# Detecting and Preventing Intruders for Cyber-Security

Martin E. Andreoni L., Otto Carlos Muniz Bandeira Duarte
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

*Abstract*—**Most of current attacks comes from trusted hosts and cannot be detected or prevented by firewall, access control, and cryptographic mechanisms. Therefore, Intrusion Detection and Prevention Systems (IDPS) are mandatory to monitor and inspect real-time network trafc, looking for abnormal patterns caused by intruders or insider abuses. In this paper we present a security framework consisting of Bro, which is an open source traffic analyzer, and OpenFlow Application Programming Interface (API). We implemented and experimented our framework in a virtual network environment on the Future Testbed Internet with Security (FITS) platform and analyzed different scenarios and attacks.**

## I. Introduction

The internet environment has changed during the years, from an academic file-exchange system to an all-purpose system with a huge number of users, traffic patterns and topological complexity of today. In this new scenario, network attacks increased in number and harshness during these years.

According to [1] between 60-70% of the attacks came from our "trusted" hosts. Although current security methods such as firewall, access control, authentication, and encryption attempt to prevent threats, they are not a fully sensitive information protection. As a consequence, Intrusion Detection and Prevention Systems (IDPS) complement security system by protecting the network, from internal and external attacks. These systems are configured to detect and respond, on real time, to security threats by both insiders and external penetrators, reducing the risk to monitored computers and networks.

Under this unsafe environment, we have developed a Smart Intrusion Detection and Prevention System based on Bro [2]. This system is a distributed IDS with hybrid methodology detection working with prevention features. Thus, as a result, our system is implemented and experimented into the Future Internet Testbed with Security (FITS). FITS is a testbed for experimenting Next-Generation Internet proposals that provides two virtualization schemes based on Xen and on OpenFlow, offering network isolation, secure access, and quality of service differentiation. FITS nodes are spread over Brazilian and European universities [3].

## II. Bro IDS

Bro is a network based open source analyzer developed by Vern Paxson in ICSIs *Center for Internet Research (ICIR), Berkeley*. Bro passively monitors and analyzes the network traffic in real time using the libpcap packet capture library. All the network activity is mapped into events, analyzed in the Bro event engine. Then, these events are passed to an upper layer, the policy layer, in which the network administrator defines its own custom policies written in Bro scripting language. Bro has many features such as highly customizable policies, high-speed large volume monitoring, no packet filter drops, real-time notifications and the possibility to work as distributed IDS with peer to peer communications between others Bro, in a clustering framework.

## III. Developed System

Bro is currently working into FITS as a distributed IDS, in which multiple sensors monitor and inspect network packets, classifying network traffic and sending their information to the manager. Once a worker sensor identifies a threat or an attack, a message is sent with the attacker features and the attack detected. This information is received by the manager and depending of the attack, it decides which kind of action is performed, communicating its decision to the openflow controller. As a result, Bro IDS analyzes the traffic and make decisions under the threaten flows in the systems.

There are two main approaches to analyze events and detect attacks:

- Anomaly based: Monitoring traffic is compared with a normal usage profile. All significant deviation for this normal profile is considered as a threat.
- Misuse based: Known threats patterns are identified on network traffic, looking for signature matching rules.

In our system anomaly and misuse detection are both applied. If a deliberately increase in TCP SYN packets from a source is seen by a sensor, a SYN Flood attack is detected as an anomaly. Then, the manager will decide to drop all packets, in order to avoid possibly damage induced by this flux. On the other hand, if packet payload for an unauthorized user is inspected and it contains the signature *"root"*, all the flows are deviated to a honeypot computer analyzing the attacker behavior, mitigating the attack and creating an attacker profile.

## IV. Conclusion and Future Work

We developed and experimented a smart framework for Intrusion Detection and Prevention based on the Bro IDS open source tool, which is currently working in the Testbed Platform FITS. Our goal is to perform a completely autonomous adaptative system with artificial intelligence to detect anomalies and auto-generate signatures, improving the detection accuracy.

## Acknowledgments

This work was supported by CNPq, CAPES, FINEP, CTIC and FAPERJ.

## References

[1] D. M. Lynch, "Securing against insider attacks," *Information Systems Security*, vol. 15, no. 5, pp. 39–47, 2006.

[2] V. Paxson, "Bro: a System for Detecting Network Intruders in Real-Time," *Computer Networks*, vol. 31, no. 23-24, pp. 2435–2463, 1999. [Online]. Available: http://www.icir.org/vern/papers/bro-CN99.pdf

[3] P. H. V. Guimaraes, L. H. G. Ferraz, J. V. Torres, A. F. Murillo P., M. E. Andreoni L., I. D. Alvarenga, C. S. Rodrigues, and O. C. M. Duarte, "Experimenting content-centric networks in the future internet testbed environment," in *Workshop on Cloud Convergence, ICC*, june 2013.