

A SYSTEM AND METHOD FOR AUTONOMOUSLY FINGERPRINTING AND ENUMERATING INTERNET OF THING (IOT) DEVICES BASED ON NATED IPFIX AND DNS TRAFFIC

Abstract

This document describes a system and method for detecting the presence of Internet of Things (IoT) from network traffic that has undergone a Network Address Translation (NAT) process, i.e., NATed network traffic, regardless of whether the network traffic comprises IP Flow Information Export (IPFIX) type of traffic or Domain Name System (DNS) type of traffic. Such a capability is crucial as the adoption rate of IoTs have increased exponentially over the past few years. In order to protect IoTs from cyber-attacks, one would first have to understand what type of IoTs are being used, and how many/how widely used these IoTs are. Once the IoT landscape has been defined, cyber defenders may then dedicate resources to identify and subsequently address vulnerabilities that may be in these IoTs.

FIGURE 1