Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Survey of Wireless Mesh Networking Security Technology and Threats

This paper will summarize the technologies and challenges related to wireless mesh networks. With the latest technologies in wireless LAN with WPA and 802.11i, enterprise deployments have finally begun to embrace wireless access networks. Wireless LAN technology has often been approached cautiously in enterprise deployments, partly due to well-known and easily exploitable attacks on early 802.11 security technology and partly due to the lack of physical control of the access medium.

Copyright SANS Institute
Author Retains Full Rights

AD

A Survey of Wireless Mesh Networking Security Technology and Threats

Technologies and challenges related to wireless mesh networks

Author: A. Gerkis

Adviser: J. Purcell

Accepted: September 2006

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Outline

1 OVERVIEW **4**

2 THEORY OF OPERATION **4**

2.1 Mesh Routing **5**
2.2 Mesh Security **6**
2.2.1 Client Access Controls 7
2.2.2 Ad-hoc Security and Research 7
2.2.3 Inter-Mesh Access Point Controls 8
2.2.4 Standardization 9

3 WIRELESS MESH PRODUCTS **11**

3.1 Cisco 1500 Series Outdoor Mesh Access Points **11**
3.2 Tropos Networks **12**

4 THREATS AND VULNERABILITIES **13**

4.1 Routing Protocol Threats **13**
4.2 Metro-WiFi Public Access Threats **13**
4.3 Physical Security Threats **14**
4.4 Wireless Intrusion Detection Limitations **15**

5 RECOMMENDATIONS **15**

5.1 Wireless security monitoring through performance management **16**
5.2 Data-center secure network architecture **16**
5.3 Information flow control **16**

6 REFERENCES **17**

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
AODV	Ad-Hoc On-Demand Distance Vector
AP	Access Point
AWPP	Adaptive Wireless Path Protocol
EAP	Extensible Authentication Protocol
IDS	Intrusion Detection Sensor
LAN	Local Area Network
LWAPP	Light-Weight Access Point Protocol
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Network
OLSR	Optimized Link State Routing Protocol
PEAP	Protected EAP
PMK	Pair-wise Master Key
QoS	Quality-of-Service
RF	Radio Frequency
SAODV	Secure AODV
SEAD	Secure Efficient Ad hoc Distance vector routing
SSID	Service Set Identifier
SUCV	Statistically Unique and Cryptographically Verifiable
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WDS	Wireless Distribution Mode
WEP	Wired Equivalency Protocol
WLAN	Wireless LAN
WPA	WiFi Protected Access

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1 Overview

This paper will summarize the technologies and challenges related to wireless mesh networks. With the latest technologies in wireless LAN with WPA and 802.11i, enterprise deployments have finally begun to embrace wireless access networks. Wireless LAN technology has often been approached cautiously in enterprise deployments, partly due to well-known and easily exploitable attacks on early 802.11 security technology and partly due to the lack of physical control of the access medium (e.g., the often cited "equivalent of Ethernet in the parking lot" concern). Often the past several years, early adoption of some 802.11i security features by the WiFi Alliance in the WiFi Protected Access (WPA) interoperability forums, as well as the standardization of the 802.11i security amendment, has greatly improved the authentication, encryption and integrity security capabilities.

However, new challenges with wireless mesh architectures using 802.11, the pending solutions with 802.11s, and the security pitfalls of metro-WiFi networks rekindle many of the original threats and technology maturity issues with ubiquitous wireless access networking. This paper contains both a survey of security technologies and the threats to wireless mesh networks. The security technologies will cover current industry capabilities and 802.11s, and the overall security architecture.

2 Theory of Operation

What is a mesh network? A mesh network is configuration of peer wireless access nodes that allow for continuous connections to a network infrastructure, including reconfiguration around blocked paths, by "hopping" from node to node. The term “mesh network” is often used synonymously with “wireless ad-hoc network”. However, ad-hoc networking typically refers to an arbitrary topology of client nodes and associated hosts, where a mesh network generally refers to a network of fixed wireless access nodes that use provide multi-hopping backhaul service between client nodes and/or the Internet. For mesh security, this subtle distinction becomes important – while most of the underlying technologies are identical, there are implicit trust assumptions assumed in a mesh network (e.g., the nodes belong to the same administrative and security domain) unlike assumed random and arbitrary collection of nodes in an ad-hoc network.

© SANS Institute 2000 - 2005 Author retains full rights.

2.1 Mesh Routing

There are multiple technologies used for wireless mesh routing that proactively and reactively determine traffic paths within the radio network. A reactive routing protocol establishes a route to a destination based on demand. A proactive routing protocol finds routing paths irrespective of the path usage or demand, often based on link state. There are vast numbers of different routing protocols that use a combination of proactive or reactive mechanisms, where most wireless mesh routing protocols are proprietary or based on academic research. However, most popular implementations for ad-hoc networks based on hybrid on-demand and link-state routing protocols, where Ad-Hoc On-Demand Distance Vector (AODV) routing is the most popular example of an on-demand ad-hoc routing protocol, which queries route information for a target destination node. The Optimized Link State Routing Protocol (OLSR) is an example of a proactive routing protocol, which uses periodic broadcasts to discover neighbor routes.

- **On-demand basic operation.** Routes discovered by issuing route request (RREQ) messages through a sub-portion of the network, and route replies (RREP) announces path to destination. Nodes maintain a list of neighboring nodes and routes to other nodes, where link breakages are reported using route error messages (RERR).

- **Link state basic operation.** Link state information is periodically exchanges between neighboring nodes in the form of periodic broadcast control messages.

Figure 1 shows and example of a hybrid AODV-based routing protocol with link-state periodic beacon messages.[1] When a node cannot find a destination in its routing list, it broadcasts a route request (RREQ) message. When the neighbor nodes receive a RREQ broadcast, a uni-cast route response (RREP) reply will be returned if the neighbor knows the route. Otherwise, the RREQ message is re-broadcast. The RREP message will a sequence number and may contains link quality information to aid in determining the optimal route. Periodically, link state information may be broadcast to advertise routing information for each node.

[1] This example shows mesh routing within a fixed wireless mesh infrastructure, which is the basic operational scenario discussed in this paper.

© SANS Institute 2000 - 2005 Author retains full rights.

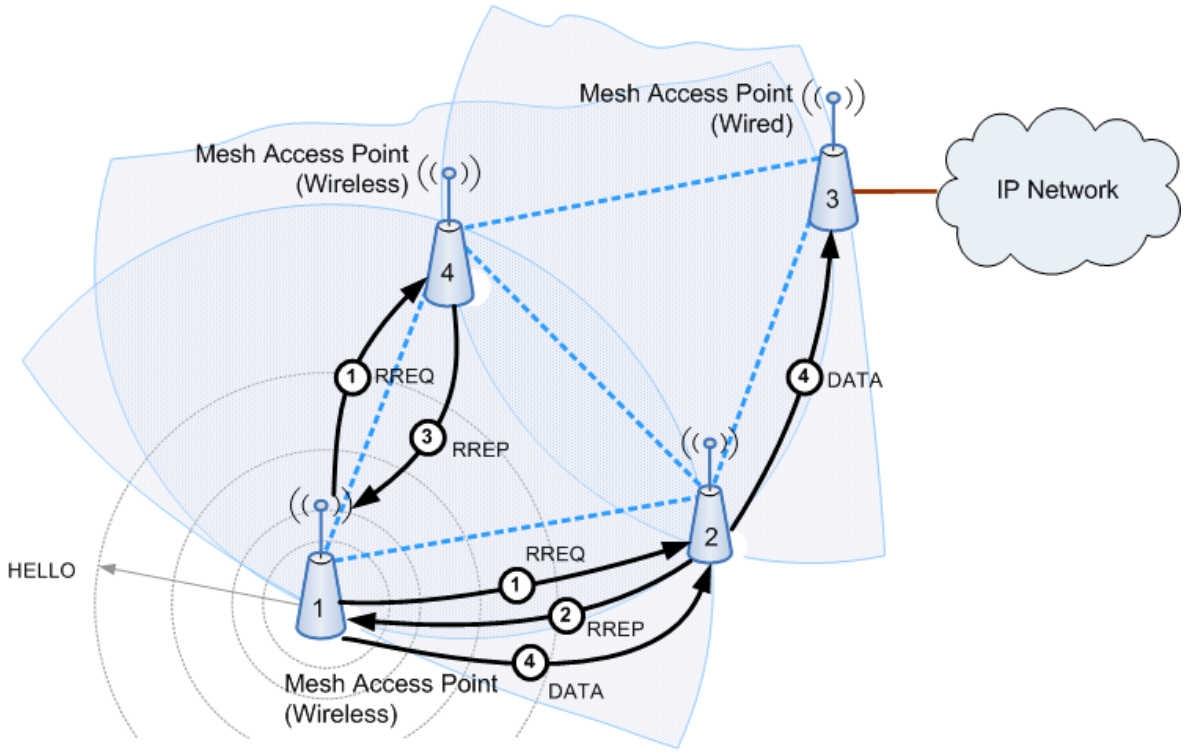

Figure 1 Hybrid mesh routing protocol example

2.2 Mesh Security

The conventional WLAN security mechanisms (e.g., such as WPA2/802.11i) provide standardized methods for authentication, access control and encryption between a wireless client and an access point. Since most wide-area mesh solutions strive to retain compatibility with commercial off-the-shelf WLAN client adapters, existing standardized WPA2 mechanisms are commonly retained (e.g., the mesh network "looks like" an access point to the client). However, there are many different types of wireless mesh architectures, where each type of architecture may use a different approach for wireless security. Many approaches for mesh security may be derived from ad-hoc security research, but any future commercial mesh products will standardize security through 802.11s (e.g., will be based primarily on 802.11i security mechanisms).

© SANS Institute 2000 - 2005 Author retains full rights.

2.2.1 Client Access Controls

Wireless mesh infrastructure networks provide access to wireless clients. In most 802.11-based wireless networks, clients are standard wireless LAN stations with no mesh networking capabilities. Some vendors, such as Motorola and PacketHop offer client mesh solutions, but all Metro-WiFi technologies are intended on providing access to non-mesh capable 802.11 stations. Client access security may vary depending on the type of network: a Metro-WiFi network may use open wireless authentication with a Layer 3 billing service access gateway, while an enterprise/private mesh network will typically use WPA2-compliant wireless access controls.

2.2.2 Ad-hoc Security and Research

Ad-hoc networks (often called Mobile Ad-Hoc Networks, or MANETs) are the evolutionary basis of mesh networking technology that forms the basis of fixed wireless mesh networks. Sharing similar concerns with fixed mesh networks, threat models for ad-hoc networks raised concerns about hackers being able to directly attack the network to delete messages, inject erroneous messages, or impersonate a mesh node. The most prevalent on-demand and link-state routing algorithms do not specify a scheme to protect data or sensitive routing information. This is mainly because any centralized entity could lead to significant vulnerability, where the security solution envisioned for ad-hoc must be based on the principle of distributed trust. [7] There are many different methods within the ad-hoc security research community to address authentication and communication protection in ad-hoc networks. Ad-hoc security research strives to resolve security issues related to trust in a dynamic and arbitrary assembly of nodes, where nodes many originate from different trust realms.

Metro-WiFi deployments will be under administrative and security control of a single network operator, where the fundamental problem is different with no real need for distributed trust. So, why does ad-hoc security matter? While the market momentum with mesh networks revolves around Internet Service Providers (ISP), companies such as PacketHop and Motorola advocate client meshing solutions. Applications for mobile ad-hoc networks are mainly in public safety, where multiple agencies may need to interoperate and communicate at an incident scene. Also, client meshing offers the ability to further extend the reach of the mesh network by providing the ability to hop through client nodes.

© SANS Institute 2000 - 2005 Author retains full rights.

In a metro-WiFi mesh deployment, the entire network infrastructure is fixed and under the administrative and security control a single entity where all mesh access points in a mesh network are assumed to belong to single logical administrative domain. Also, the 802.11s standard does not strive to secure mesh between un-trusted devices (e.g., "pure" ad-hoc networks). However, some of the concepts from ad-hoc network security provide insights into key technologies for mesh network security, where a few key ad-hoc security controls are summarized below:

- Message integrity protection using public/private key security, including transitive trust architectures, between routing peers (SUCV), or message authentication using hash chains to ensure detect tampering of routing information within the network (SEAD);
- Authentication of routing messages using digital certificates (SAODV); and,
- Protection by symmetric cryptography, using shared secrets or digital signatures (Ariadne).

2.2.3 Inter-Mesh Access Point Controls

While there are many progressive technologies available through ad-hoc security research, many commercially available mesh networks use a far more simple security model in advance of a mesh security standard. Most existing 802.11-based communication between mesh access points leverages a wireless-distribution system (WDS) mode-of-operation. A conventional (e.g., non-mesh) access point in WDS mode is simple wireless relay between wireless clients and wired access points. Many chipset vendors and mesh equipment providers offer communication protection between nodes using a static key to encrypt WDS links with WEP or AES. With the availability of fully compliant WPA2/802.11i chipsets, separate WPA2 security profiles can be defined for the WDS links (clients will be able to connect to the mesh APs with an alternate security profile – such as without encryption). Thus, there are two primary methods to protect inter-mesh AP communication in advance 802.11s standardization that are based mainly on WPA2/802.11i compliance levels for WDS mode:

- Static keys configured into the APs at both ends of the WDS link, providing WEP or AES encryptions between mesh nodes.
- WPA2/802.11i specifies how key handshake works in ad-hoc mode, letting peers derive dynamic encryption keys. This makes it possible to apply the 802.11i four-way key handshake defined for ad-hoc mode to mesh APs connected by WDS. In other words, mesh traffic relayed using WDS modes for inter-mesh AP traffic is secured by WPA2.

© SANS Institute 2000 - 2005 Author retains full rights.

It is common for each mesh AP on the network to be set with the same unique key, otherwise the mesh APs will not be able to communicate with one another. The number of session keys is directly proportional to the number of neighbors. Authentication is provided either through knowledge of a network-wide pre-shared key (e.g., in a similar manner as WPA-PSK), but some vendors already provide X.509v3-based authentication that derives unique pair-wise session keys per link.

Challenges for mesh networks relate mainly to support for broadcast between mesh APs, which is an essential component of mesh routing protocols (e.g., HELLO or RREQ/RREQ messaging). Group session keys are used for broadcast messaging, while pair-wise keys are used for unicast routing messages. The 802.11s standardization efforts will provide authentication and communication protection in consideration of these factors, and the functional requirements of the mesh routing algorithms.

The 802.11i security mechanisms and the associated WiFi-Protect Access (WPA2) profiles provide the basic building blocks for 802.11-based security (e.g., either in mesh networking or typical client access). The 802.11 security framework uses the 802.1X port-based access control mechanisms to prevent unauthorized wireless access. The client is the supplicant that requests authentication from an authentication server (e.g., typically RADIUS or in some cases the access node itself), where the authenticator (e.g., typically the AP) gates access until the client is authenticated. The authentication exchange occurs between the client and the authentication server using the EAP protocol, which encapsulates the specific type of authentication. The Extensible Authentication Protocol (EAP) is a flexible protocol used to carry arbitrary authentication information, and rides on top of 802.1X and RADIUS to protocols to transfer data between the wireless client and an authentication server. EAP does not specify an authentication method. Commonly used methods are based on TLS/SSL technologies, where a secure tunnel and network-to-client authentication can be performed using a digital certificate, and clients can authenticate using either their own client certificate (e.g., EAP-TLS) or provide a username and password authentication exchange inside the secure TLS tunnel (e.g., EAP-PEAP or EAP-TTLS). Upon success authentication, keying material is generated and distributed to enable encryption and integrity checking. The integrity checking prevents both message tampering and ensures an authenticated client cannot be impersonated. The WPA2 profile adds AES encryption and key management. The wireless security schemes for mesh networks are based on these fundamental capabilities.

2.2.4 Standardization

The IEEE is presently working on a standard for mesh networking through the 802.11s working group. The standard will use the WPA2/802.11i security methods to protect the wireless links, where the key principles in 802.11s security are summarized below:

- Standardization activities for security will focus on inter-AP security controls, where client access uses standard WPA2/802.11i authentication and encryption.

© SANS Institute 2000 - 2005 Author retains full rights.

- Standardization on security between mesh access points is still being finalized within the standard. However, link-by-link security mechanism will be based on 802.11i, with a security architecture based on 802.1X authentication.
- Mesh APs may have supplicant, authentication and authentication server roles.
- EAP 4-way handshakes must occur between all mesh routing peers, where centralized 802.1X authentication is supported. However, means of communicating between authentication server and remote mesh AP is presently not within the scope of the standard.
- The 802.11r standard for client mobility influences the security architecture by enabling a hierarchical key distribution scheme to improve mesh route maintenance. Specifically, this means leveraging key hierarchies and co-ordination with a central/trusted key-holder for pair-wise master keys (e.g., an AP acting as an authenticator will need the pair-wise master keys of the supplicant AP to generate session/transient keys prior to the EAP 4-way handshake).[2]

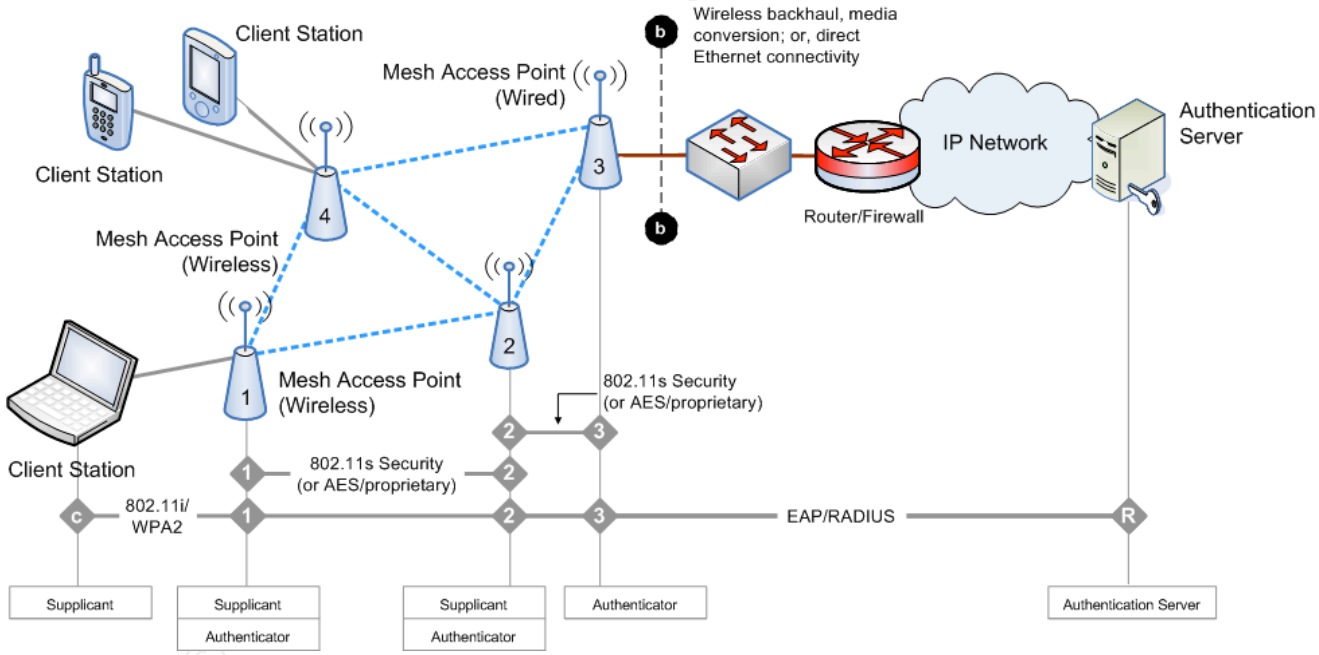

Figure 2 Wireless mesh authentication and encryption

[2] How is this different from 802.11i today? Using WPA2, the AP is always the authenticator and there is only one authenticator for the client. The pair-wise master key (PMK) is delivered to the AP by the authentication server. The same principle applies here, except that this PMK may need to be delivered to more than one AP, where the mechanism to support this is not presently defined within the scope of the standard.

© SANS Institute 2000 - 2005 Author retains full rights.

3 Wireless Mesh Products

There are a myriad of different wireless mesh networking products, where each mesh product offers different architectures and capabilities. This section briefly outlines examples of wireless security controls available in some mesh networking products.

Table 1 provides a very brief overview of wireless access controls in some mesh products. All products offer multiple SSID policies with WPA2-compliant client access; however, details regarding mesh device authentication, protection of mesh routing and multi-hopping inter-AP traffic protection vary greatly. Detailed features security features for the Cisco 1500 Series Mesh APs and the Tropos MetroMesh wireless routers are outlined in the following sections (Table 1 also provides a side-by-side comparison of the Proxim and Motorola products for comparison).

Product capabilities are often similar because the same underlying wireless security mechanisms are used for 802.11, where many competing mesh products often use the same WLAN chipsets - one can expect products based on the Atheros chipset to provide similar wireless security capabilities. Product differentiation for mesh security occurs when there are different meshes technologies or architectures. For example, in the control-plane existing mesh routing protocols ride on-top of the 802.11 MAC protocols, where the proprietary protocols themselves offer some controls. Also, security controls in the management-plane will differ greatly, whether related to device management, where the integrity of the mesh network is often directly related to the security of the device management interfaces.

3.1 Cisco 1500 Series Outdoor Mesh Access Points

The Cisco Lightweight Mesh Access Point extends the lightweight AP model to the multi-hopping mesh architecture. The Cisco mesh products were introduced following the March 2005 acquisition of Airespace, which was already developing its own mesh technology. The mesh access points connect and authenticate to a Cisco WLAN controller using a proprietary Adaptive Wireless Path Protocol (AWPP), and the products contain a rich variety of security controls as per all Cisco access points running the Cisco IOS. The following outlines some product highlights:

- 802.11i compliant station access on the first hop
- Lightweight architecture uses LWAPP with shared key or X.509v3 authentication between AP and WLAN controller
- Multiple SSID and VLAN mappings with different security policies
- Certificates pre-provisioned with digital-certificate-based trust relationship between AP and controller, where access granted by MAC address ACL tied to digital certificate
- Extensive packet filtering capabilities

© SANS Institute 2000 - 2005 Author retains full rights.

3.2 Tropos Networks

The Tropos MetroMesh™ routers provide security through conventional WPA, WEP and access control list technologies at each node, as well as a combination of controls to provide inter-mesh AP links and management traffic. The mesh access point routing uses a proprietary Predictive Wireless Routing Protocol (PWRP). The following outlines some product highlights:

- 802.11i compliant station access on the client (first) hop
- Inter-node data including end-user data protected by 128-bit AES shared key
- Multiple VLAN-to-SSID support with unique security policies, including resource priority controls through QoS support per SSID to limit bandwidth utilization
- HTTPS-based configuration and monitoring
- Mesh protocol control and management protected by 128-bit AES
- Packet filtering at the mesh edge may be configured to only allow VPN traffic to enter the mesh network

Security control	Tropos 5120	Cisco AP1500	Motorola HotZone Duo™	Proxim 4000M
WPA/2802.11i client access	Yes	Yes	Yes	Yes
Multiple VLAN/SSID security policies	Yes	Yes	Yes	Yes
Device authentication	Yes (WPA-PSK)	Yes (X.509v3)	Yes (X.509v3)	Yes (Shared Key)
Mesh protocol integrity protection	Yes	No	No	No
Inter-mesh AP payload encryption	128-bit AES (Shared key)	128-bit AES	128-bit AES	128-bit AES (Shared key)
Secure management	HTTPS SNMPv3	HTTPS SNMPv3	HTTPS SNMPv3	HTTPS SNMPv3

Table 1 Mesh product security comparison

© SANS Institute 2000 - 2005 Author retains full rights.

4 Threats and Vulnerabilities

4.1 Routing Protocol Threats

Wireless mesh networks may be susceptible to routing protocol threats and route disruption attacks. Many of these threats require packet injection with a specialized knowledge of the routing protocol; however, these threats are unique to wireless mesh networks and are summarized below:

- **Black-hole.** An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets, where attracting packets involves advertising routes as low-cost.
- **Grey-hole**. An attacker creates forged packets to attack and selectively drops, routes or inspects network traffic.
- **Worm-hole.** Routing control messages are replayed from one network location to another, which can severely disrupt routing.
- **Route error injection.** An attacker disrupts routing by injected forged route error message to break mesh links. Relative to the other routing attacks, this attack conceivably has high exploitability because it does not require detailed knowledge of the routing protocol state model (e.g., a replay attack is possible, and route errors are typically stateless).

The risk associated with these threats depends on the routing technology or mesh network architecture. In a mesh network, the exploitability of these threats may vary greatly – a network based on a known protocol such as AODV is more susceptible than a proprietary routing protocol. Similarly, a mesh network that uses message integrity checking for routing messages and device authentication will substantially decrease the threat risk (note that X.509v3-based trust or unique per hop security as per 802.11s offers greater security than basic security controls such as system-wide shared keys).

Why are these attacks interesting? Unlike denial-of-service attacks on 802.11 MAC management frames or using RF interference, mesh disruption attacks have the potential to cause service degradation far beyond the reach of a single malicious transceiver.

4.2 Metro-WiFi Public Access Threats

Metro-WiFi threats depend on the deployed mesh products, as well as the network access strategy for the wireless operator. Mesh networks that provide free public access are susceptible to attacks based on the implication of open authentication (e.g., public access is synonymous with no pre-established trust to the wireless network). While many municipal wireless projects allow free Internet access, operators typically offer shared or graded service via a Layer 3 service gateway. Companies such as Pronto Networks offer solutions that simultaneously allow for protected access, a variety of service plans, and "walled-gardens" within the same network using SSID/VLAN mapping with SSL-encrypted gateway registration and authentication.

© SANS Institute 2000 - 2005 Author retains full rights.

- **Spoofing of wireless infrastructure.** An attacker uses an "evil twin" or "man-in-the-middle" attack to execute an information disclosure threat. In an enterprise deployment, such attacks are mitigated using EAP methods that allow mutual authentication between a client and the infrastructure (e.g., EAP-TTLS, EAP-TLS or EAP-PEAP).

- **Denial-of-service attack.** An attacker may either use IP flooding as well as attacking network services, or 802.11 MAC management attacks. The 802.11i-based link level security model supports authentication, key distribution and encryption for mesh management frames, where MAC management frame protection is not addressed within 802.11s.

- **Theft-of-service attack.** An attacker steals valid user credentials or performs paid-user session hijacking (e.g., "freeloading"). Many WiFi systems use a service gateway or captive portal to secure paid access – a captive portal uses SSL-secured Web page where users authorization credentials. After authentication, the captive portal authorizes the client to network access by registering the valid client MAC and IP addresses in the gateway. Alternatively, malicious users could relay traffic across the mesh network without traversing a network gateway (e.g., peer-to-peer traffic across the mesh backhaul).

These attacks do not represent any new threats for mesh networks relative to existing WiFi hotspot services. However, mesh networking for municipal wireless has broadened the possible scope of usage and availability of public access networks.

4.3 Physical Security Threats

Conventional wireless network deployments are within an enterprise environment with physical and administrator control of the operator or agency. Outdoor wireless mesh networks require that the mesh access points be outside the physical control of the operator, typically in environments that are not trustworthy (e.g., on a light-pole or an leased building exterior).

- **Outdoor deployment poses more challenges for physical device security.** Wireless mesh access points are mounted remotely on light-posts or externally on buildings, where a wide-area deployment may have several thousand such devices in an environment that is not within the physical and administrator control of the network operator.

- **Wired mesh access points require network connectivity.** Wired network access points sometimes require wired media backhaul, which may expose sensitive network connections.

© SANS Institute 2000 - 2005 Author retains full rights.

4.4 Wireless Intrusion Detection Limitations

Intrusion detection has become a feasible means of detecting threats against wireless networks. Since the 802.11 medium access control technology is susceptible to denial-of-service attacks, as well as the possibility of spoofing legitimate access points, wireless intrusion detection systems have offered some defense through detection of wireless network attacks. However, wide-area wireless mesh networks make wireless intrusion detection much harder due to the distributed geographic distribution of wireless nodes. For example, any 802.11 MAC management vulnerabilities are mainly addressed by detection, rather than prevention. Wireless intrusion detection sensors are often used in enterprise wireless networks to detect common 802.11 attacks, including MAC management attacks as well as "evil twin" or "rogue AP" attacks (e.g., rogue AP attacks are mitigated by mutual authentication using EAP-TTLS/PEAP/TLS as per wireless network deployments best practices).

- **Open authentication will imply limits on network authentication**. Wireless intrusion detection sensors are most effectively deployed indoors in a bounded physical locale, where wireless IDS models to wide-area outdoors deployment extended is not feasible.

- **Integrated threat detection**. Mesh access points that provide integrated detection and prevention controls for wireless threats will best address the security threats. This may include security features that detect MAC management attacks (e.g., de-authentication or MAC association flooding, etc.) or report unauthorized mesh AP evils-twins broadcasting within the deployment area.

5 Recommendations

Offering recommendations can often provide a false sense of security, as threats are difficult to anticipate and may often exploit previously unknown vulnerabilities. Ultimately, proper implementation and management of security controls, as well as best practices for wireless access restrictions, are intended to mitigate risks associated with attacks against network availability or user confidentiality and privacy. Securing wireless networks must always be treated carefully, mainly due to the inherent trust disparity in a wireless network (e.g., the access medium is no longer under operator physical or administrative control) and existing limitations in 802.11 MAC protections. Wireless mesh networks amplify these challenges, where such networks now extend far beyond the physical control of the operator, and easily available open networks provide opportunities for malicious activities against unsuspecting and uneducated end-users.

Denial-of-service of the 802.11 wireless media, either through MAC packet injection or other means, still remains the foremost concern related to wireless networking. Even with known vulnerabilities in WEP, wireless networks are often successfully secured with a combination of WLAN, VPN, firewall, intrusion detection controls and application security controls such as HTTPS (e.g., the usual defense in depth strategies).

© SANS Institute 2000 - 2005 Author retains full rights.

5.1 Wireless security monitoring through performance management

For wide-area outdoor wireless mesh networks, explicit wireless intrusion detection probes are not feasible, where integrated and intelligent threat detection and management should be integrated into the wireless mesh access points. Also, mesh performance management metrics and indicators should be leveraged to alert operators to potential denial-of-service attacks. Most mesh networking products and systems provide performance management systems that focus on optimizations for the mesh routing algorithms and alert operators to potential interference problems in unlicensed bands. With appropriate element management strategies, properly interpreted performance management information can be used to identify signatures of many denial-of-service attacks (e.g., poor packet completion rate, unexpected changes in routing paths relative to a system baseline, etc.).

5.2 Data-center secure network architecture

With the proliferation of municipal wireless network using mesh-networking technology, operators must consider protection for their data center and inter-networking core networks. Firewalls, service gateways and wireless application segregation principles to enforce wireless access controls must always be employed – irrespective of advanced 802.11i-based mesh security, the wireless network will always be treated as an un-trusted network segment.

5.3 Information flow control

The business-case for wireless mesh network hinges on shared network use with combinations of public access and secure private networking (e.g., for municipal services or public safety), which implies the need for carefully architected secure network architectures to authenticate and segregate users. Despite the ability to enforce multiple concurrent wireless security policies in the mesh network, many agencies sharing such a municipal network will require VPN gateway access to their private networks. When using VLAN/SSID-based segregation and security policies, packet filtering and access control should be applied at the client-side edge of the mesh network as a defense-in-depth strategy. Also, enforcing traffic flow between wireless clients and a designated gateway can mitigate the misuse of a wireless mesh infrastructure for peer-to-peer theft-of-service.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

6 References

[1] RFC3561 Perkins, et. al., "Ad hoc On-Demand Distance Vector (AODV) Routing" (July 2003)

[2] "Multi-Layered Security Framework for Metro-Scale Wi-Fi Networks", Tropos Networks White Paper (February 2005)

[3] "Deployment Guide: Cisco Mesh Networking Solution", Cisco (Release 3.2)

[4] Klein-Berndt, L. "A Quick Guide to AODV Routing", Wireless Communications Technologies Group, NIST (http://w3.antd.nist.gov/wctg/aodv_kernel/)

[5] Jones, D., "Metro-Mesh: A Hacker's Paradise?", Unstrung: Dark Reading (May 24, 2006)

[6] Cheng, Z., et. al., "Security Analysis of LWAPP" (April 7, 2004)

[7] Milanovic, N., et al., "Routing and Security in Mobile Ad Hoc Networks", IEEE Computer Society (February 2004)

[8] Yih-Chun Hu, et. al., "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy (May/June 2004)

[9] Xia, H., et. Al., "Detecting and Blocking Unauthorized Access in Wi-Fi Networks"

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced