TOWARD A FORMAL FRAMEWORK TO EVALUATE WIRELESS SENSOR NETWORK SECURITY

Anas Abou El Kalam[1], *Andrea Atzeni*[2], *Alberto Cappadonia*[3], *Emanuele Cesena*[2], *Simone Fischer-Hübner*[4], *Stefan Lindskog*[4], *Leonardo A. Martucci*[4], *and Claudio Pastrone*[3]

[1] Université de Toulouse, IRIT / INPT, Toulouse, France
[2] Politecnico di Torino, Dip. di Automatica e Informatica, Torino, Italy
[3] Istituto Superiore Mario Boella, Torino, Italy
[4] Karlstad University, Dept. of Computer Science, Karlstad, Sweden

ABSTRACT

Wireless Sensor Networks (WSNs) are becoming widespread and pervasive, even in context where dependability and security of the deployed network could be crucial to critical and life-saving tasks. Due to the evolution rush experienced in past few years, several security aspects need to be further investigated. In this paper, we present a survey of the main vulnerabilities of WSNs and propose a specific taxonomy. This is a first step towards the definition of a formal security evaluation framework for WSNs, as we introduce in the end of this paper.

1. INTRODUCTION

WSNs are rapidly evolving and fast growing type of wireless networks. Many different applications have been proposed so far, and many more are expected for the near future. However, several technical aspects have to be resolved before the foreseen diffusion becomes a reality. Security and dependability issues are two of the main points to address.

Wireless networks share most security threats that exist for wired networks, and have in addition to deal with some specific problems. Since wireless networks typically have no geographical boundaries, security provisioning cannot be deployed in the same manner as in wired networks, i.e., by setting perimeters and protecting these perimeters with traditional security technologies such as border firewalls. Besides, means of physical protection are often limited. Also, wireless networks have to deal with location privacy threats to which mobile users are often exposed.

Moreover, resources in WSNs are often limited (computation, storage, and energy), devices are unshielded, work without human assistance, and can be deployed in remote open and hostile areas [1]. WSNs have thus several specific threats and are often targeted to several specific attacks.

To be able to trade security to an acceptable level, appropriate metrics for security are needed. Dealing with these issues and with the ultimate objective of identifying proper security measures for WSNs, we first analyze existing threats.

Our paper is organized as follows: Sect. 2 presents a threat model for WSNs and identifies the most relevant security and privacy requirements. Sect. 3 provides an overview on security and privacy attacks for wireless networks by classifying them according to the network layers that they are targeted at. The focus is on both classical non IP-based WSNs and the emerging IP-based 6LoWPANs. Sect. 4 introduces the idea of a novel security evaluation framework for WSNs, based on attack tree and attack graph techniques. Finally, Sect. 5 presents conclusions and future work.

2. THREAT MODEL FOR WSNS

Several factors deeply affect the overall risk and should be taken into account when defining a threat model for WSNs: the technology inherent constraints, the overall system vulnerabilities, the security targets, the attacker characterization and the impact of attacks on the system functioning. In the following (Sect. 2.1 and Sect. 2.2), all these parameters are briefly introduced. In addition, security requirements are presented (Sect. 2.3).

2.1 WSN Technology Characterization

WSNs introduce many specific constraints compared to traditional computer networks [2, 3].

Resource scarcity. It is probably the main constraint for this technology: WSN nodes usually adopt low-power microprocessors with limited memory and storage space. The available bandwidth and data rate are limited as well. As far as the energy provisioning to the node is concerned, external batteries are usually considered. In this scenario, the risk of resource consumption can be exploited by attackers, and an inadequate choice of security countermeasures could lead to an even worse situation.

Unreliable communication. Wireless communication is characterized by channel errors and collisions. Moreover, in a densely deployed WSN, network congestion can cause an increase in system latency and the drop of messages in overloaded nodes.

Unattended operation. According to specific scenarios, WSNs can operate unattended in a remote location for long periods of time. Therefore, WSN nodes are likely to be exposed to physical attacks (casual tampering, vandalism but also bad weather) and become an attractive target.

Distributed nature. A cooperative distributed approach is very common in WSNs. While such an approach can be used to overcome specific resource limitations, it could also be exploited by attackers.

Low-cost. The cost of a single node is expected to be low. This poses constraints that can lead to inaccurate design and implementation errors.

Application specificity. Strict computational and power constraints, along with low-cost requirements, may dictate the design of application specific solutions.

2.2 Vulnerabilities and Attacker Types

The security targets in a WSN can be organized regarding the nature of the threat. Threats can target either a specific layer in the protocol stack, i.e., the physical, data link, network, transport or upper layers, or a WSN service, such as

data aggregation, synchronization, or the distributed location service. Moreover, the vulnerabilities of such security targets can be classified as either *physical* or *logical*.

The approach proposed in [2] allows to classify attackers according to four characteristics: motive, determination, knowledge and resources. Attackers may also be categorized according to three orthogonal dimensions.

Mote-class or *laptop-class*. The former type of attacker controls sensor nodes that are limited in resources, while the latter type of attacker can leverage on devices that are more resourceful than other devices in the network [4].

Passive or *active*. Passive attackers eavesdrop data being transmitted and received by one or more target devices, collect such transmitted data and can perform traffic analysis. Active attackers, instead, can inject, modify or interrupt over the air messages.

Outsider or *insider*. Outsider attackers are not authorized to join a WSN and, thus, do not share pre-deployed cryptographic keys. Insider attackers are authorized participants of the network instead.

Other factors can impact the definition of attackers capabilities: the number of attackers and their coordination. The effect of a successful attack should also be quantified. To this aim, a proper classification allows to identify the attacks that have little or no impact, cause system performance degradation, result in services disruption, or cause an overall system disruption.

In fact, attacker modeling is a key aspect when countermeasures have to be selected. On the base of how much powerful the attacker is the trade-off between security and performance floats either more towards the former or the latter objective.

2.3 Security Requirements

The definition of security requirements is a relevant issue and may differ according to application needs [4, 5, 6]. Security is important in most application scenarios where sensitive data is considered and possible attacks against the WSN may permit damages to the health or safety of people.

Most applications require robustness against outsider attacks. In the presence of an insider attacker, mechanisms able to detect compromised nodes are desirable. In the latter case, only a graceful degradation of performance is generally conceivable. Once defined the specific requirements, it is worth recalling that WSN nodes usually have severe constraints and a trade-off between performance, security and energy consumption is needed.

The main security requirements that can be led to the well known *CIA triad*, i.e., Confidentiality, Integrity and Availability, are presented in the following.

Authenticity. Since attackers can easily inject packets, authentication is necessary. Authentication enables a node to verify that the message originates from a trusted source (source authentication) and ensures data integrity, i.e., data has not been modified in transit (data authentication).

Secrecy. In wireless networks, attackers may eavesdrop packets and gain access to sensitive and private information. Encryption is generally used for keeping data secret, along with a shared secret key between the communicating peers, hence achieving data confidentiality. Theft of sensitive information can also be achieved by accessing the sensor's stored data, available through physical or remote access.

Availability. Availability means that the sensor network maintains its functionality without interruption. The network must continue operating also after node failures or in presence of node compromise, ensuring graceful degradation.

Service integrity. The application layer services implemented in the WSN must be protected from possible malicious attacks allowing the system to perform its task.

Privacy. Information regarding personal data or information that can be linked to an individual exist in different layers of data communication, and the boundless nature of wireless communication allows passive and active attackers to collect personal data, if such information is not protected. In the case of WSNs, sensed data leakage may permit to gather information about people in the sensors environment. A solution is to anonymize information by restricting the sensor network's ability to collect data at a detail level that do not compromise privacy [7].

It is worth noting that WSNs are used in several areas such as industrial, military, environmental and healthcare applications. In such sensitive and critical environments, acceptable delay, high responsiveness, reliable results and measurements as well as data and services availability are often required. In this context, service integrity plays the key role. In the following, this aspect is better analyzed and its specific requirements are outlined.

Data freshness. Sensors report data periodically either upon demand or triggered by events. In most applications, the sent data is valuable and considered as valid only for a limited period of time. If freshness is not guaranteed, an attacker can easily replay authentic messages in the network or pre-compute responses to requests that nodes will accept, forward and proceed.

Secure localization. In many applications, sensors need to know their position to achieve their tasks (e.g., geographic routing protocols). Because equipping sensors with GPS receivers is highly energy-consuming, sensors generally rely on some more powerful WSN devices called anchors, which are GPS-enabled, to retrieve their approximate location. In this context, secure localization protocols protect the network from false anchors and from attackers perturbing the localization process.

Secure time synchronization. Because sensors often collaborate to achieve their tasks, they generally must be synchronized. Secure time synchronization protocols are thus crucial in WSNs.

Secure broadcasting. In WSNs, broadcast communication can be used for network protocols, especially when no global identification can exist in the network. Unfortunately, source impersonation and data modification are a real threat targeting broadcast communications.

Resilient key establishment. Each node must be sure that the identity of the node to which it communicates is valid (not fabricated), is unique in the network (not cloned or duplicated) and corresponds to the real (claimed, intended) sensor. Moreover, data authenticity and integrity should be ensured. Reliable and resilient key establishment protocols are thus necessary in WSNs.

Secure data aggregation. Data aggregation considerably reduces the transmission overhead in the network, and extends the network lifetime. However, new security concerns are to be considered because end-to-end security is no longer available due to the use of aggregation. If the aggregated value is not trustworthy, wrong decisions will be taken.

3. THREAT ANALYSIS

In addition to classical information and communication systems' threats, WSNs can be targeted to several specific attacks, mainly because of the WSN technology inherent characteristics. WSNs are usually made of non-tamper resistant devices. They may furthermore be deployed in a remote hostile area, and work without human assistance. It is worth observing that the above distinctive factors also contribute to make wireless networks more vulnerable to privacy infringements than their wired counterparts. Actually, traffic information generated inside such networks can potentially reveal sensitive data about ad hoc network users and their communicating partners. Malicious attackers may even leverage on WSN functioning to track users' location and build complete user profiles. To this aim, an attacker needs to gather specific information to uniquely identify devices and recognize distinct occurrences of the same device in different moments. Thus, to identify potential threats to privacy in WSNs, it is necessary to list possible sources of identifiable data that can be used by an attacker.

Additional security attacks can be performed with different objectives as previously stated. Security targets can include both specific layers of the node protocol stack or particular in-network services. In the plethora of possible attacks, a proper classification could be useful for a more effective formal threat analysis. Many approaches have been proposed in the literature [8, 9]. In this paper, we adopt the ISO/OSI reference model as support to list the potential threats to security and privacy in WSNs, also following a bottom-up approach, i.e., from the physical layer to the application layer.

3.1 Physical Layer

As mentioned above, the broadcast nature of the wireless medium makes a list of security attacks feasible. In particular, the ones performed at the physical layer can be very effective. An attack can easily intercept or jam a common radio signal, overhear or disrupt in-network services physically.

Eavesdropping is a passive attack that can be realized by unauthorized malicious users monitoring or listening to the communication between entities in a system and trying to gain access to an asset but not to modify its contents. Transmitted messages can be overheard and then analyzed to discover security material (e.g., cryptographic keys) or used to inject fake messages into network. In addition, captured messages can be stored and retransmitted (*replay attack*): this is often a prelude to other security attacks.

Jamming is an active attack which generates radio signal interference so that the messages can be corrupted or lost. The interference generated by a laptop-class attacker will be strong enough to overwhelm the targeted signals and disrupt communications.

Physical layer attacks against privacy aim either to discover the geographical location of a device in a wireless network or to identify patterns in the emitted radio frequency (RF) signals that can be uniquely associated to a given device. RF triangulation and fingerprinting are two techniques that can be used to uniquely identify a device in a wireless network. RF triangulation is used to pinpoint the geographical location of a given device. Malicious passive devices in the wireless network are able to collect signal strength information of RF emitted by a target device. By combining the data gathered by sensors, it is possible to determine the geographical location of the target device. RF fingerprinting is a general umbrella term for different methods involving the analysis and identification of unique characteristics in the RF emission by a transmitting node.

Another class of attacks performed at physical layer relates to *tampering*. In fact, an attacker can tamper with sensor nodes physically and open individual sensors in order to steal sensitive data and cryptographic keys in order to gain access to the sensor network (*node compromise*). The sensor nodes could be damaged as well. In this case, node destruction can be hardly distinguished from benign node failure. It is also worth noting that tampering is strictly related to a node compromise. It can thus be considered a feasible attack against availability, but also against secrecy, authentication and service integrity.

WSN battery driven nodes are also susceptible to *battery exhaustion attacks*. Actually, this is a Denial-of-Service (DoS) attack performed at the physical layer, since the attacker aims to exhaust the battery power of a target device and render it useless by forcing it to receive, transmit or process data that the device should not need to in a normal situation.

3.2 Data Link Layer

Attacks may target the link layer by disrupting the cooperation of the layer's protocols. Wireless medium access control (MAC) protocols have to coordinate the transmissions of the nodes on the common transmission medium. Usually, a carrier sense multiple access/collision avoidance protocol (CSMA/CA) is used to resolve channel contention among multiple wireless hosts. Obviously malicious or selfish nodes are not forced to follow the normal operation of the protocols and could interrupt either contention-based or reservation-based MAC protocols.

DoS attacks can be performed at this layer as well. An attacker is able to disrupt an entire message by simply inducing a *collision* in one octet of a transmission and exploiting properties of the MAC protocols employed. It is worth observing that intermittent collision and exhaustion attacks (performed at physical layer) or abusing MAC priority schemes can lead to unfairness. Moreover, an attacker can send spoofed link layer acknowledgments to convince the victim that a dead node is alive (*acknowledgment spoofing*).

Data link layer *attacks against privacy* involve identifying and tracking unique characteristics that exist in this layer. In such attacks, hardware MAC addresses are usually taken into account. Actually, some attacks against privacy have been defined in order to let a malicious node impersonate a fake entity (*masquerade or impersonation attacks*). Unprotected or weak authentication mechanisms usually lead to this security threat, as message sequences can be replayed and data link addresses can be easily spoofed in wireless networks.

3.3 Network Layer

Network layer protocols extend connectivity from neighboring 1-hops nodes to all other nodes in the wireless network. Routing protocols designed for WSNs are usually vulnerable to a set of attacks aiming to influence or interfere on data communication flows. For example, routing tables could be poisoned with erroneous or incorrect information. Such at-

tacks aim to cause communication disruption, logically isolate a device from the rest of the network, to disrupt services or to gather data for traffic analysis.

Attacks against ad hoc routing protocols often try to build wormholes or set sinkholes in the network. *Wormholes* consist of bidirectional tunnels in an ad hoc network that are used to forward packets, including routing control messages, from one geographical location of the network to another distant location. Setting a wormhole needs two or more colluding nodes. Wormholes make the logical topology of an ad hoc network not to reflect the actual physical topology, with undesired effects on routing protocols [10]. *Sinkholes*, also called *blackholes*, are malicious devices that lure others nodes to forward traffic through them, usually sending false routing control messages and thus manipulating the ad hoc routing table of other nodes in the proximity [11]. A device acting as a sinkhole can either capture and store the forwarded traffic for future traffic analysis. It can also selectively drop packets, e.g., forward only control packets but no data packets [12], or can simply block all network traffic.

Many other attacks may be performed against routing [4]. For example, an attacker may inject bogus (*spoofed, altered or replayed*) routing information trying to disrupt routing availability. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation.

As far as IP-based WSNs are concerned, privacy threats in the network layer include the tracking of devices using the IP address as a unique identifier and ascertaining about the linkability between two communicating devices, i.e., revealing who is communicating with whom, by analyzing the network data traffic and dissecting the *source* and *destination* fields of an IP packet. The standard ad hoc routing protocols AODV [13] and DSR [14] leak the IP addresses of sender and destination during their path discovery phase, for instance.

In comparison to physical and data link privacy threats, attacks against network layer have a significant difference regarding the attack range, i.e., the geographical area affected in an ad hoc network. The attacker, in the latter case, needs only to be part of the path linking the source to the destination, and not necessarily in the radio range of the target device.

3.4 Transport Layer

The objectives of TCP-like transport layer protocols in wireless networks include the setting up of end-to-end connection, end-to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, a IP-based WSN node is vulnerable to the classic SYN flooding attack or session hijacking attacks. During a *SYN flooding attack*, the attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. This results into a DoS. *Session hijacking* takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

Furthermore, attacks against privacy can be performed by using transport layer information to fingerprint network devices [15]. It is worth noting that attackers do not necessarily have to be in the radio range of the target device when deploying a transport layer fingerprinting, and it is enough to be part of the path connecting the sender to the recipient.

3.5 Upper Layers

Security threats at the upper layers must be considered too. In this paper, upper layers include layers 5–7 (i.e., session, presentation, and application) in the ISO/OSI reference model. IP-based protocols such as HTTP, SMTP, TELNET, and FTP provide many vulnerabilities and access points for attackers. It is important to say that upper layer attacks are attractive for attackers due to the fact that the information they seek ultimately resides within the application and it is direct for them to make an impact and reach their goals. In addition, information encapsulated in the upper layers can eventually identify the sender and/or recipient of a message, expose the communication relationship between sender and recipient, or other personal data contained in the message payload.

Malicious code attacks could be performed as well. Malicious programs could spread themselves through the network and cause the computer system and network to slow down or even to be damaged.

3.6 Multi-layer

In addition to attacks targeting a single layer, some security attacks exploit weaknesses at multiple layers. Examples of multi-layer attacks are DoS and impersonation attacks. *DoS* attacks could be launched from several layers in order to hinder normal WSN operations. Several examples have been provided in the previous sections. During *impersonation attacks*, malicious nodes can declare a fake identity at both MAC and network layers. Sometimes, this is the first step for more sophisticated attacks.

4. THE PROPOSED FORMAL FRAMEWORK

As described in previous sections, many potential problems exist in WSNs. Thus, the vulnerability level estimation and the possible countermeasures identification is an urgent and important goal. We have coherently classified threats in terms of affecting protocol stack, thus we suggest an evaluation framework capable to discern among these different layers. We argue that the development of a formal security framework is necessary to enable an aided (i.e., semi-automatic) risk analysis process on WSNs.

Specific techniques like reliability block diagrams, fault and attack trees, and particularly attack graphs could be used [16, 17, 18] to define a formal tool able to asses WSN security level. The system would be formally depicted by its possible operative states and possible changes, while the evaluation would be based on reachability analysis of the state space. Moreover, stochastic and deductive analyses could be considered to represent the system evolution after, for instance, the application of a countermeasure (e.g., by Markov chains means) [19]. In particular, we propose to adapt the attack graph general approach to the taxonomy previously

presented, by defining the single threat which influences one ISO/OSI layer as the attack graph "atomic step" (i.e., a single node in the attack graph). This approach permits to understand which targets in the network are reachable by a malicious user, exploiting what weakness in what ISO/OSI layer.

These solutions would generate events appearing at attack realization, classify their impact on the given network and represent results as scenario graphs. In fact, the classification on the basis of the ISO/OSI layers involved, makes the choice of the actual countermeasures more effective, and thus permits a more practical impact analysis on a particular WSN. To enable such analysis, the needed baseline is a targeted description of the system with respect to both strong and weak points. To formally treat the overall WSN system, functional and non-functional requirements should be considered as well. Conceptually, the following formal descriptions are needed.

Service model. A service model is a description of the WSN services (i.e., the upper layers).

Resource model. A resource model is a model of the hardware functioning. The focus is on computational load and latency, delay introduced by traffic load, energy costs, nomadic behavior, etc.

Policy model. A policy model is a set of dependability and security constraints.

This formalization allows the creation of *security models* that act as input for attack graph construction and analysis. The description of service, resource and policy models could be performed by using formal high level languages (e.g., WS-CDL).

5. CONCLUDING REMARKS AND FUTURE WORK

In this paper, we have presented a state-of-the-art analysis of security in WSNs and proposed a taxonomy based on the ISO/OSI reference model. We advocate the need of this kind of taxonomy to develop a formal framework able to identify risks and suggest possible countermeasures. A promising methodology is based on attack graph construction and analysis. Leveraging on the taxonomy presented, our purpose is to develop a formal framework that is able to:

- analyse WSN systems and identify key vulnerabilities
- provide a tool to determine the most feasible countermeasures to adopt in order to obtain a reference security level (refer to security requirements), while meeting application specific latency/energy requirements.

Future steps will be:

- taxonomy extension to include missing weaknesses,
- adaptation of state-of-the-art attack graph methodology to our proposed taxonomy, and
- adaptation/extension of state-of-the-art formal description languages in order to model hardware and interactions present in WSNs.

REFERENCES

[1] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *Communications Magazine, IEEE*, 40(8):102–114, Aug 2002.

[2] A. D. Wood and J. A. Stankovic. A taxonomy for denial-of-service attacks in wireless sensor networks. In M. Ilyas and I. Mahgoub, editors, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, pages 739–762. CRC Press, Boca Raton, FL, USA, 2004.

[3] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security: A survey. In Y. Xiao, editor, *Security in Distributed, Grid, and Pervasive Computing*, pages 367–410. Auerbach Publications, Boca Raton, FL, USA, 2007.

[4] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, Anchorage, Alaska, USA, May 11, 2003. IEEE.

[5] E. Shi and A. Perrig. Designing secure sensor networks. *Wireless Communication Magazine*, 11(6):38–43, December 2004.

[6] A. Perrig, J. Stankovic, D. Wagner, and C. Rosenblatt. Security in wireless sensor networks. *Communications of the ACM*, 47:53–57, 2004.

[7] H. Chan and A. Perrig. Security and privacy in sensor networks. *Computer*, 36(10):103–105, 2003.

[8] T. Karygiannis. Wireless network security: 802.11, bluetooth, and handheld devices. Special Publication 800–48, NIST, October 2002.

[9] W. Stallings. *Cryptography and Network Security: Principles and Practices*. Prentice Hall, Upper Saddle River, NJ, USA, 3rd edition, 2003.

[10] F. Naït-Abdesselam, B. Bensaou, and T. Taleb. Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Communications Magazine*, 46(4):127–133, April 2008.

[11] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2–3):293–315, September 2003.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM Workshop on Wireless security (WiSE'03)*, pages 30–40, New York, NY, USA, September 19, 2003. ACM.

[13] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. RFC 3561: ad hoc on-demand distance vector (AODV) routing, July 2003.

[14] D. B. Johnson, D. A. Maltz, and Y.-C. Hu. RFC4728: the dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4, February 2007.

[15] T. Kohno, A. Broido, and K. C. Claffy. Remote physical device fingerprinting. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P 2005)*, pages 211–225, Oakland, CA, USA, May 8–11, 2005. IEEE Computer Society.

[16] W. Wang, J. M. Loman, R.G. Arno, P. Vassiliou, E. R. Furlong, and D. Ogden. Reliability block diagram simulation techniques applied to the IEEE std. 493 standard network. *IEEE Transactions on Industry Applications*, 40(3):887–895, May-June 2004.

[17] L. L. Pullum and J. B. Dugan. Fault tree models for the analysis of complex computer-based systems. In *Proceedings of Reliability and Maintainability Symposium*, pages 200–207, Las Vegas, NV, USA, 22–25 January 1996. IEEE.

[18] R. W. Ritchey and P. Ammann. Using model checking to analyze network vulnerabilities. In *Proceedings of the 2000 IEEE Computer Society Symposium on Security and Privacy ((S&P 2000)*, pages 156–165, Oakland, CA, USA, May 14–17, 2000. IEEE.

[19] D. M. Nicol, W. H. Sanders, and K. S. Trivedi. Model-based evaluation: From dependability to security. *IEEE Transactions on Dependable and Secure Computing*, 1(1):48–65, January–March 2004.