A Design and Implementation of an Intrusion Detection System for Smart Home IoT Devices

Brianna Thompson; Joong-Lyul Lee, PhD
University of North Carolina at Pembroke

Abstract

Developing an Intrusion Detection System (IDS) for Smart Home Internet of Things (IoT) devices is becoming more imperative with each technological advance in society. The introduction of IoT devices that simplify and automate everyday lives begin to pose a plethora of security risks. IoT devices lack the security measures to defend against virtual attackers, making them the weakest link in a secure infrastructure. This project proposes designing and developing a three-layer Intrusion Detection System (IDS) that detects using a machine learning algorithm when an attack is occurring to a device on a network and classifies the type of attack deployed.

Purpose

We will design and implement an IDS that can detect these events when a range of attacks on the IoT devices on a wireless network occur.

Significance

Apart from smart locks easily being opened and smart cameras easily turned off, if a seemingly harmless deauthentication attack was performed on the steering wheel of a wireless car, lives are put at risk. Therefore, an IDS that can detect malicious attacks is important because it will create an environment where the security of a home is not jeopardized when people are utilizing smart IoT devices in their homes.

What are IoT Devices?

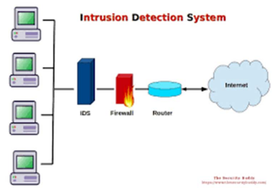
An **IoT device** is a piece of hardware with a sensor that transmits data from one place to another over the Internet. IoT devices are connected to the internet and collect, share, receive data and control devices such as door, TV, HVAC, lighting control system, and appliances.

Examples:

Amazon Echo Doorbell Cam Smart Thermostat

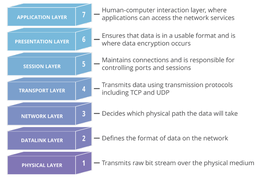
What is an IDS?

An **intrusion detection system** is a device or software application that monitors a network or systems for malicious activity or policy violations.



What are DDoS Attacks?

A **DDoS Attack** is an attempt to make an online service unavailable by overwhelming it with traffic from multiple unique IP addresses or machines. Different DDoS attack vectors target varying layers of a network connection.

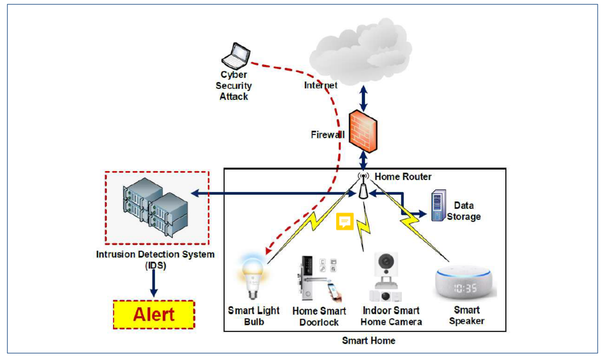


How to detect attack traffic?

The **IDS** profiles what normal behavior looks like on a network and changes defaults when necessary. We are using a **signature-based IDS methods**. Signature- based methods detects the attacks based on the specific patterns. For example, the number of bytes of number of 1's or 0's in the network traffic. The signature-based method detects on already known malicious traffic [1].

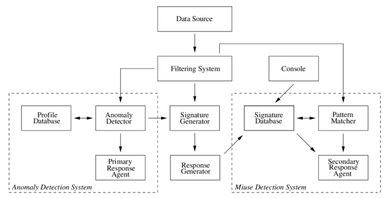
Methodology

The Intrusion Detection System is designed with three layers.
The **first layer** will be able to identify the IoT devices connected to a network.
The **second layer** will be able to identify if the device on the network is malicious or benign.
The **third layer** should be able to identify the type of attack that occurs. In this layer, we will design a detection algorithm applying a machine learning algorithm. The IoT devices chosen in the budget are strategically designed to mimic a smart home, while utilizing different kinds of IoT devices found on a network.



Experiment

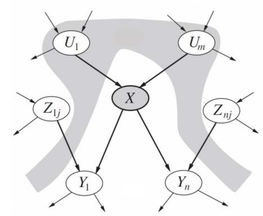
Why hybrid IDS?
In **a hybrid IDS**, (H-IDS), a host agent or system data is combined with network information to develop a complete view of the network system. The H-IDS is more effective than other IDS. Our H-IDS is a combination of SNORT's rule-based and the abductive reasoning model in the Bayesian Technique.



Why SNORT?
Snort is an open source network intrusion detection system (NIDS) created by Martin Roesch. Snort is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies.

Snort will be used to augment a rule-based system for the H-IDS.

Why the Bayesian Network?
A **Bayesian network** is a directed acyclic graph in which each edge corresponds to a conditional dependency, and each node corresponds to a unique random variable [2].



Abductive Reasoning Model

Abductive Reasoning is a mechanism for generating an inference that explains given observations with maximum likelihood. In modern literature, the abductive reasoning model is used to refer to using reasoning to justify a hypothesis, rather than the historical philosophical use to generate hypotheses [3].

We will be using the **Bayesian network** to identify an abductive reasoning model trained from pre-existing snort rules.

Results

Over the course of the semester I mostly conducted theoretical research. Through my research I have determined that to design and implement an intrusion detection system for Smart Home IoT Devices we need to use Snort rule-based system, through Linux (Kali or Ubuntu), on a Hybrid Intrusion Detection System.

The hybrid IDS will use signature-based methods to determine anomalies on the network. The hybrid system will implement machine-learning using snort rules with a probabilistic abductive reasoning model. The hybrid system will detect changes in traffic on the network and generate new rules by predicting unique combinations of conditions.

Conclusion and Future Work

In this research I have proposed the best methods for designing and implementing an intrusion detection system for smart home IoT devices. It is evident that our society's current inability to secure our smart home IoT devices poses a security threat that infringes on our freedom and safety.

Future work for this project involves developing working code that can detect the anomalies that go through the network. Throughout the semester I have developed materials that describe the current best methods other researchers have developed.

References

1. Ganesan, A., Parameshwarappa, P., Peshave, A., Chen, Z., & Oates, T. (2019). Extending Signature-based Intrusion Detection Systems With Bayesian Abductive Reasoning. *arXiv preprint arXiv:1903.12101*.
2. Davies, Scott. "Bayesian Networks." *What Are Bayesian Networks?*, www.cs.cmu.edu/afs/cs.cmu.edu/project/learn-43/lib/photoz/.g/web/glossary/bayesnet.html.
3. Douven, Igor, "Abduction", The Stanford Encyclopedia of Philosophy (Summer 2017 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/sum2017/entries/abduction/>.