A Principal Design and Recommended Solutions For Developing Secure Techniques Used In Ids For WLAN And Wired LAN

Dr. Umesh Sehgal
Department of CSE/CA, ARNI University –Indora

Abstract
A Wireless Local Area Network (LAN) is a Radio frequency (RF) data communications system. WLANs transmit and receive data Over the Air (OTA) and thus collectively combine data connectivity with ease of mobility. Wireless LANs today provide wireless access to vital network resources such as large, multi-location enterprises, small and medium size enterprises as well as Hospitals, Hotel, Airports and homes. Wireless LANs are being widely recognized as a viable, cost-effective general-purpose solution in providing high-speed real-time access to information[3]. An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. IDSs can be classified as the tools and methods that monitor computer systems and network traffic to identify. In my Research work I will define that how WLAN is more secure than wired LAN and which pattern used in the Cisco IDS.
Keywords: - WLAN Tools, IDS CISCO series, Design WLAN security concepts.

Introduction to Wireless Local Area Networks (WLAN) and Intrusion Detection System (IDS) and Snort file

A Wireless Local Area Network (LAN) is a Radio frequency (RF) data communications system. WLANs transmit and receive data Over the Air (OTA) and thus collectively combine data connectivity with ease of mobility[2]. Wireless LANs today provide wireless access to vital network resources such as large, multi-location enterprises, small and medium size enterprises as well as Hospitals, Hotel, Airports and homes. Wireless LANs are being widely recognized as a viable, cost-effective general-purpose solution in providing high-speed real-time access to information. With a WLAN, users can gain access to shared information without being bound to fixed plug-in point. WLANs can be used to replace wired LANs or simply be used as an extension of a wired infrastructure. Added to the convenience and cost advantages over traditional wired Networks some of the benefits include:

- Mobility
- Installation speed, simplicity and flexibility
- Reduced cost
- Scalability

The most distinctive benefit of WLANs is they are easy to understand and use[4]. This can be attributed to the fact that everything to do with wired LANs, with a few exceptions, also applies to a WLAN.

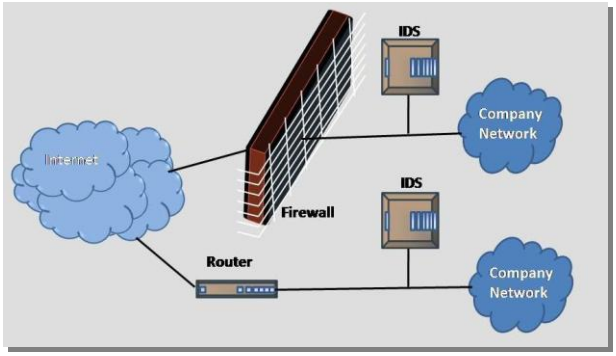

Figure 1.1 IDS Working Environment

Intrusion Detection system

An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. IDSs can be classified as the tools and methods that monitor computer systems and network traffic to identify and report possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from within the organization[4].

The genesis of intrusion detection dates from 1980 commencing with James Anderson's technical report, Computer Security Threat Monitoring and Surveillance for the U.S. Air Force. In 1985, Stanford Research Institute (SRI) was funded by the U.S. Navy to build the initial type of Intrusion Detection Expert System (IDES). Dr. Dorothy Denning assisted in leading this team and a year later published a paper entitled, An Intrusion Detection Model for the 1986 IEEE Symposium on Security and Privacy. This paper is regarded as being the seminal work on intrusion detection.

Conceptually a wireless IDS is similar to wired IDS but marked differences between wireless and wired-line networks, particularly the "structural and behavioral differences" render current IDS designs unsuitable for wireless networks. Wired intrusion detection systems operate at layer 3 (IP layer) and above of the OSI model whereas WLANs generally refer to the Physical and Data Link layers of the OSI model. A wireless IDS must therefore function at the Data Link layer or even possibly the

Physical layer if optimal security is required. There are two main classes of Intrusion[2]:

Misuse (abuse)

Intrusion is well-defined attacks on known weak points of system. All Intrusion which object is to misuse system resources and break it, are fall in this categories. Misuse intruder can be detected by watching for certain action being performed on certain objects and also by doing the pattern matching on audit trail information.

Anomaly

Intrusions are based on observations of deviation from normal system usage pattern. They can be detected by observing significant deviation from the normal behavior [5]. Anomalous Intrusion is harder to detect.

Anomaly or Anomalous may be symptoms of possible Intrusion. Anomaly detection has also been performed through other mechanism such as Neural Network. System's vulnerabilities involve abnormal use of system therefore security violation could be detected from abnormal pattern of system usage.

Challenges of Intrusion Detection

Intrusion detection systems in theory looks like a defense tool which every organization needs[1].

However there are some challenges the organizations face while deploying an intrusion detection system. These are discussed below.

1. IDS technology itself is undergoing a lot of enhancements. It is therefore very important for organizations to clearly define their expectations from the IDS implementation. IDS technology has not reached a level where it does not require human intervention. Of course today's IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection etc.

2. The success of an IDS implementation depends to a large extent on how it has been deployed. A lot of plan is required in the design as well as the implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS to benefit from both.

3. It is important to take care of sensor to manager ratio. There is no thumb rule as such for calculating this ratio. To a large extent it depends upon how many different kinds of traffic is being monitored by each sensor and in what environment. Lot of organizations deploys a 10:1 ratio. Some organizations go for 20:1 and some others 15:1.

4. The IDS technology is still reactive rather than proactive. The IDS technology works on attack signatures. Attack signatures are attack patterns of previous attacks. The signature database needs to be updated whenever a different kind of attack is detected and the fix for the same is available. The frequency of signature update varies from vendor to vendor.

5. While deploying a network based IDS solution, it is important to keep in mind one very important aspect of the network based IDS in switched environment. Unlike a HUB based network, where a host on one port can see traffic in and out of every other port in the HUB, in a switched network however, traffic in and out of one port cannot be seen by a host in another port, because they are in different collision domains.

WLAN that is more secure than Wired LAN WLAN

A systems incorporating WPA/WPA2 with AES encryption, in conjunction with 802.1x authentication, can provide a level of security for WLANs that can exceed the security of a wired LAN[5]. Although there are still exploits possible that can disrupt the communications on the WLAN, the security of the network and the integrity of the data becomes very difficult to compromise. There are always potential holes in the system. Most are attributable to human error; an unreported lost laptop, a laptop infected with a virus, or a compromised username/password combination, can all cause a security breach despite the integrity of the WLAN.

Wireless Networks do offer an additional physical layer of security when deployed in an all wireless office environment. By effectively eliminating employee or guest physical access to the network elements – jacks and cables – the hidden network becomes more physically secure. Employees can no longer plug in access points from home; guests can't erroneously misconnect LAN connections in a boardroom while trying to secure external access. The securing of the WLAN has become an enabler of the all-wireless future.

Secure wireless communication is at long last a reality. Industry standards have matured to provide a comprehensive solution to the WLAN security dilemma, but as with any form of security, wireless security will have to continually evolve to keep up with the newest and most sophisticated attacks. Furthermore, WLAN vendors are now looking beyond the IEEE standards for authentication and encryption to ensure that appropriate intrusion detection and prevention capabilities are in place to provide a complete and layered security solution.

The various companies like Siemens has developed a security solution that not only addresses the data confidentiality and authentication needs of today, but has also created an open standards-based solution that has the flexibility to adapt in the future. In conjunction with the sophisticated intrusion detection and prevention capabilities delivered by HiPath Wireless Manager, the HiPath Wireless Portfolio provides a complete, future ready solution that addresses the core tenets of wireless security. Management demands for a

cost effective approach are being met through an integrated security solution that leverages existing network infrastructure. At the same time, end-users will be satisfied that they have no need to complicate their computing experience in the least. In fact, features like secure fast roaming may actually simplify user experience.

Many enterprise network managers have resisted the introduction of wireless LAN technology, delaying the opportunity to reap the numerous benefits to be had in terms of productivity, responsiveness, and TCO reductions. While the absence of an acceptable security standard served as the chief justification for this decision, Siemens HiPath Wireless delivers a secure solution that resolves this problem and makes the enterprise ready for wireless LAN today.

The HiPath Wireless Manager architecture helps to deliver the most sophisticated RF security, location, performance optimization, and management capabilities. A unique integrated framework provides real-time coverage and allows services to leverage one another in a way that separate applications cannot. HiPath Wireless Manager HiGuard can be deployed in a phased approach. System Administrators can initially deploy HWM HiGuard in a 'sensor-less' configuration, and then gradually introduce sensors into high-risk areas to run in 'mixed mode,' until the entire enterprise is protected using 'dedicated sensors' for maximum security. HWM enables the wireless infrastructure's capabilities to adapt to the organization's needs.

The design principles for developing secure WLAN architectures.

1) Principle: Apply a Defense-in-Depth approach

2) Principle: Separate and segment the WLAN from the wired LAN

3) Principle: Require mutually authenticated access to the WLAN for all users and devices.

4) Principle: Protect WLAN traffic by implementing strong security at the Layer-2 level.

5) Principle: Restrict traffic between the WLAN and the wired network.

6) Principle: Monitor the WLAN to detect intrusion attempts.

Conclusion: - The following are recommended practices that should be considered when implementing an 802.11 WLAN[6]:

Recommendation: Create a WLAN security policy.

The organization should develop a strong WLAN security policy and educate all employees regarding the policy. The policy should outline a framework for the development of installation, protection, management, and usage procedures. All mission-critical assets and control components should be identified. Security and operational guidelines, standards, and personnel roles should be defined.

Recommendation: Do not rely on default security configurations of WLAN access points and adapters.

In general, WLAN equipment ships with minimum security features and controls enabled. For example, access point equipment will often ship in "Open Authentication" mode by default, meaning that no method of authentication between the stations and the access point is needed for the stations to establish an association (connection) to the WLAN network. Under open authentication, stations simply join the WLAN without restriction.

Recommendation: Employ MAC address filtering on the access points.

This is a low-level security control on the access point that permits only those stations with Ethernet MAC sub layer addresses on a list contained within the access point to communicate with the access point.

Recommendation: Disable SSID beacon transmissions.

Access points in most cases will by default broadcast a "Service Set Identifier", or SSID. This is essentially the name of the WLAN that a client station will use to identify a WLAN in its environment. For security purposes, it is best to disable SSID broadcast beacons so that the WLAN is not advertised to client stations that should not be allowed to connect. When the SSID broadcast is disabled, the client stations must know the SSID of the WLAN to which they want to connect. Suppressing the SSID beacon, although a minor security measure, ensures that an organization's WLAN networks, especially control system networks, are not announced or easily known.

Recommendation: Use non-suggestive SSID naming conventions.

Because SSID's serve as the name of WLAN networks, organizations will often name them according to their function or consistent with the unit of the organization that deployed it (for example, "ABC Corp", "Chlorinator", or "SCADA Dept"). It is best to not suggest the function or organization, if possible, in the SSID. It is best to not aid an attacker collecting reconnaissance information on a WLAN installation with use of a sniffer by providing the function or purpose of the network, especially if it pertains to industrial applications.

Top Ten Challenges in Wireless Data

The Top **Ten Challenges** in Wireless Data[5]:

1. Integrate unlicensed wireless securely and transparently into existing networking systems, such as wired enterprise Ethernets, the cellular system, and the public switched telephone network.

2. Develop algorithms for maximizing system throughput and capacity in large meshed networks.

3. Provide a cheap, wired backbone to enable inexpensive connectivity to the wireless mesh.

4. Provide cheap, smart antennae and the protocols that go with them. Without directional antennae, interference problems become exponentially worse

5. Create standard ad hoc routing and MAC layers that work for large meshed networks of mobile nodes with high throughput and low delay over many hops.

6. Reduce power consumption of the entire system, especially user devices.

7. Coordinate individual radios so that Quality of Service can be guaranteed in a mesh network.

8. Solve the hidden-terminal problem, which is really a question of coordinating a large number of radios to reduce interference.

9. Provide the fast handoffs that will be required for continuous mobile connectivity, as cell sizes will continue to decrease.

10. Eliminate outdated systems that tie up spectrum (broadcast television and radio, any analog system, any system that is not spread spectrum).

Reference

1. Capkun, S., Buttyan, L. & Hubaux, J. Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. *Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

2. Deng, H., Li, W. & Agrawal, D.P. (2002) Routing security in wireless ad hoc networks, *IEEE Communications Magazine*, **40**: 70- 75.

3. HuBaux, J. P., Buttyan, L. & Capkun, S. The quest for security immobile ad hoc network, *In Proc. ACM MOBICOM*, held on Oct. 2001.

4. Hsieh, H. & Sivakumar, R. *Transport OverWireless Networks*, Handbook of Wireless Networks and Mobile Computing, edited by Ivan Stojmenovic. John Wiley and Sons, 2002 Pg 325-360.

5. Hu, Y., Perrig, A. & Johnson, D. Ariadne: A Secure On-Demand Routing for Ad Hoc Networks, *Proc. of MobiCom*, (Atlanta) 2002 Pg 75-89.

6. Hu, Y., Perrig, A. & Johnson, D. Packet Leashes: A Defense AgainstWormhole Attacks inWireless Ad Hoc Networks, *Proc. of IEEE INFORCOM*, 2002.