Information Sciences 321 (2015) 179–192

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A collaborative framework for intrusion detection in mobile networks

Mauro Andreolini [a,*], Michele Colajanni [b], Mirco Marchetti [b]

[a] Department of Physics, Computer Science and Mathematics, University of Modena and Reggio Emilia, Via Campi 213/a, 41125 Modena, Italy
[b] Department of Engineering "Enzo Ferrari", University of Modena and Reggio Emilia, Via Vignolese 905/b, 41125 Modena, Italy

ARTICLE INFO

Article history:
Received 4 April 2014
Received in revised form 26 February 2015
Accepted 10 March 2015
Available online 25 March 2015

Keywords:
Network intrusion detection
NIDS state migration
Mobility-based NIDS evasion
WLAN
Mobile IPv4
Mobile IPv6

ABSTRACT

Mobile devices are becoming the most popular way of connection, but protocols supporting mobility represent a serious source of concerns because their initial design did not enforce strong security. This paper introduces a novel class of stealth network attacks, called mobility-based evasion, where an attacker splits a malicious payload in such a way that no part can be recognized by existing defensive mechanisms including the most modern network intrusion detection systems operating in stateful mode. We propose an original cooperative framework for intrusion detection that can prevent mobility-based evasion. The viability and performance of the proposed solution is shown through a prototype applied to Mobile IPv4, Mobile IPv6 and WiFi protocols.

1. Introduction

Society has become dependent on a wide array of mobile devices. For example, most credit-card swipes at restaurants are performed with mobile devices. RFID is widespread in inventory management. To lower infrastructural costs and to appease their employees, companies are seeking to enroll so-called "Bring Your Own Device" (BYOD) policies that allow workers to gain controlled access to the internal network resources through their mobile devices (mainly laptops and phones). These devices typically run a mix of enterprise and personal applications. Cisco predicts that the number of mobile devices will exceed the world population by 2014.

An inevitable consequence of the huge success of user mobility is an increasing exposure of mobile devices and networks to a wide array of attacks. In addition to eavesdropping on wireless transmissions [5,15,23], break-in [33,35], GSM impersonation [16,13], social engineering [4], we present a novel form of attacks called *mobile evasion* that can be applied to mobile protocols, such as Mobile IPv4, Mobile IPv6 and WiFi. Mobile evasion leverages the intrinsic vulnerability of mobile protocols supporting *transparent mobility* where roaming events do not interrupt established connections [14]. This is a mandatory feature for all applications requiring a stable connection, but it exposes mobile nodes and related networks to so called "stealth" network attacks. They do not exploit vulnerabilities in protocol implementations, but the effects of mobile node migrations on routing. An attacker can route different portions of a malicious payload through different network paths, thus avoiding the possibility of detection by typical defensive network mechanisms including anomaly-based [26,12,25],

* Corresponding author.
E-mail addresses: mauro.andreolini@unimore.it (M. Andreolini), michele.colajanni@unimore.it (M. Colajanni), mirco.marchetti@unimore.it (M. Marchetti).

http://dx.doi.org/10.1016/j.ins.2015.03.025
0020-0255/

signature-based [1,2,11], location-based [34] intrusion detection systems (NIDS) [30]. Existing defensive mechanisms are not designed for facing transparent mobility, hence they are inherently incapable of detecting a mobile stealth attack that is fragmented, because no portion of the payload can be matched against the NIDS signature database. Even the most advanced cooperative NIDSs (e.g., centralized [31,32], hierarchical [24,17], peer-to-peer [21,19,37,20]) are vulnerable because they cooperate by exchanging data pre-processed by one NIDS.

We initially present a model of the mobile evasion attack that can be applied to any well known mobile protocol. Then, we propose an innovative solution that leverages a novel way for NIDS cooperation. The proposed scheme allows sharing of internal state information among multiple NIDSs deployed in different networks or network segments. The overall solution is integrated into a prototype which extends Snort, but it can be easily adapted to any other NIDS because the implementation is based on a lightweight agent and a set of plugins handling different protocols. This modular design guarantees great flexibility in terms of deployment and expandability. We validate the efficacy and efficiency of the proposed framework for different combinations of migration rates and network protocols. We can conclude that the proposed solution can detect mobility-based attacks in all tested real scenarios at a negligible cost in terms of performance.

The paper is organized as follows. Section 2 compares our solution against related work. Section 3 introduces a general model of the mobile evasion attack and instantiates it for three mobile network protocols: Mobile IPv4, Mobile IPv6 and 802.11g. Section 4 proposes a novel cooperation scheme that is able to thwart mobile evasion for a wide variety of roaming implementations. Sections 5–7 present the relevant details for 802.11g, Mobile IPv4 and Mobile IPv6. Section 8 discusses functional and performance evaluation results obtained through experiments. Section 9 outlines main conclusions.

2. Related work

Mobile ad-hoc networks represent an important source of information about intrusion detection systems for wireless environments. For example, Thamilarasu et al. [28] propose a Cross-layer Intrusion Detection System (IDS) in order to mitigate DoS attacks in ad-hoc networks with a focus on collisions, misdirection and packet drops. The cross-layer design is able to detect intrusion at different protocol layers and to exploit the information from one layer to another layer. Zhang et al. [36] propose a distributed and cooperative IDS architecture where each node participates with its information resources. Other authors [22] address the issues related to a rigid response to an intrusion by proposing a flexible scheme that depends on the measured severity of attack and the degradation in network performance. We remark that all these interesting proposals focus on ad-hoc networks that are quite different from mobile Internet-based networks of interest for this paper. For a similar reason, we distinguish from approaches using host IDS [11], and from statistical profiling algorithms (e.g., [34]) that are ineffective against mobile evasion.

We differ also from proposals using distributed intrusion detection systems (e.g., [31,32,6]) that gather data from different sources and send alerts to one aggregator analyzing and correlating all available information. These solutions are based on different IDS architectures: hierarchical (e.g., Emerald [24]), hierarchical and autonomous for cloud systems [17], peer-to-peer (e.g., [21,19,37,20] where the main goal is to avoid single points of failure). All these systems are oriented to exchange high level information, filter and aggregate it with the goal of reducing the amount of transferred data and to increase the intrinsic value of alerts to human operators. On the other hand, in order to contrast mobile evasion attacks, we have to share in an efficient way raw data at the level of the NIDS internal states with minimal pre-processing work. With respect to this objective, our work is more related to NIDS architectures exploiting state migration. For example, parallel NIDS architectures [8,27,7,3,6] achieve cooperation by migrating the connection state from one NIDS to another. In [27] the authors synchronize one or more NIDS internal variables that are identified in the configuration with the goal of generating a pool of values shared among all the cooperative NIDS sensors distributed among different network links. The same mechanisms for coordinating lower-level analysis were used to implement a NIDS cluster [29], while a different framework provides methods to export/import complete state information from/into a NIDS [8,7,3]. All these solutions use state migration to pursue load balancing or to improve performance, while our proposal describes a novel scheme to prevent an attacker to exploit mobility to evade detection. This is achieved by supporting a mechanism where the state information related to a Mobile Node "follows" the Mobile Node in the new network. We improve on our previous paper [9] in several ways: we design a modular and general framework that supports different mobile protocols, we implement it by extending the Snort software and we present a large set of experimental results demonstrating functional and performance effectiveness.

3. Mobility-based NIDS evasion

We describe the mobile evasion attack by considering the most advanced stateful NIDS architectures, because stateless systems can be easily bypassed by several types of attacks and are now deprecated. In a stateful NIDS, the information of a network packet, which is relevant to intrusion, is used to create and update an internal state about all the active transport level connections. For each connection, a pre-processor maintains several metadata and two ordered lists of payloads (one for each direction) exchanged by the endpoints. The detection algorithm is then executed on the entire state information. As a consequence, although no individual packet contains enough information to detect an intrusion, a stateful NIDS can detect it by correlating information extracted from different packets. The problems originate when we consider a scenario allowing node mobility where an attacker can pursue *mobility-based NIDS evasion* that was introduced in [10]. Here, an attacker