THE THREAT-VICTIM TABLE
A Security Prioritisation Framework For Diverse WLAN Network Topographies

Jonny Milliken and Alan Marshall
Department of Electrical & Electronic Engineering, Queens University Belfast, Northern Ireland, U.K.

Keywords: WLAN, 802.11, Intrusion Detection Systems, Network Security, Kismet.

Abstract: At present there is no common means for establishing the security performance of wireless local area networks (WLANs) against threats. Furthermore, there has been little investigation into whether security performance is reliant on network topography. Consequently this paper advocates that for a range of WLAN infrastructure topographies (home, enterprise & open-access) there can be significant diversity in terms of resources, equipment, users and most importantly security, which can in turn influence attack detection performance. In order to demonstrate these detection differences, a novel framework for evaluating network security performance (the Threat-Victim Table) is developed. This framework is applied to a range of WLAN topographies using an open source (Kismet) Wireless Intrusion Detection System. Three Kismet components are utilised; client, server and drone, to represent typical IDS deployment configurations for these topographies. Analysis of the security capability of Kismet is derived as an example of this framework, for qualifying network security performance against security threats and also to assess the priority level of these vulnerabilities.

1 INTRODUCTION

Wireless network deployments can differ between installations depending on the needs and resources of the user or network. While this is evident in the distinctions between the protocols of mesh or infrastructure networks it is less evident within an infrastructure network. In particular infrastructure networks are often separated into home, enterprise & open access scenarios (Microsoft Windows Help, 2007) even if the delimiting factors between them have not been rigidly defined.

Each of these networks is subject to a multitude of attacks, across many layers, with different attack objectives and often competing defence strategies (Mirkovic & Reiher, 2004). Due to this variation it can be difficult to establish, for a given network or user, what the key threats and defences needs to be.

In order to protect these networks many strategies are employed such as firewalls, anti-virus software and Intrusion Detection Systems (IDS). IDSs can vary according to different networks (Crainicu, 2008), or focus on different layers or equipment. Currently the trend is towards Cross Layer monitoring (Thamilarasu & Sridhar, 2007).

However at present there is no standardised means of determining a network's security capabilities against threats or between security systems (Ibrahim, et al., 2008). As a consequence there has been little investigation into whether this security performance is dependent on deployment topography.

To address these issues this paper outlines a framework for representing attack detection capabilities. As a demonstration of this framework an example is developed using an 802.11 WLAN network and the Kismet layer 2 Wireless Intrusion Detection System (WIDS) software. This example demonstrates how the framework can be used to evaluate the detection performance of an IDS across different topographies. The results of this evaluation advocate a case for considering infrastructure networks as diverse as home, enterprise & open access; using characteristics such as resource availability, equipment, security and threat priority.

2 WLAN THREATS & KISMET

The convenience of 802.11 WLANs has led to their widespread deployment; however as their

Milliken J. and Marshall A. (2010).
THE THREAT-VICTIM TABLE - A Security Prioritisation Framework For Diverse WLAN Network Topographies.
In *Proceedings of the International Conference on Security and Cryptography*, pages 37-42
DOI: 10.5220/0002935400370042

deployment has expanded the security issues and the threat of attacks on them increases (Turab & Moldoveanu, 2009). These arise largely from the insecurity of MAC management frames and the unpredictability of the medium, meaning that it is very difficult to distinguish attack heuristics from common interference or legitimate activity.

As a result, WLAN security is an area of active research and a number of specific threats have been well studied and commented upon in the public domain (BBC Watchdog, 2009). This growing exposure qualifies 802.11 WLAN as a good candidate for high level security visualisation and suitable as a use case of the proposed framework.

Investigations in (Ref, 2009) & (Gill et al, 2006) have determined that common attacks against WLANs can be distilled into 4 categories:

- **Client Denial of Service Attacks:** Adversary spoofs packets from the Client seeking to deauthenticate or disassociate the user from the Access Point (AP).
- **Broadcast Denial of Service Attacks:** Adversary spoofs packets from the AP, then broadcasts to all connected clients, deauthenticating /disassociating them from the AP.
- **Masquerade Attacks:** Adversary broadcasts packets with forged headers advertising themselves as a legitimate or open AP.
- **WEP / WPA Attacks:** Adversary attempts to bypass the encryption by breaking the WEP / WPA key and gaining access to the channel.

These are the attack categories that this paper considers to be main threats against an 802.11 WLAN, although some are amalgamations of several exploits. Any IDS that purports to defend against such intrusions should recognise or detect these attacks. This does not represent an attack taxonomy but is an accurate categorisation.

2.1 Kismet

For the purposes of the research it is assumed that a typical IDS needs to fulfil some critical criteria; free & open source, modular and well known in the area. However these criteria are difficult to realise in practice due to the sparsity of WLAN IDS options. For example, Snort, (Snort, 2010) the most prevalent free IDS, has had the development of its wireless extension (snort-wireless) mothballed since 2005.

The option chosen here is Kismet, one of the foundation tools of wireless hacking, developed by Mike Kershaw and released under GNU licence (Kismet, 2010). The software provides passive, wireless traffic sniffing and network discovery features which are well documented and used within the war-X-ing communities. Of particular benefit is the modular structure of Kismet; with a Client, Server and Drone architecture that has the flexibility to represent any number of networks. In this sense it fulfils all the original criteria for the investigation.

2.2 Kismet Detection Performance

A generic Kismet configuration was set up to monitor a test network while each of the identified WLAN attacks were carried out on either the AP or additional clients connected to the AP. This Kismet module contains all the detection thresholds and signature details of the software and is an accurate representation of its total abilities. Upon detection the software brings up a text alert for the watching admin to indicate that there is illegitimate or suspicious activity and which MAC addresses are associated with it. Kismet detection performance for these threats is shown in Table 1 below.

Table 1: Kismet Detection Performance under threat from WLAN specific intrusions.

Threat	Detection	Alerts
User DoS	Yes	Deauth Flood & 10seconds between data & deauth
Broadcast DoS	Yes	Deauth Flood and Broadcast Deauth
WEP Crack	No	None
WPA / WPA2	No	None
Masquerade	On action	Channel Changed / BSS Timestamp

Although the individual alerts do not indicate the attacks explicitly, it is possible to identify each positive detection from a combination of alerts.

The results indicate that Kismet could not detect either WEP or WPA channel encryption attacks, however it was able to identify both DoS attacks and distinguish between them depending on the alerts generated. It was also able to identify a masquerading adversary under certain conditions, i.e. when an SSID impersonated another legitimate AP or changed broadcast information.

Detection performance information such as the kind provided here is not readily available or verifiable for most IDS. This raises two issues:

- It is difficult to establish the detection performance of an IDS.
- It is difficult to directly compare the performance of IDSs against each other.

Often some detection information is provided but these tend to be inconsistent between descriptions and incompatible across software. A common framework for identifying the performance of IDSs would alleviate these issues.

3 DETECTION PERFORMANCE FRAMEWORK FOR IDS

In an environment with a multitude of attacks these threats are usually distinct but not necessarily immune to classification. There must be common elements that connect them, the foremost of which being the domain in which they operate. Since each domain has a finite number of protocols and devices operating within it there will naturally be an overlap between processes and attacks.

One means of classifying these threats within a framework is by identifying two parameters:

- What services are under threat? i.e. what is the motivation of the adversary
- On what device does the service run? i.e. who is the intended victim of the attack

"Devices" here indicate autonomous equipment while a "service" is any facility provided to or by the device. In a sense the devices are nodes in the system while the services are the means in which they connect to each other; it is evident that any network can be made up of these primitives. If an adversary was to attack both devices and services this will not disrupt the classification, as these actions can be decomposed into two individual attacks being carried out simultaneously.

An attack on a service leaves devices free to avail of other services while an attack on a device allows the service to continue operating for others. The challenge is to identify these devices and services, given that the quantity and their nature can differ. As an example use-case, this framework is applied to the WLAN domain and is applied to Kismet to exhibit its use in security applications.

3.1 802.11 WLAN Threat-Victim (T-V) Detection Table

The attacks identified in Section II can be said to threaten two distinct network services. Both DoS attacks degrade or render unavailable the **link** that exists between devices, while the Masquerade and Encryption attacks can be said to threaten or compromise the **security** of the link. A DoS attack will stop communication between devices but the security of data or access will remain unaffected, while an adversary wishing to bypass security has no vested interest in collapsing the link.

Considering the devices in the network, attacks can be classified based on an adversary's intended victim. An adversary could be attacking either the **users** of the network, or the network **infrastructure** itself. An infrastructure device here will consist of an AP which will likely service a collection of user devices making links to or through it.

Having identified two device classes and two services under threat we can develop these parameters into a Threat – Victim Detection Table focussed on WLANs, as in Table 2.

Table 2: WLAN Threat-Victim Description Table.

		Victim	
		User	**Infrastructure**
Threat	**Link**	C DoS	B Dos
	Security	Masquerade	Encryption

Referencing the table we can conclude that in a given deployment the adversary could seek to:

- Perform a DoS attack against a **user link** to gain resource preference in a congested channel by either delaying or discouraging the victim from connecting.
- Perform a DoS attack against an **infrastructure link** (e.g. the AP) as sabotage / nuisance.
- Create a false identity to lure **users** to connect, bypassing **security** in order to utilise phishing or information theft.
- Attack and bypass encryption in order to gain internet / document / resource access on an otherwise restricted **secure infrastructure**.

3.2 Kismet T-V Table

Applying the T-V Table generated by this framework to the IDS detection performance of Kismet results in Table 3, a combination of Tables 1 & 2. Using colour coding to identify detection performance leads to a three dimensional table, where:

- The green area gives a concise summary of Kismet detection performance.
- The orange area shows the fields which require configuration or policy changes.

- The red area represents the areas not covered by Kismet and thus the threats that a system that uses Kismet is still vulnerable to.

Table 3: Kismet WIDS Evaluation using T-V Tables.

Key Green : Light Orange : Stripe Red: Dark		Victim	
		User	Infrastructure
Threat	Link	C DoS	B Dos
	Security	Masquerade	Encryption

The T-V table allows the framework to qualify individual IDS performance; if there is more than one IDS under consideration then it can also be used for comparison. Depending on the areas that are colour coded it is possible to evaluate the performance of different IDSs and IDS configurations.

Since no IDS exists which will perfectly detect every attack at every layer, the network security designer would have to make the choice between different performance abilities in their IDS selection. This decision creates the idea of threat prioritisation for network security, i.e. given imperfect systems how can one determine the best IDS or configuration for the deployment?

4 NETWORK TOPOGRAPHIES

When choosing an IDS there needs to be a method of determining the relative importance, or prioritisation, for the network in question. The issue is that this prioritisation will not be fixed in every instance, each network is different and depending on the goals of the deployment some threats may be more dangerous than others.

The T-V table can be applied to solve this problem, working not as an IDS evaluation tool but as a security prioritisation tool. In order to justify this assertion we must establish the characteristics of different types of infrastructure networks and their impact on security. Kismet is again used, leveraging the modularity and flexibility of the software.

Each WLAN is unique in many respects such as usage patterns, access methods and physical resource availability, and ideally the WIDS should be tailored to these characteristics. There are generally three distinct WLAN topographies in operation today: home, enterprise & open access. These cover most WLAN deployments.

4.1 Kismet Architecture

The modularity of Kismet's Client, Drone & Server system is used to construct these networks. Each of the components can be implemented in a number of connected, distributed fashions within average user equipment and / or APs. The key features of each module are:

- **Client:** Front-end interactive GUI with detection notification and network discovery. Suitable as a stand-alone detector.
- **Server:** Similar to Client minus the front-end GUI and network tracking.
- **Drone:** Distributable component which must connect to either a Server or a Client to provide detection and network discovery information

4.2 WLAN Topographies

Each of the infrastructure topographies are different in resource scarcity, structure and equipment availability and so the optimal IDS deployment architecture is expected to reflect this:

Table 4: Summary of Network Topography Differences.

	Char	Home	Enterprise	Open
Access Info	Physical	Always	Always	No
	Network	Always	Often	No
User Behaviour	Number	Low(<5)	High(10+)	Variable
	Data Usage	High & unstable	High & stable	Low & unstable
	# Admins	All users	Med	Low
Equipment	Coverage Area	Low	Med - High	Med – Low
	# APs / # Channels	1 / 1	x / ≈ 3	1-2 / 1-2
Threats	Secure Data?	Some	Yes	No
	Outside Network	Encrypt. / C & B DoS	Encrypt.	Masq.
	Inside Network	None	Masq.	Masq., C DoS

Home: Within a common home network there are two considerations: availability and reliability. The network is likely to be constructed of various portable or unreliable devices that might be turned on or off arbitrarily. The only technological constant here is the AP or router. A WIDS deployment in this environment could only rely on the router for reliability and guaranteed availability for a WLAN

to exist. For Kismet, a Server component embedded within the router is the optimal solution.

Enterprise: In an enterprise installation there will be at least one administrator. In commercial deployments the standard tactic is to employ an independent network of distributed sensors so that security is not dependent on non-admin personnel.

A WIDS deployment in this environment would be optimally implemented with a Drone in available APs connected to one or more administrator terminals running the Client for monitoring. The Client over Server permits monitoring connections and within the bounds of the enterprise, the connection to external networks can be restricted.

Open Access: A typical open access deployment will often be one router with one PC available locally for office or business admin tasks which is reliably active during operating hours.

A WIDS deployment in this environment would most likely benefit from a Drone module within the router and a Server running on the background office PC. The justification for the Server over the Client is that network tracking and connection monitoring / logging is turned off due to the greater likelihood for neighbouring networks and the quasi-legal aspect of eavesdropping these connections.

Varying the Kismet architecture over these network topographies has shown that each deployment will have different physical hardware resources to utilise, and the WIDS implementation must change accordingly.

4.3 T-V Table Prioritisation

Table 4 identifies the variation in threats with differing network topography; the T-V table can then be used to determine the associated threat priorities. From this it is possible to create a new set of tables where the colour coding is used to signify the threat priority level. To demonstrate this, the following TV tables can be derived for each of the infrastructure topographies (the colour coding uses blue to signify a HIGH priority and yellow to signify a LOW priority):

Table 5: Home Network Security Prioritisation TV Table.

Key Yellow : Light Blue : Dark		Victim	
		User	**Infrastructure**
Threat	**Link**	C DoS	B Dos
	Security	Masquerade	Encryption

The Home network is chiefly concerned with threats to the connection as well as the encryption integrity. Theft of connection through subverting encryption would be less of an issue yet the possibility of accessing shared files is a danger. Since there will typically be one router within the network and the adversary effort required to accurately mimic the network is high the danger of a Masquerade intrusion is less of a concern.

Table 6: Enterprise Security Prioritisation TV Table.

Key Yellow : Light Blue : Dark		Victim	
		User	**Infrastructure**
Threat	**Link**	C DoS	B Dos
	Security	Masquerade	Encryption

The enterprise network is chiefly concerned with security threats rather than connection threats; it would be more damaging to have data stolen or information gathered on employees than a temporary loss of network access.

Table 7: Open Access Security Prioritisation TV Table.

Key Yellow : Light Blue : Dark		Victim	
		User	**Infrastructure**
Threat	**Link**	C DoS	B Dos
	Security	Masquerade	Encryption

Due to the customer orientated aspect of this network, the major concern will be what threats or attacks can disenfranchise the users of the network and threaten their confidence in the service provided. Thus link degradation or AP spoofing would be chief concerns in this topography. However a user gaining free access from breaking encryption would be ranked lower since there should be no shared files or resources to protect.

The result of these tables is the assertion that not only are the networks distinct in equipment and resources, they are also distinct in types of security threats & security priorities as well. This threat prioritisation is useful for practical security as well as indicating that IDS research may need to address the security implications of differing topologies.

5 RELATED & FUTURE WORK

There is no research work to date which develops a network security prioritisation framework for

WLANs. (Prasad, 2007) proposes a threat identification methodology applied to a Personal Network (PN), however the approach relies on the user having expert knowledge and assumes that all vulnerabilities will be identified through brainstorming.

Another framework taking a similar approach is (Hernan et al, 2007). The procedure takes structurally similar steps but arrives at a table (Microsoft SDL Blog, 2007) which works more as a guide to a set of bins in which to store brainstorming ideas. It is also primarily for software development rather than at a network infrastructure level.

Future work will seek to enhance the T-V table to include additional factors such as bandwidth, latency, routing devices, network elements etc.

6 CONCLUSIONS

At present there is no coherent means of representing the detection performance of IDS systems for wireless area networks (Ibrahim, et al., 2008), making selection of IDS for these networks a problem. This paper presents a novel evaluation framework which provides the capability to evaluate and compare the attack detection of a range of network topographies. Such performance evaluation tools will aid the proliferation of IDS as well as help evaluate network threats.

It is demonstrated that there is a difference in attributes for network topographies even within infrastructure environments. This difference exists in resource usage and security, two important tenets of an Intrusion Detection System. This highlights the requirement that future IDS research and security tactics need to adapt to network deployment strategies in both a technology and logistics sense (e.g. resources, equipment, users).

Both issues are addressed by the development of a novel Threat-Victim (T-V) Detection Table framework which provides rapid, visual detection performance evaluation and comparison of relative IDS performance. A number of typical WLAN topographies are explored using a well-known open source IDS (Kismet). Kismet's modularity is useful in research scenarios and utilising this it is shown that any WIDS needs to be tailored according to the topography of the network deployment. The T-V tables can also be used to allow network security designers to choose the most appropriate IDS for their network depending on its detection features, their own prioritisation and on the topography of the network.

REFERENCES

BBC Watchdog, 2009. Is your Wifi Secure? *BBC Online*, [online] 29 October. Available at http://www.bbc.co.uk/blogs/watchdog/2009/10/wifi_hot_spots_not_secure.html [accessed 30 October 2009]

Crainicu, B., 2008. Wireless LAN Security Mechanisms at the Enterprise and Home Level. *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics,* pp. 306-310

Gill, R., *et al*, 2006. Specification-Based Intrusion Detection in WLANs. *22nd Annual Computer Security Applications Conference (ACSAC'06)*.

Hernan, S *et al*, 2007. *Uncover Security Design Flaws Using The STRIDE Approach*[online]. Available at http://msdn.microsoft.com/en/gb/magazine/cc163519.aspx

Ibrahim, T., *et al*, 2008. Assessing the challenges of Intrusion Detection Systems,Available at: http://www.intrusiononline.net/ docs/cisnrAC_IDS.pdf [Accessed 15 November 2009]

Kershaw, M., 2010. *Kismet* [online]. Available at: http://www.kismetwireless.net/

Microsoft SDL Blog. 2007. *STRIDE Chart.* [online]. Available at http://blogs.msdn.com/sdl/archive/2007/09/11/ stride-chart.aspx

Microsoft Windows Help. 2007. *Choosing a Network Location.* [online]. Available at http://windows.microsoft.com/en-us/windows-vista/Choosing-a-network-location

Ref, 2009. Removed

Mirkovic, J., Reiher, P., 2004. A Taxonomy of DDoS Attack and DDoS Defence Mechanisms. *ACM SIGCOMM Computer Communication Review* (34/2) pp.39-53

Prasad, N. R., 2007. *Threat Model Framework and Methodology for Personal Networks (PNs)*. In Communication Systems Software and Middleware, 2007 (COMSWARE 2007).

Snort IDS, 2010. [online] Available at: http://www.snort.org/

Thamilarasu, G., Sridhar, R., 2007. *Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks*. In MILCOM 2007.

Turab, N., Moldoveanu, F., 2009. *A Comparison Between Wireless LAN Security Protocols*. [online] University Politehnica of Bucharest. Available at: http://www.scientificbulletin.upb.ro/rev_docs/arhiva/full7970.pdf