

Vulnerabilities in wireless networks and intrusion detection

SLOBODAN PETROVIĆ



Slobodan Petrović is professor of information security at Gjøvik University College

In this paper, the most frequently exploited vulnerabilities of wireless networks that use the IEEE 802.11 standard are enumerated. Intrusion detection and prevention systems are proposed as an important line of defence in a multifaceted wireless network protection system. However, some concepts from the classical IDS theory must be redefined and there are many changes that these systems must be exposed to in order to operate correctly and efficiently in a wireless network environment. The importance of anomaly detection systems is especially stressed because of very specific attacks that are difficult to detect and respond to by misuse (signature based) detection systems.

1 Introduction

According to a recently conducted opinion poll among the top 40 US research policy makers [1], wireless technologies will be among the most important ones in the next decade. This will dramatically change computer networks, considering not only mobility, availability and quality of service but also security. It is much more difficult to ensure security in this type of network than in ordinary (wired) networks. Since most of the communications in the future will use both wired and wireless networks on the communication paths, new hardware and software technologies will be needed to ensure security. Among these, the intrusion detection and prevention (IDS/IPS) technologies will have to be exposed to the most dramatic changes.

In 1999, IEEE completed and approved the 802.11 standard [2] and this is considered the starting point of wireless LANs (WLANs) in the form that we know them today. There are several members of this standard family, of which 802.11b and 802.11g are the most frequently used. WLANs exist in either *infrastructure* mode or in *ad hoc* mode. An infrastructure WLAN consists of several clients communicating with a central device, so-called *Access Point* (AP). Ad hoc networks have multiple wireless clients communicating with each other as peers in order to share data among them without using an access point. In this paper, by wireless network we mean an IEEE 802.11 (b or g) infrastructure network.

In wireless networks, an attacker does not need physical access to communication lines. He/she can be located anywhere within the range of the wireless communication equipment, and that range cannot be precisely defined and guaranteed because of inherent properties of radio communication that are influenced by many factors. As the consequence of this imprecision, the traditional concepts of insider and outsider attacks must be redefined in wireless networks. Another traditional concept, that of host based and

network based intrusion detection, must also be exposed to changes in the wireless network environment. Wireless networks are faced with specific types of attacks that are not possible in wired networks, such as creation of unauthorized (“rogue”) access points (AP), so-called war driving (probe requests that have not set the values of specific fields), flooding APs with associations, MAC address spoofing, etc.

In order to defend not only the wireless network but also the wired network related to it, a combination of physical, technical and organizational measures has to be implemented. These measures usually include firewalls, vulnerability scanners, virus detection software/hardware, and intrusion detection/prevention systems (IDS/IPS). Bearing in mind the alterations of traditional concepts related to IDS as well as specific attacks against wireless networks, wireless IDS must implement new solutions capable of detecting and responding to the new threats. In this paper, the most frequently exploited vulnerabilities of wireless networks are first enumerated and then some wireless IDS solutions intended to defend such networks are presented. Special focus is given to anomaly detection, since this type of IDS, although more difficult to implement, may become a more complete solution to the problems of wireless networks protection.

2 Vulnerabilities in wireless networks

Wireless connectivity is related to specific vulnerabilities and backdoors for potential attackers that are not available in wired networks. The very physical access to a wireless network is easier because of the nature of radio communication. Unlike that, a wired network can only be accessed and attacked through a physical connection, usually via Internet (unless the attacker has obtained the credentials through social engineering or dumpster diving). The hardware and software tools for penetrating into wireless networks are known and publicly offered (“Net-Stumbler” soft-

ware, for example [3] and various hardware tools for so-called “war driving” – antennas, amplifiers, etc). In [4], seven major security problems related to the 802.11 wireless network standard have been identified and some solutions have been proposed from the corporate point of view:

2.1 Easy access to 802.11 networks

The access point, the key hardware device that serves as an interface between the wired and the wireless part of a network, uses so-called Service Set Identifier (SSID) to differentiate networks from one another. This SSID is broadcast every few seconds in so-called “beacon frames” in order for authorized users to find the correct network. By default, the SSID is set to a fixed value known by everybody and this often enables easy unauthorized access to such networks. On the other hand, the authentication process in the 802.11 standard is known to contain a flaw [5]; namely, before any communication can take place between the access point and a wireless client, they must first begin a dialogue and this process is called *associating*. There is a feature in the 802.11 standard that allows networks to require authentication immediately after a device associates, before it attempts any communication through the access point. There are two possibilities with this setting: *shared key authentication* and *open authentication* (default). The shared key authentication mechanism uses a challenge string that is sent unencrypted to the prospective client, upon its request to the access point. The client then encrypts the challenge string and sends it back to the access point. The fact that the challenge string is available in the radio channel in both clear and encrypted form obviously enables the reconstruction of the running key (the output sequence from the enciphering algorithm) used for encryption. Since the encryption algorithm (RC4 [6] in most cases) is known to be possible to cryptanalyse if certain circumstances are met [7-11] (and interestingly enough they have been met in the early versions of the standard [7,8]) it is also possible (although not so easy) to reconstruct the very secret key. Thus, it is sometimes better to use the open authentication than the shared key authentication, since in the open authentication everybody can access the network, but without the possibility of reconstructing the secret encryption key.

2.2 Unauthorized (“rogue”) access points

This is a problem in large organizations, in which access points may be installed without prior notification to the system administration. If no security measures are activated on such access points, the whole organization’s network may be put at risk, including the wired part of the network. Even if the organization does not officially use wireless networks at all, it may happen that such a network is installed some-

where within it without knowledge of the responsible person/department. An additional problem is that discovering unauthorized access points often requires special equipment (e.g. intelligent sensors deployed throughout the area) and goniometric procedures (triangulation).

2.3 Unauthorized use of service

If an unauthorized access point is installed or an authorized access point is misconfigured, this may result in enabling an attack against the whole organization’s network. The problems that may result from such a security breach are not only of a technical nature (bandwidth misuse). They can be of legal nature too. The unauthorized use of service opens the door to spamming and similar activities in the name of the attacked organization, which may result in severe legal consequences for it.

2.4 Denial-of-service vulnerability

Wireless LANs have the transmission capacity limited to 11 Mb/s for 802.11b and 54 Mb/s for 802.11g (these variants of the 802.11 standard are widely used in Europe). This capacity is shared by all the clients associated to a single access point. Obviously, an unauthorized client could start a massive data transfer and occupy the whole available bandwidth, which would result in a denial-of-service for the rest of the (authorized) clients. On the other hand, radio capacity of the access point can be overwhelmed by traffic coming from the wired network too, at a rate greater than the capacity permits. A *ping flood* launched from the wired segment of a network is an example of such an attack. Several directly connected access points can be attacked at the same time by using broadcast addresses. Traffic injection into the radio network without being attached to a wireless access point is also possible. The classical radio jamming is also an option for performing a denial-of-service attack.

2.5 MAC spoofing and session hijacking

No frame authentication was originally defined by the 802.11 standard. Every frame contains a source address, but it can be forged since no frame authentication is performed. Thus, attackers can use spoofed frames to redirect traffic and corrupt Address Resolution Protocol (ARP) tables. They can easily get the MAC addresses of the stations currently in use on the network and adopt those addresses for malicious transmissions. In addition to hijacking sessions, attacks can exploit the lack of authentication of access points. This fact is exploited by an attacker by presenting him/herself as an access point, since no mechanism in the 802.11 standard prevents it. Then, the attacker gets the credentials of the clients and uses them to gain access to the network through a man-in-the-middle attack.

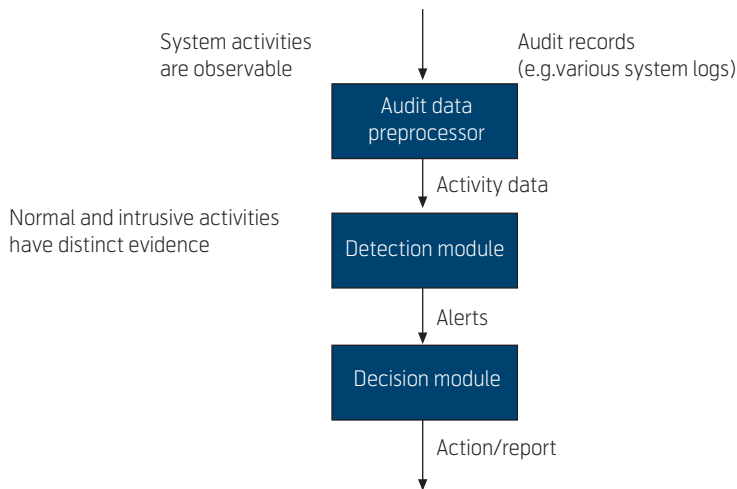


Figure 1 Components of a general IDS

2.6 Relatively easy traffic analysis and eavesdropping

The 802.11 standard does not provide any protection against attacks which passively observe traffic. Frame headers are not encrypted and the security against eavesdropping was initially supposed to be provided by a weak encryption algorithm [7] (WEP – Wired Equivalent Privacy, which is an implementation of the well known RC4 algorithm [6]). Although in the latest implementations the key management protocol changes the secret key every 15 minutes [4], the flaws in the RC4 algorithm persist, such as the existence of weak keys, possibility of related keys attack [8] or the existence of distinguishers and statistical anomalies [9-11]. The 802.11 standard evolved in order to cope with the weaknesses of the WEP encryption. As a transitional solution, the WPA (Wi-Fi Protected Access) standard extension has been introduced. This encryption framework uses the same algorithm, RC4, but the length of the initialization vector has been increased from 24 to 48 bits. However, the flaws of the algorithm that do not deal with the cipher key repetition probability still persist. As a final solution to the encryption related problems within the 802.11 standard, the WPA-2 standard extension has been recently introduced [12]. The encryption algorithm has been changed to AES [13]. The problem, however, is in the requirement that hardware must be changed in order to implement the WPA-2 framework. The reason for this incompatibility is in the need for more resources in order to implement the AES cipher.

2.7 Possibility of higher level attacks

A successful attack against a wireless network can serve as a launch point for attacks on other systems. Placing a wireless LAN inside the security perimeter is therefore considered weakening the security within the perimeter.

3 Intrusion detection – the classical concept

Formally, we can define computer intrusion as a set of actions aimed at compromising the security goals (confidentiality, integrity, availability of a computing/networking resource). Then intrusion detection can be defined as the process of identifying and responding to intrusion activities. A system that performs automatically the process of intrusion detection is called Intrusion Detection System (IDS). An intrusion prevention system (IPS) combines an IDS with a firewall, a virus detection algorithm, a vulnerability assessment algorithm, etc. The ambition of such a system is to manage both preventive and responsive actions against attacks on a computer network.

Two basic assumptions related to the successful operation of an IDS/IPS are the following:

- 1 System activities are observable.
- 2 Normal and intrusive activities have distinct evidence – the goal of an IDS/IPS is to detect the difference.

The components of a general IDS are presented in Figure 1.

Intrusion detection systems are classified:

- By scope of protection (or by deployment)
 - 1 Host-based IDS
 - 2 Network-based IDS
- By detection model
 - 1 Misuse detection systems (pattern matching)
 - 2 Anomaly detection systems (pattern recognition).

Misuse detection IDS and anomaly detection IDS structures are presented in Figures 2 and 3, respectively.

Host-based intrusion detection systems use operating system’s auditing mechanisms (various system logs) to monitor users’ activities and execution of system programs. Network-based IDS operate by monitoring signals from sensors deployed at strategic locations in the network. They inspect network traffic and monitor users’ activities.

Misuse intrusion detection systems use signature or rule based detection. Because of that, they are inca-

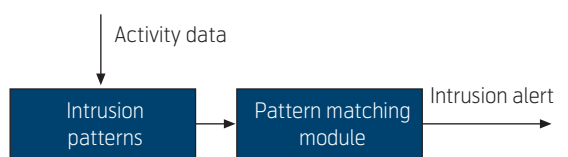


Figure 2 Misuse detection IDS structure

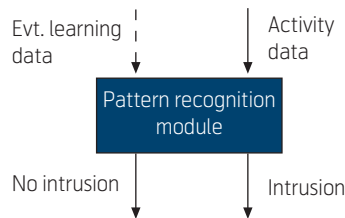


Figure 3 Anomaly detection IDS structure. It may contain a learning phase that uses labelled data

pable of recognising new attacks, which is a very serious drawback. However, all the commercial and publicly available ready-made intrusion detection systems are by now misuse detection based. There are technical and economic reasons for that. The technical reasons are easier design and good behaviour of such systems considering the probability of false alarms. The main economic reason for such a wide offer of misuse detection systems is in the dependence of clients on regular updating of attack signatures database, which includes an extra charge and increases the manufacturer's revenue.

Anomaly detection systems use pattern recognition techniques as their operation mechanisms. They look for deviations from "normal behaviour". Although they are capable of recognising novel attacks, the principal problem of their operation is the fact that these systems cannot reduce the number of false alarms easily. There are many other problems that prevent commercialization and a wider use of these systems. For example, it is very difficult to determine a sharp limit between "normal" and "abnormal" behaviour in a computer network. It is also difficult to ensure a real time operation of these systems since sufficiently precise pattern recognition requires application of complex algorithms. Anomaly detection is carried out by application of the results of various scientific methods, of which the most important ones are statistical methods (cluster analysis), artificial intelligence methods, cognitive science methods, data mining and mathematical abstractions of biological systems (neural nets, immunological system simulation, process homeostasis, etc.).

4 Intrusion detection in a wireless network environment

Unlike the ordinary wired networks, in the wireless network environment defined by the 802.11 standard it is possible to detect some intrusions even at the physical level. For example, unauthorized access points can be detected by carefully deploying radio sensors throughout the protected area and by using goniometric algorithms in order to locate unknown sources of radio transmission. This physical defence

line of the wireless network has to be combined with the lines of defence at the network level in order to be able to detect other kinds of attacks.

Because of the nature of radio propagation, the exact border between the internal and the external network is not known. As a consequence, exact classification of attackers into insiders and outsiders is impossible. Classification of attacks into insider and outsider attacks is not possible either. Thus the security policies that use host based IDS to protect against the insider attacks and network based IDS to protect against the outsider attacks make no sense in the wireless environment. Intrusions are to be detected not only within the wireless network protected area, but also outside of it, bearing in mind the possibility of attacks against other parts of the network from a wireless network as well as pure interference with other wireless networks.

Wireless intrusion detection systems can be divided into misuse based and anomaly based systems in the same way as the IDS for wired networks. Beside classical misuse and anomalies detectable in any network, wireless IDS must also detect wireless specific misuse and anomalies. In wireless misuse detection systems, the main problem is the problem of distribution of the elements of the IDS. Three approaches are possible:

1 Wireless IDS sensors and processors are integrated into the access points

The advantage of this approach over other approaches is in total network coverage at relatively low cost and in easier network management. No separate hardware is needed for the IDS, which lowers the total cost of ownership. The disadvantage of this approach is obviously in the impossibility of integration into existing networks for hardware incompatibility.

2 Overlay IDS with centralized processing

This approach uses dedicated radio frequency sensors deployed throughout the wireless network to be protected. The sensors transfer the data to the dedicated IDS server that performs all the processing and manages eventual responsive actions. The advantage of this approach is in the possibility of integration into the existing network framework. The IDS of this type can achieve the total network coverage but at a higher cost than the integrated solutions. Centralized processing of all the data from the sensors requires an expensive hardware for the IDS server in order for the overall IDS to be efficient enough.

3 Overlay IDS with decentralized processing

The IDS structure used in this approach delegates

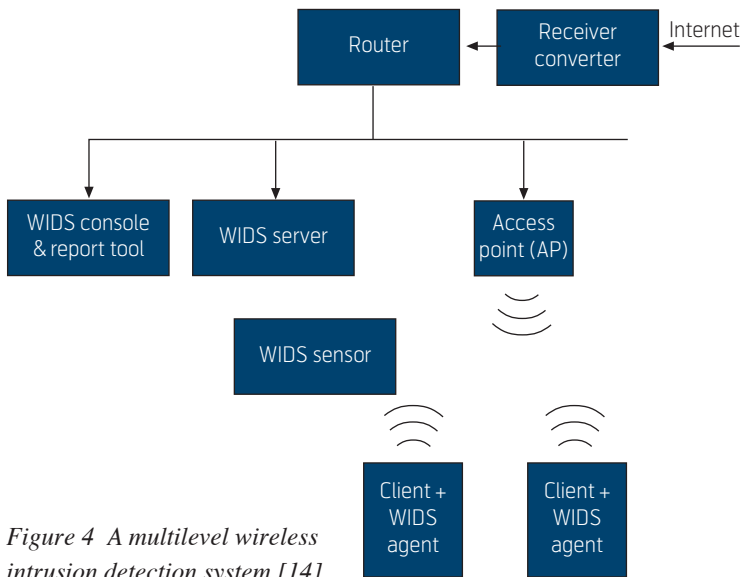


Figure 4 A multilevel wireless intrusion detection system [14]

some data processing to the very sensors reducing in such a way the processing power needed at the IDS server. The advantage of this multilevel approach over the centralized processing approach is in the cost of hardware needed for the IDS server.

Misuse based wireless IDS are incapable of detecting new attacks. Besides, the signatures of the attacks have to be updated very often, since new attacks are detected every day and many of the attacks remain undetected for quite a long time. So anomaly based systems could also be a solution to this problem. However, the problems of false alarms and real time operation persist in this case too.

In [14], a multilevel wireless IDS/IPS is proposed that uses agents on hosts, sensors, an IDS server and a reporting tool in order to combine host based and network based detection in a wireless network environment. The IDS cooperates with the firewall, the antivirus program, and other security tools in order to coordinate activities with them. The goals of the overall system are the following:

- 1 To make an efficient system to defend the wireless network;
- 2 To define attack and intrusion “axioms scope” (misuse detection);
- 3 To define conclusions mechanisms (“theorems”);
- 4 To learn in order to anticipate (anomaly detection) – there is a trade-off between the level of intelligence of the system and its efficiency;
- 5 To recognise the wireless specific attacks;

6 To launch responsive actions in order to defend the system and/or the network.

The simplified scheme of the system is presented in Figure 4.

Neural networks and fuzzy logic have been combined in this system as the means to achieve self learning and recognition of previously unknown attacks (anomalies), especially the wireless specific ones. The responsive actions are launched at both the local and the global level (multilevel detection and response), which improves the efficiency of the system as the whole.

In [15], another multilevel approach to intrusion detection is combined with *situation assessment*, a classification procedure that maps a label to the current state of a system based on data received from multiple sources. This is a general approach, applicable to many processes, such as prognosis and handling of emergencies, monitoring, securing and recovering of critical systems like nuclear power plants and electrical power grids, prediction of terrorist intents, command and control, etc. Classification of input data in an IDS of this type is performed at two levels: source-based classifiers label security status of users’ activity either as Normal or Alert. These decisions are forwarded to the upper level of decision as asynchronous data streams. The upper level classifier combines the decisions of the lower level ones and produces the final decision on the situation status.

The procedure used in [15] may be especially applicable in wireless IDS, because these systems need detection of events at two completely different levels – physical level and network level. Thus completely different sensors and processing are needed for detection of these two types of events. At the same time, it is quite probable that the events of different types are asynchronous. For example, an unauthorized access point may be installed by an insider without any malicious intent and this is detectable at the physical level from the very moment of installation. But the attack may arrive later, after the vulnerability has been detected by an attacker and only then the attack may be detected at the network level.

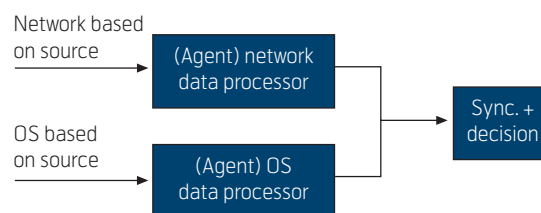


Figure 5 A multilevel intrusion detection system that applies situation assessment [15]

5 Conclusion

In this paper, the most frequently exploited vulnerabilities of wireless networks that use the IEEE 802.11 standard have been enumerated. In spite of improving the standard by strengthening security measures, there are still many problems that require careful deployment and continuous security monitoring in these networks. Wireless intrusion detection/prevention systems are still a necessary tool for this monitoring and management of countermeasures against the attacks. However, in order to cope with the wireless network specific attacks, they must be capable of detecting intrusions at the physical level too, not only at the network level. The problem of integration of host-based and network-based intrusion detection also has to be solved for this type of systems, as well as the unified treatment of insider and outsider attacks. Since it is very difficult to design a misuse-only based intrusion detection system for wireless networks, anomaly detection may play a much more significant role in this environment than in the ordinary wired network environment. This article presented two typical intrusion detection systems that use anomaly detection methods extensively.

References

- 1 Applewhite, A. The View from the Top. *IEEE Spectrum*, 41 (11), 2004, 16–31.
- 2 IEEE Standards Association. *IEEE 802.11 Standard*. <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>
- 3 *NetStumbler*. <http://www.netstumbler.com>
- 4 AirMagnet. *The Top Seven Security Problems of 802.11 Wireless*. AirMagnet Technical White Paper. <http://www.airmagnet.com/products/wp-index.htm>
- 5 ArsTechnica. *Wireless Security Blackpaper*. <http://arstechnica.com/articles/paedia/security.ars>
- 6 Rivest, R L. *The RC4 Encryption Algorithm*. RSA Data Security, Inc., 1992 (proprietary).
- 7 Borisov, N, Goldberg, I, Wagner, D. Intercepting Mobile Communications: The Insecurity of 802.11. *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, July 2001, 180–189.
- 8 Fluhrer, S, Mantin, I, Shamir, A. Weaknesses in the Key Scheduling Algorithm of RC4. *Proceedings of SAC 2001*, LNCS 2259, Springer Verlag, 2001, 1–24.
- 9 Golić, J. Linear Statistical Weakness of the Alleged RC4 Keystream Generator. *Proceedings of EUROCRYPT 97*, LNCS 1233, Springer Verlag, 1997, 226–238.
- 10 Knudsen, L, Meier, W, Preneel, B, Rijmen, V, Verdoolaege, S. Analysis Methods for (Alleged) RC4. *Proceedings of ASIACRYPT 98*, LNCS 1514, Springer Verlag, 1998, 327–341.
- 11 Fluhrer, S, McGrew, D. Statistical Analysis of the Alleged RC4 Keystream Generator. *Proceedings of the FSE 2000*, LNCS 1978, Springer Verlag, 2000, 19–30.
- 12 IEEE Standards Association. *IEEE 802.11i Standard*. <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>
- 13 *The Advanced Encryption Standard (AES)*. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- 14 Pleskonjić, D. Wireless Intrusion Detection Systems. *Proceedings of the 19th Annual Computer Security Applications Conference*, Las Vegas, USA, December 8–12, 2003.
- 15 Gorodetsky, V, Karsaev, O, Samoilov, V. On-Line Update of Situation Assessment Based on Asynchronous Data Streams. *Proceedings of the 8th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2004)*, LNAI vol. 3213, Springer Verlag, 2004, 1136–1142.

Slobodan Petrović is professor of Information Security at Gjøvik University College. He received his PhD degree in 1994 from the University of Belgrade, Serbia and Montenegro. His research interests include cryptography, intrusion detection systems, coding theory, pattern recognition, and combinatorial optimisation. From 1986 to 2000 he participated in various projects at the Institute of Mathematics in Belgrade concerning fundamentals of computer science and pattern recognition. From 2000 to 2004 he was at the Institute of Applied Physics (CSIC), Madrid, Spain, working on the projects 'Cryptographic Protection of Copyright in Digital Networks' and 'Application of Intelligent Mobile Agents in Intrusion Detection Systems'.

email: slobodanp@hig.no