Chapter 20
Performance Analysis of Mail Clients on Low Cost Computer With ELGamal and RSA Using SNORT

Sreerama Murthy Kattamuri
Sreenidhi Institute of Science and Technology, India

Vijayalakshmi Kakulapati
Sreenidhi Institute of Science and Technology, India

Pallam Setty S.
Andhra University, India

ABSTRACT
An intrusion detection system (IDS) focuses on determining malicious tasks by verifying network traffic and informing the network administrator for restricting the user or source or source IP address from accessing the network. SNORT is an open source intrusion detection system (IDS) and SNORT also acts as an intrusion prevention system (IPS) for monitoring and prevention of security attacks on networks. The authors applied encryption for text files by using cryptographic algorithms like Elgamal and RSA. This chapter tested the performance of mail clients in low cost, low power computer Raspberry Pi, and verified that SNORT is efficient for both algorithms. Within low cost, low power computer, they observed that as the size of the file increases, the run time is constant for compressed data; whereas in plain text, it changed significantly.

DOI: 10.4018/978-1-5225-3870-7.ch020
INTRODUCTION

Intrusion Detection System (IDS)

An Intrusion Detection System (Mrdovic and Zajko, 2005) is a software tool or mechanism that watches network tasks for abnormal activities or policy violations and generates reports to a management station. Intrusion Detection and Prevention Systems (IDPS) (Albin and Neil, 2012) majorly dealt with finding probable occurrences, storing data and covering number of attempts.

Freeware Intrusion Detection Systems

- Prelude Hybrid DS
- AIDE
- Suricata
- Bro NIDS (Mohd Nazri Ismail and Mohd Taha Ismail, 2009)
- Samhain
- Snort (Hussein Alnabulsi, Md Rafiquil Islam and Quazi Mamun, 2014)
- ACARM
- OSSEC HIDS (Sang-Jun Han and Sung-Bae Cho, 2003)

Nids

Network Intrusion Detection Systems (Hornig C, 1984, Mrdovic and Zajko, 2005 and Yogesh Suryawanshi and Kakde, 2013) placed within the network to watch traffic to and from all devices over the network. Preferably, one would watch all inbound and outbound traffic, which create a bottleneck that would harm the general fastness of the network.

Hids

Host Intrusion Detection Systems (Cleary, Donnelly and Graham 2000) works on individual devices or hosts over the network. A HIDS (Maziero1 and Jamhour, 2007) watches both inbound and outbound packets from device and will intimate the administrator or user of malignant task.

Snort is a freeware NIDS (Tan and Sherwood, 2005) system, and can provide real-time traffic investigation and can log packets on IP networks.

RASPBERRY PI

All Raspberry Pi (Naik and Harode, 2016) models emphasize a Broadcom framework on a chip (SoC), which includes an ARM (Kumaresan and Manivannan M, 2010) perfect focal preparing unit (CPU) and an on-chip representation handling unit (GPU, a VideoCore IV). CPU runs anywhere from 700 MHz to 1.2 GHz for the Pi 3, on board memory broaden from 256 MB to 1 GB RAM. Secure Digital (SD) cards are use to accumulate the working framework and program memory in either the SDHC or MicroSDHC sizes. Most sheets have in the proximity of first and fourth USB openings, HDMI and composite video