International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012

GENERATING REPRESENTATIVE ATTACK TEST CASES FOR EVALUATING AND TESTING WIRELESS INTRUSION DETECTION SYSTEMS

Khalid Nasr, Anas Abou El Kalam, and Christian Fraboul

IRIT-ENSEEIHT, INPT, Université de Toulouse Toulouse, France
{khalid.nasr, anas.abouelkalam, christian.fraboul}@enseeiht.fr

ABSTRACT

Openness of wireless communication medium and flexibility in dealing with wireless communication protocols and their vulnerabilities create a problem of poor security. Due to deficiencies in the security mechanisms of the first line of defense such as firewall and encryption, there are growing interests in detecting wireless attacks through a second line of defense in the form of Wireless Intrusion Detection System (WIDS). WIDS monitors the radio spectrum and system activities and detects attacks leaked from the first line of defense. Selecting a reliable WIDS system depends significantly on its functionality and performance evaluation. Comprehensive and credible evaluation of WIDSs necessitates taking into account all possible attacks. While this is operationally impossible, it is necessary to select representative attack test cases that are extracted mainly from a comprehensive classification of wireless attacks. Dealing with this challenge, this paper proposes a holistic taxonomy of wireless security attacks from the perspective of the WIDS evaluator. This proposed taxonomy includes all relevant necessary and sufficient dimensions for wireless attacks classification and it helps in generating and extracting the representative attack test cases.

KEYWORDS

Attack Taxonomy, Attack Test Cases, Wireless Intrusion Detection System, Wireless Attacks

1. INTRODUCTION

Along with growing reliance on wireless networking technology in recent years, the challenges of wireless network security have been increasing. One of the pivotal elements in wireless network security is the wireless intrusion detection system (WIDS) that is considered as a second line of defense for detecting any leaked attacks form the first line of defense such as firewall and encryption. Characteristics of WIDSs do not deviate much more from the wired intrusion detection systems (IDSs); just the RF (radio frequency) sensors, wireless communication features and wireless attack features are taken into account for WIDSs. WIDS monitors the radio spectrum and system activities to identify malicious activities, and then alerts the complementary prevention part to combat the detected attacks.

There are two main detection techniques used by WIDSs; signature-based and anomaly- based techniques. Signature-based technique concerns with detecting any evidence of attacks, according to a predefined and established model for specific known attacks. This technique presents low false positives, but it couldn't be able to detect the novel attacks which may cause high false negatives. For the second technique, anomaly-based, it concerns with detecting the misuses and abnormal behaviour in the monitored system on the basis of observing any deviations from a predefined and established model of the normal and expected behaviour through the system, and thus it may cause high false positives and low false negatives. As a consequence of the defects of these two techniques, there was a trend to combine their

DOI : 10.5121/ijnsa.2012.4301

advantages to develop a third one called specification-based technique which tries to keep the WIDS with low false alarms.

Selecting a reliable WIDS system depends significantly on its functionality and performance. Despite the importance of WIDSs in wireless network security, their efficiency and performance are sometimes not satisfying in practice. Thus, WIDSs evaluation is a pressing necessity. By evaluation we mean a systematic assessment that measures the ability of a WIDS to meet the intended security and performance. It is worth mentioning that there is a great lack of WIDSs evaluation in wireless networks. Comprehensive and unbiased evaluation logically necessitates taking into account all possible attacks. While this is operationally impossible, it is necessary to develop an attack classification that groups the common attack characteristics under expressive categories. This facilitates generating and extracting the valid and representative attack test cases by combining the terminal classes of the classification.

In this paper, we study and classify holistically the wireless attacks from the perspective of the WIDS-evaluator, and then extract accordingly the possible and valid representative test cases of attacks. Our proposed taxonomy of wireless attacks takes into account all sufficient and necessary dimensions for holistic classification of wireless attacks. Taxonomy can be defined as a classification system that ensures a systematic arrangement into groups or categories according to established criteria [1].

The rest of this paper is organized as follows. To better understand our context, Section 2 presents the main objectives of the attack classification and the requirements for a satisfactory and holistic taxonomy. Section 3 discusses some previous works concerned with the attack classification. After that, Section 4 presents our proposed taxonomy and the methodology of classification. Afterward, Section 5 explains how to generate and extract the representative attack test cases. Finally, section 6 presents our conclusions and future work.

2. BACKGROUND

In the network security domain, we believe that the classification of security attacks can be oriented towards one of the following two purposes: *1) security defense* or *2) security-countermeasure evaluation.*

In the first direction, the attacks are classified from the perspective of the security defender. The considered taxonomy is created by extracting the attack signs or signatures from all possible attacks and assembling the common attack signs under representative dimensions. These taxonomy dimensions guide to techniques and mechanisms that can be followed by the security-defender to prevent the attacks. This taxonomy is called *defense-centric taxonomy*.

In the second direction, the attacks are classified from the perspective of the security-countermeasure evaluator. Dimensions of this taxonomy guide to the attack generation process and help in extracting the attack test cases. In this taxonomy, the evaluator generally describes the main phases of attack; preparation-phase, exploiting-phase and infecting-phase. This taxonomy is called *evaluation-centric taxonomy*.

Several attempts of attack classification were developed, but most of them concerned with wired networks [2, 3, 4]. Besides, some taxonomies focused on the security flaws [5], others focused on the exploited vulnerabilities, and others just listed the terms and types of attacks [6, 7, 8]. To our knowledge, there is no a holistic taxonomy of wireless attacks that can cover all necessary and sufficient dimensions for attack classification, especially from the perspective of the security-countermeasure evaluation. We thus concern in this paper with developing a WIDS evaluation-centric taxonomy of wireless attacks.

Before defining our classification attributes, it is important to first define some important requirements for a satisfactory and holistic taxonomy:

- *Objectivity* - Classification objective must be clearly determined and defined; defense-centric or evaluation-centric.
- *Completeness/Exhaustive* - Taxonomy should consider all possible attacks and develop the corresponding representative categories.
- *Methodical* - Classification should be built on a clearly specified methodology.
- *Mutually exclusive* - Each attack should only be classified into one category.
- *Repeatable* - Taxonomy should be repeatable and ensures always the same classification of an attack regardless of who is classifying.
- *Unambiguous* - Each category of the taxonomy should be clearly and precisely defined.

3. RELATED WORK

This section presents some of the previous works related to the attack classification. We study and categorize these taxonomies from the perspective of the defense-centric and evaluation-centric as mentioned in the previous section. It is worth mentioning that many of the proposed taxonomies, that have been originally developed to help the security defender, have followed the direction of the security-countermeasure evaluation.

3.1. Defense-Centric Taxonomy

Kumar in [9] proposed an attack taxonomy that seems as a defense-centric one. This classification was based on inspecting attack signatures, to help ultimately in designing and building a signature-based IDS. The author classified the attack signatures under the following dimensions: *Existence, Sequence, Regular Expression patterns,* and *other patt*erns that contain all other intrusion signatures that cannot be represented directly in one of the earlier categories. *Existence patterns* look for evidence that may have been left behind by an intruder. For *Sequence patterns*, some attacks manifest themselves as a sequence of events. *Regular expression patterns* include events that often specify several activities to be done jointly.

Killourhy et al. in [10] classified the attacks from the perspective of the anomaly-based IDS defender. This classification is based on observing the anomalies of attack manifestation: *Foreign Symbol, Minimal Foreign Sequence, Dormant Sequence,* and *Non-Anomalous Sequence*. In *foreign symbol*, the attack manifestation contains a system call which never appears in the normal record. For *minimal foreign sequence*, the attack manifestation contains a system call sequence which never appears in the normal record, but all subsequences appear in the normal record. In *dormant sequence*, a sequence of system calls in the attack manifestation matches a subsequence in the normal record, but does not match the full sequence. In *non-anomalous sequence*, the attack manifestation entirely matches the normal sequence without any anomaly.

3.2. Evaluation-Centric Taxonomy

In this section, we will study the attack taxonomies that followed one step or more towards the evaluation-centric taxonomy.

The most famous taxonomies in this direction concerned with two main dimensions: *passive* and *active* attacks [11, 12, 13]. These two broad classes or dimensions are then subdivided into terminal subclasses. Passive attacks are subdivided into; (1) *Traffic analysis* and (2) *Eavesdropping*. Active attacks are subdivided into; (1) *Masquerading*, (2) *Relay*, (3) *Message modification*, and (4) *Denial-of-service*. This is not much more useful, as a complete taxonomy, neither for security countermeasure evaluation nor for designing appropriate security

countermeasures. This taxonomy can be used as an assistant object in the preparation phase of the evaluation-centric taxonomy, but to be efficient it needs more details about attack features, attack tools and techniques, exploited vulnerabilities, and attack objectives.

The taxonomies presented by Wood and Stankovic in [14] and Howard in [15] followed close methodologies and provided nearly similar categorizations. Due to space limitations, we couldn't list all dimensions of these taxonomies. These taxonomies can be adapted to become a complete evaluation-centric taxonomy; by deleting some unuseful redundant dimensions and adapting others according to the evaluator's point of view.

Gad El Rab et al. in [4] proposed an attack taxonomy that seems helpful for the IDS evaluation process. This taxonomy has five dimensions; (1) *Firing* source: indicates the launching point of attack, (2) *Privilege escalation*: refers to the elevated access gained by an attacker to the system resources, (3) *vulnerability*: specifies the exploited network vulnerabilities, (4) *Carrier:* describes the auxiliary means by which the attack reaches the victim; either via network traffic or through a local action, (5) *Target*: refers to the attack objectives. Although this taxonomy is interesting, it does not cover all dimensions of attacks from the perspective of the IDS evaluation, especially for the wireless environment.

In the following section, we treat the shortcomings of the previous attempts of attack classification in direction of the evaluation-centric, and accordingly we develop a new taxonomy of wireless attacks.

4. THE PROPOSED TAXONOMY

In this section, we propose the necessary and sufficient dimensions for creating a holistic and satisfactory taxonomy of wireless attacks from the perspective of the WIDS-evaluator. Basically, these dimensions can be extracted from the conception of the attack generation process. The logical sequence of this process begins by determining what does the attacker want? i.e., attack objectives. Then, according to the *network mode* and *access privileges*, the *attack objectives* can be achieved via exploiting *network vulnerabilities* using certain *attack techniques and mechanisms*. This sequence interprets the methodology of our classification. In the following subsections, we will explain the importance of each dimension in our taxonomy which is summarized in Figure 1.

4.1. Network Modes

The first dimension in our taxonomy focuses on specifying the wireless network mode which is considered as a foundation of the attack test cases in wireless environments. It helps in determining the manifestation and launching point of attack. There are two main modes in wireless networks; wireless *infrastructure* mode and wireless *ad-hoc* mode. Many attacks objectives depend on the network mode; for example, in wireless infrastructure mode the wireless access point (AP) is the most attractive target for attacks.

It is worth mentioning that the deployment and configuration of the WIDS system depend on the wireless network mode. For example, in infrastructure wireless networks, WIDS systems are often deployed wherever the access points (APs) are located to protect them from any directed attack to them. But, in Ad-hoc networks each wireless node may be a target of attacks.

4.1.1. Infrastructure Mode

In wireless infrastructure mode, the wireless nodes associate themselves with a wireless access point (AP) to get the network services and/or communicate with each other. The AP is usually connected to a wired network and provides a communication link between the associated wireless nodes and the wired network services (usually Internet). As well as, AP functions as a

radio relay to forward information between the wireless nodes that are too distant to communicate directly with each other.

Based on the wireless infrastructure mode, we can differentiate between two main architectures; *standalone* and *distribution system* modes.

4.1.1.1. Standalone Mode

Standalone infrastructure network is mainly configured around a central access point (AP). The basic architecture of this mode is called infrastructure *basic service set* (*BSS*). However, a BSS covers a small limited area around the AP that serves neighbouring nodes in the range. It is worth noting that there is no restriction on the distance between the mobile nodes in the BSS coverage range.

4.1.1.2. Distribution System Mode

The coverage area of wireless infrastructure network can be extended by joining BSSs with a backbone network to form *extended service set* (*ESS*) that serves the distribution system mode. In the distribution system mode, multiple APs are interconnected with each other by wired or wireless backbone system. This enables the wireless nodes to roam between the APs, thus providing greater range and mobility. In this mode, if a mobile wireless node moves out the coverage range of an AP, but it keeps its existence in the ESS range, the node will re-associate with the next AP in the ESS range.

Basically, each AP announces its presence to the wireless nodes in the range by periodically broadcasting beacon frames that carry a service set identifier (SSID). SSID is used to identify WLAN by 1-32 characters unique ID as a network name. Basically, in infrastructure networks, SSID may consist of one or more Basic SSIDs (BSSIDs) which present the MAC addresses of the access points in the range. SSID helps in distinguishing between wireless LANs (WLANs) in the range. A wireless node scans SSIDs in the range, and selects the intended one to associate with. Sometimes an AP may resort to conceal the SSID by disabling the broadcasting of it, and consequently the wireless nodes would not be able to identify and associate with the AP and they instead need foreknowledge of the SSID. This mechanism is not considered as an effective security mechanism, where despite stopping the broadcast of SSID on the beacon frame, it may be sent out in other management frames.

It is worth mentioning that the AP can buffer frames unicast to a specific node, when it goes to the sleeping mode. When the node wakes up, it sends PS-Poll (Power Save Poll) request frame to the AP to retrieve the buffered frames. An attacker may spoof PS-Poll frame to get the buffered frames instead of the node.

4.1.2. Ad-hoc Network

Wireless Ad-hoc network is a self-organized network which is a collection of autonomous wireless nodes that can be deployed and communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. In Ad-hoc networks, the wireless nodes can interact as routers to forward packets without relying on any fixed infrastructure support such as access points, routers, or base stations.

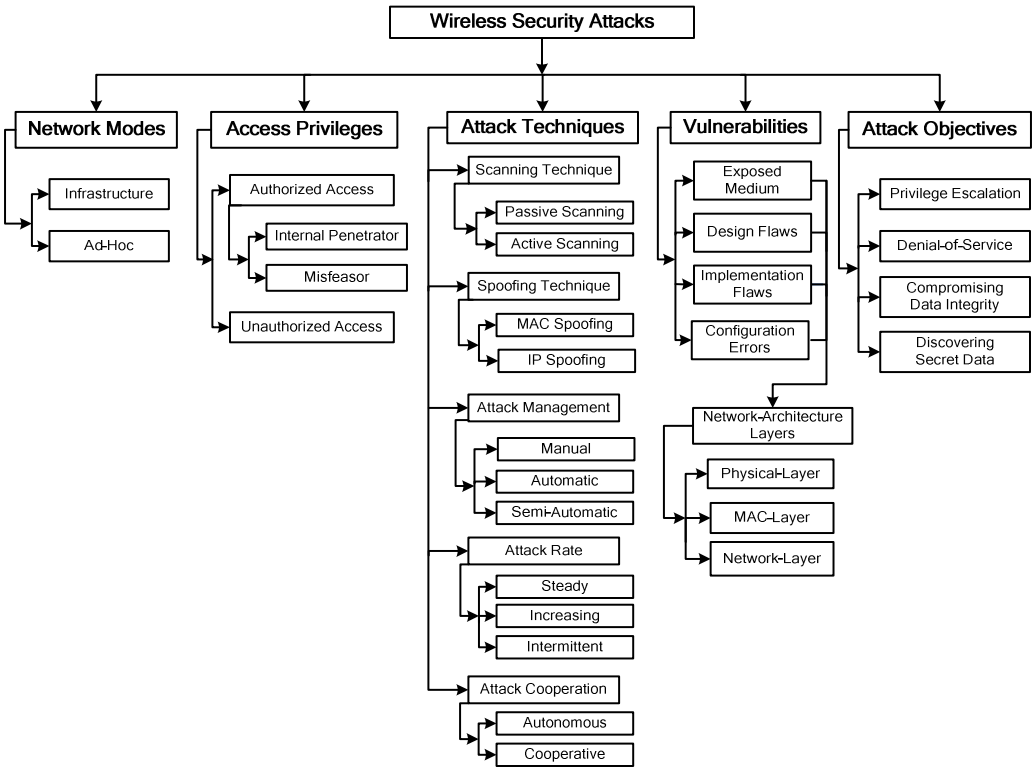

Figure 1. WIDS Evaluation-Centric taxonomy of wireless security attacks

Ad-hoc networks are also called *independent BSS* (*IBSS*), where the nodes communicate directly with each other through their direct communication range. Basically, ad-hoc networks generate a random BSSID with the Universal/Local bit set to 1 to prevent conflicts with officially assigned MAC addresses; it is called Independent BSSID (IBSSID).

Usually, mobile nodes in mobile ad-hoc network (MANET) work with limited power, and the efficient utilization of this power is important for increasing the lifetime of the individual nodes as well as the overall network. An attacker can exploit this vulnerability to exhaust the energy of the mobile nodes. For example, an adversary may consume the power of the sensor nodes in wireless sensor networks (WSNs) by sending several fake requests in order to cause denial of service (DoS) attacks.

4.2. Access Privileges

Access privilege restriction is one of the important security measures for organizing the access rights of the users, and limiting the data exposure and system resources utilization. Based on access privilege, we differentiate between *authorized* and *unauthorized access*.

4.2.1. Authorized Access

Authorized access privilege determines what level of access that a particular authorized user should have to the secured data and resources. Each of them, system user and administrator, has a determined access privilege to perform his assigned tasks. From the perspective of the authorized access violation, we can differentiate between the *internal penetrator* and *misfeasor*.

4.2.1.1. Internal Penetrator

Internal penetrator refers to a malicious user, who is authorized to access a certain determined area of the network services and resources using the network devices or his own devices, but he is not authorized to access another specific one; he may violate this restriction by performing a number of malicious activities to hack the restricted or prohibited area of the network.

4.2.1.2. Misfeasor

Misfeasor refers to a malicious administrator who misuses his authorized access privilege to the system resources and databases. However, system administrator has a superior level of authorized access to the system and its data. He is able to assign the users' access privileges, monitor and log the activity of users' sessions, and know where the highest value of information resides. He may discover the users' private information such as users' profile data, bank account details, and confidential data.

4.2.2. Unauthorized Access

Unauthorized access can be defined as an accidental or deliberate violation of the system security policy or bypassing the system security countermeasures to disclose, alter, or steal private accounts, messages, files, or confidential information without legal permission, superintendence, or authority. The intruder or adversary tries to penetrate the security system by exploiting the system vulnerabilities, using several compromising and hacking techniques, to achieve intended objectives.

4.3. Attack Techniques and Mechanisms

Attack techniques and mechanisms clarify the tactics that can be followed to prepare and execute the attack. Based on attack techniques and mechanisms, we differentiate between *scanning techniques, spoofing techniques, attack management, attack rate organizing,* and *attack cooperation*.

4.3.1. Scanning Techniques

The premier intuitive procedure in the preparation phase of wireless attacks is the scanning process. It helps to locate the vulnerable services, wireless stations, access points, in addition to discovering the secret data, passwords, and so on. Based on scanning techniques, we differentiate between *passive* and *active scanning*.

4.3.1.1. Passive Scanning

In wireless networks, an attacker can use the radio channels in RF (radio frequency) monitor mode to listen in the network traffic broadcasts over the wireless medium. The most intended attack objective for passive scanning technique is sniffing the service set identifier (SSID) which leads to discovering the MAC addresses of APs. As we mentioned, each AP announces its presence by broadcasting beacon frames that carry SSID. The attacker exploits this broadcasting process to sniff the beacons and SSIDs. At a certain level of network security, the network administrator may disable the SSID broadcast. In this case, an attacker can wait and sniff for any associate request from a legitimate station that already carry the network SSID. Then, the attacker can take steps to scan passively and collect the MAC addresses. KisMAC [16] AirFart [17] are examples of passive scanning tools.

4.3.1.2. Active Scanning

When the attacker is unable to collect the intended information using passive scanning technique, or if he does not wish to wait patiently for voluntary associate requests from

legitimate stations that carry network(s) SSID(s), he resorts to use active scanning technique. In active scanning, an attacker sends out probe requests or artificially constructed packets that contain a spoofed source MAC address to trigger useful responses from the target [18]. The probe response frames from APs contain the SSIDs and other information similar to that in the beacon frames. The attacker sniffs these probe responses and extracts SSIDs, and consequently collects the MAC addresses.

4.3.2. Spoofing Techniques

Using spoofing techniques, the attacker can forge his identity to masquerade as another one, or even creates multiple illegitimate identities. The attacker may resort to use this technique to evade detection by security defense systems, impersonate another network device, bypass access control mechanisms, gain unauthorized access, or falsely advertise services to wireless clients. In our context, we will focus on MAC address and IP address spoofing.

4.3.2.1. MAC Address Spoofing

MAC address is a layer 2 unique identifier that is burned into network devices or network interface cards (NICs) during manufacturing. However, MAC address is 6-bytes long, the first 3-bytes are assigned by IEEE and indicate which manufacturer fabricated the NIC, and the last 3-bytes are assigned by the manufacturer to differentiate between the NICs. MAC spoofing refers to altering the manufacturer-assigned part. By using MAC address spoofing, the attacker may be able to bypass the access control mechanisms or advertise fake services to achieve intended objectives.

In wireless networks, typical Aps usually predefine access permission for a set of machines or nodes with MAC addresses registered in an assigned address-set. The attacker may spoof a legitimate MAC address of a node that already exists in the MAC address-set to have an ability to associate with the AP. Also, the attacker can create a fake AP with spoofed MAC address to deceive wireless nodes in the range to associate with it, and thus he may be able to capture secret information of the associated nodes or overwhelm the neighbouring nodes by beacon flood attack.

In certain attacks such as DoS attacks, the attacker needs a heavy number of MAC addresses than he could collect by sniffing. This stimulates the attacker to generate random MAC addresses. However, the attacker generates a random MAC address by selecting an IEEE-assigned part appended with additional 3-bytes manufacturer-assigned [18]. SMAC [19] and MAC MakeUP [20] are examples of MAC spoofing tools that alter the software based MAC addresses; not the hardware burned-in MAC addresses.

4.3.2.2. IP Address Spoofing

IP address is a layer 3 unique identifier for the host connection and packet routing in the network. Every IP address consists of 32-bits that are divided into two parts, one part identifies the network and another identifies the host, according to the address class and the subnet mask. IP addresses are usually assigned as static or dynamic addresses. Static IP address is a fixed permanent address that is assigned to a network host by an administrator or Internet service provider (ISP). Dynamic IP address is a temporary address assigned to a network host each time it accesses the network. The main difference between MAC address and IP address is that although the MAC address is a unique identifier for the network devices, it doesn't know how to route the packets through the network; which is the main function of IP address. In other words, direct connected transmission uses MAC addresses for frame delivery, and routed transmission uses IP addresses for packet delivery.

IP spoofing refers to the creation of IP packets with a forged source IP address. By IP address spoofing, an attacker may intercept a link between two communicated nodes and pretends alternately as an end-point to each one of them. The attacker thus can control the traffic, alter or eliminate information exchanged between the two points, i.e. this type of attack is called man-in-the-middle (MITM) attack. By the same way, the attacker can disclose confidential information by deceiving the victim.

Another type of attacks that depend significantly on IP spoofing is the denial of service (DoS) attacks that aim to consume network resources and bandwidth. However, there are many scenarios for DoS attacks. One of these scenarios is flooding the victim by a heavy traffic with spoofed IP address to conceal the attack origin. Another scenario is sending request to a set of network nodes with a spoofed IP address of a targeted victim to redirect the reply to the victim to exhaust its resources.

The little difference between MAC address spoofing and IP address spoofing is that, by IP spoofing the sender spoofs its address as a request whereas in MAC spoofing the response is received by the spoofing party. RafaleX [21] and SendIP [22] are examples of IP spoofing tools.

4.3.3. Attack Management

This dimension refers to the management of the attack phases. However, depending on the system immunity, exploited vulnerabilities, and attack objectives, one or more of the attack phases; preparation, exploiting, and infecting phases can be managed either manually, automatically, or semi-automatically [23].

4.3.3.1. Manual

It refers to executing all phases of the attack process manually. Only some of the early attacks were managed manually from the preparation phase until the infecting phase. The attacker scans the system vulnerabilities manually and exploits them to reach the intended objectives also manually. This technique is rarely used in the present, especially by the skilful attackers, where a lot of time is spent and much more effort is exerted with little results of infected victims or obtained information.

4.3.3.2. Automatic

On the contrary with the manual attack technique, using automatic attack technique all phases of attack are performed automatically. All attack features such as attack type, duration, and victim addresses are pre-programmed in the fired attack code.

However, some attackers compromise and recruit agent machines to launch certain attacks. A chance of the attack origin concealment is increased using this tactic, where the communication link between the attacker and the recruited agents is not continuous; just at the firing time of the attack code. Thus, if the victim detects the attack, it may not be able to discover the attack origin.

4.3.3.3. Semi-Automatic

Semi-automatic attack technique merges between both manual and automatic techniques. For example, in some attacks such as the distributed DoS (DDoS) attack, the attacker may perform preparation and exploiting phases automatically and infecting phase manually by specifying the attack type, onset, and rate. Some attackers prefer to use this technique to have more control of the victim. During the attack, the attacker may be able to manage all the attack features according to the state of the victim and the intended attack objectives.

4.3.4. Attack Rate Organizing

One of the pivotal techniques that are used to reinforce the attack impact is the attack rate organizing. Basically, attack rate can be organized according to analysis of the real-time state of the targeted system and the intended attack objectives. The attack can be managed at steady, increasing, or intermittent rate.

4.3.4.1. Steady Rate

Using several tools, the attacker may be able to generate a steady number of attack packets during the attack interval. DoS attack, which is the most dangerous attack in network security, can use this tactic to overwhelm and flood the victim resources by a heavy steady rate of traffic to exhaust the victim resources. The main challenge in combating DoS attack is the difficulty in distinguishing the malicious traffic from the legitimate traffic. DoS attack is more severe when the attacker recruits agent machines to overwhelm simultaneously the victim resources; this is a form of the distributed DoS (DDoS) attack.

4.3.4.2. Increasing Rate

Typical successful attack resorts to many tactics to evade the attack detection. One of these tactics is the generation of attack at a gradually increasing rate. This can lead to a slow exhaustion of the victim resources, as aimed by some flooding attacks, and thus delays the early detection of the attack.

4.3.4.3 Intermittent Rate

Another successful tactic with low probability of attack revealing is generating the attack at an intermittent rate. With the intermittent rate tactic, the attacker generates an attack during a certain interval (*on-state*), and holds it during another alternate interval (*off-state*). At the end of *off-state*, the attacker resumes the attack again and so on. The attacker adjusts the *on* and *off* intervals according to the real-time state of the victim. As well as, during *on-state*, the attacker may use steady constant rate or gradually increasing rate.

4.3.5. Attack Cooperation

This dimension determines the cooperation degree between the attack entities. Based on the attack cooperation, there are two main strategies to prepare and perform the attack; autonomous or cooperative attack.

4.3.5.1. Autonomous Attack

Autonomous attacker can prepare and launch an attack independently without any contribution or help from any other entity. In this category, the attacker is responsible for discovering the system vulnerabilities, determining the targets, planning the attack, selecting the appropriate tools and techniques, launching and managing the attack autonomously. However, autonomous attack is commonly used and easy to be managed, where the attacker doesn't need any arrangement or organizing with any other entity for intervention or help for the attack management.

4.3.5.2. Cooperative Attack

Cooperative attack concerns with the collaboration between the attack entities to perform intended objectives. However, cooperative attack can be performed by one of two strategies. The first strategy is a contribution between autonomous attackers to reach and achieve a common goal. In the second strategy, an attacker can compromise and recruit multiple agents

(centrally controlled) to be cooperated to launch an intended attack against a certain victim. DDoS attack is a clear example for this category of attacks.

4.4. Vulnerabilities

Vulnerability is a weakness or fault in system security procedures, design, implementation, or communication medium that could be accidentally triggered or intentionally exploited, and results in a security breach [24]. Basically, we can identify two main categories of wireless network vulnerabilities; physical vulnerabilities and logical vulnerabilities. Physical vulnerabilities which are exploited by tampering and vandalism attacks are outside the WIDS evaluation interest. Therefore, we will focus only on the logical vulnerabilities, which are found in the network services, protocols and applications, and can be exploited by logical attacks.

In this section, we classify the logical vulnerabilities into four main categories; *design flaws, implementation flaws, configuration errors,* and *exposed medium*. After that, we introduce and explain in details the most exploited vulnerabilities according to the network-architecture layers.

4.4.1. Exposed Medium

Due to the openness of the exposed wireless medium, the attacker can easily eavesdrop on the wireless connection, intercept the messages exchanged between wireless nodes, and access the wireless network with poor authentication. However, most of wireless networks are not configured securely and often only MAC address spoofing is required to gain full access. Radio-jamming and man-in-the-middle (MITM) attacks are examples of attacks that exploit the openness vulnerability of wireless medium. Radio-jamming attack overwhelms wireless communication or corrupting received signals using radio interference by transmitting radio signals to the intended victim at the same frequency band or sub-band as the transmitter uses. In MIMT attack, an adversary eavesdrops the communication between the communicated points on the network and intercepts the data transferred between them to discover secret information and/or inject false information.

4.4.2. Design Flaws

Design flaws refer to the protocol breaches that can be exploited to violate assumption of the normal behaviour in the network, while conforming the protocol specification design. For example, there are significant design flaws associated with the wired equivalent privacy (WEP) protocol such as keystream reuse and initialization vector (IV) reuse problems. Basically, WEP encrypts the data to be sent by XORing the plaintext with a generated keystream to produce the ciphertext to be transmitted to the destination. The plaintext will be recovered at the destination by decrypting the ciphertext by XORing it with the same keystream that is used at the sending point. If two ciphertexts use the same keystream, the attacker can easily sniff that and by XORing the two ciphertexts he can extract the two plaintexts XORed. If the attacker knows one of the two plaintexts, then he is able to reveal the other one; this is called the keystream reuse problem.

To avoid this problem, WEP uses initialization vector (IV) that is associated with the keystream by RC4 algorithm, and it helps in generating different keystreams for each transmitted packet. Initialization vector (IV) is 24 bit long, and then it gives only 2^{24} different available IVs. These IV set space is too small, it may be consumed in short time, and this may lead to reuse the same IV for multiple messages, and thus exposes the system to keystream reuse attacks [25].

4.4.3. Implementation Flaws

Implementation flaws refer to errors in hardware construction or software coding due to the unfamiliarity with the programming language or the ignorance of security issues. For example,

inadequate boundary checking which may result in a buffer overflowing with attacker-controlled contents [26]. Some implementation flaws are translation of some design flaws that can be avoided by taking the security issues into account. For example and as a complement to the IV reuse design problem that has been mentioned in the previous section, some wireless network cards reset the IV to zero each time they are re-initialized and regularly increase the IV by one for each packet transmitted [25]. Frequent re-initialization of these wireless network cards confirms design flaws of IV reuse and keystream reuse.

4.4.4. Configuration Errors

Configuration errors are the result of improper settings of a particular environment, threat model, or programs/utilities that are installed in a wrong place, or incorrect installation of program/utilities parameters [10].

In the following, we will examine deeply the wireless vulnerabilities according to the wireless network-architecture layers. This can help the WIDS evaluator to have a closer view for the wireless network vulnerabilities and the related threats and attacks.

A. Physical-Layer

The main vulnerability at physical layer is the openness of wireless communication medium. The attacker can exploit this vulnerability to execute radio frequency-interference attacks, such as radio-jamming attack which is considered as a severe form of denial of service (DoS) attack against the physical layer.

Another vulnerability at this layer is mainly related to the access-control mechanisms. In wireless networks, there are two access-control mechanisms which are designed to avoid transmit collision and provide fairly share for the transmission medium. These mechanisms are physical carrier-sense at physical layer and virtual carrier-sense at MAC layer. Our concern here is with the physical-carrier sense, and we will explain the other mechanism at the MAC layer. Unfortunately, the attacker can exploit the advantages of the physical carrier-sense mechanism to launch an attack, where he/she sends many short packets in rapid succession, causing all nodes within the range believe that the medium is already in use. The victim nodes then listen patiently to their fair turn to communicate, but as long as the attacker is sending packets, this turn never comes and the victim nodes are hindered to transmit.

B. MAC-Layer

The 802.11 MAC layer is designed to address specific problems related to the wireless networks. Its function includes the ability to discover, join and leave networks and coordinate access to the radio medium [27]. The vulnerabilities at this layer can be categorized into *identity* and *media-access*.

1) Identity vulnerabilities

The Identity vulnerabilities are related to the identification of the wireless nodes, and include deauthentication, disassociation, and power saving vulnerabilities. Basically, when a wireless node wishes to join an IEEE 802.11 network, it must first go through an authentication and association process before allowing it to access the network [28].

a) Deauthentication

In order to control the access to the wireless network, wireless nodes or stations must first be authenticated. A part of the authentication framework is the deauthentication message which allows a wireless node and access point to explicitly request deauthentication from each other. Unfortunately, this message itself is not authenticated using any keying material [27].

Therefore, the attacker can spoof this message, pretending to be either the access point or the wireless node, and directs it to the other part which will exit the authenticated state and refuse all further packets until authentication is re-established. This attack usually is called the deauthentication attack.

b) Disassociation

Once a wireless node or station has been authenticated, it may then associate itself. The association message uses data from the MAC layer header and follows the authentication message between the wireless node and access point. Where the association protocol is also unauthenticated, it suffers a vulnerability like that is found with the deauthentication message, where the disassociation message is a part of the association frames. This vulnerability gives an attacker the ability to spoof a disassociation message and terminate the association session. The disassociation attack is slightly less efficient than the deauthentication attack, where the victim node can return to the association state by a small effort than which it can be done with the deauthentication attack.

c) Power Saving

The IEEE 802.11 standard provides a power save mode to conserve the wireless node energy. Actually, before entering the power save mode, the wireless node informs the access point (AP) that it will go to the sleeping state. At this state, the AP starts to buffer data destined to this wireless node. When the wireless node wakes up, it checks the Traffic Indication Maps (TIM), and sends poll message to demand the buffered data (referenced by its MAC address). When the AP receives the poll message, it delivers the buffered data to that wireless node and subsequently discards the contents of its buffer [29]. The Identity vulnerability here is the ability of attacker to spoof a poll message on behalf of the wireless node while it is in sleep state, and hinders it from receiving the buffered data which is discarded from the access point.

2) Media Access Vulnerabilities

At MAC layer, the attacker exploits the vulnerability of virtual carrier-sense mechanism. Virtual carrier sensing is provided by the Network Allocation Vector (NAV), which is the timer that indicates the amount of time the medium will be reserved [30]. Wireless stations or nodes set the NAV to the expected time for using the medium. When NAV is nonzero, the virtual carrier-sense indicates that the medium is busy and all stations or nodes set their NAV and wait to observe an idle media when the NAV becomes 0. The attacker can exploit this feature to send relatively few packets with forged duration field within the packet to reserve a very long transmission period. All other nodes will set their NAV to this adjusted period value which keeps them silent and they have to wait until NAV becomes zero. During this period, the fooled nodes don't even use their physical carrier sense mechanism to check if the medium is really busy [28].

C. Network-Layer

Most common vulnerabilities at the network-layer are related to the routing-protocols. Routing protocols allow routers to advertise dynamically and learn routes, and determine which routes are available and which are the most efficient ones to the destination. In this subsection we present the most famous vulnerabilities and threats against routing protocols and algorithms.

1) Spoofing, Altering, or Replaying Routing Information

The routing information exchanged between wireless nodes is an attractive target for attacks at network layer. The attacker may spoof, alter, or replay routing information in an attempt to

create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, and/or increase end-to-end latency [31, 32].

One of the most common attacks that exploit routing protocol vulnerabilities is the sinkhole attack. In wireless senor networks (WSNs) multiple distributed sensor nodes monitor their surrounding conditions, collect sensing data, and send it to the base station called sink. An attacker can deceive and attract these sensor nodes with unfaithful routing information, and then alters the data passing through his/her node or performs selective forwarding; this called a sinkhole attack. The sinkhole attack prevents the base station from receiving a correct integrated data.

2) Black hole

Black hole attack [33, 34] is a severe attack in mobile ad hoc networks (MANETs). In black hole attack, a malicious node exploits vulnerability of the route discovery of the routing protocol to claim falsely itself as having the shortest route to the destination node. During the route discovery process, the source node broadcasts route request (RREQ) packets to find a fresh route to the intended destination node. An attacker is able to listen in the request packets for the route, and then he/she creates a route reply (RREP) consisting of a forged short route. If the malicious node reply reaches the source node before the reply from the benign nodes, then the source node has been deceived and a fake route has been created via the malicious node (black hole node). The main objectives of black hole attacks are either denying the service by dropping the packets from the source node instead of relaying them to the destination node, or exploiting its place on the route between the source and destination nodes to take the first step towards MITM attack.

3) Wormhole

A wormhole attack [35, 36] is a low-latency link (tunnel) between two far away nodes in the network. This link can be exploited by the attacker to apply other kinds of attacks. In a wormhole attack, an attacker captures and records packets at one point in the network and tunnels them to another point (at a distant location), and then replays them there into the network from that point. The wormhole tunnel can be established via a wired or wireless link. Most of the ad-hoc routing protocols are vulnerable to the wormhole attack which is one of the most dangerous threats.

4.5. Attack Objectives

Attack objectives are the ultimate goals of the attack. They can be classified into four main categories; privilege escalation, denial of service, compromising data integrity and discovering the secret data.

4.5.1. Privilege Escalation

Privilege escalation is the act of exploiting system vulnerabilities to gain elevated access to the system resources that are normally protected against any unauthorized use. However, a malicious unauthorized user can climb or escalate the access privilege of an authorized user (i.e., remote-to-local (R2L) privilege escalation), or a trusted user may escalate to the administrator level (i.e., user-to root (U2R) privilege escalation). Usually, this task is considered as a penultimate goal that is used to reach another ultimate goal.

4.5.2. Denial-of-Service

Denial-of-service goal can be achieved by hindering a targeted system from serving the legitimate users. DoS attacks intend to disrupt the normal operation of the system by exhausting its resources (CPU time, memory, band-width, battery power, etc.) or creating fake requests to deauthenticate and disconnect the legitimate nodes form the network. Despite the exerted effort to combat DoS attacks or mitigate their impact, the communication systems still suffer from threats of DoS attacks. The main challenge associated with DOS attack is the difficulty of differentiation between legitimate traffic and malicious traffic (i.e. where the DoS malicious traffic seems usually compliant with the specification of the legitimate traffic).

4.5.3. Compromising Data Integrity

Data integrity refers to the accuracy, consistency, and completeness of data during operations of transfer, storage and retrieval; data is never altered and reaches the destination intact. Usually, data integrity is imposed on the database at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines. Data integrity can be compromised by altering the data stream. However, the attacker may intend to modify the contents of the system data or inject complete created packets into the data stream, or replace relevant information with nonsensical or offensive content. Airpwn [37] and File2air [38] are examples of attacks tools against data integrity. Airpwn is a wireless packet injection tool. It listens in the transmitted packets, and if the data matches a pattern specified in the config files, Airpwn spoofs the response from the AP with custom content and injects it to the client; this is similar, but not identical to a classic MITM attack. File2air tool is a command-line utility for injecting 802.11 frames from binary files into the wireless channel using airjack drivers. It allows the attacker to specify the binary file that will be used for the injected frames.

4.5.4. Discovering Secret Data

Due to the exposed wireless medium and other network vulnerabilities, an attacker can sniff and probe the wireless beacon frames or access illegitimately the system database to look for and discover the secret data. Attacks that concern with discovering the secret data are called confidentiality attacks. They attempt to discover private and secret data by eavesdropping and intercepting it over the wireless link, escalating to gain access to the confidential data under a fake identity, or deceiving the wireless nodes in the range to associate with a fake AP. Eavesdropping, encryption key cracking, rouge-AP phishing, and MITM attacks are examples of confidentiality attacks. For example, the attacker may intend to discover the WEP shared secret key. One of the available tools for WEP cracking is AirSnort [39] that passively monitors and captures the transmitted packets. Once enough packets have been gathered, AirSnort can compute and extract the WEP key. As well as, one of the available eavesdropping tools is WireShark [40] which is a packet analyzer used to passively capture 802.11 packets being transmitted over the wireless link.

5. ATTACK TEST CASES GENERATION

On the basis of our proposed taxonomy of wireless attacks, we can generate all possible attack test cases and extract the valid and representative ones. The appropriate and best compatible tool for our classification is Classification-Tree Editor (CTE) tool [41].

Classification-Tree Editor (CTE) is a graphical editor tool that is based on the Classification-Tree Method (CTM) which supports test cases design using descriptive tree-like notation. Using CTE, test cases are designed in regard to systemic classification of the test objects into a finite number of mutually exclusive terminal classes. CTE gives a compact and clear presentation of the overall test objects.

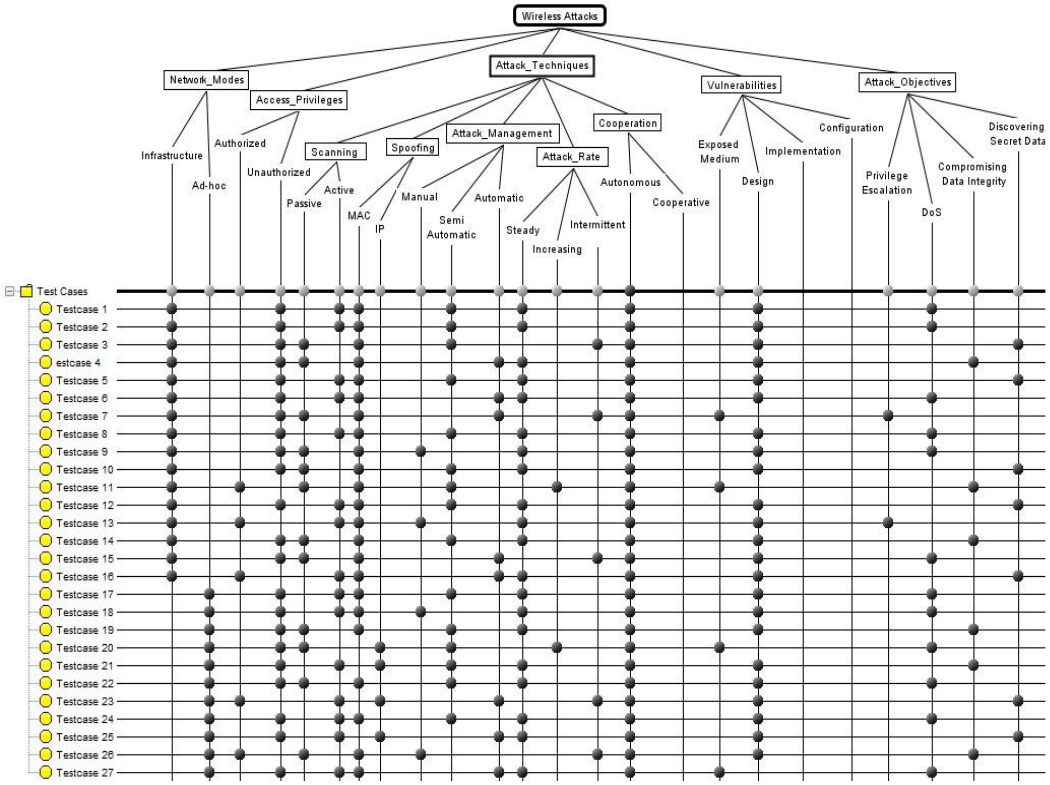

Figure 2. Some Representative Test Cases of Attacks in Wireless Networks

Regarding our concern, attack test cases can be generated using CTE through two main steps. The first step is specifying the test-relevant aspects and classes (i.e. each aspect includes disjoint terminal classes), and organizing them in a tree-like classification according to our classification of wireless attacks. The second step is generating the attack test cases, on the basis of the designed classification tree, by combining terminal classes under different aspects.

The scope of the test and the combination of terminal classes can be managed by using logical rational rules which are written and supported by CTE tool. However the generated test cases may contain some invalid test cases, thus the expert tester or evaluator can revise and extract the valid representative ones which are the input situations to be tested. The main advantages of using CTE are that the evaluator can easily modify the test specification when necessary, and can control the complexity and number of test cases according to the scope of the test.

As an example, figure 2 presents some representative attack test cases in wireless networks. These test cases extracted from all possible test cases that were generated according to the following CTE rule [Network_Modes * Access_Privileges * Attack_Techniques * (Design + Exposed_Medium) * Attack_Objectives)]; where "*"represents the AND logic operator, and "+" means OR.

6. CONCLUSIONS AND FUTURE WORK

This paper developed a holistic taxonomy of wireless attacks from the perspective of the WIDS evaluator. This proposed taxonomy helps in generating all possible attack test cases and extracting the valid representative ones. Our proposed taxonomy respects the requirements of

the satisfactory taxonomy, taking into account all the sufficient and necessary dimensions for wireless attacks classification. We have followed our taxonomy to generate and extract some representative attack test cases in wireless networks. As a result, this taxonomy gives a guide-line to WIDS-developers, network administrators and security analysts to be able to evaluate the WIDSs, and manipulate any drawbacks for the new design. In the future work, we will use our taxonomy and the generated test cases in a real experimental test to evaluate the security and performance of WIDSs in different network modes, and according to quantitative measurement metrics.

REFERENCES

[1] Merriam-Webster Editorial Staff, (2003) "Merriam-Webster's Collegiate Dictionary", Merriam-Webster Inc, 11th Edition.

[2] D. L. Lough, (2001) "A Taxonomy of Computer Attacks with Applications to Wireless Networks", PhD Thesis, Faculty of the Virginia Polytechnic Institute and State University.

[3] S. Hansman & R. Hunt, (2005) "A Taxonomy of Network and Computer Attacks", In Computers and Security, Elsevier, U.K., Vol. 24, No. 1, pp. 31-43, 2005.

[4] M. Gad-El-Rab, A. Abou El Kalam, & Y. Deswarte, (2007) "Defining Categories to Select Representative Attack Test-Cases", In Proceedings of ACM Workshop on Quality of Protection, Alexandria VA, USA.

[5] C. E. Landwehr, A. R. Bull, J.P. McDermott, & W.S. Choi, (1994) "A Taxonomy of Computer Program Security Flaws", ACM Computing Surveys, Vol. 26, No. 3, pp. 211-254.

[6] F. Cohen, (1997) "Information System Attacks: A Preliminary Classification Scheme", Computers & Security, Vol. 16, pp. 29–46.

[7] F. Cohen, (1995) "Protection and Security on the Information Superhighway", John Wiley & Sons.

[8] D. Icove, K. Seger, & W. VonStorch, (1995) "Computer Crime: A Crimefighter's Handbook", 1st Edition, O'Reilly & Associates, Sebastopol, CA.

[9] S. Kumar, (1995) "Classification and Detection of Computer Intrusions", Ph.D. thesis, Purdue University.

[10] K. S. Killourhy, R. A. Maxion, & K. M. Tan, (2004) "A Defense-Centric Taxonomy Based on Attack Manifestations", In Proceedings of International Conference on Dependable Systems and Networks (DSN'04), pp. 102-111, Florence, Italy.

[11] J. B. Robert, (2004) "Wireless Threats and Attacks", Handbook of Information Security, Vol. 1, pp.165-175.

[12] T. Karygiannis & L. Owens, (2002) "Wireless Network Security:802.11, Bluetooth and Handheld Devices", NIST Special Publication 800-48.

[13] W. Stallings, (2003) "Cryptography and Network Security Principles and Practices", Prentice Hall Inc., 3rd Edition.

[14] A. D. Wood & J. A. Stankovic, (2004) "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Handbook of Sensor Networks, Compact Wireless and Wired Sensing Systems, CRC Press.

[15] D. J. Howard, (1997), "An Analysis of Security Incidents on The Internet 1989-1995", PhD thesis, Department of Engineering and Public Policy, Carnegie Mellon University.

[16] KisMAC. http://trac.kismac-ng.org/

[17] AirFart. http://airfart.sourceforge.net/

[18] H. Bidgoli, (2005) “Hacking Techniques in Wireless Networks”, Handbook of Information Security, 1st ed., John Wiley & Sons.

[19] SMAC. http://www.klcconsulting.net/smac/#Description

[20] MAC MakeUp. http://www.gorlani.com/portal/projects/mac-makeup-the-original

[21] M. D. Spivey, (2006), “Practical Hacking Techniques and Countermeasures”, Auerbach Publications, Taylor & Francis Inc, New York.

[22] SendIP. http://snad.ncsl.nist.gov/ipv6/sendip.html

[23] J. Mirkovic, (2003) “D-WARD: Source-End Defense against Distributed Denial-of Service Attacks”, Ph.D. Thesis, Computer Science Department, University of California.

[24] G. Stoneburner, A. Goguen, & A. Feringa, (2001) “Risk Management Guide for Information Technology Systems”, NIST Special Publication 800-30, Washington, DC.

[25] N. Borisov, I. Goldberg, & D. Wagner (2001) "Intercepting Mobile Communications: The Insecurity of 802.11", In Proceedings of the 7th ACM Annual International Conference on Mobile Computing And Networking (MOBICOM'01), Rome, Italy.

[26] Y. Hsu, G. Shu, & D. Lee, (2008) “A Model-based Approach to Security Flaw Detection of Network Protocol Implementations”, In Proceedings of IEEE International Conference on Network Protocols (ICNP’08), pp. 114-123.

[27] J. Bellardo & S. Savage, (2003) “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, In Proceedings of the USENIX Security Symposium, Washington D.C.

[28] D. Boom, (2004) “Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks”, Master Thesis, Naval Postgraduate School, Monterey, California.

[29] F. Guo & T. Chiueh, (2005) “Sequence Number-Based MAC Address Spoof Detection”, In Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection (RAID), pp. 309-329.

[30] M. Gast, (2002) “802.11Wireless Networks: The Definitive Guide”, O'Reilly & Associates, Sebastopol, CA.

[31] C. Karlof & D. Wagner, (2003) “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures” Elsevier AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, pp. 293-315.

[32] P. Radmand, A. Talevski, S. Petersen, & S. Carlsen, (2010) “Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries”, In Proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia.

[33] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, (2007), "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No. 3, pp. 338–346.

[34] E. A. Mary Anita, V. Vasudevan, (2010), “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining”, International Journal of Computer Applications, Vol.1, No. 12, pp. 21-2.

[35] Y.-C. Hu, A. Perrig, & D. Johnson, (2006) “Wormhole Attacks in Wireless Networks”, In IEEE Journal on Selected Areas in Communications, Vol. 23, No. 2. pp. 370-380.

[36] M. Khabbazian, H. Mercier, & V. Bhargava, (2009) “Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks”, In IEEE Transactions on Wireless Communications, Vol. 8, No. 2, pp. 736 - 745.

[37] Airpwn. http://airpwn.sourceforge.net/Airpwn.html

[38] File2air. http://www.wve.org/entries/show/WVE-2005-0059

[39] AirSnort. http://airsnort.shmoo.com/

[40] WireShark. http://www.wireshark.org/

[41] CTE. http://systematic-testing.com/functional_testing/cte_main.php?cte=1

Authors

Khalid Nasr received BSc. degree in electrical engineering, communications and electronics (2001), and MSc. degree in electrical engineering, telecommunication network security (2008), from Faculty of Engineering, Minia University, Egypt. He is a PhD student at IRIT, ENSEEIHT-INPT, IRT Group, Touulouse, France. His research interest concerns with network security, security protocols, firewalls, and wired/wireless intrusion detection systems (IDSs).

Anas Abou El Kalam is an assistant professor of network security at the "Institut National Polytechnique", Toulouse, France. He is in charge of teaching and research activities on security at the Department of Networks & Telecommunications. He had several responsibilities as the head of the Computer Science Department at ENSIB. He is / was member of the program committees of several conferences such as IEEE ACSAC (Annual Security Application Conference), IFIP SEC (International Information Security Conference), ESORICS (European Symposium on Research in Computer Security), IEEE CRiSIS (International Conference on Risks and Security of Internet and Systems), etc. His current research interests concern security & QoS of embedded systems, network security, wireless security, security policies and models, intrusion detection systems.

Christian Fraboul received the Engineer Degree from INPT-ENSEEIHT in 1974. From 1974 until 1998 he worked as a research engineer at ONERA. Since 1998 he is full time Professor at INPT where he is in charge of Telecommunications and Networks department of ENSEEIHT and of IRT team of IRIT laboratory. His main fields of interest are embedded networks architectures and performance evaluation of such architectures (mainly in avionics context).