classes.

d. What kind of physical access attackers have to computing devices and infrastructure.

e. Civil libertarian and business threats.

4.3.1.3 User account management

It is desirable to provide an economical and feasible mechanism for addressing the registration and user management for the transient visitor class of users. Without account management, it is impossible to mitigate the confidentiality and integrity threats against this category of users and devices. One such effort to address user account management is Wi-Fi CERTIFIED Passpoint^{TM} from Wi-Fi Alliance®.

4.3.2 Convention Center/Public Venue Wi-Fi Network Use Case

4.3.2.1 High Level Description

The convention center Wi-Fi usage is distinguished by its classes of users and the types of data each exchanges over the network. It should be noted that in convention centers, events often overlap and occur simultaneously in different sections of the facility. Also, events range in purpose from business to business (industry buyers and sellers on a tradeshow), business to consumer (a local auto show in which attendees potentially purchase a car from a local car dealer), social events (a community fundraising dinner and auction), community event (volleyball tourney or cheerleading competition) and many more. Among the classes of users for this usage are

1. Event planners or show management who sponsor the event and execute a license agreement with the convention center to license meeting rooms and/or exhibition space. Event planners often provide wireless services to attendees and exhibitors as both a convenience and to facilitate business demonstrations and other transactions between the attendees and exhibitors.

2. Event attendees, i.e., those who attend events, conferences or tradeshows for educational, social and/or business purposes, who use Wi-Fi as a local attachment point to the Internet for personal use or as part of the conference to facilitate business or learning opportunities.

3. Exhibitors who license space on the tradeshow floor from the show manager who erect an exhibit booth for as small as 100 square feet and as much as 25,000 square feet to demonstrate products to attendees. Exhibiting customers utilize the wireless network to demonstrate products, execute financial transactions with attendees (buyers), enable

VPN services, amongst other needs.

4. Casual or transient visitors to a convention center’s lobby, restaurants, shops, and the like, but who otherwise maintain no relationship with the hotel, who also use Wi-Fi for personal reasons.
5. Convention center staff or permanent service companies who operate and maintain the convention center per se and serve the needs of the convention center’s patrons. Convention venues often outsource key services to third party vendors. These permanent service companies include food service/catering companies, business center services, technology services providers, security services, electrical services, audio visual providers, etc. There is a range of different kinds of data exchanged by this category of users: business and customer data, credit card transactions, shipping services, telemetry on the convention center’s physical plant, training, and the convention center staff’s personal data.
6. Temporary service companies contracted by the event planner to set up and manage services for the event. These services include a general service contractor (GSC) who organizes the setup up, move in and tear down of tradeshow and conference. The GSC lays out the tradeshow floor plan of exhibit booths, receives all exhibitor freight, schedules the tradeshow floor setup, sets up exhibit booths, rents furniture and carpet to booths, etc. Additional contractors hired by the event planner will provides electrical services, rigging, registration services, audio visual services, etc. Additionally, large exhibitors who regularly participate in major tradeshows hire their own exhibit setup company to erect their exhibit. All these service companies utilize Wi-Fi to manage the scheduling process of freight. delivery, order processing, labor management, billing services, amongst others to ensure the show opens on time. The convention center’s IT staff or third party service provider, who are charged with operating and maintaining the convention center’s network and computing infrastructure, who uniquely configure the Wi-Fi network for each event, and who collect and analyze network data.
7. Public safety personnel, such as fire and rescue, emergency medical, police, and the like, who access the network when their intervention is required.

A user may appear in different categories serially through time or simultaneously. An example of the former is someone who visits the convention center’s restaurant on one occasion and then utilizes the business center to ship materials back to their home office at the end of the show. An example of the latter is a member of the convention center’s IT staff may assist a temporary audio visual provider with an internet drop to facilitate a speaker’s presentation download for the keynote speech.

4.3.2.2 Potential Security Threats

Convention Centers and large public venues suffer from many, if not all, of the same threats previously described in this document. The challenges outlined below are particularly troublesome for large venues due to their application and potential scope and scale.

a. Spectrum Management – Management of the unlicensed spectrum.
b. Malicious Rogue APs – Malicious actors trying to spoof legitimate Wi-Fi networks in order to carry out attacks or identity theft described previously in this document, or

denial of service attacks.

c. Reconfiguration of Floor Space – The constant and ever evolving network design.
d. Time – Time to detect and mitigate threats in large public venues.

4.3.2.3 Spectrum Management

Spectrum management is particularly challenging in convention centers due to the size, density, and public nature of the venue. Spectrum planning in dense environments such as convention centers must be meticulously managed in order to maximize efficient usage of the limited RF spectrum given to Wi-Fi. Unlike an office environment where the RF environment remains relatively static, the RF environment inside a convention center can be extremely volatile, varying drastically day to day. At any time, actors both bad and good bring devices without notice into the facility that operate in the 2.4Ghz and 5Ghz unlicensed spectrum potentially throwing an otherwise well managed RF environment into disarray.

The sheer size and density of a convention center additionally complicates spectrum management in such a volatile environment only to further highlight the security threat. IT teams may not be able to physically reach impacted areas of a venue in a timely manner in order to identify the device or devices affecting network operations. Since many of the transmitters brought into the facility are mobile, an IT team member may arrive at a location only to find the transmitter has moved to a different part of the facility. Bad actors could hide the offending device in hard to reach areas or one of the many cavernous areas of the building. IT teams, through policy and technological means, need to have ways to quickly identify, locate, and mitigate these threats to operations. Ultimately, the challenge is not whether the device is authorized or maliciously placed, it is controlling the airspace inside the venue to address threats.

4.3.2.4 Misconfigured or Malfunctioning Rogue APs

In high density environments such as convention centers, it is imperative to minimize the coverage cell and channel bandwidth of each transmitter to cover only what is necessary due to the limited resource that is the ISM and UNII bands allotted for Wi-Fi.

Many of the transmitters brought into the facility by visitors are devices that are designed for home or small office use. As such their default configurations, which are rarely modified, are typically greedy for RF space set to maximize coverage area usually with maximum allowed ERP, as well as dominate the largest RF footprint possible given the device’s supported standards (80MHz with 802.11ac). These greedy default settings greatly impede network operations disrupting an overwhelmingly large number of neighboring networks and access points in a wide area (sometimes as more than 100,000 square feet) all for the purpose of covering what is typically only a 100 to 200 square foot exhibit space.

Low grade or malfunctioning Wi-Fi access points may also disrupt services in a wide area in a variety of ways of which could be intentional or unintentional. Regardless of intent, malfunctioning access points can negatively impact network operations in high density environments by needlessly causing excessive retransmissions. Transmissions being slightly off-channel, inverted I & Q planes of a signal, failure to properly validate Clear Channel Assessment (CCA) prior to transmission all can be the effect of a low grade or malfunctioning access point and can cause Collision Avoidance (CA) protection mechanisms of normally operating systems to fail, thus causing excessive retransmissions. Once this begins to happen in a crowded environment, the effect can snowball since the reaction to excessive retransmissions in most chipset drivers is to fall back to a lower data rate. Since lower data rates will take more air-time to transmit the same data, the chances of collisions due to the same malfunctioning access points becomes greater, thus causing even more retries. This can continue until every device is communicating at the lowest possible data rate and duty cycle reaches 100%, effectively jamming the channel.

Facility operations that rely on the in-building Wi-Fi network to carry critical systems' data may become intermittent or unreliable due to the added competition for the spectrum from unnecessarily greedy or malfunctioning devices. As more of the venue operations begin to rely on Wi-Fi connected systems for things such as point of sale systems, security cameras, HVAC, lighting controls, etc., the security implications of spectrum management become more prevalent.

Convention Center IT teams must be informed of, and have the discretion to coordinate fair and reasonable use of devices entering the facility to ensure all network operations continue to function properly. The unintended consequences of allowing undisclosed Personal Area Networks (PAN), or other transmitters to compete for the allocated spectrum without convention center IT staff awareness could result in a critical breakdown of key systems as well as those undisclosed PANs themselves.

4.3.2.5 Malicious Rogue APs

Due to size and public nature of the convention center environment, these facilities see vast numbers of guests from various classes as previously described. Guests to these facilities rely on the convention center management to provide a safe environment to stay connected whether via the facility provided Wi-Fi or their own hotspot. Given the large volumes of Wi-Fi client devices traversing the building, and highly dynamic environment of a convention center, these guests are particularly vulnerable to the range of identity theft attack vectors such as man-in-the-middle, evil twin, spoofing, etc. previously described. Guests commonly seek the building Wi-Fi as a reputable source for connectivity, however an attacker may easily conceal a rogue AP in a backpack spoofing a legitimate SSID such as the building Wi-Fi or responding for any SSID client devices are searching for, luring victims onto their device leaving the victim's personal and transactional data vulnerable. Wireless network users have little to go on as to whether the operator is legitimate or a bad actor.

4.3.2.6 Time to Mitigate Impact of Rogue APs

As described earlier in this document, Rogue APs may pose a danger to the public at large. While spectrum management affects the operation of authorized transmitters by possibly disrupting or degrading their signals, Rogue APs in large public venues can both have the same effect as being a problematic transmitter in the 2.4Ghz or 5Ghz spectrum, but also they can be configured to fool the unsuspecting public into believing they are a legitimate part of the authorized wireless network infrastructure. While modern WLAN controllers can help identify Rogue APs, what they cannot do is determine the intent of the individual or group that setup the Rogue networks in the first place. To determine intent, Convention Center IT staff must be dispatched to the approximate location of where the Rogue AP was seen. Then they must proceed to play detective looking for the offending device, which in itself can cause a delay.

While an enterprise grade access point tends to be a larger device and harder to conceal, a Rogue AP's profile does not need to meet the typical footprint of an enterprise AP. It could be something as small as a smartphone in someone's pocket, a MiFi in a backpack or other type of bag, or just a PC. Weeding through an event investigating both the attendee and exhibitor asking to see their personal belongings is socially awkward and essentially turning IT staff into the wireless police and at best a gray area. Furthermore, before the investigation even begins, the staff member has to travel to the approximated location of the Rogue AP. It could be a significant amount of time before the staff member reaches the location due to several factors. First, the size of a venue may prohibit the ability for IT teams to get to an area of the building quickly. Then there's navigating a crowded facility which also slows the process. Meanwhile, every minute an unsuspecting user is connected to a malicious Rogue AP, they run the risk of having their personal information stolen. Without the aid of technology, along with policy, stopping these devices in large venues by manpower alone is prohibitive. Even under the best of conditions, as a resource, IT staff members need to prioritize between making sure the network is functioning as it should be or hunting down Rogues APs.

5 Analysis, Findings and Recommendations

5.1 Analysis & Findings

5.1.1 Best Practice: Common Sense Rules for Public Venues

Wi-Fi services are vulnerable to interference from wireless devices such as wireless routers, wireless cameras, cellular phones, and personal hotspots. These issues can be particularly acute in public venues, such as convention centers, due to the user activity in congested areas, limited wireless spectrum, and the closed space of the exhibit halls. Excessive wireless interference in the exhibit halls, meeting rooms and auditoriums may degrade the ability of exhibitors to demonstrate their products, prevent sales representatives from placing orders, block keynote addresses being live streamed, and impede other activities. In order to maintain a stable and secure wireless environment that minimizes interference through cooperation, coordination and good wireless policies, the convention and meetings industry has adopted the Common Sense Rules delineated below.

1. Be considerate of others.

The wireless network has finite resources, so more users will degrade the wireless experience for everyone. Many visitors do not realize that their personal devices are turned on in a manner that degrades the wireless network. We ask that all visitors be considerate of the needs of the exhibitors, speakers and their fellow attendees. Upon entering the Convention Center, everyone is requested to voluntarily turn-off the Wi-Fi and Bluetooth broadcasting features ("personal hotspot") of their wireless cameras, cellular phones, gaming devices and other portable wireless devices. By voluntarily disabling these features, each visitor will enhance the wireless experience for the entire community in the Convention Center.

Security Benefit

- Leaving Wi-Fi or Bluetooth radios on in a public environment can lead to several security risks:
    - Devices could attach to Wi-Fi networks without the user's knowledge, leaving the device vulnerable to attack without the owner's knowledge;
    - While not actively connected to a Wi-Fi network, common Wi-Fi chipsets continuously probe a list of Wi-Fi networks the device has previously connected to. These probes are broadcast for all within transmission radius to receive in clear text. While seemingly innocuous, a collection of these network names can quickly build up a profile for a would be attacker. In many cases these can divulge sensitive personal information from which an attacker could glean a home address via public Wi-Fi mapping sites. These probes also give would be attackers a list of networks they can spoof in order to compromise the probing system by tricking it to automatically connect.
    - Bluetooth radios left on are vulnerable to attackers with devices designed to attach to Bluetooth radios. There have been numerous public reports of attackers stealing data from highly visible members of the public. (http://www.nbc12.com/story/22152269/bluebugging-hackers-target-bluetooth)
- These security risks become particularly enhanced in crowded large public venues due to the additional shroud of anonymity it provides would be attackers.

2. Don't overpower your neighbors.

Exhibit halls, meeting rooms, and auditoriums in the Convention Center are closed spaces where high-power wireless devices may interfere with many other wireless users. This is unfair to your neighbors and may disrupt the event. For the convenience of your fellow attendees, a wireless device that requires a continuous connection to an electric outlet (or a battery independent of the wireless device) for its operation may neither be utilized nor plugged into an electrical outlet. At the discretion of the Convention Center or their designated representatives, the operator of such device will be required to unplug and remove the device from the Convention Center. Failure to unplug the device within 30 minutes of notification may jeopardize the wireless network for fellow attendees and is a license violation by the operator. In the event of such violation the Convention Center may require the operator of the offending device to discontinue its use for the remainder of the event and/or to undertake a wireless engineering & coordination plan for the neighboring wireless devices and bill the operator of the offending device the appropriate charges. If neither option is adhered to, the Convention Center may require the operator to leave the Convention Center.

Security Benefit

- Leaving Wi-Fi signal strength high leaves Access Points and Wireless networks vulnerable to attack from far distances. Wi-Fi signal strength set appropriately to cover only the intended area would require an attacker to be in much closer proximity to the intended target, and therefore more easily detected.
- There is a common misconception among lay people that as long as your signal is stronger than your neighbors', your network will be preferred. This misconception can lead to the effects snowballing with neighbors attempting to compete, driving transmit power of each other higher until all are transmitting at the maximum allowed. More is not better in this case. Adequate transmit power to cover the intended area protects both the operator's network as well as a misinformed neighbor that attempts to compete for signal strength.

3. One user. One channel. *Please*.

For many years, Wi-Fi technology only allowed for access to one channel at a time. The latest Wi-Fi protocols (such as 802.11ac) allow users to combine or bond multiple channels. Doing so, however, may significantly degrade your neighbors' ability to use the common wireless network. For the benefit of the entire wireless community in the Convention Center, please do not hog the spectrum through channel bonding or other techniques.

Security Benefit

- Channel bonding can drive up channel utilization, creating degraded connection quality for all users of the spectrum within transmission range. This degraded quality can lead the lay person to respond by increasing transmit power further exacerbating the problem as well as weakening overall security as noted in the previous section.

4. Acceptable use makes it fair for all.

Please be considerate and share the wireless spectrum and bandwidth with your fellow attendees and exhibitors. Please do not use peer-to-peer traffic applications (such as Bit Torrent) nor actively scan the wireless network because these practices consume a disproportionately large amount of bandwidth and wireless network resources.

Security Benefit

- Scanning networks is the first step in an attack on a wireless network. If we know scanning should not be taking place, and detect it, action can be taken to locate the potential threat. Without banning scanning, we would be left without a way to determine who is a threat and who is not.

5.1.2 Best Practices to Deal with Rogue Access Points

For enterprise Wi-Fi networks, it is a good practice to prevent, detect, locate and eliminate rogue access points. On the other hand, it is a good idea to exercise caution understanding that some rogue access points may elude detection, or it takes time to detect and eliminate rogue access points.

1. Many rogue access points are established by employees for convenience. An enterprise should establish security policies that mandate conformance with effective security policies and coordination with the IT organization before installing an access point. All employees should know the security policies and the risks of not following the policies.
2. Deploy tools that can detect and eliminate rogue access points. Depending on the network and budget, different tools may be used. Large enterprise networks may use Wireless Intrusion Prevention System (WIPS) for full-time air surveillance. Ideally, the WIPS can be combined with management tools to locate and eliminate rogue APs, or manage switches so that suspicious ports, once identified, can be closed immediately. Small businesses that have more budget constraints can use periodic air surveillance (which is less effective but can still detect certain rogue access points), or use managed WIPS provided by the service providers (when such services are available). In addition, stand-alone host WIPS programs can be installed on client devices to monitor air activities on client devices.
3. Critical resources in the enterprise network should only be allowed to be accessed through encrypted channels such as HTTPS or VPNs. Even when a rogue AP is not detected and eliminated timely, data encryption can help to protect the data.

For public Wi-Fi networks that are open networks or Wi-Fi networks that are created for temporary usages (e.g., in convention centers), detecting and eliminating rogue APs may not be practical. In such networks, consumers should understand the risks of using such networks, and exercise caution. Avoid using such networks for any service that may involve sensitive information (username, password) unless absolutely necessary. The following are suggested practices for dealing with rogue APs in such networks.

1. Manage Wi-Fi adapters explicitly. Turn off Wi-Fi adaptors by default. Turn it on manually when needed to connect to a Wi-Fi network. Disable automatic connection to a list of recorded Wi-Fi networks.
2. Use a local firewall on client device. It can prevent malware from infecting devices and can stop data interception attempts by blocking suspicious traffic.
3. Use a VPN. Some browsers offer free secure VPN services. Use such VPN services or VPN services provided by the enterprise IT service. Enterprise should enforce that remote access to enterprise network resources need to be through VPNs (or HTTPS).

The above does not consider the situation where a personal device purposely emulates an access point to allow new Wi-Fi services, e.g., the wireless connection between a laptop and a conference room projector. The above usage essentially constitutes rogue access points intentionally injected into an enterprise's IT infrastructure since the laptops that emulate access points are not deployed and managed by the IT. While the usage may have legitimate purposes, it can lead to security attacks. How to support the intended functionalities while maintaining the security of the network is still an open problem. One partial solution might be to configure the devices (e.g., projectors) that need to connect to personal devices to demand that security is enabled, e.g., using a password projected with the other set-up help, and they will not be associated unless the laptop runs the appropriate security. However, this solution does not address the problem when a personal device is purposely set up as a genuine rogue access point. It seems like the technology can only address part of the problem. We need to convince the users that they are responsible to limit connections within the enterprise's environment. In addition, they are responsible to use access points that can demonstrate that they have been secured by running WPA2 with a company configured password.

5.1.3 Best Practices from CSRIC Working Group 2A

The following are the Wi-Fi best practices from the CSRIC Working Group 2A final report[1]:

Number	Priority	Description
9-8-8600	Critical	Ad-hoc Wi-Fi Policies: Service Providers and Network Operators should implement policies and practices that prohibit ad-hoc wireless networks. An ad-hoc wireless network is a peer-to-peer style network connecting multiple computers with no core infrastructure. They are not considered secure and are commonly associated with malicious activity.
9-8-8601	Critical	Wi-Fi Policies: Service Providers and Network Operators should establish policies to ensure only authorized wireless devices approved by the network managing body or network security are allowed on the network. Unauthorized devices should be strictly forbidden.
9-8-8602	Critical	Wi-Fi Standards: Service Providers and Network Operators, should implement applicable industry standards for wireless authentication, authorization, and encryption (e.g. WPA2 should be considered a minimum over WEP which is no longer considered secure).
9-8-8603	Critical	Wi-Fi Standards: Service Providers and Network Operators should implement applicable industry standards to ensure all devices on the Wireless LAN (WLAN) network enforce network security policy requirements.
9-8-8604	Highly Important	Wi-Fi Intrusion Prevention/Detection: Network Operators should consider installation of a Wireless Intrusion System at all locations to detect the presence of unauthorized wireless systems. At a minimum, routine audits must be undertaken at all sites to identify unauthorized wireless systems.
9-8-8605	Important	Wi-Fi Signal Strength: Service Providers and Network Operators should minimize wireless signal strength exposure outside of needed coverage area.

[1] Available at https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf

5.1.4 Best Practices from Cisco

The following are Wi-Fi best practices from Cisco:

Network Type	Enterprise Networks - Open Access & No Encryption	Enterprise Guest Networks - Web Authentication without Encryption	Enterprise Guest Networks - Authentication and Encryption	Enterprise Networks - Encryption & No Authentication	Enterprise Networks - Authentication with Encryption
Access Type	Open to anyone, public access	Sponsored Guest	User utilizing a Service Provider Hot Spot 2.0 service	Consumer devices on enterprise network & IoT	Enterprise User
Network Use	Serving the public, i.e., convention centers, retail, some municipal WiFi	Serving the public, i.e., convention centers, retail, enterprise allowing contractor/visitor access	Retail, convention centers, Service Provider Wi-Fi	Enterprise devices (printers/sensors/video cameras, building automation, "headless" devices that do not permit data entry, such as sensors)	Enterprise devices or approved BYOD
Authentication	None	Web Authentication	802.1x mutual authentication with Certificates	MAC Address Registration/ Authentication with Pre-Shared Key (PSK)	802.1x with either certificate or username/pass-word authentication
Encryption	None	None	WPA2-Enterprise AES Encryption	WPA2-Personal AES Encryption	WPA-2 Enterprise AES Encryption
Wireless End User Threat Level to Clients and the Network	High (allowing anyone and anything) No encryption or authentication results in complete lack of control of who is on the network and allows others to intercept all traffic from unsuspecting clients	Medium-High Users are Authenticated via a Web page – but no encryption is used. Enterprise controls access to the network – but not the privacy of the data being transmitted	Low Users are authenticated via mutual authentication to the Service Provider with x.509 certificate and data is encrypted providing authentication and confidentiality	Medium Devices, not users, are authenticated via MAC address – encryption is provided with Pre-Shared Keys. MAC Addresses are easily spoofed and WPA2-PSK has known vulnerabilities with weak Pre-shared Keys.	Low Users are authenticated via mutual authentication to the Enterprise with x.509 certificate or Username/Pass-word and data is encrypted providing authentication and confidentiality
Enterprise Network Operator Recommendations	Configure administrator access – passwords, encryption of communications to the network, login history; lock login after period of time; HTTPS	Configure administrator access – passwords, encryption of communications to the network, login history; lock login after period of time; HTTPS	Configure administrator access – passwords, encryption of communications to the network, login history; lock login after period of time; HTTPS	Configure administrator access – passwords, encryption of communications to the network, login history; lock login after period of time; HTTPS	Configure administrator access – passwords, encryption of communications to the network, login history; lock login after period of time; HTTPS
	Network Security assessments – frequency & scope	Network Security assessments – frequency & scope	Network Security assessments – frequency & scope	Network Security assessments – frequency & scope	Network Security assessments – frequency & scope
			WPA2 with EPOL/802.1X – strong encryption and generation of session keys; authentication at the network layer; tamper detection (Message Integrity Check)	WPA2-PSK with significantly long/entropy pre-share keys. Note – that once the pre-shared key is given out it is compromised.	WPA2 with EPOL/ 802.1X – strong encryption and generation of session keys; authentication at the network layer; tamper detection (Message Integrity Check)
	Limit wireless session time to prevent users from "camping"	Limit client access time to prevent users from "camping"	Limit wireless session time to force fresh session encryption keys to be generated	Limit wireless session time to force fresh session encryption keys to be generated	Limit wireless session time to force fresh session encryption keys to be generated

Network Type	Enterprise Networks - Open Access & No Encryption	Enterprise Guest Networks - Web Authentication without Encryption	Enterprise Guest Networks - Authentication and Encryption	Enterprise Networks - Encryption & No Authentication	Enterprise Networks - Authentication with Encryption
Enterprise Network Operator Recommendations	If allowing complete and open access – separate WLAN from the rest of corporate infrastructure if possible	Use network segmentation techniques (virtual LAN, CAPWAP, GRE, MPLS, VRF) to tunneling traffic to DMZ for this SSID	Use network segmentation techniques (virtual LAN, CAPWAP, GRE, MPLS, VRF) to tunneling traffic to DMZ for this SSID	Use network segmentation techniques (virtual LAN, CAPWAP, GRE, MPLS, VRF) to provide separation of this lower security SSID from the rest of the enterprise network	
			Ensure clients and infrastructure devices have valid certificates (CRL or OCSP)		Ensure clients and infrastructure devices have valid certificates (CRL or OCSP)
	Rate limit users to prevent consuming excessive bandwidth (avoid DoS attack)	Rate limit users to prevent consuming excessive bandwidth	Rate limit users to prevent consuming excessive bandwidth		
	When two devices are connected to the infrastructure, data should transit the infrastructure – not travel peer to peer (no impact to personal hot spot)	When two devices are connected to the infrastructure, data should transit the infrastructure – not travel peer to peer (no impact to personal hot spot)	When two devices are connected to the infrastructure, data should transit the infrastructure – not travel peer to peer (no impact to personal hot spot)		
Enterprise Network Operator Recommendations	Software updates to include security patches				
	Automated management tools to assess normal operations & detect threats; log security events				
	Automated tools to direct network to change channels to avoid threat				
	Intrusion protection technology – best practice is policy guidance to administrator				
	Access Points: Physical security should be maintained				
	Design of radio footprint should cover intended area only				

5.2 Recommendations

5.2.1 Deauthentication

RECOMMENDATION: The FCC should resolve the policy and legal issues regarding the ability of enterprise customers or network operators to use deauthentication to protect Wi-Fi users from legitimate cybersecurity threats.

However, the specific actions that a Wi-Fi operator can take to protect consumers are unclear. For example, it should be permissible for a network operator to use deauthentication, which is part of the IEEE 802.11 standard, to ensure network security, such as to shut down access point spoofing or other cyberattacks. The FCC's Part 15 rules do not preclude such use, and former FCC Chairman Tom Wheeler acknowledged in a letter to Congress that deauthentication has a "legitimate use." Letter from Tom Wheeler, Chairman, FCC, to Senator Ron Johnson, Chairman, Senate Committee on Homeland Security and Government Affairs, at 2 (June 29, 2015).

Regardless, the FCC's reading of Section 333 appears limited to the use of deauthentication "to intentionally disrupt[] the *lawful operation* of neighboring Wi-Fi networks."[2] Unfortunately, the FCC has not addressed previously the use of deauthentication for cybersecurity purposes. Thus, it remains unclear whether a person using a Wi-Fi network to engage in access point spoofing or to launch a cybersecurity attack would be engaged in "unlawful" use and against which deauthentication would be permitted to stop.

Neither the Commission's cybersecurity goals nor the public interest are well served by leaving Wi-Fi operators to speculate about the specific actions they can or should take to protect consumers from harm. Accordingly, the FCC should complete a rulemaking or other administrative proceeding to provide guidance to network operators regarding the use of deauthentication to protect Wi-Fi users from cybersecurity threats.

Situation in which the use of deauthentication support enhanced security on Wi-Fi networks:

> Example: In the case of a large venue (convention center, large enterprise, military base, stadium, airport, etc.), in which a breach has been detected and confirmed through IPS, Monitoring or other best practice technique. However, due to the size of the venue it will take some time to physically get to where the attack is sourced from. Think of the Orange County Convention Center in Orlando with a 7 million square foot campus, in two physically separate buildings. IT support staff is housed literally a mile from sections of the North/South building, across a public street. If during the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) event for military computer modeling and simulation, the FBI cyber team determines that a local attack has been launched, deauthentication could stop the attacker until assets can be put in place to assess and resolve the issue.

The threat of spoofed deauthentication and other management plane attacks exists in a Wi-Fi network, which makes it possible for an attacker to create a denial of service attack against Wi-Fi clients. Technology exists in the form of 802.11w to mitigate those attacks, but it's important to keep in mind that not all clients support 802.11w. While the working group recommends the use of 802.11w, the working group does not recommend requiring it for clients to join a network. Also, even with 802.11w enabled, radio-level jamming can still cause denial of service attacks.

5.2.2 Mutual Authentication (network and clients)

<u>Overview</u>

It is highly recommended that the businesses provide for registration of clients and enforce mutual authentication when joining the network. After mutual authentication we assume that the network connection will also be encrypted. These recommendations are to ensure the clients have a secure experience, and to mitigate threats such as evil-twin and man-in-the-middle attacks that can compromise data on the wireless network.

Ideally, a business or enterprise can control their client configuration and provide true mutual

[2] For instance, the FCC Enforcement Bureau has alleged and a divided FCC found in 2015 that the use of deauthentication violates 47 U.S.C. § 333. See In re M.C Dean, Inc., Notice of Apparent Liability for Forfeiture, FCC 15-146 (rel. Nov. 2, 2015) (Commissioners Pai and O'Rielly dissenting and issuing separate statements), response pending (filed Dec. 1, 2015).

authentication of both clients and server using x.509 certificates. However, in our typical use case, the business (Wi-Fi network provider) is expecting various temporary customers (clients) to connect to their network. The service might be provided for a one-time use, but more likely has a set duration - a conference, a hotel stay or a single airline flight. Thus, the network provider may provide for certificate based authentication, and require clients use a temporary user-id and password.

To be sure, the client should know to connect securely to their bank or other location before conducting sensitive business. In this case, the security of the underlying network connection may not matter. However, this recommendation is for those businesses and service providers that want to ensure customers can authenticate the Wi-Fi network itself, and establish a relatively trusted and secure connection. Corporate and tech savvy consumers know a Wi-Fi network is not trustworthy if it cannot be authenticated. They know to connect through to a known service, such as their own VPN or other known and trusted endpoint on the Internet, before conducting business or sending any sensitive data. Presuming this VPN is itself secure, mutually authenticated, and the data stream is encrypted, the Evil Twin threat is virtually eliminated. General consumers may not understand these factors, and they expect the basic Wi-Fi network to be “secure”.

Even if a Wi-Fi provider dispels legal liability the business contracting for or hosting this service may still have business risk. Not the least of which is to their reputation. It should be important to the business to ensure the clients have a secure experience, and that their credit card data is not at risk of fraudulent access points. But also, the network provider should have some basic tracking of the clients and devices that do join their network.

<u>Recommendation</u>

The CSRIC Working Group 9 recommends that the business or wireless network provider implement an authenticatable network using an X.509 certified network identity or SIM cards, and also a more robust registration method for short-term clients. This registration process has two objectives, both of which are necessary to be able to provide for mutual authentication:

1. Provide a unique temporary user id and password to each client. The client understands this identifies them exclusively when they join the network, and that activity may be logged, and attributable to them.

2. Provide the details of the network authentication credentials and ways for the client to manually verify them. In general, a properly configured wireless supplicant would reject fraudulent (non-trusted) certificates. But general consumer devices may be misconfigured, or they may click through and accept “untrusted” certificates anyway. Worse a fraudulent access point already has obtained a seemingly legitimate certificate from less-then-trustworthy certificate authorities, that do not provide proper vetting before issuing certificates. The list of “built-in” known certificate authorities is too big and growing on most consumer devices.

   Today, network providers could provide printed details of their network setup, the keys and the certificate authority in use, along with ways to further verify these when the client connects.

Unfortunately step two above is quite awkward using today’s technology. Further, most consumers don’t want to deal with manual verification, and many will not be able to do so, even if enough detail was provided to them. The client may not understand that failure to properly validate and verify the network authenticity increases their vulnerability to attacks carried out via fraudulent and malicious access points.

Future Technology

The CSRIC Working Group 9 recommend that a method and technology be developed that allows a client, during their registration to use a wireless network, be able to securely obtain and “pin” specific network authentication keys in their client device(s). This better protects the client from third-party trust store problems. The wireless supplicant could therefore alert on illegitimate network credentials, and not allow connection, thus protecting the clients. If a bypass is allowed, the client must be made to accept this.

Appendix A: Suggested Background Reading

This Appendix contains a list of suggested readings for background information on Wi-Fi security.

- "XCS: Cross Channel Scripting and its Impact on Web Applications" by Hristo Bojinov, Elie Bursztein, and Dan Boneh, 16th ACM Conference on Computer and Communications Security, November 9-13 2009, Chicago, Illinois; http://crypto.stanford.edu/~dabo/pubs/abstracts/xcs.html
- Wi-Fi Alliance article "Wi-Fi CERTIFIED Passport – Transforming the Wi-Fi hotspot experience"; http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint
- Wi-Fi Alliance "Discover Wi Fi: Security"; http://www.wi-fi.org/discover-wi-fi/security
- "Four lesser-known Wi-Fi security threats and how to defend against them"; http://www.techhive.com/article/3161450/wi-fi/four-lesser-known-wi-fi-security-threats-and-how-to-defend-against-them.html

Appendix B: Acronyms

This Appendix contains the acronyms that are referenced within this report.

Acronym	Definition
AP	Access Point
BIOS	Basic Input / Output System
BYOD	Bring Your Own Device
CA	Collision Avoidance
CCA	Clear Channel Assessment
CSRIC	Communications Security, Reliability and Interoperability Council
DoS	Denial of Service
ERP	Effective Radiated Power
FCC	Federal Communications Commission
GSC	General Service Contractor
HVAC	Heating, Ventilation, and Air Conditioning
NIST	National Institute of Science and Technology
PAN	Personal Area Network
PKI	Public Key Infrastructure
RF	Radio Frequency
SSID	Secure Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wireless Protected Access
WPA2	Wireless Protected Access 2