Protecting Residential Internet-Enabled Devices with Multi-Factor Authentication

Yu Liu (Computer Science)
Advisor: Professor Craig A. Shue (Computer Science)

Introduction

In recent years, residential users have increasingly installed Internet-enabled devices in their homes. Unfortunately, these users often lacking cyber security expertise and do not sufficiently protect their devices, which can introduce some serious issues, such as:

- Potential espionage and the release of private information,
- Sabotage of connected devices,
- Physical attacks leveraging the devices, such as arson,
- Energy waste, meter fraud, and other financial crimes.

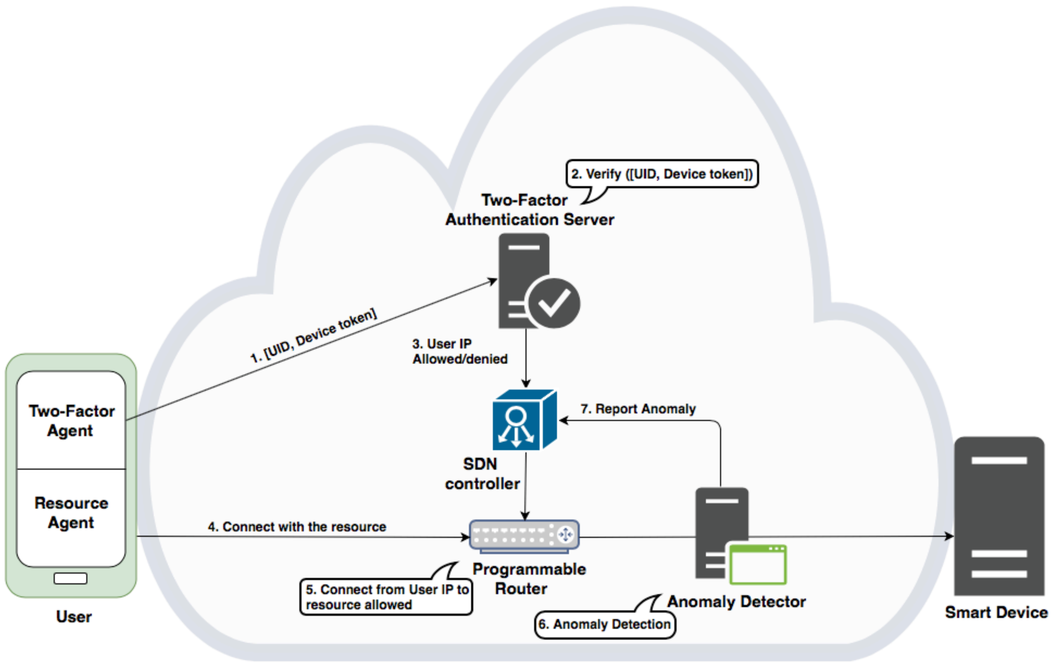
To address these problems, we propose an additional mechanism to ensure requests originate from legitimate users. We also analyze the commands to smart devices to detect anomalous and potentially malicious requests.

We seek to protect devices across manufacturers without requiring user expertise.

Research Questions

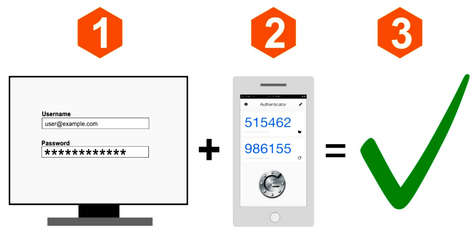
- How can we enable an additional authentication mechanism, beyond a username or password, to control access to devices?
- How can we detect or stop compromised members of the network from manipulating smart devices?
- How can such an approach ensure compatibility across device types and manufacturers?

Architecture



Approach

- Using the OpenFlow protocol, the residential router asks a cloud-hosted controller for guidance when it must make access control decisions.
- The controller analyzes network requests and decides whether to allow traffic.
  - Unless the client has successfully authenticated with the Two-Factor Authentication server, the controller denies the request.
  - For authenticated clients, the controller examines the network packets for unusual behavior.
- Anomaly Detection Features:
  - Whitelists of known packet sequences, sizes, direction, and payloads.
  - Differences in arrival time between packets in the sequence.



Evaluation Methodology

- Second-Factor Authentication: Determine whether system distinguishes authenticated clients from those that are unauthenticated.
- Anomaly Detection Sensitivity: Reinject slightly altered packets from the known valid data set and determine the detection rate and false classification values.
- Performance Analysis: Measure the end-to-end delay of interacting with a smart device with and without using our system. Perform timing measurements of key functions to characterize the overheads.

Expected Results

- Only registered users will have access to the smart device.
- Even minimally altered packets can be detected and discarded. We expect we will be able to fully customize enforcement for each smart device.
- We expect that the delays associated with the system will be small enough that they will not be perceptible by the user.

Future Plans

- Integrate additional anomaly detection techniques in the controller modules
- Examine more device types and work to automate signature generation