Wireless Network Intrusion Detection System: implementation and architectural issues

Gianluca Papaleo

Doctoral Thesis Proposal submitted to
Dipartimento Informatica e Scienze dell’Informazione
Università degli Studi di Genova

November 2006
Abstract

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software has to be supported by other security solutions.

There is a need to search for new architecture and mechanisms to protect the wireless networks and mobile computing applications. We must include intrusion detection in the security architecture for mobile computing environment. Intrusion detection in wireless networks has become an indispensable component of any useful wireless network security systems, and has recently gained attention in both research and industry communities due to widespread use of Wireless Local Area Networks (WLANs). Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. How to do it differently and effectively is a challenging research problem.

In this thesis I first examine the vulnerabilities of a wireless network, the reason why there is a need of an intrusion detection system, and the reason why the current methods cannot be applied directly. The main goal is to design an efficient architecture for an intrusion detection system in an infrastructure-based wireless network and try to use anomaly-detection techniques to detect different types of attacks within the wireless network. In fact the general unavailability of benchmark data on wireless attacks (i.e. data with known attack types) lead us to research about unsupervised models for wireless intrusion detection.
# Contents

Abstract

1 Introduction

2 Wireless Security
   2.1 Possible Security Threats
      2.1.1 Passive Attacks - Accidental users
      2.1.2 Active Attacks - Brute force attack
      2.1.3 Denial-of-Service attacks
      2.1.4 Man-in-the-middle attack
      2.1.5 Session High-Jacking
      2.1.6 Replay
   2.2 Wireless Security Protocols
      2.2.1 Wireless Equivalent Privacy (WEP)
      2.2.2 Temporal Key Integrity Protocol (TKIP)
      2.2.3 Wi-Fi Protected Access (WPA)
      2.2.4 Wi-Fi Protected Access 2 (WPA2)
      2.2.5 Extensible Authentication Protocol
      2.2.6 Robust Secure Network (RSN)
      2.2.7 Future developments - Protected Management Frames

3 Intrusion Detection for WLAN
   3.1 Background on Intrusion Detection
   3.2 Anomaly Intrusion Detection
   3.3 Problems of Current IDS Techniques
   3.4 Architecture

4 Preliminary Results
   4.1 Clustering-based Approach to Intrusion Detection
4.2  WIDS development issues .............................................. 20
  4.2.1  Additional Security solutions ................................. 21

5  Planned Work  ......................................................... 23
  5.1  Implementation of the system ................................. 23
  5.2  Experimental setup ............................................... 23
  5.3  Theoretical activity .............................................. 24
  5.4  Thesis drafting .................................................. 24
  5.5  Work plan sketch ................................................. 24

Bibliography .......................................................... 25
Chapter 1

Introduction

The nature of mobile computing environment makes it very vulnerable to an adversary’s malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

The problem of detecting anomalies, intrusions, and other forms of computer abuses can be viewed as finding non-permitted deviations (or security violations) of the characteristic properties in the monitored (network) systems. This assumption is based on the fact that intruders’ activities must be different (in some ways) from the normal users’ activities. However, in most situations, it is very difficult to realize or detect such differences before any damage occur during break-ins.

A data mining approach to network intrusion detection provides an opportunity to learn the behaviors of network users by mining the data trails of their activities. While recent research has investigated data mining for intrusion detection [1], considerable challenges remain unexplored, including intrusion detection models for wireless networks and intrusion detection without prior knowledge of relationships between attack types and attributes of network audit data.

The aim is to develop and implement an efficient WIDS (Wireless Intrusion Detection System) in an infrastructure-based wireless network and try to use anomaly-detection techniques to detect different types of attacks within the wireless network.

To do this we investigate in recent evolution in intrusion detection using data mining
approaches and use the skills in intrusion detection developed during this year. The main difficulty is to use the intrusion detection techniques knowns in wired network and adapt them in a wireless environment.
Chapter 2

Wireless Security

Wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location.

With the benefits of Wi-Fi there are also some risks which users should be aware of. Without any security implemented, unauthorised users may steal data or load malicious code onto the network with the intention of creating havoc. Unlike wired networks, the radio signal produced by wireless networks can penetrate walls, ceilings, floors and are therefore not confined to a building. Hackers can effortlessly pick up these signals from the outside of the building using easily available wireless detection tools.

Many WLANs used in the home still operate with no measure of encryption. However, there does arise something of a problem for the home user when establishing a WLAN, namely which encryption protocol to use.

The majority of wireless networks use the IEEE 802.11 standard for communication. Initially the IEEE 802.11b was the de-facto security standard for wireless networking technology for small businesses and home users, with all Wireless Access Points equipped with Wired Equivalency Protocol (WEP). Flaws in WEP were soon discovered and in response to this, the 802.11i task group were developed to address the major problems with security. They addressed three main security areas: authentication, key management and data transfer privacy. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) as a Wi-Fi standard, which accelerated the introduction of stronger security. As the security standards have evolved other wireless security options have become available which are preinstalled on devices, these include WPA and Temporal Key Integrity Protocol (TKIP).

Initially, when Wi-Fi networking was in its infancy, war-walking, war-driving and war-chalking were well publicised phenomena. Developed by Peter Shipley in April 2001, these terms describe the process used by hackers walking or driving around areas looking
for unsecured wireless networks.

Symbols were left on the walls or pavements to indicate the security status of nearby Wi-Fi points. War-driving did highlight the worrying results that firstly a large proportion of Wi-Fi users do not enable any form of encryption and secondly that the standard wireless encryption protocol (Wired Equivalency Protocol - WEP) can easily be cracked.

Even after much publicity about wireless encryption and new improved protocols were made available, a survey conducted by WhiteHat in January 2005 [2] found 51% of businesses, within a one-mile radius of Bristol town centre, did not use any form of encryption. Of those who did use encryption, 25% used the default service set identifier (SSID) and therefore probably still had the factory passwords.

2.1 Possible Security Threats

Like wired networks, wireless networks are subject to malicious attacks. The radio signals do not remain within the confines of the building, and indoor routers have a range of approximately 20-150 metres, depending on the 802.11 standard and the data rate. Therefore, the radio signal can easily be detected externally or in a neighbouring building.

This means the attacker does not need to infiltrate the building to hack the network. With the right equipment, it is possible for the radio signal to extend up to 125 miles [3]. However, such distances can only be reached in certain environments such as deserts, which lack structures such as buildings and trees. Obstacles such as walls and distance can cause the radio signal to attenuate and the threat of attack will decrease. Wireless detection devices work in two modes, passive and active. The passive mode listens for the access points’ broadcast, which may or may not contain the SSID. Whereas active mode uses the probe request and response to detect access points, which involves the access point responding to the probe request. Attacks on WLANs can be categorised as passive attacks which include War-Driving and Sniffing (via a promiscuous mode); and active attacks include Spoofing (impersonation), Denial-of-Service attacks (DoS) and Man-in-the-middle attacks.

2.1.1 Passive Attacks - Accidental users

Occasionally when trying to connect to an Access Point the computer may automatically connect to a different network and the user may "accidentally" use that connection without realising it belongs to a third party. However, it is illegal in Italy to use bandwidth
2.1 Possible Security Threats

without the consent of the owner according to articles 615 and 617 of italian penal code \(^1\). This may occur in the work place when users are unfamiliar with the company’s SSID and pick up a neighbouring company’s unsecured network.

2.1.2 Active Attacks - Brute force attack

A brute force attack is the systematic testing of different letters, numbers and symbols until the correct password or key is guessed. There are a number of software programmes available on the Internet that can be used to recover encryption keys on wireless LANs, these include AirSnort [4] and WEPCrack [5]. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been collected, AirSnort can guess the encryption password in under a second. WEP can easily be cracked because the Initialisation Vector is sent as plaintext within the encrypted packet. This means that if anyone intercepts the data using a sniffer package, they will be able to decipher the secret key.

The newer encryption standard WPA can also be cracked using a tool called WPA Cracker that uses dictionary brute-force attack, which can check 16-18 passwords/second on a 1.4GHz notebook [6]. It is therefore recommended that passphrases are at least 20 characters long and do not contain dictionary words.

2.1.3 Denial-of-Service attacks

A Denial-of-Service attack (DoS) can cause a network to slow down or become unusable. A DoS attack may occur if the attacker generates a lot of traffic on the network, which may block the server for hours or by attacking the resource itself. Another form of DoS attack is the use of a strong radio signal.

This denies legitimate users from accessing a resource. Distributed Denial-of-Service attacks (DDoS) occurs when many computers are used against the target. A single master program can be loaded onto a commandeered computer via an insecure wireless network; the master program can communicate to "agent" computers anywhere on the Internet infected with the agent program and initiate an attack.

2.1.4 Man-in-the-middle attack

A Man-in-the-middle attack occurs when an attacker is able to read and modify communications between two parties without them being aware of the attacker’s presence.

\(^1\)LEGGE 23 dicembre 1993 n. 547.
An Evil Twin attack (also known as base-station cloning/access point cloning) is similar to a Man-in-the-middle attack. The term is used for fake hotspots/access points, which pretend to be a legitimate hotspot. The Evil Twin is a malicious server, which may be used to extract sensitive information such as bank details. The hacker sets up the SSID to be the same as the local hotspot or corporate wireless network. The hacker may disrupt or disconnect the access point by directing a Denial-of-Service attack against it, or by creating radio signal interception around it. The hacker may then intercept the traffic. The user is unaware that they are not using a legitimate hotspot and may unknowingly provide their user name and password as they log on to the fake hotspot. Evil Twin networks may be avoided by enabling the WEP or WPA security, so the user is unable to join the "evil network" as the key will not match.

2.1.5 Session High-Jacking

Session High Jacking is an attack against the integrity of a session. The attacker takes an authorized and authenticated session away from its proper owner. The target knows that it no longer has access to the session but may not be aware that the session has been taken over by an attacker. The target may attribute the session loss to a normal malfunction of the WLAN. Once the attacker owns a valid session she may use the session for whatever purposes she wants and maintain the session for an extended time. This attack occurs in real-time but can continue long after the victim thinks the session is over.

2.1.6 Replay

Replay attacks are also aimed at the integrity of the information on the network if not necessarily the integrity of a specific session. Replay attacks are used to gain access to the network with the authorizations of the target, but the actual session or sessions that are attacked are not altered or interfered with in any way. This attack is not a real-time attack; the successful attacker will have access to the network sometime after the original session(s).

In a replay attack, the attacker captures the authentication of a session or sessions. The attacker then either replays the authenticated session at a later time or uses multiple sessions to synthesize the authentication part of a session. Since the session was valid, the attacker establishes an authenticated session without being privy to any shared secrets used in authentication.
2.2 Wireless Security Protocols

To prevent attacks on wireless networks, access point devices such as routers have built-in security settings. Over time, the level of security has increased with the realisation that the original security settings were flawed.

2.2.1 Wireless Equivalent Privacy (WEP)

WEP is a scheme to provide security in wireless networks. It was developed to work as a part of the IEEE 802.11 standard. In 1997, WEP was developed by the 802.11b task force with the introduction of wireless technology, and was the first encryption protocol to be deployed with wireless networks. WEP incorporates two types of protection, a secret key and encryption. The secret key, comprising of a 5- or 13-character simple password, is shared between a mobile device and a wireless access point. This key is used in the encryption process to scramble each packet of information with a unique password before transmission. An integrity check ensures that packets are not changed during the transmission. The secret key is used to encrypt packets before they are transmitted. WEP also uses an Initialisation Vector (IV) to augment the shared WEP key (secret key) to avoid encrypting two cipher texts with the same key, this produces a different RC4 key for each packet.

RC4 is a stream cipher that generates a pseudorandom stream of bits. Before a data packet is transmitted, an integrity check (IC) computes a checksum. Then WEP concatenates the data and IC with the keystream using the exclusive-or (XOR) function. Without an IV, the plaintext would always produce the same ciphertext. An eavesdropper would be able to see patterns and predict plaintext. With the IV, the ciphertext changes as the IV changes, so it would be more difficult for an eavesdropper to see patterns and predict plaintext. The WEP key is available in two strengths, 64-bit and 128-bit. The WEP keys are also referred to as 40-bit and 104-bit as the initialisation vector is 24-bit.

WEP uses the RC4 algorithm for encryption and the same key used to encrypt and decrypt the data. The purpose of the RC4 algorithm is to keep hackers from altering the data during the transmission. The RC4 algorithm then generates the keystream from the secret key and IV. By regenerating the RC4 keystream from the IV and the known key, the recipient can decrypt the data by running XOR.
WEP weaknesses

It was soon discovered that the WEP security protocol was flawed and in 2001, Fluhrer et al. [7] published a cryptanalysis of WEP that exploited the way the RC4 algorithm and IV was used in WEP. It was discovered that a passive attack could recover the RC4 key after eavesdropping on the network for a few hours and collecting 100,000-1,000,000 packets. A hacker could use an XOR function to mathematically link two packets of a session that have been processed with the same IVs, i.e. identical RC4 keys, which can be used to recover the key.

Another fault with the WEP protocol was that the authentication only verifies the client machine, not the actual user accessing the machine [8]. This occurs as the only key condition is that the WLAN card and the access point use the same algorithm. Therefore, everyone on the local network uses the same secret key, which the RC4 algorithm uses to generate an infinite, pseudorandom keystream. Both the 40-bit and the 104-bit keys are vulnerable to attacks, due to various weaknesses internal and external to the protocol supporting WEP.

These vulnerabilities include the heavy reuse of keys, the ease of data access in a wireless network, and the lack of any key management within the protocol [9]. For example, the IV will be duplicated within 5 hours at a busy access point when 1500-byte packets (the standard Maximum Transition Unit for an Ethernet network) are transmitted at a rate of 11 Mbps. It is therefore possible to determine the RC4 keystream over several hours after the IV has been repeated.

Originally, it was thought that increasing the key size from 40-bits to 104-bits would overcome some of the security problems [10], however the implication of 128-bit WEP has caused problems for heterogeneous environments in which interoperability was an issue. In 2005, using a combination of statistical techniques focusing on unique IVs captured and brute-force dictionary attacks to break 128-bit WEP keys, the U.S. Federal Bureau of Investigation cracked WEP in 3 minutes [11]. With the proper equipment, it is possible to eavesdrop on a WEP-protected network from distances of a mile or more away from the target [12]. With the tools and information available on the Internet, an inexperienced hacker could crack WEP encoded data in a matter of days. A report conducted in 2005 by Webtorials found 40% of the users surveyed still used WEP for securing their wireless network and only 22% deployed WPA2/802.11i security [13].
2.2.2 Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP) was the immediate replacement for WEP, which aimed to fix the problems associated with WEP including small initialisation vectors (IV) and short encryption keys. TKIP is a suite of algorithms that wrap around the WEP protocol to make it more secure. The reason why TKIP is an improvement on WEP is that it rotates the temporal keys; therefore, a different key is used for each packet. Each packet transmitted using TKIP has a unique 48-bit serial number that is incremented every time a new packet is transmitted.

Each time a wireless station associates with an access point, a new base key is created. The base key is built by hashing together a special session secret with some random numbers generated by the access point and the station as well as the MAC address of the access point and the station. This mixing operation is designed to put a minimum demand on the stations and access points, yet have enough cryptographic strength so that it cannot easily be broken. Putting a sequence number into the key ensures that the key is different for every packet.

This resolves another problem of WEP, called "collision attacks," which can occur when two messages have the same key. With different keys, collisions are prevented. TKIP also utilises an integrity-checking feature called Message Integrity Check (MIC or Michael).

This part of TKIP closes a hole that would allow a hacker to inject data into a packet, which allows the hacker to deduce the streaming key used to encrypt the data. MIC uses a cryptographically protected oneway hash in the payload, which ensures packet tampering detection occurs immediately upon decryption. Compared to WEP, TKIP is a costly process and may degrade performance at many access points, where it can consume every spare CPU cycle.

TKIP also uses RC4 as the encryption algorithm, but it removes the weak key problem and forces a new key to be generated every 10,000 packets. In addition, it hashes the initialisation vector (IV) values that were sent as plaintext in WEP. TKIP is useful as it can be used on old hardware, which supports WEP but not WPA, and new hardware that only supports WPA.

2.2.3 Wi-Fi Protected Access (WPA)

WPA was created by the Wi-Fi Alliance once the flaws associated with WEP were discovered, and used as an intermediate standard until the IEEE 802.11 working group developed a more secure protocol. WPA was based on the WEP protocol, but utilises the
stronger encryption technology used in TKIP, which offers pre-packet key mixing and a message integrity check.

Although WPA is stronger than WEP, it is, however, vulnerable to Denial-of-Service attacks. Initially designed as a safety feature, WPA shuts down the network if at least two packets using the wrong key are sent every second. A hacker could use this security feature to their advantage and can potentially bring down a WPA protected LAN. If this happens the access point assumes the hacker is trying to gain access to the network. The access point shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Thus, a continuous string of unauthorised data could keep the network from operating indefinitely. While this feature was designed to safeguard against breaches of security, it presents a prime opportunity for a hacker. WPA comes in two modes, enterprise mode and consumer mode. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication. The RADIUS server checks that the information is correct using the authentication scheme Extensible Authentication Protocol (EAP) to process the information. If accepted, the server will then authorise access to the ISP system, select an IP address and Layer 2 Tunnelling Protocol parameters.

Although the 802.1X standard uses RADIUS for authentication, it does not specify that it must be RADIUS, other authentication protocols could be used such as TACACS+ (Terminal Access Controller Access Control System). RADIUS is the de facto standard for authentication and other protocols are rarely used. A RADIUS server can be used for different internet connections other than dial-up. The authentication server is a certificate authenticator that only allows client stations to connect with the access point if it sees a valid certificate on the client, which the server provided earlier. Many access points now come with integrated Authentication Servers (AS), which act as RADIUS servers, giving Small Office and Home Office (SOHO) users the ability to use WPA-802.1X authentication schemes if they want, even for small groups. The Enterprise mode is more complex and expensive to install because it requires the use of a RADIUS server to manage keys and is therefore not suitable for home users.

The consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC. The consumer version is typically used in homes or small offices, which require each user to enter a common password. If consumer mode users select the typical 6-8 character passwords that corporate networks require for login purposes, the resulting system will still be insecure. WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key) is the better choice for SOHO users, because of its simple setup and deployment across a multi-vendor environment. Although WPA-PSK was originally
2.2 Wireless Security Protocols

intended for home users, it has been adopted by small offices due to the cost and difficulty in setting up a RADIUS server.

**Cracking WPA-PSK**

Brute-force cracking tools such as coWPAtty are capable of cracking WPA-PSK by systematically testing numerous passwords and combinations of characters. It is estimated that on a Pentium 4 3.8 GHz system, coWPAtty can try 70 words per second, however it would take over 3452 days to test all the possible eight letter passwords (over 208,000,000,000 combinations). Therefore, it is unrealistic to use such a tool to crack a key and the information still to be relevant.

2.2.4 Wi-Fi Protected Access 2 (WPA2)

The current standard for wireless security, Wi-Fi Protected Access 2 (WPA2), was introduced in September 2004. The IEEE 802.11i standard WPA2, addresses three main security areas: authentication, key management, and data transfer privacy. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is backward compatible with WPA. Like WPA, WPA2 is also available in Personal and Enterprise modes.

WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. However, although WPA2 implements the full standard, it will not work with some older network cards.

The encryption algorithm used in the 802.11i security protocol is AES-Counter Mode CBC-MAC Protocol (AES-CCMP). It uses the AES block cipher, but restricts the key length to 128 bits.

AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBCMAC).

The counter mode uses an arbitrary number that changes with each block of text, making it difficult for an eavesdropper to spot a pattern. The CBC-MAC protocol (Cipher Block Chaining- Message Authentication Code) is a message integrity method, which ensures that none of the plaintext bits that were used in the encryption were changed.

2.2.5 Extensible Authentication Protocol

WPA and WPA2 enterprise modes both utilise the Extensible Authentication Protocol (EAP) as an authentication framework. EAP is an 802.1X standard that allows developers to pass security authentication data between the RADIUS server, the access point and
wireless client. EAP has a number of variants, including EAP MD5, EAP-Tunnelled TLS (EAP-TTLS), Lightweight EAP (LEAP), and Protected EAP (PEAP). EAP resides in the access point and keeps the network port disconnected until authentication is completed. Depending on the results, either the port is made available to the user, or the user is denied access to the network.

2.2.6 Robust Secure Network (RSN)

Robust Secure Network (RSN) is a protocol used for establishing secure communications over an 802.11 wireless network, and is an element of the 802.11i standard. RSN dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless access point and wireless clients. This means that as new threats are discovered, new algorithms can be added.

2.2.7 Future developments - Protected Management Frames

Protected Management Frames (PMF) otherwise known as 802.11w, is a new standard that is due to be deployed in 2008. PMF improves the Medium Access Control layer to increase the security of management frames and data frames. As Wireless LANs send system management information in unprotected frames, they are vulnerable to interception. PMF protects against network disruption caused by malicious systems that create disassociation requests that appear to be sent by valid equipment.
Chapter 3

Intrusion Detection for WLAN

Intrusion prevention measures, such as encryption and authentication, can be used in wireless networks to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys.

The history of security research has taught us a valuable lesson: no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in.

Intrusion detection presents a second wall of defense and it is a necessity in any high-survivability network. In summary, mobile computing environment has inherent vulnerabilities that are not easily preventable.

To secure mobile computing applications, we need to deploy intrusion detection and response techniques, and further research is necessary to adapt these techniques to the new environment, from their original applications in fixed wired network.

3.1 Background on Intrusion Detection

When an intrusion (defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [14]) takes place, intrusion prevention techniques, such as encryption and authentication, are usually the first line of defense. However, intrusion prevention alone is not sufficient because as systems become ever more complex, and as security is still often the after-thought, there are always exploitable weaknesses in the systems due to design and programming errors, or various "socially engineered" penetration techniques. For example, even though they were first reported many years ago, exploitable "buffer overflow" security holes, which can lead to an unauthorized root shell, still exist in some recent system softwares.
Furthermore, as illustrated by the Distributed Denial-of-Services (DDoS) attacks launched against several major Internet sites where security measures were in place, the protocols and systems that are designed to provide services (to the public) are inherently subject to attacks such as DDoS. Intrusion detection can be used as a second wall to protect network systems because once an intrusion is detected, e.g., in the early stage of a DDoS attack, response can be put into place to minimize damages, gather evidence for prosecution, and even launch counter-attacks.

The primary assumptions of intrusion detection are: user and program activities are observable, for example via system auditing mechanisms; and more importantly, normal and intrusion activities have distinct behavior. Intrusion detection therefore involves capturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. Based on the type of audit data used, intrusion detection systems (IDSs) can be categorized as network-based or host-based. A network-based IDS normally runs at the gateway of a network and "captures" and examines network packets that go through the network hardware interface. A host-based IDS relies on operating system audit data to monitor and analyze the events generated by programs or users on the host. Intrusion detection techniques can be categorized into misuse detection and anomaly detection [22] [23].

Misuse detection systems, e.g., IDIOT [15] and STAT [16], use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. For example, a signature rule for the "guessing password attack" can be "there are more than 4 failed login attempts within 2 minutes". The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the truly innovative (i.e., newly invented) attacks. Anomaly detection (sub)systems, for example, the anomaly detector in IDES [17], flag observed activities that deviate significantly from the established normal usage problems as anomalies, i.e., possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in his or her login sessions. If for a session that is being monitored, the frequencies are significantly lower or higher, then an anomaly alarm will be raised. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what the attack is and may have high false positive rate.
3.2 Anomaly Intrusion Detection

The objective of anomaly detection is to establish usage patterns within user audit trials over duration of time and use these usage patterns as profiles of normal system activity. An audit trail that is found to deviate from use established usage pattern is flagged and brought to the attentions of the administrator. The anomaly detection techniques directly address the problem of detecting a new attack. In order of the intrusion detection system to recognize anomaly behavior it must learn the user behavior by forming a user profile to describe his normal behavior. The normal behavior of a user can be described by the set of actions given by him. This is because a wireless local area network user exhibits regularities in his interaction with the wireless node. That is the regularities exhibited by the users can be used to form a user profile so that unusual occurrences can be detected by comparison of the current input stream to the user’s profile.

3.3 Problems of Current IDS Techniques

The vast difference between the fixed network where current intrusion detection research are taking place and the mobile network makes it very difficult to apply intrusion detection techniques developed for one environment to another. The most important difference is perhaps that the latter does not have a fixed infrastructure, and today’s network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment.

A significant big difference is in the communication pattern in a mobile computing environment. Mobile users can be stingy about communication and often adopt new operation modes such as disconnected operations [18]. This suggests that the anomaly models for wired network cannot be used as is.

Furthermore, there may not be a clear separation between normalcy and anomaly in mobile environment. Intrusion detection may find it increasingly difficult to distinguish false alarms from real intrusions.

3.4 Architecture

A wireless IDS can be centralized or decentralized. A centralized wireless IDS is usually a combination of individual sensors which collect and forward all 802.11 data to a central management system, where the wireless IDS data is stored and processed. Decentralized wireless intrusion detection usually includes one or more devices that
perform both the data gathering and processing reporting functions of the IDS. The
decentralized method is best suited for smaller (1-2 WAP) WLANs due to cost and
management issues. The cost of sensors with data processing capability can become
prohibitive when many sensors are required. Also, management of multiple processing
reporting sensors can be more time intensive than in a centralized model.

WLANs typically encompass a relatively large physical coverage area. In this
situation, many WAPs can be deployed in order to provide adequate signal strength to
the given area. An essential aspect of implementing a wireless IDS solution is to deploy
sensors wherever a WAP is located. By providing comprehensive coverage of the physical
infrastructure with sensors at all WAP locations, the majority of attacks and misuse can
be detected. Another benefit of positioning the sensors in close proximity to the WAPs is
the enhanced ability to physically pinpoint the geographical location of an attacker.

In this system, every sensor in the network participates in intrusion detection and
response.

IDS agents will cooperatively participate in global intrusion detection actions. These
individual IDS agent collectively form the IDS system to defend the wireless network.
Chapter 4

Preliminary Results

In this chapter I show what are the research results about wireless intrusion detection and what are the skills I developed during this year.

4.1 Clustering-based Approach to Intrusion Detection

Clustering-based intrusion detection methods are more suitable to real-time intrusion detection systems since they require minimal human interaction and can potentially discover new attacks or anomalous behaviors [27].

Clustering is the task of identifying groups of records that are similar within a group but dissimilar between groups. Over the past few decades significant research on clustering techniques have been performed.

In [24][26][28] Shi Zong et al. proposed a relative simple but effective clustering technique for their experiments.

The wireless log they use for this work have been studied by Balanziska and Castro [29]. In their study, they were constrained by the metrics that are available in the recorded wireless logs rather than having all the metrics that are theoretically required to model common wireless attacks. Common metrics are presented in Table 4.1.

The main difficult is to choose useful metrics for our detection. The aim of the thesis is to overcome the constraints of the Balanziska and Castro logs, to develop an intrusion detection system that considers the others important metrics like MAC address and client IP, that are essentials in a real scenario. The configuration of WLAN we consider, is an infrastructured network. This year I improved my knowledge about Data Mining

---

1Wireless Network Metrics are the measurable parameters or features that an intrusion detection system can use to model the various wireless attacks on the network as well as normal traffic.
Table 4.1 Possibly relevant metrics for characterizing wireless network attacks.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>ARP/IP pair changes</th>
<th>packet leash</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUI</td>
<td>Static/Dynamic IP</td>
<td>Loopps/alternate routes</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>SSL/Encryption in use/WEP</td>
<td>Timeout for RTS</td>
</tr>
<tr>
<td>IP address</td>
<td>Antenna type</td>
<td>3DES or RC4</td>
</tr>
<tr>
<td>Change of MAC allowed in NIC</td>
<td>VPN in use</td>
<td>Frag headers</td>
</tr>
<tr>
<td>Sequence number of Client</td>
<td>Retry bit in control frame</td>
<td>MAC list in AP</td>
</tr>
<tr>
<td>Sequence number of AP</td>
<td>Spoofed disassociate msg</td>
<td>NIC in promiscuous mode</td>
</tr>
<tr>
<td>2-bit state (Unauth &amp; Associated)</td>
<td>802.1x extension in use</td>
<td>CCM Mode</td>
</tr>
<tr>
<td>Class 1 frames RTS/CTS/ACK/POLL</td>
<td>Buffer overflows allowed</td>
<td>Switch/hub</td>
</tr>
<tr>
<td>NIC vendor</td>
<td>PPP enabled</td>
<td>TKIP</td>
</tr>
<tr>
<td>Deauth msg + spoofed msg</td>
<td>AdHoc Network</td>
<td>MAC address overload</td>
</tr>
<tr>
<td>Reason Code</td>
<td>Authentication attempts</td>
<td>Signal/noise ratio</td>
</tr>
</tbody>
</table>

techniques publishing an article for PRISE 2006 [34]. Besides I attended a course in Data Mining at BISS06 [33].

4.2 WIDS development issues

To start to develop our WIDS (Wireless Intrusion Detection System), we need to place our sensors near access points. We have to put our wireless cards in monitor mode to capture all the wireless traffic. Windows doesn’t support very well this feature, thus we use Linux to develop our WIDS, in particular we use a distribution called Auditor [30]. The Auditor security collection is a Live-System based on KNOPPIX with over 300 security tools; it offers supports for a lot wireless cards, for all tested devices see [31].

Unfortunately there isn’t one command to put your card in monitor mode, but it depends by the card chipset. For a detailed list of available commands see [32]. In this year I developed various packet capture module for different applications in wired environments using the pcap library, both in C language and in Perl language. I will use this experience to develop the packet capture module in a wireless environment. Usually traditional packet analyzer focuses solely on its structure and characteristics. Consequently, the result is a list of raw packets sorted by its collected time; therefore, no distinct relationship is established between them. Hence network administrator would not be able to utilize this information efficiently.

In order to overcome this obstacle, it is necessary to design an algorithm to rearrange the packets into individual session groups. As defined in IEEE 802.11 standard there are three types of frames that must be recognized in WLAN:
4.2 WIDS development issues

1. Management Frames: WLAN uses these frames to perform authorization and establish connections between AP and credits

2. Control Frames: they are responsible for media access control

3. Data Frames: they are used to deliver data

In this year I developed a tool able to reassemble SMTP session starting by pcap files. I start from the experience acquired in developing this tool to build the tcp analysis module.

4.2.1 Additional Security solutions

In order to achieve a more security level to our WIDS we have to add these security features

- Honeypot

A Honeypot is a security resource whose value lies in being probed, attacked or compromised [35]. This means, that a honeypot is expected to get probed, attacked and potentially exploited. In fact, honeypot provides additional and valuable information about the hacker.

WIDS must incorporate honeypot features, which diverts attacker to fakedAP that eventually leads to a honeypot where events are quarantined from the production network, with the target being deceived, it starts to record every single move made by it. Hopefully, these records can be used as a learning material and reference.

- Address Rule Matching

This feature is necessary to detect if duplicated mac addresses are being used in our network. To understand if some client try to spoof some MAC addresses availables, we need to trace the MAC addresses that are being used in our network and compare them in our database of mac address knowns to be authorized to access our network.

- War-Driving attempts

Before connecting to a WLAN, client device must first find an AP either by listening for AP’s beacon or broadcasting probe request consecutively. As stated in 802.11, AP must reply a probe response, as to inform its existence, to the client that issues the request to establish connection. War-Driving takes the advantage of such vulnerability to scan every AP within radio signal range by broadcasting probe request frames. Two indicators can help us to detect war-driving attempts:
1. NetStumbler signature:
   NetStumbler [36] is the most popular tool for War-Driving. However, it is possible to detect NetStumbler, because it always sends out a special packet whenever an AP is detected. This packet contains a unique value that can be used to identify NetStumbler.

2. Probe Response Traffic:
   War-driving forces AP to generate probe response frames and is likely to increase the traffic of these frames. Such abnormal increase in traffic can be revealed by monitoring probe response frames. However, legitimate users may also request for AP response. Therefore, detailed analysis is required to determine the main cause of the increased traffic.
Chapter 5

Planned Work

5.1 Implementation of the system

In the first period I will design and implement all the algorithms needed for the WIDS. In the first phase I develop the basis to capture and analyse the traffic, then I use the captured traffic for an off-line analysis to model our scenario. The statistics so gathered are used to build clusters useful to distinguish between normal an anomalous traffic. An on-line detector module will be then developed on the basis of the obtained results. In addition, the WIDS will be supported by additional security features.

- Packet capture
- TCP session Analysis
- Off-line Statistic Analysis
- Cluster builder
- On-line detector
- Additional security features

Starting date: 1 January 2007
Closing date: 31 December 2007

5.2 Experimental setup

In our scenario we try to execute malicious attacks to verify the performance of the algorithms developed. We compare various clustering algorithm and other anomalous
detection solution to improve the algorithm and eventually exploit new solutions. We try to minimize the false positives rate but detect all the attacks in our network.

Starting date: 1 January 2008
Closing date: 31 September 2008

5.3 Theoretical activity

My theoretical activities will involve in:

- New security wireless protocols
- Architectural issues in WIDS
- Review of recent anomalous detection techniques

Starting date: 1 January 2007
Closing date: 30 June 2008

5.4 Thesis drafting

Starting date: 1 January 2008
Closing date: 31 December 2008

5.5 Work plan sketch

![Figure 5.1 Work Plan.](image)
Bibliography


[3] 3rd Annual Defcon Wifi Shootout Contest. 2.1


[9] W. Stallings. IEEE 802.11: Wireless LANs from a to n, 2004 2.2.1

[10] E. Perez. 802.11i (How we got here and where are we ahead), August 21, 2004 2.2.1


4.2


[34] Maurizio Aiello, David Avanzini, Davide Chiarella, Gianluca Papaleo. Worm Detection Using E-mail Data Mining. PRISE 2006, Primo Workshop Italiano su PRIVacy e SEcurity, pp 18-21. 4.1

[35] Honeypots: Definition and Value of Honeypots, 2003 4.2.1

[36] Netstumbler. www.netstumbler.com 1