2008 International Conference on Computer and Electrical Engineering

HIDMN: A Host and Network-based Intrusion Detection for Mobile Networks

Shahriar Bijani
Engineering and Technology Research Center (ETRC)
Shahed University
Tehran, Iran
bijani@shahed.ac.ir

Maryamosadat Kazemitabar A.
Engineering and Technology Research Center (ETRC)
Shahed University
Tehran, Iran
kazemitabar@ce.sharif.edu

Abstract

Network-based methods of intrusion detection alone are not adequate to encounter current and future threats in mobile networks. In this paper, we introduce HIDMN, a host and network-based Intrusion Detection and Prevention system for mobile networks. In addition, we outline some patterns for significant attacks in the GSM mobile network. This system can detect most attacks which we divide them into three classes: Denial of Services, fake BTS-based attacks and SIM cloning. Using SIM-based methods as a main part of IDS for detecting and responding to attacks is another novelty of HIDMN.

Keyword: ***Mobile Security, Intrusion Detection, Mobile Networks, GSM, SIM, SAT.***

1. Introduction

Many intrusion detection systems in mobile networks concentrated on detecting stolen mobile devices and toll fraud by using network anomaly detection [3][7][9][10][11] and behavioural profiling [2][3][4][5] of users. Spafford and Zamboni [6] argue that from the point of view of intrusion detection systems, host-based data collection is in most cases preferable to network-based data collection. Miettinen and Halonen [1] show that host-based approaches are required, since network-based monitoring alone is not sufficient to encounter the future threats.

Different attacks and threats are known in the cellular mobile networks, especially in GSM[1] [12][13]. We categorize the most important attacks in the GSM network into three following classes:

- Fake BTS based attacks: Common devices in most attacks are fake BTS2 and modified Mobile Station (MS).
- Denial of Service (DoS) and Distributed Denial of Service (DDoS): Prevent one or more cells to service in mobile networks by setting up too many calls and SMSs are well-known methods of attack [14].
- SIM Cloning: Breaking COMP128, COMP128/2, and COMP128/3 algorithms after gaining physical access to the SIM, is another method to clone the SIM, as an alternative to methods using fake BTS[3].

We design a host-based and network-based intrusion detection model for the GSM mobile network and outline some important patterns for the three main classes of attacks. The host part of HIDMN, used to detect attacks in the mobile network is the most important part of HIDMN. We used Gemalto Developer Suite and the Java programming language for implementation and simulation.

2. HIDMN Architecture

[1] Global System for Mobile
[2] Base Transmitter Station
[3] Basic Transceiver Station

978-0-7695-3504-3/08 $25.00 © 2008 IEEE
DOI 10.1109/ICCEE.2008.183