Chapter VI

Intrusion and Anomaly Detection in Wireless Networks

Amel Meddeb Makhlouf
University of the 7th of November at Carthage, Tunisia

Noureddine Boudriga
University of the 7th of November at Carthage, Tunisia

ABSTRACT

The broadcast nature of wireless networks and the mobility features created new kinds of intrusions and anomalies taking profit of wireless vulnerabilities. Because of the radio links and the mobile equipment features of wireless networks, wireless intrusions are more complex because they add to the intrusions developed for wired networks, a large spectrum of complex attacks targeting wireless environment. These intrusions include rogue or unauthorized access point (AP), AP MAC spoofing, and wireless denial of service and require adding new techniques and mechanisms to those approaches detecting intrusions targeting wired networks. To face this challenge, some researchers focused on extending the deployed approaches for wired networks while others worked to develop techniques suitable for detecting wireless intrusions. The efforts have mainly addressed: (1) the development of theories to allow reasoning about detection, wireless cooperation, and response to incidents; and (2) the development of wireless intrusion and anomaly detection systems that incorporate wireless detection, preventive mechanisms and tolerance functions. This chapter aims at discussing the major theories, models, and mechanisms developed for the protection of wireless networks/systems against threats, intrusions, and anomalous behaviors. The objectives of this chapter are to: (1) discuss security problems in a wireless environment; (2) present the current research activities; (3) study the important results already developed by researchers; and (4) discuss the validation methods proposed for the protection of wireless networks against attacks.

INTRODUCTION

Wireless has opened a new and exciting area for research. Its technology is advancing and changing every day. However, the biggest concern with wireless has been security. For some period of time, wireless has seen very limited security on the wide open medium. Along with improved encryption schemes, a new solution helping the problem resolution is the wireless intrusion detection system (WIDS). It is a network component aiming at protecting the network by detecting wireless attacks, which target wireless networks having specific features and characteristics. Wireless intrusions...
Intrusion and Anomaly Detection in Wireless Networks
can belong to two categories of attacks. The first
category targets the fixed part of the wireless
network, such as MAC spoofing, IP spoofing, and
denial of service (DoS); and the second category
of these attacks targets the radio part of the wire-
less network, such as the access point (AP) rogue,
noise flooding, and wireless network sniffing. The
latter attacks are more complex because they are
hard to detect and to trace-back.
To detect such complex attacks, the WIDS
deploys approaches and techniques provided
by intrusion detection systems (IDS) protecting
wired networks. Among these approaches, one
can find the signature-based and anomaly based
approaches. The first approach consists in match-
ing user’s patterns with stored attack’s patterns (or
signatures). The second approach aims at detect-
ing any deviation of the “normal” behavior of the
network entities. The deployment of the afore-
mentioned approaches in a wireless environment
requires some modifications. The signature-based
approach in wireless networks may require the
use of a knowledge base containing the wireless
attack signatures while an anomaly based ap-
proach requires the definition of profiles specific to
wireless entities (mobile users and AP). Recently,
efforts have focused on wireless intrusion detec-
tion to increase the efficiency of WIDS. Based on
these efforts, models and architectures have been
discussed in several research works.
The objective of this chapter is to discuss the
major research developments in wireless intru-
sion detection techniques, models, and proposed
architectures. Mainly, the chapter will: (1) discuss
security problems in wireless environments;
(2) present current research activities; (3) study
important results already developed; and (4)
approve validation methods proposed for WIDS.
The remaining part is organized as follows: The
next section discusses vulnerabilities, threats, and
attacks in wireless networks. The third section
presents wireless intrusion and anomaly detection
approaches. The fourth section introduces models
proposed for detecting wireless intrusions. The fifth
section presents WIDS architectures, proposed by
researches papers. The sixth section presents the
wireless distributed schemes for intrusion detec-
tion. The seventh section discusses mechanisms
of prevention and tolerance provided to enhance
the wireless intrusion detection. Finally, the last
section concludes the chapter.

VULNERABILITIES, THREATS, AND
ATTACKS IN WIRELESS NETWORKS
To present vulnerabilities, threats, and attacks
targeting wireless networks, we have to discuss
first the security requirements of wireless systems,
including those concerning security policy. This
section presents the concepts of wireless intrusion,
anomaly, and attack scenario in wireless networks,
in order to highlight intrusion and anomaly detec-
tion requirements. In particular, it discusses some
attacks and attack classification that make security
in wireless systems very special.

Security Requirements in Wireless
Environments
Securing a communication channel should satisfy
at least the following set of requirements: integ-
ry, confidentiality, and availability. Moreover,
wireless communications require authentication
of the sender or/and the receiver and techniques
that guarantee non-repudiation. In the following,
we discuss technical security and security policy
requirements which help reducing vulnerabilities
and attack damages.
Because of their technical architecture, mobile
communications are targets for a large set of threats
and attacks that occur in wired networks, such as
identity spoofing, authorization violations, data
loss, modified and falsified data units, and repu-
diation of communication processes. Additionally,
new security requirements and additional measures
for wireless networks have to be added to the se-
curity requirements of wired networks (Schäfer,
2003). Vulnerabilities, threats, and attacks, existing
in wireless networks represent a greater potential
risk for wireless networks. One among technical
requirements is the enforcement of security of
the wireless links, because of the ease of gaining
direct physical accesses. Moreover, new difficulties