



CITAS GROUP LLC

Audit • Enterprise Risk Services • Technology

Designing and Deploying a Secure 802.11 Wireless Infrastructure

Everett Washington
Managing Partner
Enterprise Risk & Technology Services
Citas Group, LLC
www.citasgroup.com
678.925.1447

- What is a Secure Wireless Deployment
- Why the Need for a Secure Wireless Infrastructure
- Overview 802.11 Wireless Standards
- Steps for Deploying Wireless Securely
- Summary
- Additional Information
- Questions

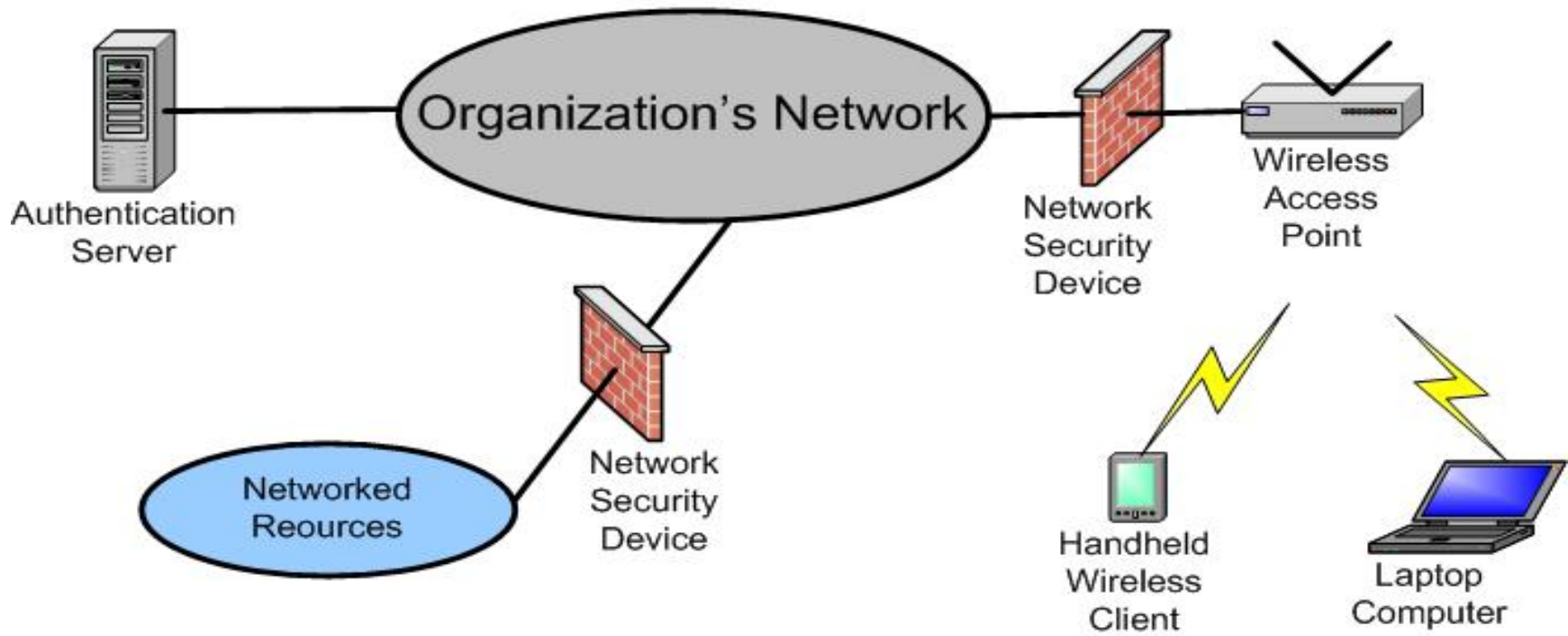
What is a Secure 802.11 Deployment?



- A deployment that satisfies an organization's operational needs and requirements while adhering to the established security policy.

What is a Secure 802.11 Deployment?

Security Architecture



Why is Security Needed?



- Three options for wireless proliferation
 - Planned
 - Unsupported
 - Ad-hoc
- Deployment of wireless within an organization extends the boundaries of the network, increasing the exposure of the infrastructure.
- Increased risk of attack and compromise

Why is Security Needed?



“...Intruders first hopped onto the Wi-Fi network at the Lowe's store in Southfield, Michigan....They used the store's network to access the company's central data center at Lowe's North Carolina headquarters....The intruders returned at least six times over the following two weeks and used the network to access store networks at seven other Lowe's locations around the country, in Kansas, North Carolina, Kentucky, South Dakota, Florida, and two stores in California. The intruders deployed unspecified hacking software at some of the stores, in one case crashing the point of sale terminals at a Lowe's in Long Beach, California...”

Overview of 802.11

- 802.11 wireless (Wi-Fi) devices use Radio Frequency (RF) technology to facilitate communication
 - Currently defined standards
 - 802.11 – Original standard established in 1997
 - Operates in the 2.4Ghz range with a maximum throughput of 1-2mbps
 - 802.11a
 - Operates in the 5Ghz range with a maximum throughput of 54Mbps
 - 802.11b
 - Operates in the 2.4Ghz range with a maximum throughput of 11Mbps
 - 802.11g
 - Operates in the 2.4Ghz range with a maximum throughput of 54Mbps

- 802.11 Related Organizations
 - IEEE 802.11 Working Groups
 - Defines official 802.11 standards
 - Comprised of individuals
 - Wi-Fi Alliance
 - Consortium of companies within the wireless industry
 - Primary importance is in the area of security certification
 - Responsible for the Wi-fi Protected Access (WPA) standard that addresses weaknesses in WEP

Overview of 802.11

- 802.11 Security Standards
 - Wired Equivalent Privacy (WEP)
 - Included as part of original standard
 - Insecure, easily broken
 - Wi-Fi Protected Access (WPA)
 - Addresses weaknesses of WEP
 - Short-term solution
 - 802.11i
 - Based on WPA
 - Supports 802.1x
 - Enables enhanced authentication
 - RADIUS
 - Certificate

Steps to Securely Deploy



CITAS GROUP LLC

Audit • Enterprise Risk Services • Technology

802.11

- Plan
- Design
- Deploy
- Support

- **Determine Business Need**
 - Identify factors driving the deployment of 802.11 within your organization
 - Increased productivity
 - Decreased costs
 - Portability
 - Executives/senior management

■ Define Requirements

□ Business

- Document in detail the specific business requirements an 802.11 deployment will address
 - Integration with business partners
 - Supply chain
 - Inventory tracking
 - Data entry
 - Check in procedures

- Define Requirements
 - Security requirements
 - Complies with your organization's Security Policy
 - Adheres to organization's Security Strategy
 - Integrates into the Security Architecture

- Define Requirements
 - Technical
 - Detail interface, throughput, latency, protocols
 - Compare against other wireless solutions
 - Cellular
 - GSM
 - CDMA
 - Satellite
 - Operational
 - Support requirements
 - Roles and responsibilities

- Perform Site Survey
 - Determine areas that need wireless coverage
 - Identify possible wireless leak issues
 - Physical location and security
 - Power and environmental issues

■ Select Solution

- Use detailed requirements and site survey data to select equipment
 - Ensure that

- Design document
 - Document details of the configuration
 - Location of equipment
 - Type of equipment

- **Develop implementation plan**
 - Develop a detailed implementation plan for building the architecture
 - Ensure that resources are available and trained
- **Document the configuration**
 - Create diagrams and detailed configurations to assist in supporting and maintaining the deployment
- **Review the deployment**
 - Compare defined requirements and objectives against the deployed solution
- **Perform security review**

- Plan the deployment
 - Develop a detailed implementation plan for deploying the solution
 - Ensure that resources are available and trained
- Document the configuration
 - Create diagrams and detailed configurations to assist in supporting and maintaining the deployment
- Review the deployment
 - Compare defined requirements and objectives against the deployed solution

- Develop support and maintenance plan
 - Document roles and responsibilities
 - Document configurations
- Plan and budget for continued growth
 - Once deployed, the use of Wi-fi in an organization generally grows rapidly
- Perform a periodic security review of the infrastructure
 - Identify rogue access points or unauthorized clients

- Plan the deployment by identifying business needs, detailing specific requirements and objectives
- Design the solution to meet business and security requirements
- Document deployment procedures and follow the plan
- Support and maintain the wireless infrastructure once deployment is complete

Additional Information



- <http://www.wardrive.net/>
- <http://www.drizzle.com/~aboba/IEEE/>
- <http://www.wi-fiplanet.com/>
- <http://www.kismetwireless.net/>

Questions

