Security Monitoring of IoT Communication

Malombe Victor

Digital Learning Assistant

@iLabAfrica

Quick Overview

Introduction

Research Questions

Research Gap

Methodological Approach

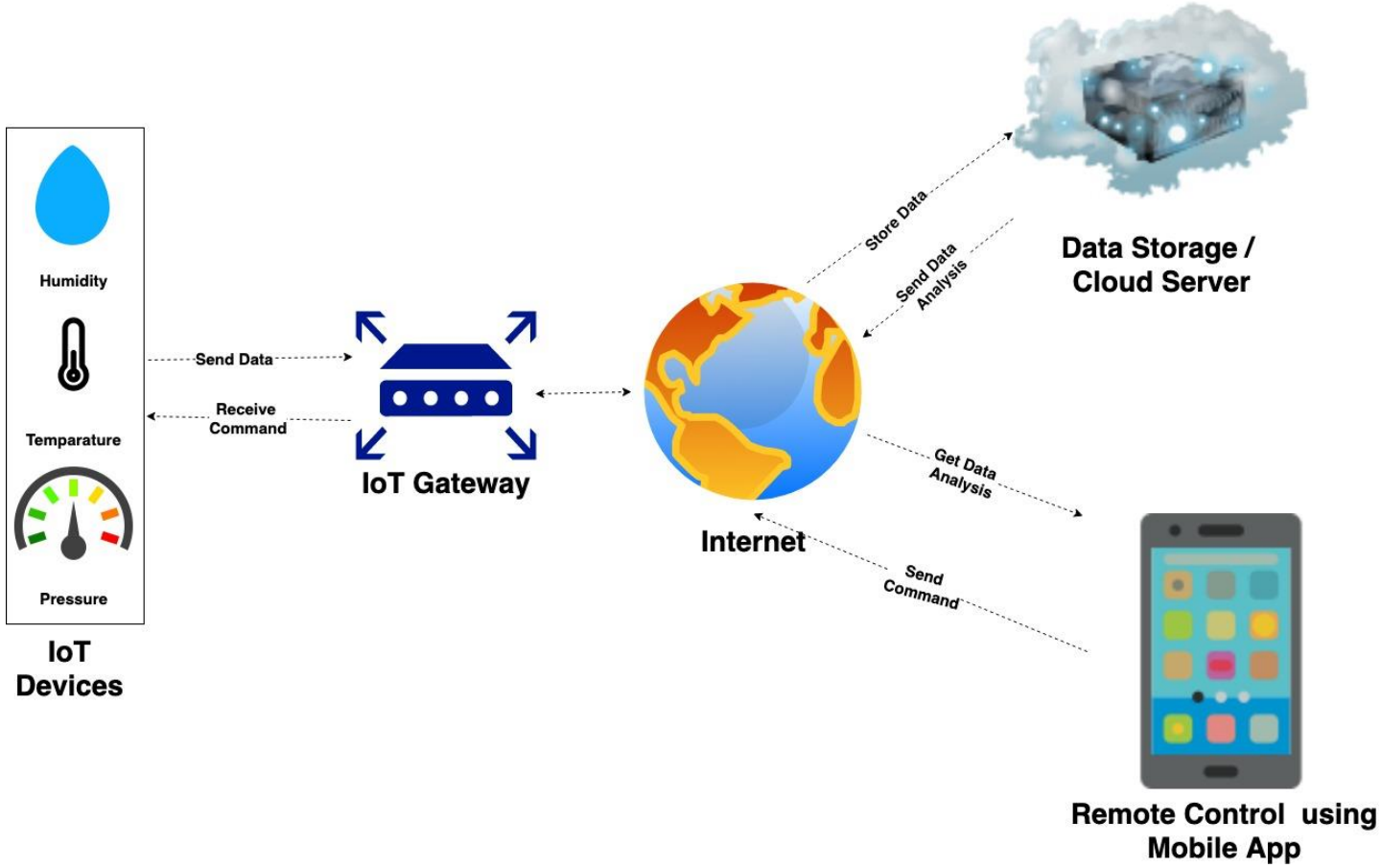
Validation

What is IoT?

Network of devices with an IP address that have the capability of sensing, collecting and sending data using embedded sensors, communication hardware and processors.

- Industrial devices
- Wearable devices
- Healthcare devices
- Home devices

IoT Concept


Humidity
Temparature
Pressure
IoT Devices
Send Data
Receive Command
IoT Gateway
Internet
Store Data
Send Data Analysis
Data Storage / Cloud Server
Get Data Analysis
Send Command
Remote Control using Mobile App

IoT Concept

Sensing Technology	• Sensors embedded in the devices sense a wide variety of info from their surroundings
IoT Gateways	• Bridge gap between the IoT device (internal network) & the end user (external network)
Cloud Server/Data Storage	• Store & analyse data
Remote Control using Mobile App	• Monitor, control, retrieve data and take specific action on IoT devices remotely

IoT Threats

IoT devices include many software applications that are used to access the device remotely.

Due to the hardware constraints such as memory, battery, etc. these IoT applications do not include complex security mechanisms to protect the devices from attacks.

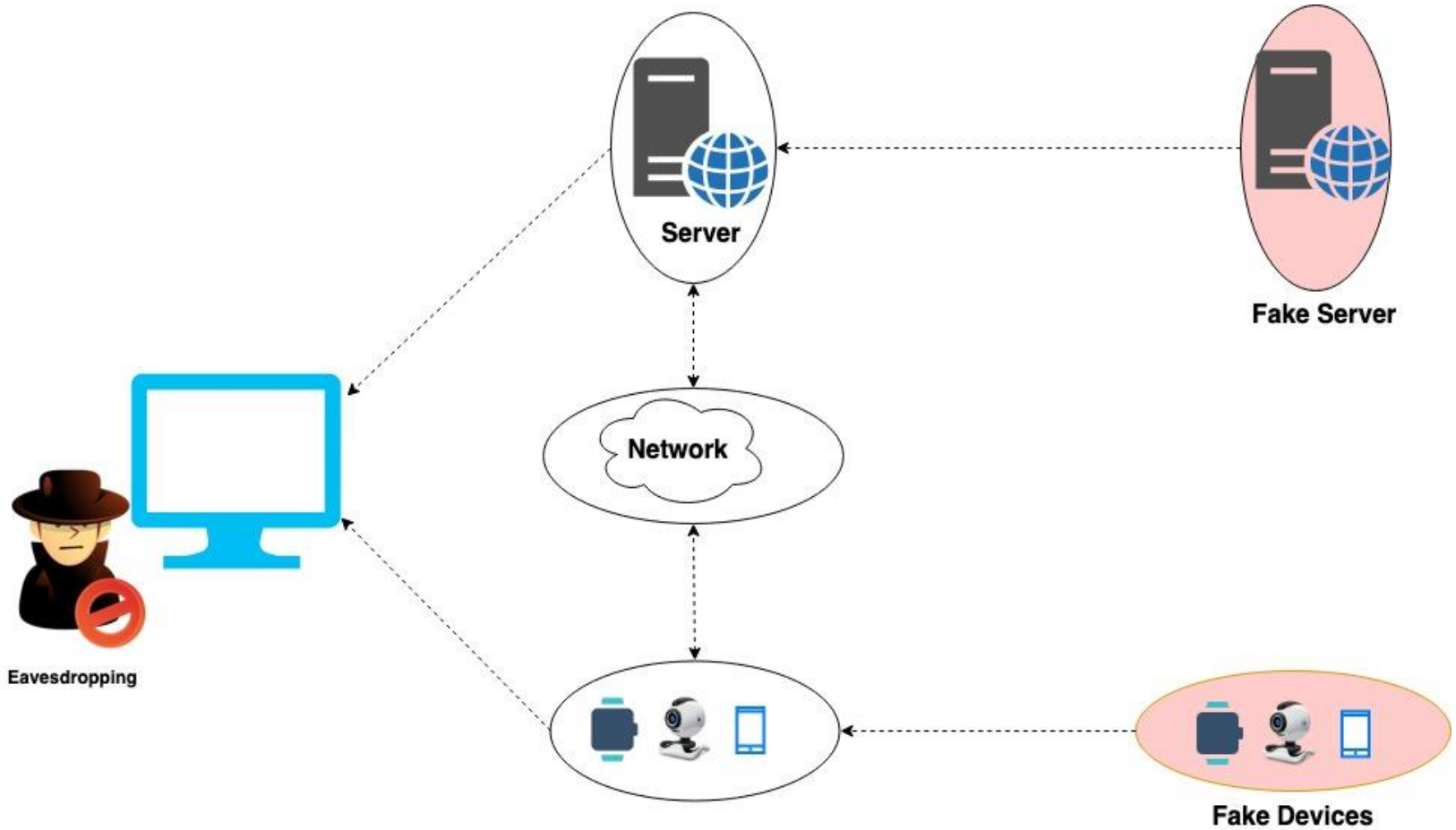
Security Challenges of IoT

- Lack of Security & Privacy
- Vulnerable Interfaces
- Physical Security Risk
- Lack of Vendor Support
- Default, Weak, Hardcoded Credentials
- Interoperability Issues

Attacks against IoT devices

- DDoS Attack
- Attack on HVAC Systems
- Rolling Code Attack
- BlueBorne Attack
- Jamming Attack
- Remote Access using Backdoor
- Remote Access using Telnet
- Sybil Attack
- Man-in-the-Middle Attack
- Replay Attack
- Forged Malicious Device
- Side Channel Attack
- Ransomware

General Hacking Scenario



Research Questions

1. What methods are used to monitor the security of IoT?
2. How secure are standard home automation sensors and gateways based on security assessments using standard penetration testing tools?
3. How can a system of IoT security monitoring, if implemented, improve the security of standard home automation sensors and gateways?
4. How well does the IoT security monitoring system address the gaps and challenges in standard home automation sensors and gateways?

Research Gap

- Traditional monitoring techniques are limited:
  - Internet Control Message Protocol (ICMP) logging,
  - Simple Network Management Protocol (SNMP), &
  - NetFlow.

ICMP Logging

ICMP (rfc792) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information such as:

- When a datagram cannot reach its destination,
- When the gateway does not have the buffering capacity to forward a datagram, and
- When the gateway can direct the host to send traffic on a shorter route.

The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

SNMP

Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Implementation issues: SNMP implementations vary across platform vendors.

Security implications: A significant number of software tools can scan the entire network over SNMP, therefore mistakes in the configuration of the read-write mode can make a network susceptible to attacks (Andrew & Mark, 2001).

NetFlow

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic.

Collecting, visualizing, and reporting on IoT device flow data is an extremely effective mechanism for reducing security risks associated with IoT devices.

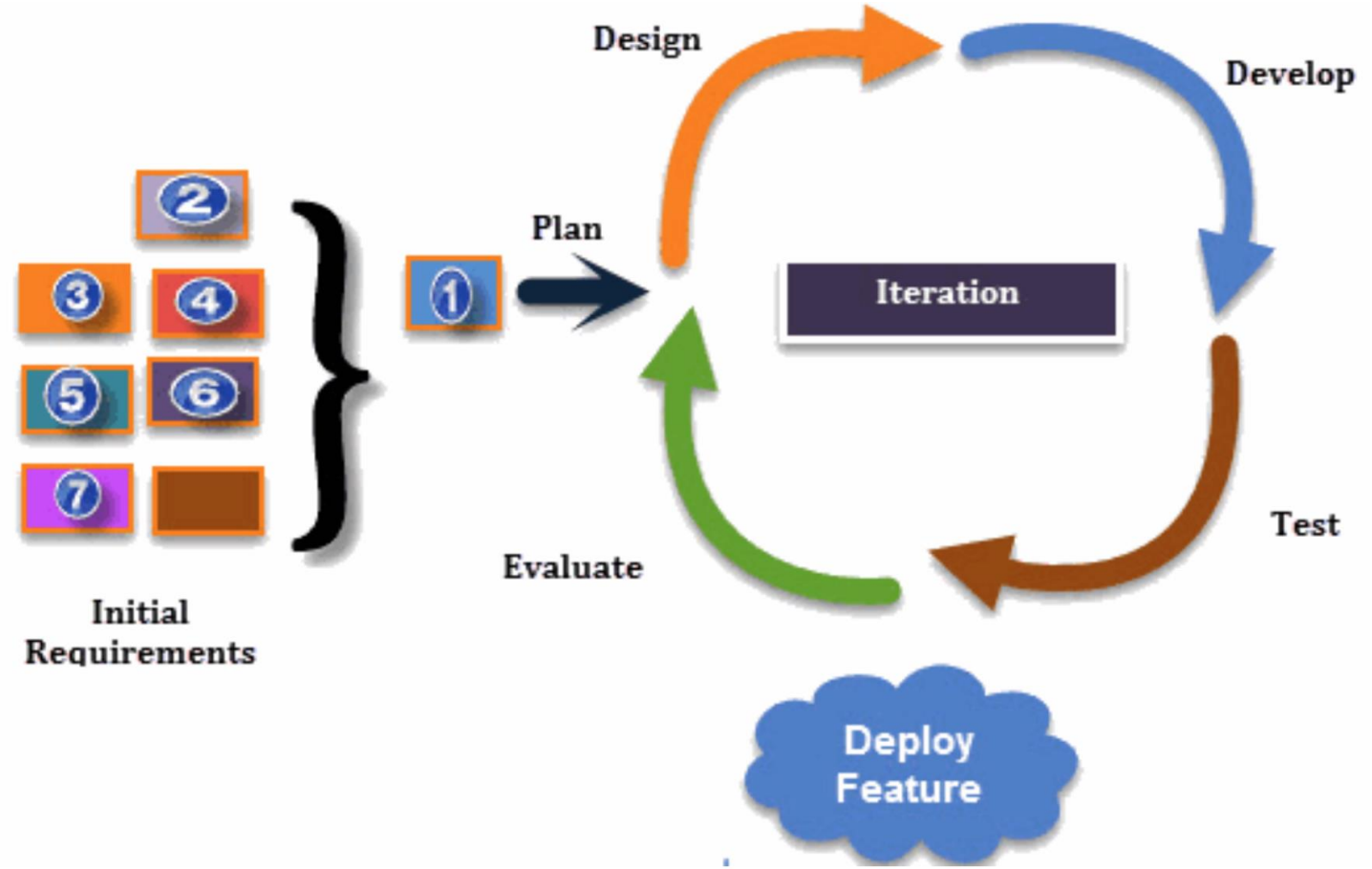
Extension of traditional systems

NEW SNMP OBJECTS,

EXTENDED IPFIX RECORDS, AND

PROVIDING DETECTION OF SELECTED ATTACKS ON THE SIEM SIDE.

Research Methodology: Agile



Research Work Plan

Examine standard communication of IoT devices

Review traditional monitoring techniques

Perform typical attacks against IoT devices

Develop a system of monitoring of these IoT devices and communication which requires extension of traditional systems

Validation

Implementing typical attacks and see how these attacks can be detected using proposed monitoring techniques.

Thank You

References

- Andrew G. Mason & Mark J. Newcomb (2001). Cisco Secure Internet Security Solutions. Cisco Press. ISBN 9781587050169.