White Paper

The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular

According to the Wi-Fi Alliance, about 200 million households use Wi-Fi networks, and there are about 750,000 Wi-Fi hotspots worldwide. Wi-Fi is used by over 700 million people and there are about 800 million new Wi-Fi devices every year. Cisco has shipped over 11 million access points to customers worldwide.

Until recently, mobile operators have viewed the unlicensed spectrum and Wi-Fi as an extension of their fixed broadband business or as a complementary hotspot business, but not as a viable extension of their mobile business. With the introduction of smartphones such as Apple's iPhone and Google's Android and the transition from a mobile voice business model to a mobile data model, more tier-one mobile operators are taking a closer look at how to take advantage of the unlicensed spectrum and Wi-Fi as part of their mobile strategy. They realize that the operator with the best licensed and unlicensed strategy will deliver the most data service and the best mobile experience at the highest profit margin.

This white paper provides:

- A review of the usability problems and security vulnerabilities of today's hotspots.
- A description of how IEEE 802.11u, Wi-Fi Protected Access 2 (WPA2)-Enterprise and standards-based Extensible Authentication Protocol (EAP) methods can be used to solve the security and usability problems of today's hotspots, making Wi-Fi as secure and as easy to use as 3G cellular. It also includes an introduction to the Wi-Fi Certified Passpoint™ program to establish interoperability criteria for these technologies.
- An introduction to Mobility Services Advertisement Protocol (MSAP), a new protocol that facilitates service discovery, connecting users securely, easily, and immediately to venue-based services.

In short, this white paper describes Cisco's vision for the Next-Generation Hotspot, which moves the Wi-Fi network from an untrusted network to a trusted and integral part of a carrier's network.

Growing Data Demand

Let's start by viewing hotspots against the backdrop of the seemingly insatiable growth of consumer demand for mobile data. The Cisco® Visual Networking Index has noted or predicted the following growth[1]:

- In 2010, global mobile data traffic nearly tripled (it grew to be 2.6 times larger than the previous year) for the third year in a row, despite a slow economic recovery, increased traffic offload, and the advent of tiered pricing.
- Global mobile data traffic will increase 26 times from 2010 to 2015, a 92 percent compound annual growth rate (CAGR).

[1] Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast, 2010-2015.

- The average mobile connection speed will increase by a factor of 10 from 2010 (215 kbps) to 2015 (2.2 Mbps), a 60 percent CAGR.
- The average mobile connection speed will increase 10 times from 2010 (215 kbps) to 2015 (2.2 Mbps), a 60 percent CAGR.
- By 2015, global mobile data traffic will reach an annual run rate of 75 exabytes per year. 75 exabytes is equal to 75 times more than all IP traffic generated in 2000, or 19 billion DVDs, or 536 quadrillion SMS text messages.

This demand increase began because of the popularity of the Apple iPhone, Research In Motion's Blackberry, and subsequently Android-based phones. Tablets, gaming consoles, laptops and netbooks, machine-to-machine communications, and non-smartphones are only adding to the demand. Cellular carriers are looking for solutions to offload this data traffic from their cellular networks. Offloading data to hotspots is an economically attractive alternative, because many carriers already operate a substantial number of hotspots. Mobile operators would like to provide a user experience on Wi-Fi networks similar to that provided on 3rd Generation networks. This means making Wi-Fi as easy to use as cellular and providing it with cryptographically equivalent mutual authentication and link-layer security.

Usability Problems in Today's Hotspots

Along with the growing popularity of hotspots, using WebAuth (that is, captive portal authentication) brings a number of usability problems that can frustrate users:

- **Login process.** After association to a hotspot, the user launches a browser to enter credentials. If this was not the first application launched after association, services are unavailable. For example, if a user launches an email client first, email would not work (due to protocol blocking as the user is unauthenticated). This remains confusing to many users since the mobile device's connection manager[2] indicates that the device is connected.
- **Time-limited credentials.** Problems occur when the user has authenticated with time-limited credentials (for example, at a hotel). When the time runs out, network access is suddenly lost, but the connection manager continues to indicate that the device is connected.
- **Hotspot selection.** In many locations, multiple Wi-Fi networks are within radio range of the mobile device. If the mobile device recognizes a service set identifier (SSID), it typically joins that network. However, if the mobile device doesn't recognize an SSID, the user needs to go through a long list of steps to gain Internet access. The user must launch the device's connection manager, select the SSID in order to connect to the network, launch a browser, enter a new URL, and then enter credentials. While this may be tolerable at times, it drains the device's battery and is subject to errors. Because it's time-consuming, it can be a problem for hosted services with mobility requirements (for example, voice call handover). Furthermore, because it's manual, it severely limits data offload.
- **Hotspots operated by roaming partners.** In situations where the mobile device needs to log in to a hotspot operated by a roaming partner of the home service provider, the SSID will often be new to the mobile device. This necessitates a manual login process requiring user intervention. Consequently, carriers lose the opportunity for their roaming policies to affect network selection. This can result in higher roaming fees paid to nonpreferred hotspot operators, reduced service levels, and increased user frustration.

[2] Software on the mobile device responsible for network discovery, selection, association, and authentication.

Because of these usability issues, some Wi-Fi Alliance members banded together to develop **Wireless Internet Service Provider roaming** (WISPr) 1.0. The specification was completed in 2003 (later the specification was officially withdrawn and the Wi-Fi Alliance chose not to develop a WISPr certification). WISPr 1.0 was one of the first attempts to automate hotspot login and authentication. WISPr 1.0 provided automated login by embedding XML data structures within the webpages delivered to mobile devices during WebAuth. However, WISPr 1.0 met with limited success as interoperability problems ensued.

Over the years, carriers, device manufacturers, and third-party software vendors have continued to produce proprietary solutions to automate hotspot login. Today, the market is fractured with many different, noninteroperable solutions available. In addition to the bewildering array, these solutions have shortcomings. It's time for the hotspot industry to move on.

Security Threats in Today's Hotspots

Many of the attacks reported by the press stem from the fact that today's hotspots employ open associations, which don't offer any form of link-layer security. This leaves users open to the following attacks:

- **Evil twin attack.** In this attack, an attacker sets up a rogue access point whose SSID is set to the same name as that of an access point deployed by a legitimate hotspot provider. This attack can be used for identity theft.
- **Session hi-jacking.** In this attack, an attacker mimics the access point to which the user's mobile is associated and causes the user's mobile device to disassociate from the Wi-Fi network. The attacker then assumes the victim's session, resulting in theft of service.
- **Session side-jacking.** In a side-jacking attack, the attacker snoops on unencrypted Wi-Fi communications and intercepts a victim's session cookie. The attacker can then access the victim's personal, private webpages (for example, Facebook pages).
- **Eavesdropping.** Unencrypted Wi-Fi communications can be intercepted by an attacker. This subjects personal information such as passwords, credit card numbers, photographs, and email to exploitation.

It should be noted that private enterprise networks (which are managed, trusted networks) do not suffer from these attacks because they use IEEE 802.11i security and EAP authentication. These technologies have already been certified by the Wi-Fi Alliance's WPA2-Enterprise certification. If WPA2-Enterprise technology could be applied to Wi-Fi hotspot networks, these attacks could be mitigated in public networks as well.

One of the barriers to deployment of WPA2-Enterprise in hotspots is that the access point's 802.1X port blocks all communications prior to authentication. This means that a user is blocked from accessing any portal page that lets them know they're authenticating to the desired Wi-Fi network; similarly, it blocks them from accessing a help page if they're having trouble. Furthermore, a mobile device's connection manager (or user) has no alternative other than trial-and-error when choosing an EAP method and credential to use for hotspot authentication. This is time consuming and drains the mobile device's battery.

Another barrier to deployment of WPA2-Enterprise in hotspots is the difficulty in roaming situations. Typically, if the mobile device's connection manager doesn't recognize the SSID for a roaming partner's network, it won't even attempt to join that network. Additionally, users often don't know the SSID for a roaming partner's network either, so manual connection is not attempted.

Next-Generation Hotspot Data Offload

Carriers are addressing the exponential growth in data and finding ways to deploy smaller cells to take advantage of unlicensed spectrum.

An important consideration in offloading mobile data traffic in a managed, trusted network is the so-called selective IP traffic offload (SIPTO). Mobile data traffic destined for the public Internet need not be backhauled to the carrier's core network; doing so would only increase its congestion. Rather, many carriers prefer that mobile data traffic be routed locally to the Internet. Only traffic-to and traffic-from services provided by the carrier core network (for example, IPTV) are backhauled.

A second consideration in offloading data traffic in a managed, trusted network is the preservation of quality of service (QoS), particularly for voice and video services. Typical bandwidth bottlenecks in an end-to-end connection are the hotspot's air interface (Wi-Fi link) and the WAN link. Proper QoS markings for packets traversing these links are essential if real-time services are to be delivered unimpaired. The access network (including the WAN link) needs access to the packet headers to perform packet classification and QoS re-marking. Proper QoS packet marking helps to ensure that each link's transmitter can provide differentiated services by transmitting packets via the correct queue. If packet headers become opaque - for example, because the packets are transported in an IPsec tunnel (for instance, between the mobile device and Packet Data Gateway (PDG), QoS classification and re-marking can become impossible. For example, when packets in an IPsec tunnel originating from a carrier's IPsec gateway pass though a transit ISP on their way to a hotspot, and the transit ISP's routers re-mark the differentiated service's code point (differentiated services code point [DSCP] in the IP header) to best effort, the QoS marking is lost and the packets cannot be reclassified by the hotspot infrastructure.

In unmanaged, untrusted hotspots - that is, hotspots that are operated by neither the carrier nor its roaming partner - IPsec can provide an effective security solution. For example, I-WLAN (3GPP TS 23.234), which employs an IPsec tunnel, can be secure. However, in managed trusted networks, an IPsec tunnel between a mobile device and carrier gateway should be avoided for the reasons given in the preceding paragraphs. If IPsec is used in a managed, trusted Wi-Fi network, it has the side effect of forcing double encryption (IPsec and Wi-Fi link-layer security) with a negative impact on battery life.

Hotspot 2.0 Task Group

In 2010, Cisco and industry leaders formed the Hotspot 2.0 Task Group in the Wi-Fi Alliance. The goal was to rally the industry around a common set of standards that would vastly improve an end user (subscriber) hotspot experience and fully support service provider business objectives.

For the end user, fulfilling this means making network access at a Wi-Fi hotspot both as easy and as secure as cellular network access. This is accomplished by providing consistent, secure, automated connectivity worldwide.

For the service provider, fulfilling this means increasing revenue via improved subscriber satisfaction, optimizing operations by maximizing the use of Wi-Fi for data services, enhancing value with subscription-based provisioning, and further enabling of services through roaming agreements.

The key elements of the Hotspot 2.0 Task Group for Release 1 of the Wi-Fi Certified Passpoint™ certification program, which Wi-Fi Alliance launched in June 2012, are as follows:

- **Network discovery and selection:** Mobile devices will discover and automatically select and connect to Wi-Fi networks based upon user preferences and network optimization.
- **Streamlined network access:** Mobile devices will be automatically granted access to the network based upon credentials such as SIM cards, which are widely used in cellular devices today. No user intervention will be required.
- **Security:** Over-the-air transmissions will be encrypted using the latest-generation security technology (Wi-Fi Certified WPA2-Enterprise).

The key elements for Release 2 of the Wi-Fi Certified Passpoint™ certification program, anticipated to launch in Q4CY2013, are as follows:

- **Immediate account provisioning:** The process of establishing a new user account at the point of access will be simplified, eliminating many user steps and driving a common provisioning methodology across vendors.
- **Provisioning of operator policy for network selection:** A mobile device's connection manager uses this policy to select the best Wi-Fi network to join when multiple networks are available.

Cisco is proud that some of our products are included as part of the Wi-Fi Certified Passpoint reference test bed, thus helping fulfill the promise of delivering an industrywide ecosystem of interoperable products based upon Hotspot 2.0.

In summary, Wi-Fi Certified Passpoint™ will help ensure authentication and roaming interoperability for equipment vendors and operators.

The Cisco Next-Generation Hotspot builds on Hotspot 2.0 by enabling service providers and venue operators to better manage and monetize their hotspots.

Next-Generation Hotspot Technologies

There are three technology pillars to Next-Generation Hotspot: IEEE 802.11u, WPA2-Enterprise, and EAP-based authentication. All these technologies are an integral part of Wi-Fi Certified Passpoint™. The following sections provide details about these technologies.

Next-Generation Hotspot Secure Authentication

In order to take full advantage of Next-Generation Hotspot capabilities, carriers and users alike require an easy-to-use authentication mechanism. Network selection by a mobile device and authentication to the selected network should be carried out autonomously by the device without the need for user intervention (for example, the user entering a username and password). The natural choice for GSM carriers is to use the subscriber identity module (SIM) credentials already carried in their subscribers' mobile devices, combined with EAP-SIM authentication. Similarly, the natural choice for Universal Mobile Telecommunications Service (UMTS) carriers is to use USIM credentials in conjunction with Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA). Indeed, the Wi-Fi Alliance's WPA2-Enterprise certification already provides an option for EAP-SIM and EAP-AKA interoperability testing.

That said, nearly all carriers need to handle a wide variety of mobile devices on their networks. Some devices will have SIM cards (for example, smartphones); some devices may not (for example, Apple's iPad, laptops, and netbooks). Therefore, most, if not all, hotspot networks will need to support several different credential types along with their associated EAP methods. For example, X.509 certificate credentials can be used, and they provide equivalent authentication robustness as SIM credentials. Furthermore, nearly all hotspot operators have the need to provision username and password credentials for their "walk-up" customers. Code division multiple access (CDMA) carriers would likely employ username and password credentials for Wi-Fi hotspot authentication. Table 1 shows the credentials and EAP methods that provide a solid foundation upon which to establish a roaming framework.

Table 1. Credentials and EAP Methods for Roaming Networks

Credential Type	EAP Method
SIM	EAP-SIM (RFC-4186)
USIM	EAP-AKA (RFC-4187)
X.509 Certificate	EAP-TLS (RFC-5216)
Username/Password	EAP-TTLS (RFC-5281)

Next-Generation Hotspot Network Discovery and Selection

IEEE 802.11u, the amendment addressing "Interworking with External Networks," was completed by the 802.11u task group in mid-2010 and approved by the IEEE for publication in February 2011. The purpose of the amendment is to provide an effective interface between an IEEE 802.11 access network and carrier networks. The amendment adds to IEEE 802.11 the following services (this is not a comprehensive list):

- Network discovery and selection
  - Provides for the discovery of suitable networks (pre-association) through the advertisement of access network type (private network, free public network, for-fee public network), roaming consortium, and venue information.
  - Generic Advertisement Service (GAS), which provides for Layer 2 transport of an advertisement protocol's frames between a mobile device and a server in the network prior to authentication. The access point is responsible for the relay of a mobile device's query to a server in the carrier's network and for delivering the server's response back to the mobile.
  - Provides Access Network Query Protocol (ANQP), which is a query and response protocol used by a mobile device to discover a range of information, including roaming partners accessible through the hotspot along with their credential type and EAP method supported for authentication; IP address type availability (for example, IPv4, IPv6); the hotspot operator's name; and other metadata useful in a mobile device's network selection process.
- QoS map distribution
  - This provides a mapping between the IP's differentiated services code point (DSCP) to over-the-air Layer 2 priority on a per-device basis, facilitating end-to-end QoS.

The following is a, simplified sequence of events used by an IEEE 802.11u-capable mobile device to authenticate with a hotspot:

1. The mobile device comes within radio range of one or more hotspots and receives their beacons. These beacons indicate support for the IEEE 802.11u protocol via the Interworking element. The SSID element in the beacon provides the Wi-Fi network name. (In the next steps, it's assumed that the mobile device doesn't recognize any of the received SSIDs.)
2. The mobile device uses GAS to post an ANQP query to an access point for each of the SSIDs discovered in step 1. In response, each access point provides the hotspot operator's name and network access identifier (NAI) realm list.
3. The mobile device next retrieves its credential (realm) from local storage and uses it to authenticate. The mobile device then compares that realm to the list of roaming partner's realms it retrieved in step 2 (in the NAI realm list). If there is a match, the mobile device knows it should be able to successfully authenticate with that network. If there is more than one match, the mobile device uses operator policy to determine which Wi-Fi network to join.
4. The mobile device next retrieves its operator policy for network selection from local storage and looks up an ordered list of operator name and preference-level pairs for each of its roaming partners. The mobile device then compares the hotspot operator's name(s) received in step 2 with this list and selects the network having the highest preference level.
5. The mobile device authenticates to that network using its credential. In cases where the mobile device is in possession of more than one credential (for example, the mobile has a SIM and username/password credentials), it can use the NAI realm list to learn the acceptable credential type(s) and EAP method(s).

As we've just described, using ANQP with GAS, a mobile device can query the network prior to authentication to determine if the hotspot is operated by one of its roaming partners, as well as the EAP method and credential type to use. A mobile device's connection manager can now autonomously (that is, without user intervention) determine which hotspot to select taking into account operator policies, authenticate to that Wi-Fi network, and establish link-layer security using WPA2-Enterprise. Wi-Fi has become as easy-to-use and as secure as 3G cellular!

MSAP: Making Next-Generation Hotspots Even Better with New Service and Revenue Opportunities

Many venues that have deployed Wi-Fi access networks don't fall under the common understanding of hotspot, such as coffee shops, airports, and hotels. For example, Wi-Fi is being deployed in sports stadiums, retail shopping malls, and other public places. Often, these venues wish to deploy local services not accessible through the public Internet. Increasingly, carriers are operating these networks on behalf of venue owners as part of a managed service offering.

Mobility Services Advertisement Protocol (MSAP) is a protocol for service discovery, enabling the connection of users to venue services. Because MSAP is transported via IEEE 802.11u GAS, mobile devices can query for local services prior to authenticating to a Wi-Fi network. Mobile devices performing an MSAP query securely retrieve icons and service URLs; the mobile device's UI displays the icons (when enabled/requested by the user). When the user clicks on the icon, the mobile device launches an application, such as a browser to the URL, thereby accessing the service. In so doing, users are securely, easily, and immediately connected to venue-based services. Examples of such services in a stadium include display of a stadium map showing food kiosks and restrooms, looking up player statistics, and watching instant replays.

MSAP messages are Simple Object Access Protocol (SOAP) methods carrying XML payloads. An MSAP client (software on the mobile device) queries an MSAP server for service advertisements. Service advertisements include an icon, URL, related metadata, and a digital signature. The XML digital signature is used to verify the authenticity and integrity of the service advertisements. This is critical, as service advertisements are delivered prior to authentication; therefore, there is no Layer 2 security association that can protect their integrity.

Next-Generation Hotspot Deployment

As can be seen from the preceding sections, the technologies used to implement Next-Generation Hotspots are a mix of well known, well established methods, such as WPA2-Enterprise and EAP based authentication, and recently completed work (802.11u).

Although these technologies can be easily installed as software upgrades, careful planning is still required for a successful deployment. Wireless network infrastructure (access points, controllers, authentication servers), and client devices (phones, tablets, laptops) alike need new software, but hotspot functionality also needs configuration from the service provider and/or hotspot operator (venue owner).

Since a key innovation for Hotspot 2.0 is providing information to a mobile Wi-Fi device **before** it has associated and authenticated to the network (in effect, providing information to assist the mobile device in selecting a network), there are a number of potentially interesting parameters to be configured as discoverable. Examples include (but are not limited to): Venue Name, Venue Info, Operator Friendly Name, Hotspot Query and Hotspot Capabilities lists, 3GPP Cellular Network information (for hotspots having roaming relationships with cellular operators that use a SIM-based infrastructure), Network Authentication Type, IP Address Type Availability, and Roaming Consortium list.

Conclusion

Wi-Fi networks are an essential component to meet the ever-growing demand for mobile broadband. The business value of Wi-Fi will continue to expand by offering users consistent, portable connectivity. What's more, that business value will be realized via seamless authentication, provisioning, and roaming.

Cisco's innovative Next-Generation Hotspot strategy - which is based on IEEE 802.11u, WPA2-Enterprise, standards-based EAP methods, and MSAP - enables carriers to optimize their networks by offering Wi-Fi as an additional mechanism for secure mobile access of data traffic, while also helping to ensure a superior user experience. The strategy moves the Wi-Fi network from an untrusted network to a trusted and integral part of a carrier's network. The Cisco Next-Generation Hotspot provides a platform for delivering a host of new features that enhance the end-user experience with unique, context-aware services and web-based applications to increase revenue and market share through subscriber retention.

For More Information

Learn about Cisco's Outdoor Wireless Network Solution.

Read about Cisco Service Provider Wi-Fi.

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 www.cisco.com/go/offices.

Printed in USA C11-649337-04 08/12