

A WIRELESS INTRUSION DETECTION SYSTEM BASED ON OPEN-SOURCE SOFTWARE

Abstract

The use of wireless networks is growing constantly, not only for public internet access in urban areas, but also to connect computer equipment where wired networks would be impractical. But wireless networks are vulnerable to numerous forms of attack, from breach of confidentiality to denial of service. Since more and more devices can take advantage of wireless networks, and a large number of businesses are relying on wireless network in their day-to-day operations, the potential consequences of these vulnerabilities are getting increasingly serious. While proprietary solutions do exist to address these challenges, they are often expensive and complex to use. This whitepaper describes a simple wireless intrusion detection system, or WIDS, that can be built and operated easily using cheap off-the-shelf hardware and open-source software.

Wireless vulnerabilities

Wireless networks are natively quite vulnerable to security issues, the WEP1 encryption weakness probably being the most famous. Due to the nature of radio waves, a wireless network cannot be concealed like wired local area network. This means that security relies mostly on the communication protocols, which are not always designed and implemented correctly.

The first critical vulnerability of wireless networks is signal jamming: it is quite easy to jam the access points' signal using a more powerful emitter. There aren't many solutions to that problem; techniques like spread spectrum or frequency hopping can run afoul of the official frequency regulations, and their use remains mostly confined to the military.

Because radio waves cannot be concealed easily, one must consider that all information transmitted over the wireless network can be intercepted by anyone. Moreover, anyone is able to inject information into the wireless network. This leads to a huge need in authentication, integrity and privacy measures. WEP, one of the first wireless encryption protocols, was supposed to ensure all these three essential properties, but has proved insecure and can be broken in a few minutes. The more recent standards, WPA2 and WPA2, are considered reasonably secure for now, but do not offer full protection against some design weaknesses in the IEEE 802.11 standard.

The first weakness lies in the fact that anyone can easily forge a MAC3 address, which the IEEE 802.11 standard uses to identify equipment on the network. Being able to forge the MAC address enables anyone to send frames that look like they are coming from one chosen regular host.

A second design flaw, which can also lead to serious threats, is the fact that the management frames used in several operations (such as association with an access point or roaming) are not authenticated.

Finally, several attacks exploit specific vulnerabilities in the communication stack, the drivers or the firmware of the networking equipment.

WEP has proved insecure and can be broken in a few minutes.

Management frames used are not authenticated.

¹ Wired Equivalent Privacy (deprecated)

² Wi-Fi Protected Access

³ Media Access Control, a 48-bit quasi-unique address assigned to each network adapter

A typical attack: the de-authentication flood

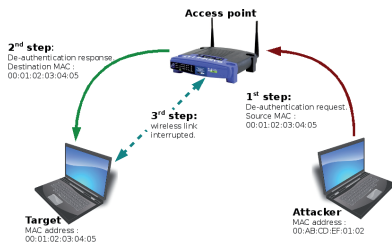


Figure 1: The de-authentication flood attack

Kismet Wireless is a powerful open-source software tool and can be used as an intrusion detection system.

Kismet wireless

Kismet Wireless is a powerful open-source software tool for the discovery and monitoring of wireless networks, and can be used as an intrusion detection system. It can sniff the wireless network using a local wireless adapter, or by gathering data captured from any piece of connected equipment that runs the Kismet drone program.

Kismet can detect various types of intrusions (refer to the Kismet website to obtain a complete list), using two detection mechanisms: analysis and filtering of certain bytes in each packet to discover some very byte-specific attacks, and dedicated automata to spot unusual patterns that can be interpreted as an attack attempt.

We have identified a number of areas where Kismet's already impressive capabilities should still be improved to fit our purposes:

- The detection of MAC address spoofing could be better.
- Detected potential attacks are printed on a terminal, which forces the user to constantly monitor the Kismet terminal to be notified of potential attacks.
- The number of false positives (i.e. legitimate traffic flagged as an intrusion) can be fairly high; the ability to attach a severity level to each alert would help to mitigate this problem.

The concept of Alert Manager

In order to take care of our extra requirements while minimizing changes to Kismet itself, the best solution was to build our new features into a separate component. Our solution was to design an Alert Manager that receives alerts from Kismet and processes them. The major change required in Kismet was then simply a mechanism to send alerts to the Alert Manager (other changes can optionally be introduced in Kismet to improve detection).

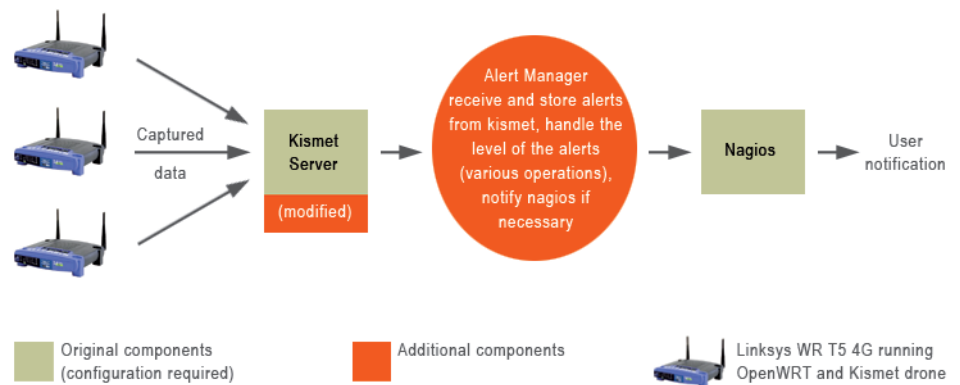


Figure 2: The Alert Manager integration

Packaging the solution

The WIDS software is made up of three interoperating modules, each one with its own configuration files. This leads to a slightly delicate installation and configuration process. The WIDS only runs under Linux, since the monitoring state required for the wireless adapters can only be set with Linux drivers⁷.

In order to make the final solution easier to be deployed, we have packaged the WIDS software into a Linux live distribution (we chose BackTrack⁸ because it is specially made for pen-testing and supports a lot of wireless adapters), which is installed on a USB flash drive. The WIDS can thus be pre-configured to be immediately useable at boot and both the captured data and the configuration files can be saved on a writable partition of the flash drive.

The live distribution allows the user to plug the flash drive in any available computer, boot from it, and immediately use the WIDS.

The live distribution allows the user to plug the flash drive in any available computer, boot from it, and immediately use the WIDS. A graphical configuration wizard written in perl-gtk helps the user to set up the most relevant configuration options for the network to be monitored.

Known limitations

In its current status, our WIDS still raises a number of false positives, and only a detailed analysis of the captured packets allows an experienced user to detect whether or not the alert is an actual attack. Also, as with any other IDS, it is almost impossible to guarantee that there won't be any false negatives. Several improvements are possible to mitigate these limitations, especially in the level handler and in the Kismet detection mechanisms.

Conclusion

Wireless intrusion detection is tricky, and is far from being an exact science. Apart from the attack detection possibilities, the real challenge is to give more or less credit to the raised alerts and to find the right balance between false positives and false negatives. Our chosen design allows a lot of flexibility on both sides, and can lead to some interesting possibilities. The IEEE 802.11w project intends to enhance the MAC layer to provide, as appropriate, mechanisms to improve data integrity, data origin authenticity, replay protection, and data confidentiality for selected management frames. These improvements will hopefully eliminate a lot of wireless vulnerabilities.

IT-Solutions by ELCA

ELCA Informatique SA	ELCA Informatik AG
Av. de la Harpe 22-24	Steinstrasse 21
1000 Lausanne 13	8003 Zürich
Switzerland	Switzerland
Phone + 41 21 613 21 11	Phone + 41 44 456 32 11
Fax + 41 21 613 21 00	Fax + 41 44 456 32 00
	info@elca.ch
	www.elca.ch

⁷ Windows Vista would allow a more flexible use of the network adapters

⁸ BackTrack is a Linux live-distribution focused on penetration testing