A POLICY-BASED ARCHITECTURE FOR PROTECTING 802.11 WLANS AGAINST DDOS ATTACKS

Alan Marshall, Wenzhe Zhou
School of Electrical & Electronic Engineering, Queen's University of Belfast, Belfast, Northern Ireland, UK

Keywords: Network Security, WLANs, Policy, DDoS

Abstract: The security mechanisms available in 802.11WLANs are considered to be extremely vulnerable to malicious attacks. This paper proposes a policy-based architecture to protect 802.11 WLANs against Distributed Denial of Service (DDoS) attacks. The architecture proposed is based on the 802.1X standard, which forms the basis of the Robust Security Network (RSN) framework. The main focus of our work is to develop a policy-based server that can control certain actions taken by WLAN access points so that proper countermeasures will be taken whenever a DDoS attack occurs. The policies are both rule and case based and are contained in a Policy Based Security Server (PBSS). The approach taken is to simulate the behaviour of this architecture when faced with a range of DDoS attack strategies, and to use this to characterise the type of security policies required by the PBSS.

1 INTRODUCTION

In a very recent timeframe, the security of wireless networks has become a critically important topic worldwide. Since the emergence of the first DDoS attack tool toward mobile phones, known as the SMA-flooder (L.Sherriff, http://www.theregister.co.uk/content/1/12394.html), wireless security has attracted much more attention from researchers. DDoS is generally considered to be one of the most powerful forms of attack because of the high damage to network services. In fixed networks, large servers can be rendered inactive in seconds by the millions of packets generated by DDoS attacks. This situation is further compounded in the WLAN environment, where any attacker can eavesdrop on all network services without any fear of detection. In the 802.11 WLAN infrastructure mode, every station communicates through the access point (AP). If a malicious attacker launches a DDoS attack towards the AP, all services in the WLAN may be disrupted. Unfortunately, 802.11 standards don't have strong security mechanisms. The first security protocol, the wired equivalency protocol (WEP) was launched in 1999, and this was shortly found to have serious weaknesses. Two new solutions have been proposed: the Wi-Fi Protected Access (WPA) is an interim standard and the forthcoming new standard will be 802.11i (Jon Edney et al., 2003). Unfortunately, neither of these protections is against DDoS attacks.

This paper aims at designing a framework to protect against DDoS attacks in 802.11 WLANs. DDoS attacks can span a range of protocol layers, from MAC to transport, and we propose to design a policy-based architecture, which can make appropriate strategies at each layer whenever an attack occurs. In our approach, we imagine that the WLAN is programmable, under the control of the policies. We introduce a Policy-Based Security Server (PBSS), which resides in the fixed network. The PBSS monitors the security information of 802.11 WLANs via the access points and initiates appropriate countermeasures should an attack be detected. The rest of this paper is organized as follows. Section 2 gives a brief overview of the 802.11 security protocols. Section 3 describes the DDOS threats to 802.11 WLANs. Section 4 introduces the policy framework, and section 5 describes future work and conclusions.

Marshall A. and Zhou W. (2004).
A POLICY-BASED ARCHITECTURE FOR PROTECTING 802.11 WLANS AGAINST DDOS ATTACKS .
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 107-112
DOI: 10.5220/0001393901070112

2 REVIEW OF SECURITY MECHANISMS IN 802.11

2.1 Security Protocols and Basic Security Mechanism

Privacy (WEP). Previous work has shown that WEP is absolutely insecure (Nikita Borisov et al., http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf). In order to address the vulnerabilities in WEP, the IEEE group has designed the Robust Security Network (RSN), which is based on 802.1X standard.

2.2 IEEE 802.1X Standard and RSN

The IEEE 802.1X was originally a simple standard for passing EAP (Extensible Authentication Protocol) messages over a wired or wireless LAN. With 802.1X, EAP messages are transmitted in Ethernet frames rather than PPP. There are three terms in 802.1X: the Supplicant, the Authenticator and the Authorizer. Figure 1 shows the IEEE 802.1X reference model. RSN provides mechanisms to restrict network connectivity (at the MAC Layer) to authorized entities only via 802.1X. In the WLAN the users are the supplicants and the AP is the authenticator. The function of an AP is to forward the traffic. It doesn't need to know the detail of the authentication procedure. This is the idea of 802.1X, which can guarantee both scalability and flexibility. Our work is based on this idea. Our approach also introduces a centralized server, based on a policy architecture, which is responsible for determining security threats, and implementing various security policies.

While RSN improves the key management (TKIP per-packet key used), the management frames are not authenticated. It is therefore easy to forge the management frames to generate attacks. The authentication method in RSN is one-way, and thus clients may be easily compromised by an attacker who pretends to be an access point.

3 DDoS ATTACKS

3.1 General Situation

Distributed Denial-Of-Service attacks generally follow the architecture shown in figure 2. The primary goal of the attack is to deny the victim(s) access to a particular resource (CERT Coordination Center, 2001). The services are denied by sending a stream of packets to a victim that either consumes some key resources, thus rendering it unavailable to legitimate clients, or providing the attacker with unlimited access to the victim's machine so that he can inflict arbitrary damage (J.Mirkovic et al., 2002). The DDoS strategy uses a classic Agent/Zombie control topology with direct communication via custom TCP, UDP, and ICMP protocols. Packet flooding attacks used UDP floods, TCP SYN floods and ICMP echo request floods (CERT Coordination Center, 2001).

In order to connect to an Access Point (AP) and transmit data, a client must complete both authentication and association. The primary authentication methods are open system and shared key authentication, and MAC address based access control lists. The security solution in the classic 802.11 standard is called the Wired Equivalent

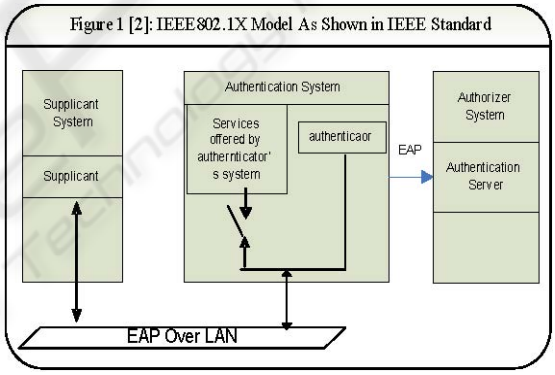

Figure 1: (Jon Edney et al., 2003): IEEE 802.1X Model

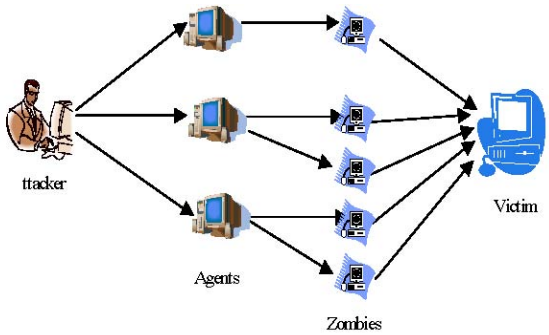

Figure 2: DDoS attack architecture

3.2 DDoS Threats to 802.11 WLAN

DDOS attacks threaten both the lower and the upper layers of the network. In the infrastructure network,

TCP and UDP are used. Hackers can use current attacking tools to perform DDOS attacks against the TCP, UDP and ICMP protocols. Denial of service can be performed in different layers in 802.11. Attacks in the IP and TCP layers are exactly the same as in the fixed network, and include SYN flood attack, ICMP ECHO request floods. Several denial-of-service scenarios in the MAC layer are described:

(i) Because the disassociation and deauthentication frames permit use of the broadcast MAC address as the target station, the attacker forges some disassociation or deauthentication frame and sends it to either the AP or the wireless station (STA). The AP thinks that the STA wants to disconnect from the network and grants the request and closes the association service.

(ii) An attacker can deny service to a STA when there is more than one AP on the same WLAN. It can send a forged Association-request message to any other AP with which the legal supplicant is not connected, with the victim's MAC address. The AP approves the association (authenticate after association in 802.11 (Tim Moore et al., http://www.drizzle.com/~aboba/IEEE/11-01-TBD-I-Authenticated-FastHandoff.ppt)) and sends out a layer 2 update frame to the wired LAN. The router or switch now begins forwarding traffic to the AP that just sent the layer 2 update, and the actual station no longer receives any traffic (Jon Edney et al., 2003)

(iii) The attacker compromises a group of Zombie STAs. These zombies send bogus information to the AP such as forged STA MAC addresses. The resources on the AP are exhausted and the AP either reboots or no longer permits new stations to associate to it (Jon Edney et al., 2003).

(iv) Because there is only one-way authentication, the attacker forges an AP's MAC and network addresses (BSSID and ESSID). The victims will think the forged AP and the real AP are the same and connect to the bogus one. The attacker can now do whatever it wants to the victims.

(v) Vulnerabilities that appear during the authentication can cause denial of service attacks as well. For example, an attacker can inundate the access point by large numbers of authentication requests. Figure 7 shows the EAP message format in 802.1X. The Identifier field has 8 bits. The IEEE 802.1X indicates that it should be incremented for each message sent. Thus the access point limits the parallel associations to 255. A single attacker can use a random MAC address and send 255 parallel requests to prevent any other station from joining the access point. Another example is EAP failure message spoofing (Mishr A. et al., 2002). Once the supplicant receives the EAP failure message, it goes into to a hold state for up to 60 seconds before returns into the next state (a detailed state description is available in (IEEE Draft P802.1X/D11, 2001)). An attacker can keep sending a fake EAP failure message every 60 sec to the target so that it always stays in the hold state without getting any service. The attacker can also forge the EAP success message and send it to the target. Thus the victim's state goes to authenticated (IEEE Draft P802.1X/D11, 2001) and the attacker can receive all network traffic from the supplicant.

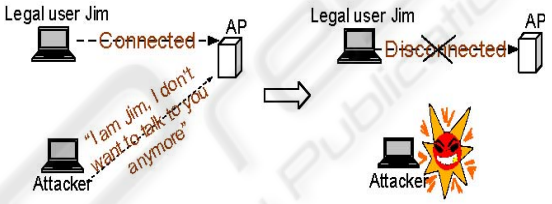

Figure 3: Denial of Service Attack case

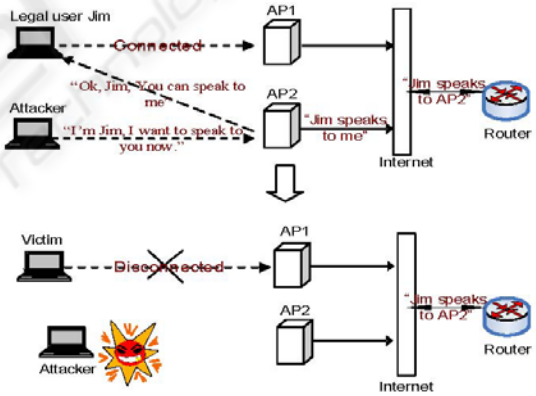

Figure 4: Denial of Service attack case (ii)

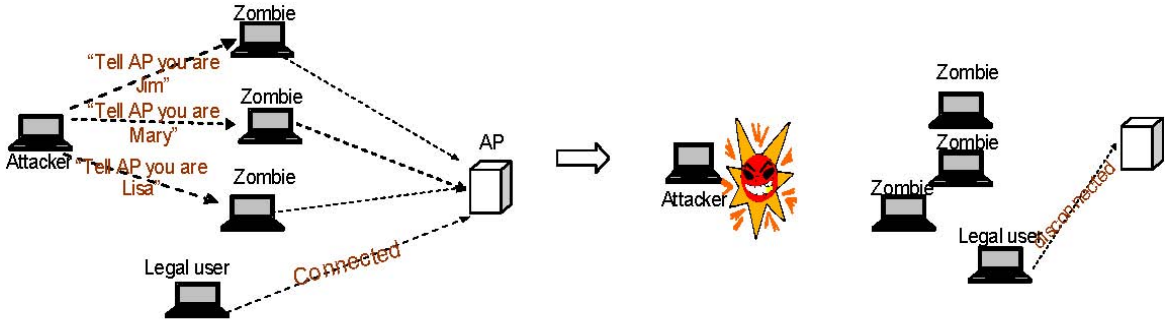

Figure 5: Denial of Service attack case (iii)

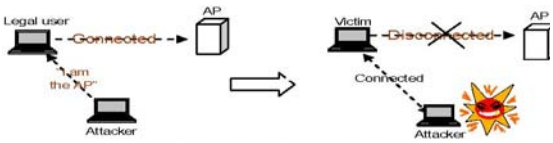

Figure 6: Denial of Service attack case (iv)

Code	ID	Length	Data

Figure 7: EAP packet form

The above cases are several examples of DDoS attacks in IEEE 802.11 WLANs. Additional attacks can be performed according to the vulnerabilities in both the encryption algorithm and the protocol implementation process.

4 THE POLICY-BASED ARCHITECTURE

4.1 Policy-based Framework in 802.11

The previous sections described the security mechanisms and the insecurity in IEEE 802.11. A proficient attacker can easily listen to the wireless channel, forge unencrypted management frames and perform a DDoS attack. This section elucidates the model to protect against the DDoS attacks identified. Figure 8 shows the policy-based security architecture. For flexibility and scalability, we introduce a central policy-based security server rather than build up security countermeasures in each access point. This architecture is based on the idea of "Thin access points" and the approach to security found in IEEE 802.1X. Here an AP plays the role of a gate guard who passes the supplicants' requests to a secure server.

The **P**olicy **B**ased **S**ecurity **S**erver (PBSS) actively monitors the performance of the wireless LANs. It sends probes to enquire about the activity in the access points. For example, a good question can be: "Are there a lot of disassociation requests in the networks now?" or "Have you rebooted? Why?" At the same time the access point sends reports to the PBSS when it suspects something may be wrong. For example, when attack in case (iii) occurs, the access point will ask the PBSS: "I have to reboot because it seems a lot of my clients have changed." According to the abnormal phenomenon, the PBSS sends some 'capsules' (packets with commands encapsulated) to the access points to tell them how to deal with the current situation.

4.2 The Policy-based Security Server (PBSS)

Figure 9 indicates the construction of the model. There are three modules: *the DDoS attack repository* module which collects different DDoS attack phenomena, the attack information is input according to known attacks and new attacks which are recorded automatically; *the policy rules* module which stores the countermeasures for different kinds of attacks; *the decision point* module which makes decisions

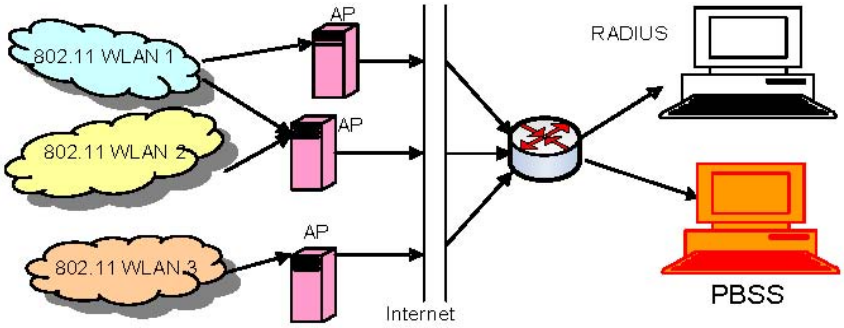

Figure 8: A policy-based security architecture for 802.11 WLAN

about a possible attack. The enforcement point in this model is the access point, which accepts the commands from the PBSS and executes them for the corresponding WLAN. According to the APs responses to the probes, the PBSS does a rule-based search in its attack repository and checks whether there is a matching case. If not, the PBSS ignores the report and continues listening to the next report. If yes, the PBSS then decides on the appropriate policy and sends it to the corresponding AP. Figure 10 shows the state machine of the PBSS.

The PBSS and AP communicate with each other through a COPS (Common Open Policy Service) protocol over TCP connection. When an AP receives commands from the PBSS, it applies the policies to its 802.11 WLANs. The countermeasures could involve either changing the topology of the WLAN, or finding out the attack source. In general the countermeasure policy will depend on the specific phenomena of the attacks, and here it is intended to implement a heuristic classification engine.

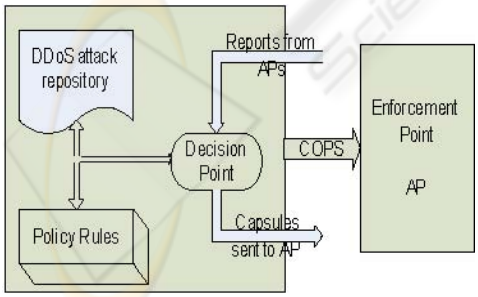

Figure 9: Architecture of PBSS

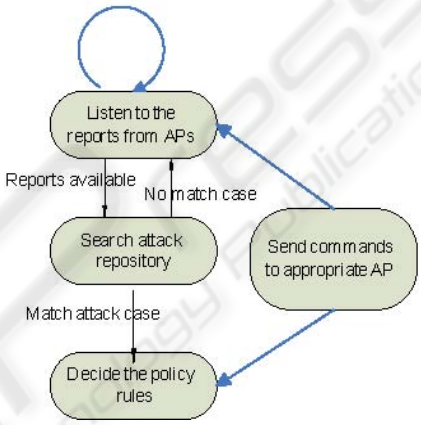

Figure 10: PBSS state machine

4.3 Distributed PBSS

Generally, a number of WLANs may be scattered over a large area. In this a single PBSS is not effective for controlling all the security situations, and a distributed architecture of PBSSs located in different areas is required. Figure 11 shows a distributed PBSS network. Here PBSSes exchange

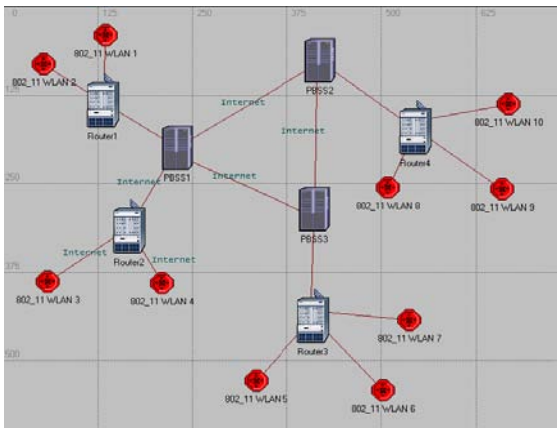

Figure 11: Distributed PBSS

policy information between each other to obtain frequent updates. This distributed architecure provides better robustness for the WLANs. For example, a roaming attacker can be discovered more readily though the cooperation of several PBSSs.

5 CONCLUSIONS

The importance of security in a wireless environment can never be underestimated. Because of the nature of wireless transmission and the security mechanisms in 802.11, DDoS attacks can always take place. Unfortunately, the RSN mechanism doesn't protect WLANs against the attacks demonstrated in this paper. Deficiencies in both the encryption algorithm and the security protocols have highlighted the vulnerability of WLANs to DDoS attacks. As a result, extra security countermeasures are necessary to protect the network's resources. Currently firewalls are the most popular approach for implementing security in networks. The main mechanism employed by them is packet filtering. However this approach has vulnerabilities as it only addresses attacks at one (the network) level. In this paper, a new approach to implementing countermeasures based on a Policy-Based Security Server (PBSS) is presented. The PBSS construction aims at defeating the attacks by considering the entire behaviour of the network system (PBSS, AP, Mobile clients). At the same time as the clients filter the defined packets, the PBSS periodically sends probes. It asks the APs about the current status of the network. If any abnormal phenomenon is found, the PBSS sends 'capsules' (packets encapsulated with programs or pointers) to the AP. The AP then changes the topology of the WLAN and cooperates both the AP and wireless users to defeat the attack. The main feature of the PBSS framework is that it is designed to organize the members in the network to defeat viruses rather than do it solely, so that a single infected machine won't affect the whole network's performance. A number of typical DDoS attack strategies are identified and these will be used to define the policy countermeasure employed. However the approach can also be applied to other types of attack. A number of typical DDoS attack strategies are identified and these will be used to define the policy countermeasure employed. However the approach can also be applied to other types of attack.

Future work will focus on the implementation of the policy-based security server. Our design of the security architecture aims at the reacting performance of the wireless LAN, we will use a network simulation package, OPNET to build up the model and test its performance over a range of DDoS attack strategies

REFERENCES

L.Sherriff, "Virus Launches DDOS for mobile phones", *http://www.theregister.co.uk/content/1/12394.html*

Jon Edney, William A. Arbaugh, "Real 802.11 Security----Wi-Fi Protected Access and 802.11i", Addison Wesley, July, 2003

The 802.11 Security Web Page *http://www.drizzle.com/~aboba/IEEE/*

Nikita Borisov, Ian Goldberg, David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

CERT Coordination Center, "Denial of Service Attacks", *http://www.cert.org/tech_tips/denial_of_service.html, 2001*

J.Mirkovic, J.Martin, P.Reiher, "A Taxonomy of DDOS Attacks and DDOS Defense Mechanisms", *ACM CCR, July, 2002*

CERT Coordination Center, "Trends in Denial Of Service Attack Technology" *http://www.cert.org/archive/pdf/DoS_trends.pdf, Oct, 2001*

IEEE 802.11 Tgi, Tim Moore, Bernard Aboba, "Authenticated fast handoff", *http://www.drizzle.com/~aboba/IEEE/11-01-TBD-I-Authenticated-FastHandoff.ppt*

Mishr, A., and W.A.Arbaugh. 2002. "An Initial Security Analysis of the IEEE 802.1X Standard." *Technical Report CS-TR-4328. College Park, University of Maryland.*

IEEE. "Standard for local and metropolitan area networks: Standard for port based network access control". *IEEE Draft P802.1X/D11, March 2001.*