Global Information Assurance Certification Paper

UNDERSTANDING SECURITY ISSUES
&
ADDRESSING THE CHALLENGES IN DEPLOYING
&
PROTECTING ENTERPRISE WIRELESS NETWORKS

Version 1.4b
Option 1
GSEC Certification

Shikhar Parjan

07/25/2004

Table of Contents

i.	Abstract	2
ii.	Introduction	2
iii.	Overview of the Wireless Enterprise	3
iv.	Wireless Network Security Vulnerabilities	3
v.	Active versus Passive Attacks	5
vi.	How secure are Enterprise Wireless Networks?	6
vii.	Implications for the Enterprise	7
viii.	Implementing Wireless Policy Management	8
ix.	WLAN Policy Management & Deployment Process	9-15
x.	Simple processes and guidelines for the IT Manager	15-20
xi.	Summary	20
xii.	Bibliography / List of References	20-21

Table of Diagrams

Fig. 1	Wireless Access Attempts and ways of data Theft/Manipulation	4
Fig. 2	'Man in the Middle' attacks	5
Fig. 3	Counterfeiting results in user authenticating to Rogue AP	5
Fig. 4	Active and Passive Wireless Attacks	6
Fig.5	Overview: Implementing Wireless Policies	9
Fig.6	Sample Nmap display	18
Fig. 7	A Driftnet screen capture	19
Fig.8	Enforcing Security Mechanisms	19

Abstract

This paper presents an overview of challenges and scenarios encountered by Enterprises, covers recommended stages and phases in a wireless LAN deployment and the need for management approval and buy-in. After outlining the Management processes and responsibilities from a policy standpoint, the coverage extends to provide a brief insight into some Best-known-methods (BKMs), suggested practices and tools available at the level of the person responsible for seamless day-to-day functioning of the Wireless Network – The IT Manager.

A wireless network is as secure as the policies behind it, and due diligence should be imparted in rooting out hidden vulnerabilities and avoiding common implementation pitfalls and security holes. Wireless LANs are great tools for increasing workplace productivity, therefore a little extra care during setup will go a long way in improving user satisfaction, providing seamless-yet-secure connectivity and ensuring inter-operability with existing wired networks

Introduction

As modern Businesses –Small,medium and large- seek to maximize their operating efficiency by rolling out 802.11 based Wireless networks, they need to ensure that the rollout is secure, smooth and protects the security and reliability without impinging on the accessibility and ease of administration aspects

With the increasing deployment of wireless networks, a lot of exciting opportunities and new horizons have opened in terms of user connectivity, enablement and productivity.

A study by Intel's IT department found that wireless connectivity delivers 16 minutes of additional productivity per day and a return on investment of over $6,000 per person-and that is just at the office.
(http://www.intel.com/business/bss/infrastructure/mobility/build_foundation.pdf)

Even the standard assumption about what defines a network has undergone a transformation from typical LAN environments to wireless ISPs to ad-hoc networking. This change has been predominantly brought about by acceptance of IEEE 802.11 wireless protocol suite, leading to dramatic changes in costs, adoption rates and technical implementation of wireless networks.

Of course, like any other paradigm shift, there are associated risks and security issues which come with the freedom to go wireless, causing many a headache and challenges to end users and network administrators. The lack of physical security, access to free auditing tools that double as attack tools, and the ability to monitor traffic without risk of being noticed make wireless networks an easy

target for malicious hackers. Every link of the wireless network needs to be protected in order to properly secure Enterprises' data. It is important to know the potential and scope for attacks and the real risks in deploying a wireless network before attempting to secure one.

Overview of the Wireless Enterprise

According to recent IDC predictions, by 2005, there will be 489 million wireless users globally and will outpace wired users who will be at 400 million. (http://www.airshare.org/learn/articles/features/symantec.cfm).
Driven by lower retail prices, availability of sturdier models with good battery life and deployment of 'desktop replacement' laptops –where a laptop with high disk capacity, large RAM and faster processor is deemed to be the successor of previous enterprise desktop- has led to adoption of laptops in large numbers by enterprises globally. Employees on the road stay in touch with a basic wireless connection – be it waiting in airport lounges or having meals on the go. Smaller handheld PDAs, Blackberry devices and smarter cell phones have paved the way for a convergence of boundaries between analog, digital, cellular and wireless worlds, imparting added responsiveness and increased productivity

Wireless Network Security Vulnerabilities

This increased mobility presents scenarios which have an increased element of risk associated with them. For example, with built-in support for 802.11, Bluetooth, Infra-red and WLANs, there is a proportional increase in the number of ways to open a backdoor into the Corporate network.

Enterprise workstations, which till recently were secured in the physical confines of the workplace increasingly find their way in public places like airports, hotel rooms & cafes.

The same ease of seamless connectivity and easy exchange of business information now presents itself to the whole world for potential misuse and hacking, and if left unsecured can cause incalculable loss of a Company's Intellectual Property (IP) and can be a goldmine in the hands of the competition. Added to this is the scenario of physical loss of assets during airport security check-ins, theft and getting misplaced in public locations, and the security vulnerabilities increase manifold.

Enterprises worldwide are spending approx. $20 billion *per year* on IT security alone, yet costly breaches continue to occur with unfailing regularity. To further complicate matters, a Gartner study estimates that 3 out of 4 external attacks come in by tunneling through applications and as such are able to bypass the traditional security mechanisms.

Wireless technology - by it's unbound and unhindered nature – is all pervasive in within it's radius of deployment, with transmitted signals capable of passing from the data center, to the boardroom, to the neighboring parking lot –and potentially the whole world, including beign intercepted by a hacker parked nearby

This worrisome scenario calls for a brief coverage of ways and means a legitimate business's Intellectual Property (IP) – its trade secrets, email communications and financial data – can be compromised. What follows is a discussion on unauthorized wireless access, wireless network disruptions and hacking attempts.

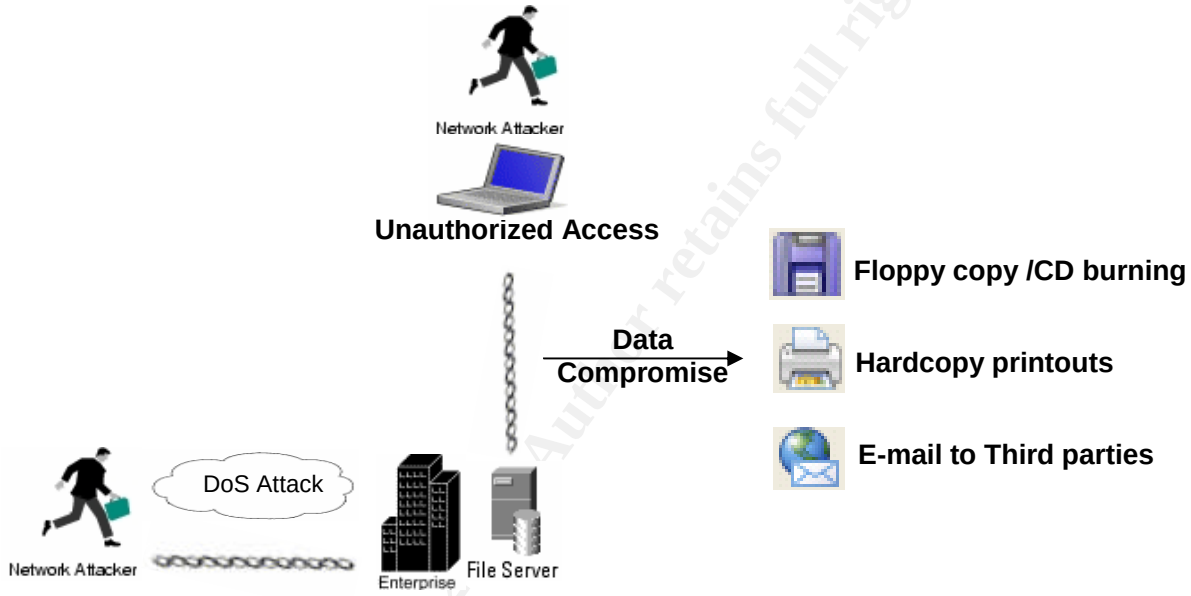

Fig.1 Wireless Access Attempts and ways of data Theft/Manipulation

As shown in Fig.1, there are several ways by which a hacker/intruder can; by initially breaking through and gaining access to a Company's business Network and file servers, and then proceed to steal data through several means available (burn to CDs of technical designs, take printouts of payroll info and gain access to Corporate Exchange Servers' Address book for sale to spam vendors).

A more serious breach can take place where a technically adept attacker can launch a Denial-of-Service (DoS) attack on the Website and e-commerce gateways of the company, effectively paralyzing business and turning away web customers.

Often, hackers launch '**Man-in-the-middle**' attacks, where a Wireless client receives a spoofed Authentication message, on receipt of which, the client starts sending data which is intercepted by the hacker.

This type of attack is shown as:

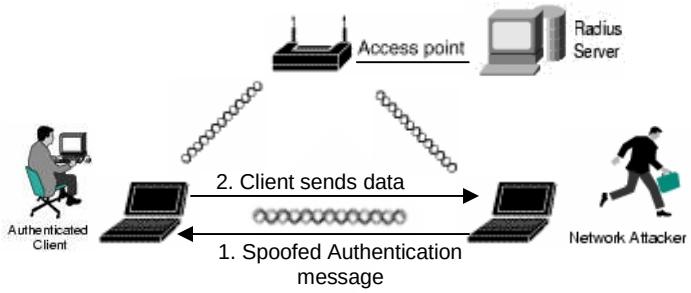

Fig. 2 'Man in the Middle' attacks

Another variation example that can be discussed here ,is the increasingly common technique employed by experienced hackers of '**Counterfeiting**' which attempts to hijack the credentials of bona fide users during Association/Disassociation from Access points by setting up rogue Access points to lure valid authorized users to pass on their credential information to them. This effectively intervenes and masquerades as an Access Point of the Enterprise's Wireless network. Data so gleaned from such 'sessions' can be used to get valuable numbers such as Credit card and Social Security Numbers etc. These can easily be seen as

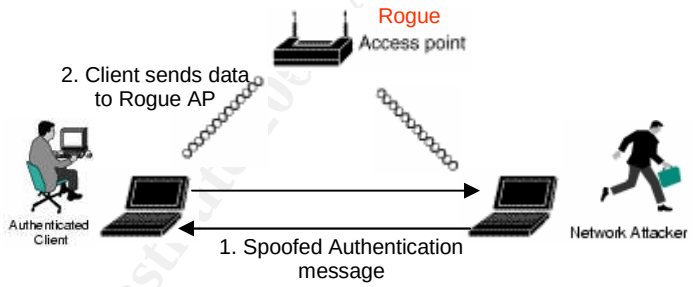

Fig. 3 Counterfeiting results in user authenticating to Rogue AP

Active vs. Passive Attacks

In essence, therefore the various types of Wireless Attacks can be classified as Active or Passive Attacks. In an Active attack, the hacker (say from a rival company) launches a Denial-of-service (DoS) attack or after gaining access, seeks to destroy, alter and delete data so as to render the business potential and activities of the attacked company useless and incapable.

A passive attack takes a more subtle form -similar to Industrial espionage – where the aim of the intruder is to sniff out info and gain a knowledge of Corporate policies etc by relying on methods which would normally avoid detection such as Capture and replay of passwords, eavesdropping on secure connections and using protocol Analyzers and other tools.

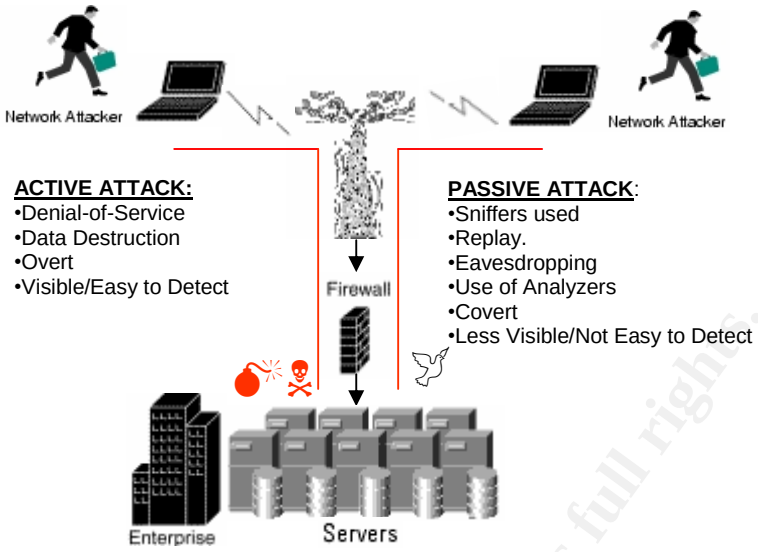

Fig. 4 Active and Passive Wireless Attacks

How secure are Enterprise Wireless Networks?
It would appear that the challenges and security implications briefly outlined above would appear daunting to even the most die-hard IT manager, and can either deter an Organization from implementing Wireless Solutions ; for a good reason, given the fact that data can so easily land in wrong hands.

Or, it could be argued that all the Enterprises going in for Wireless deployments would have taken enough and suitable steps to avoid the pitfalls of data loss and secured their networks end-to-end.
The actual reality is somewhere in the middle:
While enterprises are increasingly convinced about the benefits of wireless technology, and have been proactive in allotting resources and installing wireless networks in their businesses and warehouses, a quick check reveals that in several,if not most cases there are several lacunae and loopholes in their wireless network in terms of overall security, ease of intrusion and simple authentication and access controls which can be hacked into by any intruder with a standard laptop.

The reasons given by Enterprises for rolling out Wireless networks without a proportionate focus on security can be listed as:

Added Expense:
Setting up Wireless Security is an additional expense which gets sacrificed at the cost of increasing the reach/ number of users with wireless capability

Expensive to maintain:
Security measures call for regular audits, testing and upgrading which makes it expensive to maintain

Inconvenience:
There is an 'inconvenience factor' associated with following security procedures such as longer access times when going through an Authentication server, on top of a slower Wireless connection that may lead to a lowering of guard in terms of providing the right security envelope for the wireless network

Too much learning time:
Often, the end-users complain of the multiple times they might have to provide their credentials, remember passwords for different systems (Windows logon, VPN logon etc.) and may not be inclined to learn, understand and follow basic security procedures, and might go down an easier path

Financial risk:
As wireless is still an emerging technology, its security issues are still being discovered and therefore can lead to a situation where an Organization finds that it's customer and business needs need multiple levels of diverse technologies and applications which may not yet have been suitably tested or deployed over wireless, thus introducing an element of financial risk for Management

Implications for the Enterprise

An understanding at the enterprise level, that wireless resources need security and configuration management policies, just like their wired counterparts, will lead to an increasing awareness in the workforce of the need to be secure and protective of their data while using handhelds and laptop systems away from the secured office network. (Office LAN based networks (conventional Ethernet deployments) have their own vulnerabilities, but those are already well documented and are not the focus of this document).

Undoubtedly, this proliferation of planned as well as ad-hoc wireless networks throws up interesting combinations of hitherto unavailable deployment scenarios as well as issues such as securing a network from a intruder sting with a laptop in a car in the parking lot. In essence, the implications for the enterprise can be listed as:

- Benefits accrued in terms of user productivity and expected RoI (Return on Investment) of a Wireless deployment can be negated just as easily if there is an absence of a security and management policy, and a lack of audit and enforcement of the same.

- Given the potential of misuse and loss of data, there is a high degree of risk in terms of legal liabilities e.g. loss of data from clients covered under strict NDAs (non-disclosure agreements), financial loss and adverse impact on a Corporations brand equity.

- The level of complexity of a Enterprise network goes up, when , in additional to the task of putting and managing firewalls, VPNs, authentication procedures and anti-virus software, for the wired network comes the added task of managing the independent and numerous wireless devices from different manufacturers, each with potentially different security and management vulnerabilities

- This in turn means an expansion of the network perimeter, and adding these devices under a security and configuration management umbrella. With companies adopting wireless and handled devices faster than any other platform, there is a very serious risk here.

- Analysts predict that by year 2007, there will be nearly 120,000 WLAN hotspots (gateways for wireless access) worldwide, allowing wireless connectivity to public and private networks for over 200 million mobile platforms

- Another prediction estimates that more than 60% staff in Global 2000 companies will be accessing, over wireless, their corporate applications and also that 40% of corporate data will be on handheld devices by 2005 – data like address books, contacts, meeting notes, enterprise applications etc

The key take-away from these scenarios is that Enterprises need to be that much more proactive in establishing a policy for the adoption of Wireless LANS, in view of the rapid proliferation of Wi-Fi enabled laptops and the inevitable emergence of rogue networks. A lack of understanding and resources to address these challenges would simply risk losing network integrity, and bring down the value-add from these otherwise excellent productivity tools

Implementing Wireless policy management:

Having understood the problem definition in the scenarios listed above, it makes sense to talk about what can be done from the enterprise standpoint, to safeguard infrastructure investments, manage network resources and derive the maximum productivity at a minimum risk to the security and privacy of corporate networks.

A wireless network can, by breaking down constraints of wired connectivity can give a strong boost to employee access to resources and make him more productive, yet at the same time it does call for proper planning in doing so and needs to be done in a phased manner

This can be defined in terms of a process which can be outlined as:

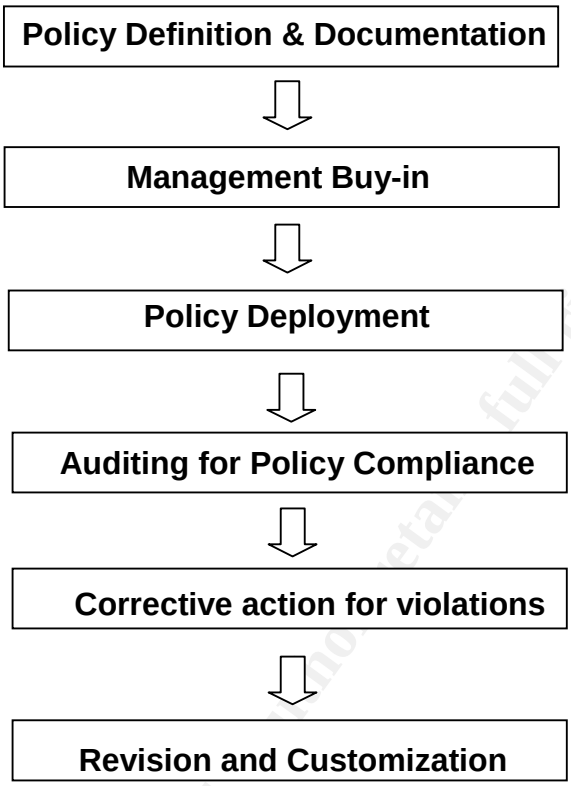

Fig.5 Overview: Implementing Wireless Policies

WLAN Policy Management & Deployment Process

The process for proposed implementation, along the lines of the flow chart shown above should be discussed, reviewed and documented. In the event of a rollback for example, due to budget or any other consideration, or for implementing a revised plan, this kind of 'milestone based' deployment can be used to restore the network to a 'as-is' state –say for more testing and verification through pilot programs.

Like any other project implementation, it would be useful to conduct a Product Life Cycle based comparison (PLC Proposal) to understand stages such as Concept Approval by management, Uniform Specifications and guidelines pertaining to Access Points, Violation recording procedures etc. so as to have a consistent rollout across different locations, in a 'no-surprises' cookie cutter format. The process can be defined as:

1. Policy definition and Documentation:
The initial step in addressing management of WLAN assets would be documenting the features, requirements and procedures for an enterprise WLAN policy. The key features of a WLAN policy can be outlined as:

- WLAN usage
- Network Configuration
- Security
- Network Performance

a. **WLAN usage policies**: Definitions to cover permitted applications to be run on WLANs, and also locations where WLANs can or cannot be deployed would form the basis of corporate wide deployment of Wireless Networks. Further details can also give guidelines for roaming policies between access points within a building and also across different locations, as well as policies for allowing public hotspot access.

b. **Choosing applications to run on WLANs**: Even though most of the applications can be run on wireless LANs, there would be concerns about running sensitive applications due to absence of strong and foolproof security standards. Some applications, by virtue of their requirement of running over high-speed Networks such as ERP server farms etc may lead to slower response times when implemented on Wireless networks which may be found to be unacceptable to end customers. The decision whether to deploy an application on Wireless can only be satisfactorily made if the key decision makers are comfortable and aware of the capabilities and limitations of Wireless technology.

c. **Bandwidth usage**: An area of concern would be use of unauthorized apps such as music downloads, unauthorized P2P networks which can effectively reduce total available bandwidth for legitimate applications and restrict WLAN capabilities

d. **Network roaming**: Need for roaming comes with the security concern arising due to a station not authenticating itself to each access point. There would be a strong need to establish policies for roaming within the WLANs. User based permissions can be set for WLAN access within a particular location, or allowing roaming capability within the enterprise.

e. **Policy for public hotspot usage**: Increased proliferation of public hotspots , while providing ease of connectivity- a very key feature for popularity of WLANS, also allows hackers to take advantage of users and also cause unauthorized associations with neighboring networks

f. **Home Wireless connectivity**: As users increasingly bring their laptops home and try to connect to work using their home wireless LANs, it should be emphasized that such a connection needs to have a personal firewall

for all traffic to pass through, and give out instructions for management of personal firewalls

g. **Encryption & Authentication for all WLAN traffic:** The security loopholes associated with Wired Equivalent Privacy (WEP) are many fold – WEP's key can be broken by Statistical Key derivation – a Passive form of attack, where computing power alone will, over time yield the Key Scheduling Algorithm from the RC4 cipher used in WEP- within 4 hours. Other attacks like the Inductive Key Derivation based Active Network Attacks and Initialization Vector replay attacks are covered in detail in a Wireless LAN Security White Paper at: http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

   It is surprising at the number of wireless networks that do not enable even this minimal security feature, allowing for easy sniffing of their networks. In addition to basic WEP encryption, enterprise policies can be tailored around vendor proprietary implementations such as Cisco, which offers LEAP (Lightweight Extensible Authentication Protocol) & PEAP (Protected Extensible Authentication Protocol).Stronger encryption, as offered by WPA (Wi-Fi Protected Access) and 802.1x based deployments are also good, secure ways to administer authentication.

h. **MAC filtering/RADIUS deployment:** MAC filtering does allow a basic level of security based on filtering of unauthorized MAC addresses, thereby preventing unauthorized access and also giving a degree of QoS (Quality-of-Service) to existing users . RADIUS servers can be used in larger enterprise deployments with multiple users and need to force all Access Points to pass user traffic through a RADIUS server

i. **Renaming the Network SSIDs:** Default SSIDs (Service set Identifiers) are attractive to hackers for gaining access to vulnerable WLANs

Other significant steps can include changing the default settings in Windows XP, so as to prevent a device from scanning and associating with any available WLAN, thereby putting network security at risk .Another step is to clamp down hard on any unauthorized access point being setup in workplace by users, thereby by passing existing network policies and allowing intruders access to the network, from say a parking lot outside the office.

How much is not enough: Perform a risk and benefit analysis

Before deploying an Wireless Network, key stakeholders –Managers and IT- must conduct a close review of the associated risks that every component of the enterprise's network presents. They must think - 'What if this component were attacked and rendered useless?' and then consider what security options are available to protect the component or resource.

2. Management buy-in:
This is a essential step in granting authority and rights to the implementation team to have an effective implementation on ground- thereby indicating the seriousness with which the management is interested in having a secure, functional wireless network in place. It needs to be documented, discussed, reviewed and approved by key stakeholders, thereby ensuring the right expectations when it comes to gauging performance, business case and RoI on a WLAN deployment. Without appropriate management buy-in, it would be extremely difficult to have users implement the recommendations of the technical team and will lead to constant issues like security flaws, unauthorized access and complaints of slow networks- all of which can be traced down to loopholes in implementation.

Another benefit of having commitment from management at the outset, through the formation of a Wireless Implementation Task Force or Committee is that a milestone-based implementation can be carried out, which provides audit and oversight capability over the technical team assigned with doing the implementation. Thus, if, in the future, unforeseen scenarios like reassignment of IT personnel, funding issues arise, then the Management can make a decision of giving the project a requisite push in terms of additional funding and manpower.

3. Policy Deployment: The process of implementation of Wireless Policy needs to pay utmost attention to activities which fall under the preview of Policy Based Deployment and Management.

This is obviously the most significant and critical phase of the whole process which would eventually be used as a milestone or reference point for subsequent phases of wireless rollout.
Critical milestones in this can be:

- Setup of a pilot implementation – in a department, building or lab
- Identification of end users and systems on which initial wireless deployment will occur
- What benchmarks will be used to measure the success of a pilot deployment
- What constitutes unacceptable levels of performance?

On success of the pilot deployment, the process can move into an Implementation phase where:

- Enterprise wide rollout is planned and milestones laid out
- End customers and stakeholders (warehouse, HR, shipping) notified about forthcoming Wireless implementation
- Establishment of a Plan-of-record (POR) for the deployment process
- Discussion on employee training in terms of assigning batches and teams which will get the rollout, and in what order.

Policy based Management: Wireless deployment issues can be worked out by using policy based management which is laid out as:

Usage policies

- Applications across WLAN
- Network roaming
- Uncontrolled environments

Configuration policies

- Encryption & authentication for all wireless traffic
- MAC filtering and authorization using RADIUS server
- Changing default SSIDs
- Resetting default Windows XP settings

Security policies

- Prohibiting unauthorized Rogue access points
- Banning ad-hoc networks
- Vendor standardization for hardware
- Curbing off-hours usage

Performance policies

- Maximum number of stations that can connect to an access point
- Maximum Bytes allowed between AP and wired network
- Maximum Bytes allowed between AP and a node

Employee education and training:
For effective compliance, the employees need to be educated and trained about the capabilities, advantages and also the limitations of wireless networks. This can be done by periodically holding training sessions, conducting workshops and classes which demonstrate common pitfalls and security vulnerabilities and laws and also advising them about potential signs of misuse /intrusion. Users can be given a training guide for their reference and also be educated on setting up secure wireless connections at their homes. In case of detection of security violations or flaws, effort must be made to educate the users about the implications rather than assign blame and report them, without educating them.

4. Auditing for Policy compliance:
Like any other network deployment, effective auditing policies ensures justified usage of resources, prevents unauthorized usage and generally holds employees and managers responsible about their duties in ensuring a stable, secure network. This can be carried out by using:

Wired-side scanners- These devices carry out polling of network devices, using TCP signatures for identifying different devices. They have some limitations in terms of usage, such as their need to have a accurate database of all IP devices, need routers to cross subnet boundaries and lack of monitoring for SSID names,

encryption and authentication of wireless traffic, insecure Windows XP installs etc

Wireless sniffers and scanners- Using handheld scanners, a network admin can periodically sniff the network for policy compliance, network usage and setting up baselines. They are however, limited by the need to be hand carried for effective use and also have pretty limited reporting capabilities

In a typical secure environment there are logging, alerting, and monitoring services going on continually. These normally useful tools can be used against the administrator, too, by obscuring malicious assaults.

A hacker may intentionally cause a flood of traps or alerts by sending traffic that is likely to prompt violations, resulting in log entries, traps or alerts. Thereafter, he may undertake other sneak attacks, presuming that the high influx of event alerts would inundate and distract the administrator. Also, some alert and log services, and sometimes their servers, can be made to fail if log sizes exceed a size limitation

5. Corrective action for violations:
Results of audits and day to day operations must be analyzed to root out bandwidth leaks through unauthorized access, rogue access points and incorrect network configurations. Clear steps must be outlined defining what constitutes unlawful access and whose duty it is to ensure remedial action is taken and in what time frame must such activity be carried out.

A distinction should be made as to what is a error in judgment vis-à-vis a deliberate attempt to hack in /leak out company info and steps should be taken accordingly. A vigilant IT staff can help in cutting on any unauthorized access point proliferation and can therefore, be counted on to secure the boundaries of the network

6. Revision and customization:
Using constant feedback from end-users and managers regarding effectiveness of deployment and value add of wireless networks, future steps can include decision making for increasing the deployment, from say all office areas, to all locations in the corporate building, such as cafeterias, meeting rooms etc. It should be that the wireless policy and deployment should meet the needs of the organization, and not vie versa.

The initial deployment should not be considered a 'be-all' kind of a process, but rather as a continuous process based on testing, feedback and changes – all based within the changing framework of a modern Enterprises' business needs. As Wireless is a continuously evolving technology, technologies and tools that were state-of-the art a few years ago are getting replaced by newer and more advanced successors.

As the hacker community is always trying to place itself one step ahead of the IT community in their unending quest for ways and means to gain access to technology and resources like Bandwidth, this process will always need to be paid attention to, and improved in future rollouts.

Simple processes and guidelines for the IT Manager:
This document would not be complete if coverage is not provided to various tools and real-world security practices which are at the disposal of the IT Manager to strengthen the security envelope around the wireless network, and more importantly, translate the management objectives covered so far into a successful and secure wireless deployment

These can cover a whole range of norms, practices and BKMs - defining and ranging from user and device authentication before access to Enterprise data, centralized policy management backed with software based manageability features , managing data security in transit as it is beamed from workstation to PDA to laptops, ensuring a hardware reset does not lapse into factory default, which is typically without any security safeguards – all go a long way in ensuring overlapping layers of security and provide a safer wireless deployment.

A key point to bear in mind is that several of these procedures and activities are common to wired as well as wireless networks. However, the underlying objective remains the same –securing the enterprise network

Enforcing physical security

Attention should be paid to managing access to Access Points and other aspects of physical security, such as training security personnel to identify any unlawful sniffing going on close to office building from persons sitting in parked cars, keeping access points at locations which while providing wireless capability are also tamper-resistant and secure from pilferage, weather related issues and also provides good and overlapping coverage patterns.
Often overlooked as a vital security consideration, physical security can considerably reduce an Enterprise's security risks. It's important to know who is entering and leaving the facilities, and why they are there. Consider especially any wireless networks: A poor security infrastructure on a wireless network can potentially negate any physical security measures.

Reducing available information to outsiders

Information is a hacker's best friend, so the less information is provided the less accurate and effective a hacker's attack will be. It's impossible to cover all the tracks, but attention must be paid to propagation of discovery protocols and management protocols like SNMP, if they can be viewed from a user's office cube, as they can yield model numbers and software versions of the network infrastructure, giving a hacker a head-start in building and fine tuning his attacks.

Physical Separation between Management & User Traffic

Management traffic does not have to traverse the same physical links as user data and voice. Routers, switches, firewalls, and the like, can in almost all cases be configured with physically separate management links, which if properly implemented can be invisible and inaccessible to hackers. Data and voice traffic can be separated, or use VLAN-based traffic to separate traffic logically

System level hardening

Attention should be paid, and time and resources spent to see what is running on the business's servers and who can access and manage them. If there are services and/or protocols running that are unnecessary for your operation, they must be disabled. Likewise, user passwords need to periodically be changed, and unused accounts closed down. Admin and manager accounts should also be role-based, where these people only have access to what they need to perform their duties. Logs should be used to track all activity.

Implementing encryption based on streams and management

Encryption can provide a cloak to mask signaling and management, and prevent tapping into data, media or other forms of data flows. Encryption that's available today can prevent hackers from gathering information they can use to identify targets and possible vulnerabilities. A wireless admin should always remember that eavesdropping no longer requires being on the same physical wire as the call. Many tools permit data streams to be captured and replayed, but not when the traffic is encrypted.

Strengthening Authentication endpoints and handshake procedure

Security breached and vulnerabilities arising out of older technologies such as PPP, CHAP – which could be captured and played back - can be effectively addressed by requiring that end nodes use stronger authentication-based tools, like certificates, which have a much stronger control than passwords.

Implementing Port-based security methods for network connections

Protocols such as 802.11x, based on Extensible Authentication Protocol (EAP) provide port-based Network Access control mechanisms which provide an added layer of security, where before a requesting client gets access ot a network's resources and data, it has to authenticate itself. Client goes through an Authenticator system, which checks the provided credentials with a internal database such as a RADIUS server and then, based on success or failure of authentication, provides or denies access.

A detailed on EAP methodology is seen at www.sans.org/rr/wireless/802.11.php (also refer to the new link about Phillip Craiger's excellent paper at : http://www.giac.org/practical/GSEC/Phillip_Craiger_GSEC.pdf)

Implementing detailed logging, effective alerting, and attentive monitoring

Even with automated security measures in place, a human somewhere still needs to regularly monitor the logs, alerts, traps and reports that network devices generate. Logs and reports often allow knowledgeable administrators to trace the events that reveal a security breach, so holes can be patched. Effective alerting can reveal that a violation has occurred and give users a fighting chance to stop an attack in progress. There are several PC/MAC/PDA-aware tools available that help in this.

Netstumbler, available at www.Netstumbler.com offers a easily installable, which is useful to System Admins, as well as Hackers in identifying available Wireless hotspots. So if a Company's wireless signal is propagating beyond the building, it can be picked up by a hacker. It also gives MIDI feedback for signal strengths (useful for aligning antennas) and can be configured for a faster network scan.

Other passive monitors include other Layer 2wireless detectors and sniffers such as **Kismet**, available at http://www.kismetwireless.net/ . Kismet is totally passive and detects Access Point and Client Traffic across multiple cards, and needs a 802.11G card with RF Monitoring ability. But alerts need to be fine tuned, so an administrator doesn't get swamped, and then miss the really important problems.

For Mac OS X there is a similar wireless application, called **KisMac**, available at http://www.download.com/KisMac/3000-2147-10278145.html

Identifying rogue Wireless clients using MAC address:
Some amount of wireless activity will always be visible in areas with several companies having wireless networks of their own, in a limited space, e.g. in a Financial High-rise near Wall Street in New York –Home of several financial firms. However, if there is regular and persistent detection of same systems on the wireless network, then it merits a look-into.

Wireless devices have MAC addresses associated with them and IEEE maintains a listing of IEEE Organizational Unique Identifiers (OUIs), that map the MAC strings assigned to various makers and their names.
This is available at http://standards.ieee.org/regauth/oui/index.shtml. So if a device appears with a MAC ID of 00-00-00, then it is made by Xerox Corporation A listing of Wireless Radio Manufacturers will immediately identify if a MAC address belongs to the Company-authorized wireless NIC supplier or some other party.

Monitoring Network Activity
Monitoring what goes on a company's network is a primary job responsibility for a network admin. One has to know what is expected on the company network in the first place to be able to monitor and take preventive measures for suspicious

traffic. Network activity can be easily monitored and benchmarked with several tools available, such as **TCPDump, Ethereal** and **Nmap**.
TCPDump is an extremely popular monitoring tool that allows for monitoring network activity and has the ability to capture filter or print relevant data e.g.by issuing the following command, an admin can have a TCPDump collected for server Filenet, after ignoring SSH traffic

```
Filenet# tcpdump –i eth0 –n 'port | 122'
```

Ethereal gives real time statistics of protocols in use. Once installed, it can be used by clicking `Start->Tools->Protocol Hierarchy->Stats` and has capabilities to drill down high level protocols such as HTTP.
It can also be used to reassemble a TCP Stream by going on Tools->`Follow TCP Stream`.

Nmap is a free open source utility available at www.insecure.org/nmap/ for network exploration or security audit and can be used to interrogate the network.

Nmap can scan vast networks with thousands of systems and uses raw IP packets to determine available hosts, services offered, Operating System running version info etc. When running as a root, it uses advanced TCP fingerprinting techniques for detailed info about a network or a server such as:

```
Filenet # Nmap –o 10.11.23.1
Starting Nmap v. 3.55 (www.insecure.org/nmap/)
Interesting ports on Filenet.mktg.com (10.11.23.1)
(1450 ports scanned but not shown are in closed state)

Port            State               Service
22/tcp          open                ssh
53/tcp          open                domain
80/tcp          open                http
179/tcp         open                bgp
443/tcp         open                https
260/tcp         filtered            zebra

Remote Operating system gives : Linux kernel2.4.0-2.5.20
Uptime is 65.98 days
Nmap run completed.1 IP Address(1 host up)scanned in33 sec.
```

Fig.6 Sample Nmap display

Controlling and discouraging in-appropriate usage:
A growing area of concern is that of spam, mal-ware and file-sharing services reaching into the Office network using Applications such as Napster, Kazaa etc porn images in the workplace. They are counter-productive and from a bandwidth point of view, waste office resources.

A good tool which listens to network traffic and picks out images from TCP streams is Driftnet; available at http://www.ex-parrot.com/~chris/driftnet/ is very suitable in an implementation on a system with lots of web traffic. It re-assembles graphic images and presents info about what kind of pictorial and graphical data is going in/out of office network.

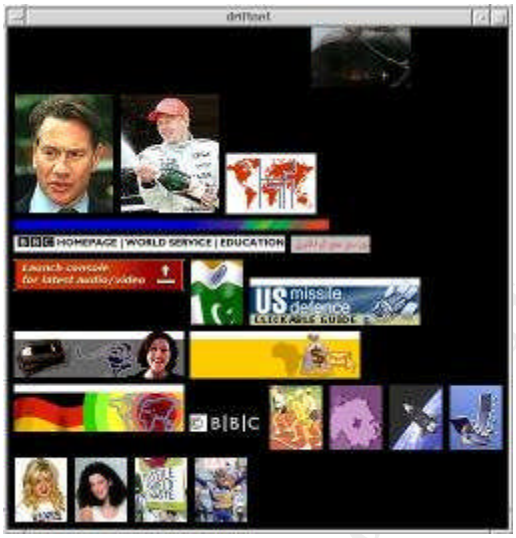

Fig. 7 A Driftnet screen capture

Preventing wireless attacks before they occur using IDS and HIPS

Many intrusion detection (IDS) and host-based intrusion prevention systems (HIPS) can detect and possibly deter application layer exploits, hacker scanning, and denial-of-service attacks before they reach their target. Proper tuning is often required to provide useful alerts.

Intrusion Detection Systems (IDS) operate on the principle of Pattern Detection and are either Network-based (NIDS) or Host-based (HIDS) and are passive systems

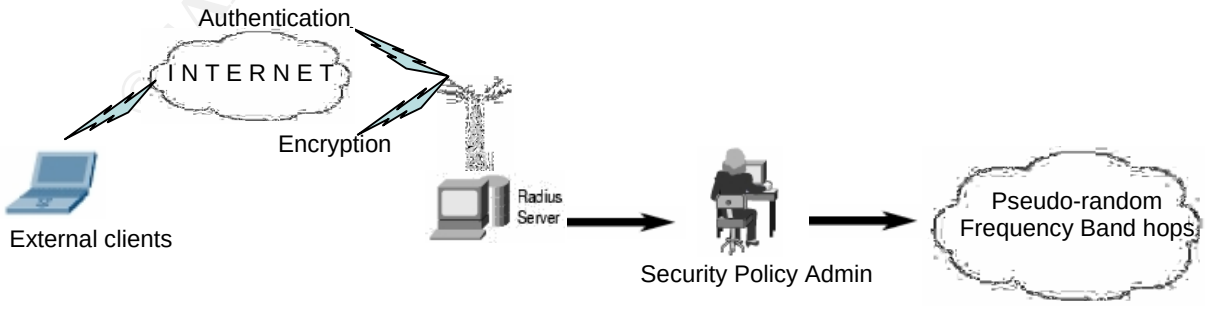

Fig.8 Enforcing Security Mechanisms

An effective security environment would constitute secure and tested policies for Enterprise connectivity; covering Authentication and Encryption Processes and having a dynamic environment such as an implementation of frequent change in transmission along a pre-set frequency pattern, so as to make the very option of hacking into the Enterprise unattractive for the hacker by virtue of the need for high-end systems needed to break the keys.

Summary

In essence, an Organization stands to grow and stay competitive in the business world by having a thoughtful and proactive deployment of WLANs and can have a sustained RoI in terms of lower hardware and administrative costs and higher end user productivity and satisfaction, provided they stay on a planned course set at the outset of the Wireless deployment process, so as to have a harmonious deployment which is secure, manageable and effective and have a good, milestone-based follow-through so that the implementation process stays on track

BIBLIOGRAPHY/REFERENCES

Publications:

1. Mathew Gast "802.11 Wireless Networks : The definitive Guide – Creating and Administering Wireless Networks" Apr 2002 (Chapters 1,5,7)

2. Ingelbrecht, Dulaney, Chapman et al "Mobile Communications Worldwide : Methodology and Definition" Gartner Group Mar 2004 (pages 27-36)

3. Philip Redman "Control costs & Boost ROI for Wireless Networks" Apr 2004 (4-9)

4. Ron Fuller & Tim Blakenship "Building a Cisco Wireless LAN" Jan 2001 Syngress (Chapter 3-5)

URLs: (Used as reference within the paper)

1. Intel White Paper –'Building the foundation for anytime, anywhere computing' http://www.intel.com/business/bss/infrastructure/mobility/build_foundation.pdf

2. Wireless and Wired users in 2005 http://www.airshare.org/learn/articles/features/symantec.cfm

3. SANS White Papers on 802.11 , 802.1x and Wireless Security (www.sans.org/rr/wireless/802.11.php) & Phillip Craiger' White Paper

http://www.giac.org/practical/GSEC/Phillip_Craiger_GSEC.pdf

4. Netstumbler -www.Netstumbler.com
   Kismet - http://www.kismetwireless.net/
   KisMac - http://www.download.com/KisMac/3000-2147-10278145.html

5. IEEE OUI and Company ID assignments :
   http://standards.ieee.org/regauth/oui/index.shtml

6. Nmap Network mapper: www.insecure.org/nmap

7. Driftnet Application : http://www.ex-parrot.com/~chris/driftnet/

8. Cisco Wireless LAN Security White Paper
   http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

Additional References (Used for understanding, NOT as reference)

1. Wi-Fi Security – Wi-Fi Alliance
   http://www.wi-fi.org/OpenSection/secure.asp?TID=2

2. www.cisco.com – For symbols used in creating diagrams

3. 802.11 Security-Intel Developers' Forum- Duncan Glenndining
   Sep 2003
http://www.intel.com/idf/us/fall2003/presentations/F03USMOBS169_OS.pdf

4. An IEEE 802.11 Wireless Security White Paper, Jason King ,
Oct 2001 URL: http://www.llnl.gov/asci/discom/ucrl-id-147478.htmll

Last Updated: October 17th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event