Towards a Threat Model for Mobile Ad-Hoc Networks

DAGMARA SPIEWAK, THOMAS ENGEL, and VOLKER FUSENIG
University of Luxembourg
Faculty of Sciences, Technology, and Communication
6, r. Richard Coudenhove-Kalergi, L-1359 Luxembourg
LUXEMBOURG
Dagmara.Spiewak@uni.lu Thomas.Engel@uni.lu Volker.Fusenig@uni.lu
http://wiki.uni.lu/secan-lab/SECAN-LAB.html

Abstract: - The increasing number of mobile devices enabled by wireless communication significantly change security issues and challenge threat modeling research in many ways. Particularly because of the vulnerability of wireless communication channels in addition to the insecure and lacking infrastructure, Mobile Ad-Hoc Networks (MANETs) require an adjusted Threat Model in contrast to the Threat Model faced when dealing with traditional networks. Moreover, mobility implicates ad-hoc routing methods to send data in an open wireless medium and facilitates adversaries in performing various attacks threatening the MANET's security. For this purpose threat modeling is employed to understand the adversary's view, to characterize the security of the system, and to identify the system's threats. In this paper we summarize and discuss protection challenges unique to Mobile Ad-Hoc Networks. We alter the Threat Model Process to Mobile Wireless Ad-Hoc Networks settings based on traditional security principles: Confidentiality, Integrity, Availability, Authentication, and Anonymity (*CIAAA*).

Key-Words: - Threat Model, Passive Attacks, Active Attacks, Vulnerabilities, MANETs, Adversary

1 Introduction

Mobile Ad-Hoc Networks (MANETs) have the ability to establish an immediate communication infrastructure for many mission-critical or time-critical applications, for example military applications or during a disaster recovery scenario. However, the typical characteristics of Mobile Ad-Hoc Networks, such as node mobility, wireless communication and wireless links breakage, make them vulnerable to security attacks. Nevertheless, security sensitive data and applications transmitted within mobile wireless networks, including MANETs, require a high degree of security. We consider a crisis scenario with MANETs support. Mobile wireless communications are essential to protect own troops from traversing dangerous and hostile areas. Evidently, the communication has to be secured from unauthorized and hostile access, so that no high-tech adversarial group can explore the communication traffic and can trace the mobile nodes in order to organize counterattacks. In this case, providing anonymity of own troops is critical and involves the detection of threats that can occur [1]. Unfortunately, MANET protection has classical trade-offs. For example, the use of strong cryptography [2] provides Confidentiality but can complicate the Availability of services and may introduce denial-of-service DoS vulnerabilities [3]. The use of flooding or redundancy-based mechanisms in Mobile Ad-Hoc Networks may provide connection-availability [4] of participating nodes but might also increase network traffic resulting in high latency for message delivering, network unavailability or even network breakdown. When designing a protection solution for mobile wireless networks, such as MANETs, the computer scientists responsible for security cannot just make use of every protection mechanism, since their results are often in conflict, but must rather evaluate the costs of each security countermeasure against the vulnerabilities and threats existing in a special environment. Furthermore, the meaning of security principles is dependent on the application. Thus, it is essential to understand all the threats and vulnerabilities existing in Mobile Ad-Hoc Networks before developing any MANET security solution, like for example a new secure routing protocol. Subsequently, these threats will determine the necessary security countermeasures. Doing the other way around, it might result in the fact that the selected MANET protection solution does not match the vulnerabilities and threats in the current application. The consequences are waste of resources, performance decrease, or service unavailability.

Unfortunately, security solutions are mainly based on attacks listed by brainstorming [3] or by reacting to exploits that recently occurred. This procedure is not systematic [5] and may not completely fill the feasible attack space. Figure 1 demonstrates the accurate position of Threat Modeling Process. After Threat Modeling, threats are used as basis for the conceptualization of Security Requirements intended for the use of MANETs in defined environments. Finally, the development of Security Mechanisms, such as secure routing protocols, should cover all requirements in order to avoid the feasible threats. Each stage feeds back to the preceding

stage and consequently to the stage before in order to catch mistakes made in one of the three stages.

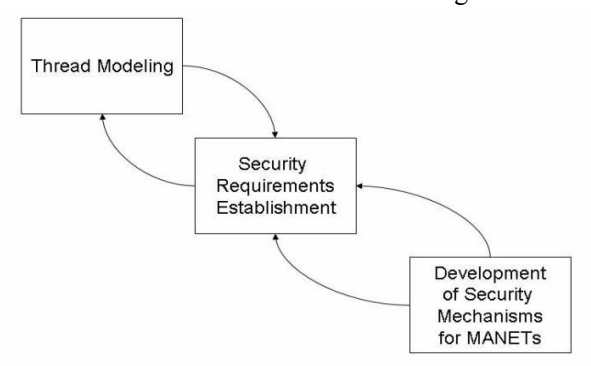

Fig.1 Threat Modeling Procedure [5]

Consequently, while designing a protection solution for MANETs, two central questions accrue. At first *"What are the threats in the MANET under specific assumptions or in a special application?"* and then *"Which security principles are necessary and do they match the MANET's security needs?"*
The remainder of this paper is organized as follows. In Section 2 we discuss the unique challenges of protecting Mobile Ad-Hoc Networks. Subsequently we introduce the threat modeling process for Mobile Ad-Hoc Networks in Section 3 and 4 followed by an outline of related work in Section 5. Finally, in Section 6, we present our conclusions and some ideas for future work.

2 The Challenge of Protecting Mobile Ad-Hoc Networks

Security in Mobile Ad-Hoc Networks has its own set of unique challenges compared to conventional and hierarchical network systems. Especially, because of the dynamic self-organized network topology in combination to principally missing infrastructure, security in Mobile Ad-Hoc Networks is assumed trickier. Unfortunately, traditional and approved security mechanisms such as Public Key Infrastructures (PKI) with central certification authorities (CA) or other trusted third parties (TTP) are not applicable in such almost anarchistic network structures [6]. Because of the absence of fixed base stations in Mobile Ad-Hoc Networks, nodes form and leave the network dynamically, sometimes even without leaving a trace and the network topology may change rapidly.
Particularly, *Anonymity* in Mobile Ad-Hoc Networks has a challenged significance and semantics compared to the notion of *Anonymity* in traditional networks [1]. Mainly *Mobility*, which is enabled by wireless communication, is the reason for the deviation of semantics.
In addition, the widespread notion is that wireless communication might be protected by strong cryptographic techniques at *end-to-end* or *hop-to-hop* level. Nevertheless, devices that form the Mobile Ad-Hoc Network are generally resource constrained and do not have capabilities to run complex algorithms. This requires lightweight security solutions to reach security in MANETs. We summarize the unique challenges of MANET protection:

- No fixed infrastructures
- Devices are resource constrained
- Shared wireless medium for communication
- Mobility of Nodes
- Dynamic changes of network topology

3 Threat Modeling Process for Mobile Ad-Hoc Networks

The development of a comprehensive and suitable threat model requires a systematic process [3]. Simply brainstorming the attacker's intention, capabilities, and listing possible attacks does not present an accurate basis for security requirements and countermeasures. Consequently, in order to ensure that all known and unknown threats and vulnerabilities are addressed, the systematic threat modeling process is indispensable. Firstly, we clarify the concrete meaning of the terms *Threat*, *Attack*, *Vulnerability* and *Countermeasure:*

A *Threat* is an undesired event that will have a negative impact on the Mobile Ad-Hoc Network system including all its protocols and components. The *Threat* can be malicious or not malicious, and might be for example caused by *Nature*.

A *Threat* is enabled through:

An *Attack* is a malicious action taken by utilization of vulnerabilities in the Mobile Ad-Hoc Network in order to realize a *Threat*.

An *Attack* takes place through:

A *Vulnerability* is a weakness in some components or protocols of the Mobile Ad-Hoc Network making an *Attack* possible.

A *Vulnerability* is mitigated with:

A *Countermeasure* addresses a *Vulnerability* to reduce the probability of *Attacks* or the impacts of *Threats*. They do not directly address threats; instead, they address the realization factors that define the threats. *Countermeasures* range from improving application

design, over improving the code, to improving an operational practice.

3.1 Network Model and Adversary's Capabilities

Maybe the first appearing question is how we model our Mobile Ad-Hoc Network which means *"What assumption do we make towards our Mobile Ad-Hoc Network functionalities?"*.

The most general assumption regarding Mobile Ad-Hoc Network functionality is that nodes can join and leave the MANET dynamically and that new nodes may get access to the existing MANET.

Secondly, the interesting and important questions to ask are *"Who are the attackers in our Mobile Ad-Hoc Network?"* and *"What can the attacker do in our Mobile Ad-Hoc Network (what are the attacker's capabilities)?"*.

The adversary is commonly defined as someone whose purpose is opposed to, or conflict with, the system's purpose. Generally, attackers may capture and compromise individual mobile nodes in the existing MANET or they may introduce new malicious nodes to the network. The adversary's capabilities can be characterized by the following attributes:

- Passive vs. Active
- Static vs. Adaptive
- Computationally bounded vs. Computationally unbounded
- Byzantine
- Mobile

These attributes can be combined, like for example the attacker may be active, adaptive and mobile.

Passive vs. Active:

The adversary is passive, if he does not actively initiate malicious actions in order to disturb the functionalities of the protocol. A passive adversary is often called *honest-but-curious*. He rests unnoticed in the background and tries to glean additional worthwhile information by eavesdropping on the routing traffic. For instance, if the malicious node observes that the connection to a certain node is requested more frequently than to other nodes, the passive adversary would be able to recognize, that this node is crucial for special functionalities within the MANET, like for example routing [6]. These *honest-but-curious* adversaries follow the protocol and do not disturb its functionality.

The active adversary can directly interfere the functionalities of the protocol, and interrupt the accurate execution of a routing protocol for example by modifying routing data, by fabricating false routing information, or by impersonating other nodes.

Static vs. Adaptive:

The differentiation between static and adaptive attackers is very important. Although both adversary models may for example corrupt a certain set of nodes in the Mobile Ad-Hoc Network, the significant difference between the models is the following. In the static case, the set of nodes is determined previous to the execution of the protocol, whereas in the adaptive case nodes of the set are selected during the execution of the protocol. This means that the adversary may select nodes to corrupt more efficiently based on retrieved information. Consequently, adaptive adversaries are more flexible and have a better ability to react to the mobility of the system.

Computationally bounded vs. Computationally unbounded:

The determination of the adversary's power is of enormous importance. The adversary may be unbounded in his resources, like for example in his storage and power capacities. On the other hand the adversary may be bounded to probabilistic polynomial time.

Byzantine:

The Byzantine adversary has complete control over a set of nodes in the Mobile Ad-Hoc Network. Furthermore, he is constrained to corrupt up to a threshold k (number of nodes) in the MANET. We call this Byzantine adversary also *k-adversary*. The Byzantine adversary has now the capability to corrupt an arbitrary set of nodes only limited by the threshold k.

Mobile:

The adversary is *mobile* if he has the capability to change the set of corrupted nodes of the Mobile Ad-Hoc Network from period to period, for instance as reaction to the dynamic changes of the MANET's topology [7].

3.2 Adversary's Intentions

The adversary executes the attack with a specific intention in mind, covering the goals of a threat. In a Mobile Ad-Hoc Network the adversary has the possibility to affect the following incomplete list of items in order to reach his goal:

- Routing
- Data Integrity
- Data Availability
- Data Confidentiality
- MANET Anonymity

4 The CIAAA Threat Model Process

Mobile Ad-Hoc Network security must mainly cover five aspects: *Confidentiality, Integrity, Availability, Authentication,* and *Anonymity (CIAAA)*. Hence, these five attributes might be threatened by an attack on the part of the adversary.

In this section we classify different types of attacks on Mobile Ad-Hoc Network into five groups according the *CIAAA* typology. This helps to address the attacks by deploying *CIAAA* security methods.
Firstly, we present the application of each *CIAAA* item to Mobile Ad-Hoc Networks followed by the listing of specific attack instances [3]. We notice that some attack instances may be associated with different categories of attacks. The lists are not complete and must be extended. However, as new attacks are emerged the *CIAAA* typology remains constant.

4.1 Confidentiality Attacks

Confidentiality Attacks always effort to extract information, for example of transmitted data-packets within the Mobile Ad-Hoc Network, without accurate authorization. If the adversary appears as an authenticated MANET node, for instance by performing a *Spoofing* attack, he may get the permission to get access to sensitive data by mistake. To avoid this security problem in static networks strong encryption techniques are used, mainly by the use of PKI. These protection techniques are assumed as not adequate for message encryption within Mobile Ad-Hoc Networks, because of the non-existence of fix and continuously accessible servers for key management as well as the high computational complexity of asymmetric encryption algorithms. For this reason the notion of *Trust Establishment in MANETs* [6] gets more and more important mainly in order to avoid the need of centralized entities. We identify the following confidentiality attacks on Mobile Ad-Hoc Networks:

Eavesdropping:
Unencrypted or weakly encrypted data traffic in Mobile Ad-Hoc Networks might be analyzed and filtered by the Eavesdropping attack. This is a passive attack allowing the adversary to extract worthwhile information about data transferred within the MANET.

Spoofing:
The adversary modifies either the MAC or the IP address in outgoing packets in order to adopt another identity in the MANET and appear as a good-natured node. Consequently, by this technique he is able to operate as a trustworthy node and might for example get access to confidential data.

Sybil Attack:
Here, the adversary may not only impersonate one node but can even represent multiple identities by maintaining false identities. By launching a Sybil Attack the adversary can pretend that the allegedly different paths are formed by disjoint nodes, although in reality these paths share at least one node which is the adversary's one.

4.2 Integrity Attacks

Integrity Attacks always effort to modify information in Mobile Ad-Hoc Networks without having the right to do. By launching this type of attack the adversary may drop messages, redirect traffic to a different destination, or compute longer routes to the destination in order to increase the communication delays. For example, by sending fake routing packets to other nodes, all traffic can be redirected to the attacker or another compromised node [6]. We identify the following integrity attacks on Mobile Ad-Hoc Networks:

Blackhole Attack:
Here the adversary lies and announces itself, during the route discovery phase of a routing protocol, as knowing an accurate path to the requested target node, in order to be able to intercept packets. Finally, all packets are transferred to the attacker's node and he discards all of them. Consequently, the adversary represents the Blackhole in the Mobile Ad-Hoc Network, where all packets will be swallowed.

Greyhole Attack:
As an extension of the *Blackhole attack*, the adversary might generate a *Greyhole*. In this case, the adversary's *grey* node has the ability to switch its course of action from forwarding routing packets or discarding others. The decisions of its behaviour depend on the intention of the attack. For example, for the purpose of isolating particular nodes in the Mobile Ad-Hoc Network the adversary's *grey* node drops packets which pilot towards their destination. Packets meant for other nodes rest unmodified and are forwarded according to their destination.

Wormhole Attack:
The adversary generates a tunnel between two or more cooperating and by him controlled nodes within the Mobile Ad-Hoc Network. This attack allows the adversary to short-cut the normal flow of routing messages in the MANET. The adversary records packets or parts of packets at one selected location in the MANET. After tunnelling them to another point in the network he replays the packets into the network. The advantage of the *Wormhole* for the adversary is his possibility to discard selected data packets or to maintain a *Denial of Service* attack, because no other route to the destination can be determined as long as the attacker controls the Wormhole [8].

4.3 Availability Attacks

Availability Attacks attempt to make data, data transmissions or services *unavailable*. Mobile Ad-Hoc

Networks appear on-demand and are created on-the-fly without the pre-establishment of infrastructure. Therefore, the availability of data and services in these networks is a critical condition since nodes can join and leave the network dynamically and may change their geographical positions due to their mobility capacity. We identify the following availability attacks on Mobile Ad-Hoc Networks:

Denial-of-Service Attacks:
Particularly *Denial-of-Service Attacks* weaken data and service availability by exhausting resources or isolating nodes in order to avoid data transfer.

Flooding:
Flooding is an effective attack to weaken data availability. The adversary might flood the Mobile Ad-Hoc Network with useless, false or replicated routing messages which loop in the network effectively using bandwidth and resources.

Rushing Attack:
This kind of attack acts as an effective Denial-of-Service attack against all currently proposed on-demand Ad-Hoc network routing protocols, including those designed to be secure. An adversary rapidly spreads routing messages all through the network, disabling authorized routing messages with the consequence that nodes delete them as multiple copies. Consequently, also routes to a destination get unavailable.

4.4 Authentication Attacks

By masquerading as a legitimate node, the adversary can run authentication attacks in the Mobile Ad-Hoc Network. Unrecognized he may operate as an authenticated node from the inside and get access to sensitive data and services. We identify the following authentication attacks on Mobile Ad-Hoc Networks:

Spoofing:
The adversary modifies address information in packets and adopts an authenticated identity in the network in order to operate as a trustworthy node.

Sybil Attack:
In this case the adversary may not only impersonate one legitimate node in the Mobile Ad-Hoc Network but can even represent more identities by maintaining multiple false identities. This attack particularly weakens systems and protocols employing redundancy. By launching a *Sybil Attack* the attacker can pretend that the allegedly different paths are formed by disjoint nodes, although in reality these paths share at least one node which is the attacker's one.

4.5 Anonymity Attacks

Anonymity Attacks are launched in order to disclose sensitive information in Mobile Ad-Hoc Networks. In the face of Anonymity Attacks critical information includes:

- Sender Identity
- Recipient Identity
- Location of specific nodes in the Mobile Ad-Hoc Network

In contrast to traditional fixed networks, where the network topology is determined *a priori*, in MANETs not only the identity of communicating entities pose a risk to be threatened by Anonymity Attacks that are mainly performed by passive adversary. Beyond, mobility of nodes implies additional threats to Anonymity by uncovering the geographical location of nodes as well as their motion. Consequently, *Privacy* of the Mobile Ad-Hoc Networks topology turns out to be a supplementary *Anonymity* factor in MANETS. We identify the following anonymity attacks on Mobile Ad-Hoc Networks:

Sender or Recipient Identity Discovery Attack:
This attack targets to disclose either the identity of the sender or the identity of the recipient or even both of them. By intercepting route request packets, normally send during the route discovery phase in on-demand Ad-Hoc Routing Protocols, the adversary may discover the sender's and the recipient's identities.

Motion pattern inference attacks:
The goal of this attack [1] is to track the movement of nodes in the Mobile Ad-Hoc Network. The adversary may monitor the motion of nodes within his listening range. However, by corrupting multiple nodes within the MANET he may cover a wide listening range and in the extreme case the transmission area of the whole MANET. Consequently, the adversary may combine the gathered information and reconstruct the motion pattern of the observed node in the Mobile Ad-Hoc Network.

Location Privacy Attack:
Facing the [1] listening range of the adversary's node, the adversary may glean worthwhile information about:

- Set of active nodes within his listening range
- Size of the set of active nodes
- Active Communications

Route Tracing Attack:
The adversary [1] tries to collect route information about a certain node within the MANET. He monitors the routing traffic in order to gather details about routes to other nodes in the network as well as to assure with whom this specific node is communicating.

5 Related Work

In this section we highlight significant related works we have not yet referenced. Threat modeling presents a process of evaluating and formalizing security risks of a system. Bruce Schneier [9] pioneered *Attack-Trees* to model threats. This method assumes to know the attacker's goals first, because each goal will form an *Attack-Tree*. At first, all attacks against each goal have to be added to this *Attack-Tree*. This process is repeated top-down until no new attack can be discovered. Problematic in this procedure is the possibility to forget about one attack. Especially at higher level of the *Attack-Tree*, this may provoke a big attack-space resting completely unconsidered. Further threat models are described in [10] for the Domain Name System and in [11] for the Internet Browser. Microsoft proposes the *Threat Modeling Tool* and a book written by Swiderski and Snyder [12] for modeling threats while concentrating on software applications.

In [13] the authors discuss threat models for *Ubiquitous Systems*. Particularly the famous *Dolev-Yao Threat Model* [14] is examined on its applicability to ubiquitous computing systems and adjudged as unrealistic and unsuitable. The *Dolev-Yao Threat Model* characterizes the adversary that can overhear, intercept, and produce any arbitrary message and is only limited by the constraints of the cryptographic methods. This model is also impractical for Mobile Ad-Hoc Network mainly because of its assumption: "a secure public directory contains all *(X, E_X)* pairs" [14], where X represents the network entity and *E_X* its encryption function *(public-key)*. The requirement of a continuously accessible, central public directory is critical in the MANETs setting mainly because of the mobility of nodes and the principally missing infrastructure.

6 Conclusions and Further Work

Mobile Ad-Hoc Networks present unique security challenges. In this paper we present the Threat Modeling Process upon which to base the MANET protection. The process is founded on traditional security principles: Confidentiality, Integrity, Availability, Authentication, and Anonymity *(CIAAA)*. We categorize the threats into several classes of attacks in order to match the security principles with the purpose to cover all possible attack instances.

Further work is needed to crystallize out and to develop realistic threats on MANET security principles based on the *CIAAA* typology. Formalizing the Threat Model and its principles will be essential in order to examine the MANET's vulnerability to attacks based on existing threats.

References:

[1] X. Hong, J. Kong, and M. Gerla, Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks, *Special Issue on Wireless Network Security,* Wiley Interscience Press, 2006

[2] L. Ertaul and N. Chavan, Security of Ad Hoc Networks and Threshold Cryptography, *2005 International Conference on Wireless Networks, Communications, and Mobile Computing Wirelesscom*, 2005

[3] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik, Toward a Threat Model for Storage Systems, *International Workshop on Storage Security and Survivability (StorageSS)*, November 2005

[4] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, Flooding for Reliable Multicast in Multi-Hop Ad Hoc Networks, *Proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, Seattle WA, 1999

[5] S. Myagmar, A. J. Lee, and W. Yurcik, Threat Modeling as a Basis for Security Requirements, *Symposium on Requirement Engineering for Information Security*, 2005

[6] D. Spiewak and T. Engel, An Overview of Models applying Trust as a Component of Security Services in MANETs, *Proceedings of WSPWN 06*, Miami Florida USA, March 2006

[7] R. Ostrovsky and M. Yung, How to withstand mobile virus attacks (extended abstract), *Proceedings of the tenth annual ACM symposium on Principles of distributed computing*, Montreal Quebec Canada, 1991

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Network. *Rice University Department of Computer Science, Technical Report TR01-384*, December 2001

[9] B. Schneier, Attack Trees: Modeling security threats. *Dr. Dobb's Journal*, December 1999

[10] D. Atkins and R. Austein, Threat Analysis of the Domain Name Service (DNS), *RFC 3833*, August 2004

[11] I. Griggs, The Browser Threat Model. *http://iang.org/ssl/browser_threat_model.html*, 2004

[12] F. Swiderski and W. Snyder, Threat Modeling, *Microsoft Press*, 2004

[13] A. Roscoe, M. Goldsmith, S. Creese, and I. Zakiuddin, The attacker in ubiquitous computing environments: Formalizing the threat model, *Proceedings of First International Workshop on Formal Aspects in Security and Trust*, Italy, 2003

[14] D. Dolev and A. Yao, On the security of public key protocols, *IEEE Transactions on Information Theory* 29(2), 1983, pp. 198—208.