# Securebox
# A Platform for Smarter and Safer Networks

Ibbad Hafeez, Aaron Yi Ding, Lauri Suomalainen,
Sasu Tarkoma

University of Helsinki

# Progress

- Agenda
- Motivation
- Goals
- Platform:
  - Design, Architecture, Deployment, Implementation
- Use cases
- Challenges & State of the art

# Motivation

- Bring Your Own Device in Enterprises.
- Lack of coordination for network management.

Insecure SOHO Networks

Internet of
(too many)Things

# Use Network data for improving network

- (Not so) efficient use of terabytes of network data.

# Goals

- Low Cost.
  - Can be deployed at SOHO.
- Easy to manage and deploy.
  - Does not need professionals.
- Scalable.
  - Use as much you want, Pay as much you use.
- Robust.
  - Self improving and healing
- Interactive.
  - Better user experience

# Progress

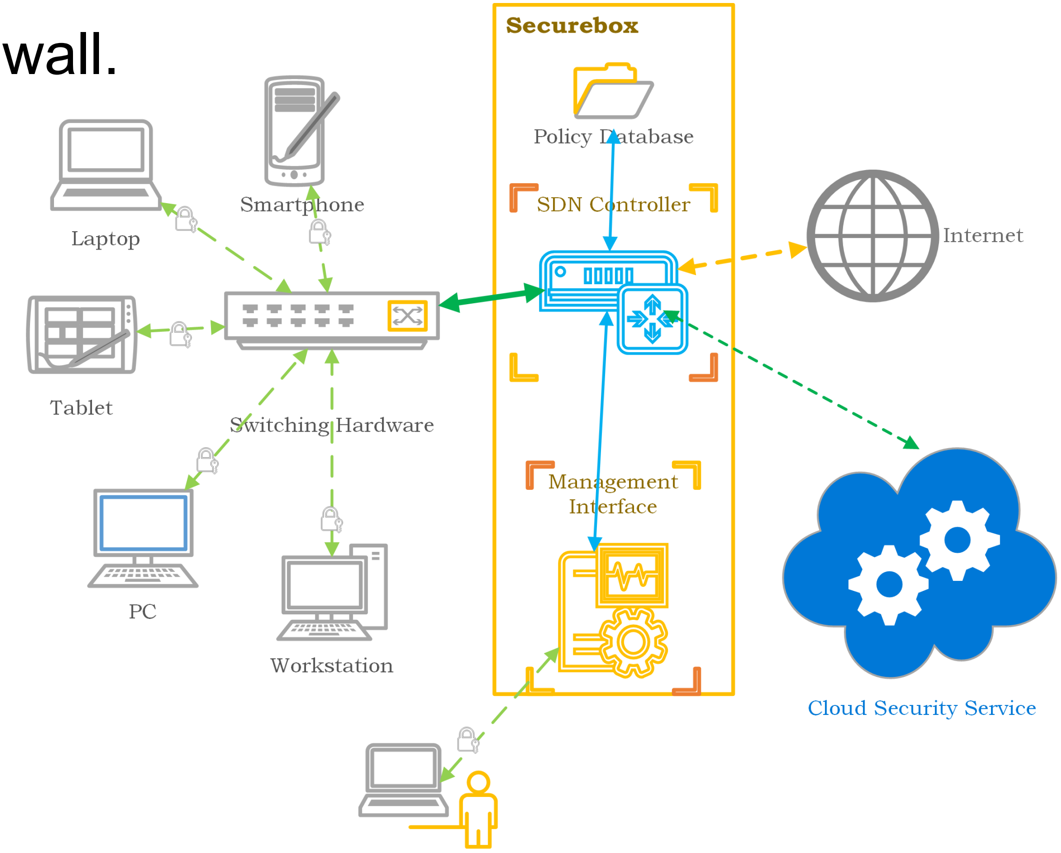
- Agenda
- Motivation
- Goals
- **Platform**:
  - Design, Architecture, Deployment, Implementation
- Use cases
- Challenges & State of the art

# Design

- Network Management and Security as a Service.
- Decoupling middleboxes from the network.
    - Automated configuration updates for software based middleboxes.
- Global view of the network for better management and analysis.
- Automated management, threat detection and configuration at network vantage points.
- Proactive, collaborative security
- Notifications about network operations, threats (network and devices) etc.

# Architecture: Securebox (Sensor at the edge)

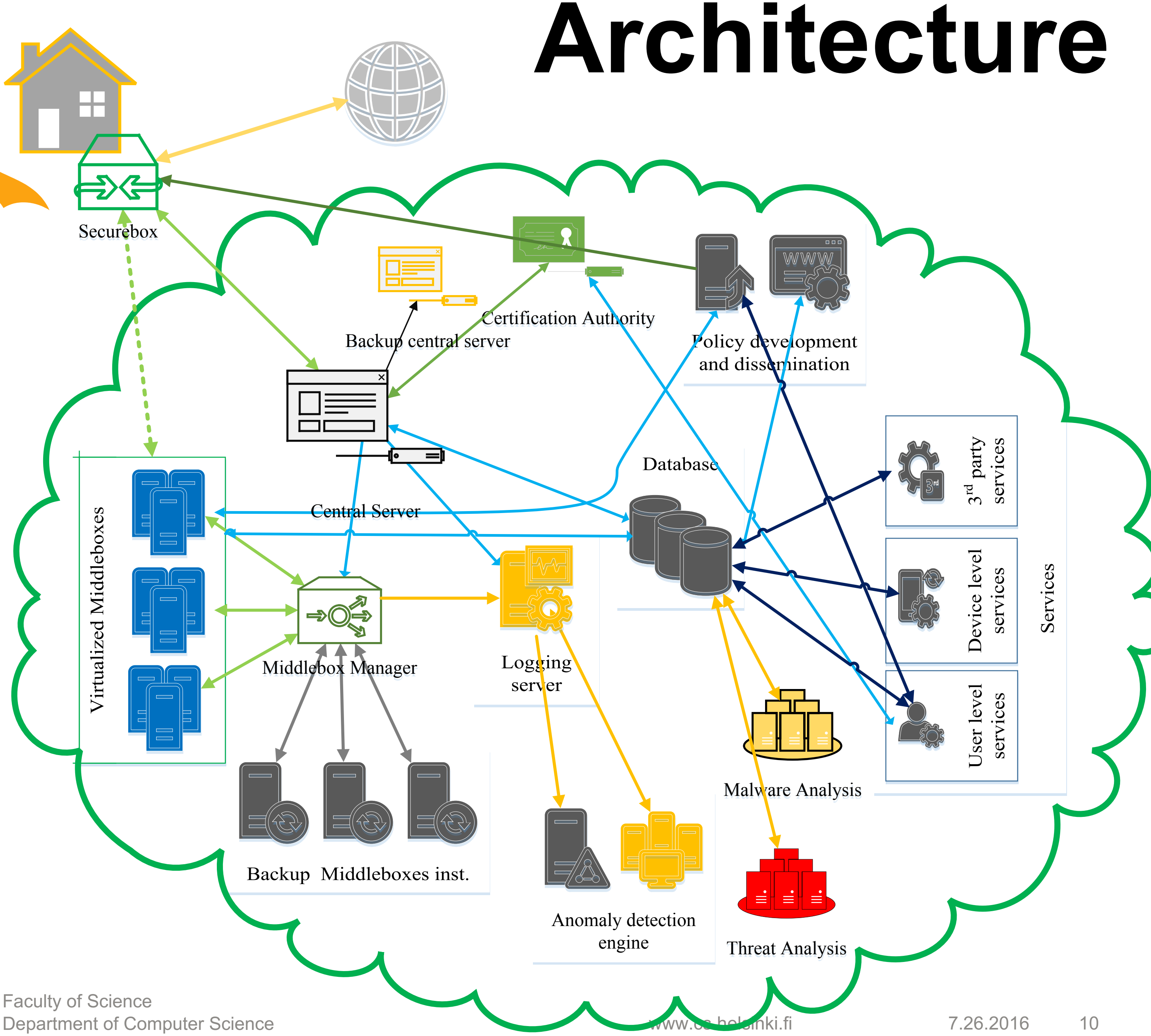
- SDN-capable access point for network edge.
- Dynamic firewall.



# Architecture
# Security and Management Service

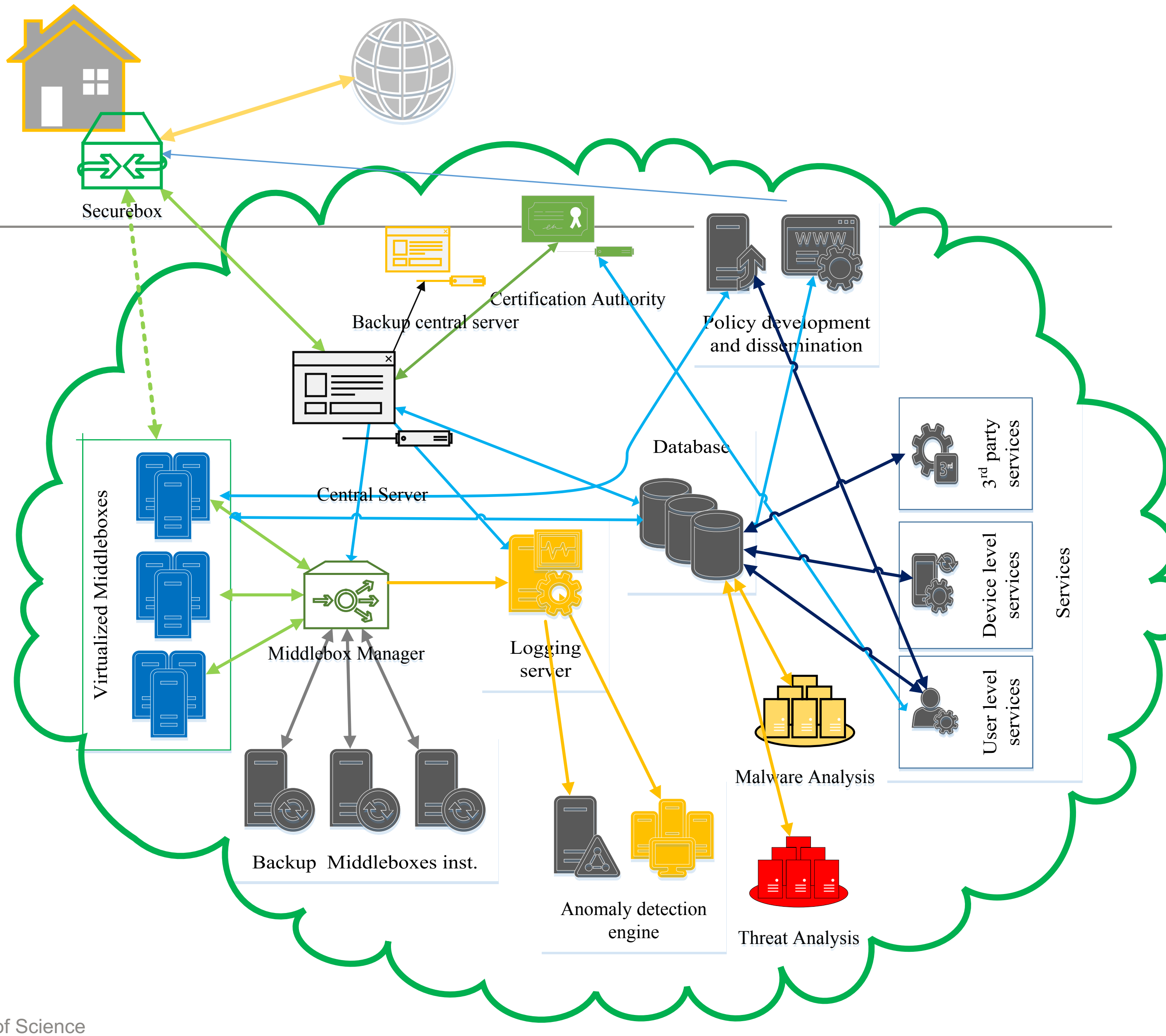
- Security and Management Service
  - User management.
  - Device management.
  - Service mobility.
    - Device roaming across APs.
  - Collaborative Security
  - Micro security services and virtualized middlebox deployment.
  - Network traffic data analysis.

# Architecture

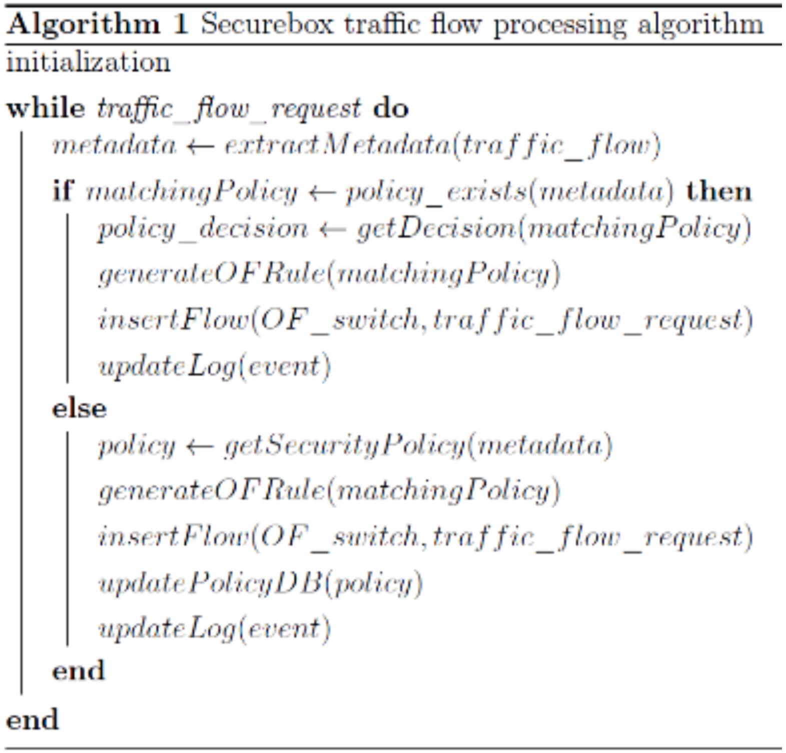


# Architecture

## Security and Management Service

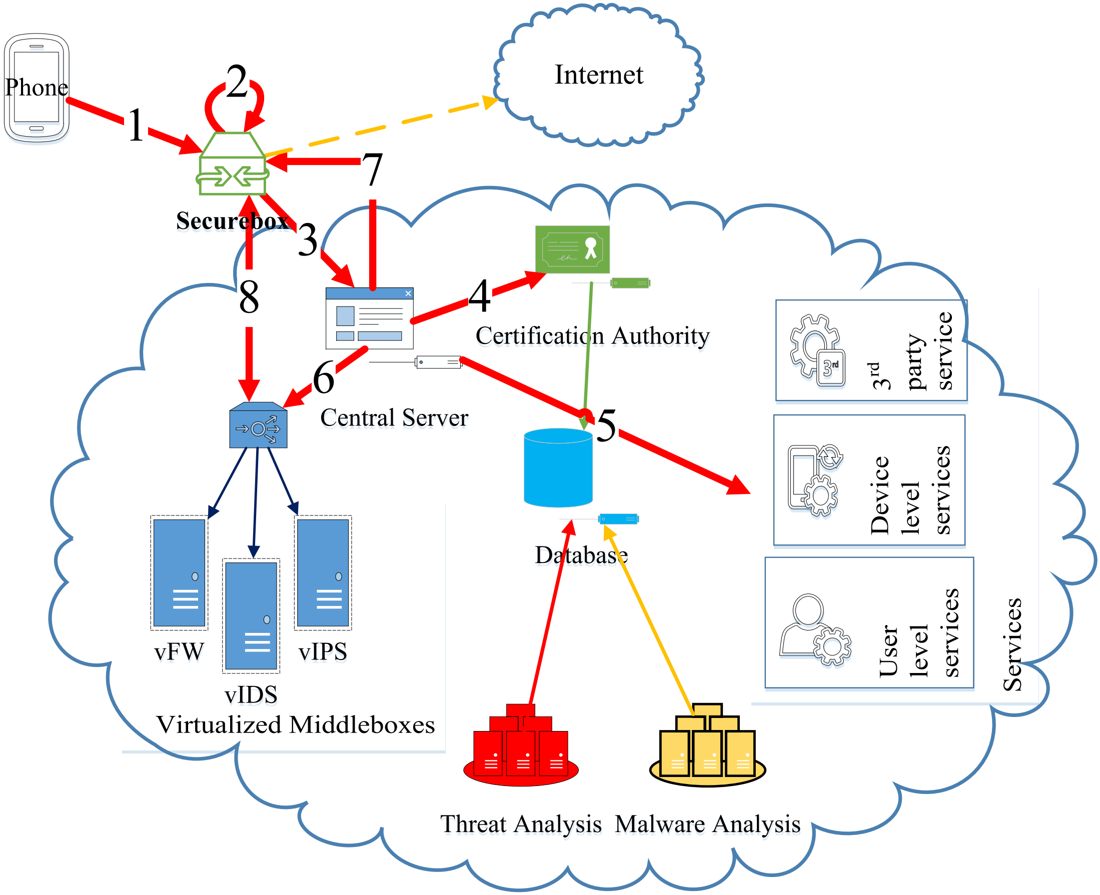


# Functioning



**Algorithm 1** Securebox traffic flow processing algorithm

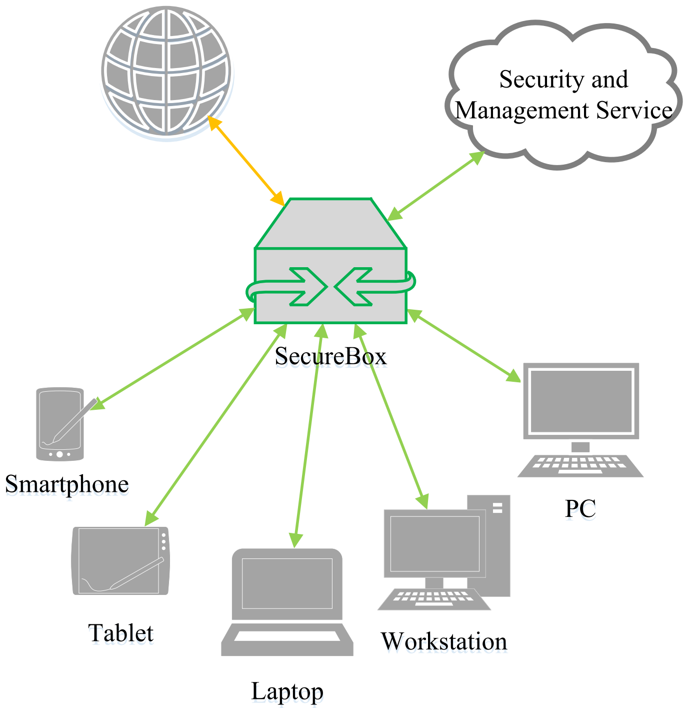
```
initialization
while $traffic\_flow\_request$ do
    $metadata \leftarrow extractMetadata(traffic\_flow)$
    if $matchingPolicy \leftarrow policy\_exists(metadata)$ then
        $policy\_decision \leftarrow getDecision(matchingPolicy)$
        $generateOFRule(matchingPolicy)$
        $insertFlow(OF\_switch, traffic\_flow\_request)$
        $updateLog(event)$
    else
        $policy \leftarrow getSecurityPolicy(metadata)$
        $generateOFRule(matchingPolicy)$
        $insertFlow(OF\_switch, traffic\_flow\_request)$
        $updatePolicyDB(policy)$
        $updateLog(event)$
    end
end
```



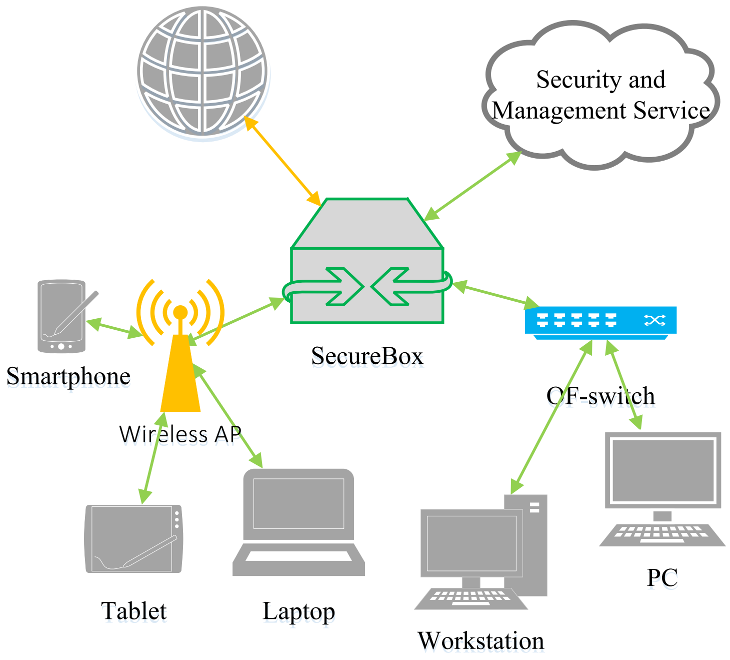
# Goals (Recap)

- **Low Cost**
  - Security and Management as a Service based solution with minimal hardware required.
- **Easy to manage and deploy**
  - Automated management with minimal configuration.
- **Scalable**
  - Cloud resources to scale.
- **Robust**
  - Automated analysis, self learning system (with minimal supervision).
- **Interactive**
  - User involvement through feedback and notification.

# Deployment Models



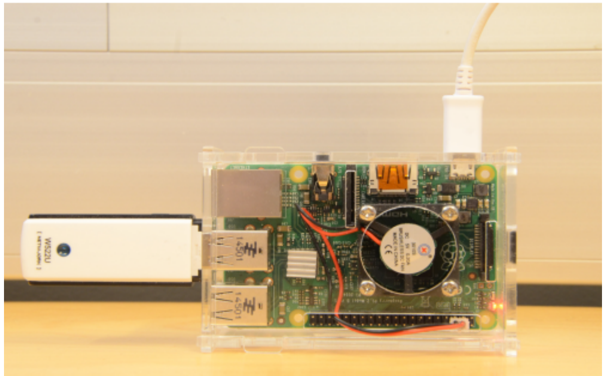
Securebox as AP



Securebox as SuperAP

# Implementation Securebox

- Hardware
  - FitPC3 (Mobicom, 2015)
  - Raspberry PI (SEC, 2016).
- Floodlight SDN Controller
- Open vSwitch
- Lightweight policy storage (file-based, SQLite).
- Can be included in IoT hubs.



# Architecture
# Security and Management Service

- Web application
  - User, Device, Securebox management.
  - Network policy management.
- Mobile device notifications.
- Amazon, Google, Azure cloud.
- Kubernetes cluster (Lauri Suomalainen)
  - Docker containers.

# Progress

- Agenda
- Motivation
- Goals
- Platform:
  - Design, Architecture, Deployment, Implementation
- **Use cases**
- Challenges & State of the art

# Home and Small Office Networks Deployment Preferences

- Securebox deployed as APs.
  - Sensors in edge networks.
  - Data collection.
- SMS maintained by a service provider
  - User subscribes to the services.
  - Micro (security) services.
  - Leased middleboxes for traffic analysis.

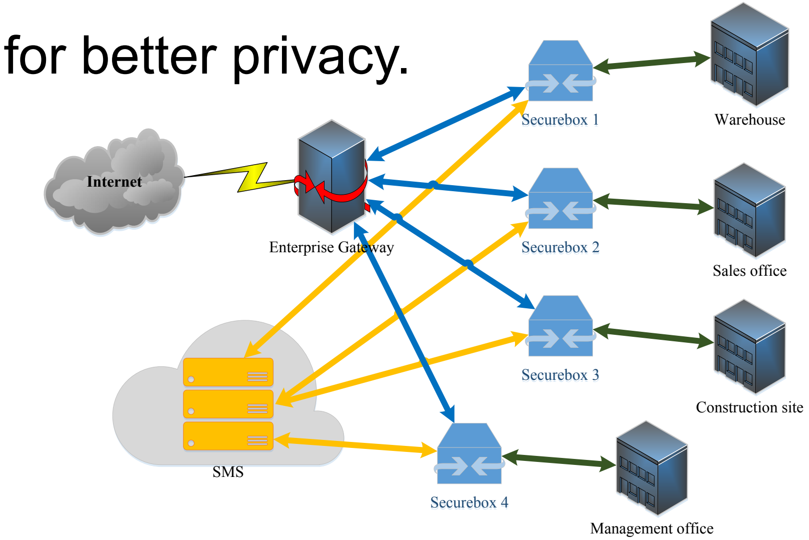
# Home and Small Office Networks

## Advantages

- Automated Network management.
- Enterprise grade security for SOHO users.
- Better device, network management.
  - Data usage, data privacy.
- Block botnet, spam, ransomware.
- User interactive system.
  - Notifications, updates, feedback.

# Enterprise Environments Deployment Preferences

- Securebox
  - Replace APs at network vantage points.
- SMS
  - Centrally managed.
  - In-house deployment for better privacy.



# Enterprise Environments Advantages

- Central control over the network.
  - Less management overhead.
  - Less human resource required; automated configuration updates.
- Coherent network policies across enterprise.
  - Avoid configuration loopholes.
- Lower deployment costs.
- Efficient use of enterprise network traffic data.
- Better scalability of networking security infrastructure i.e. Middleboxes.

# Setting up secure Wi-Fi environments

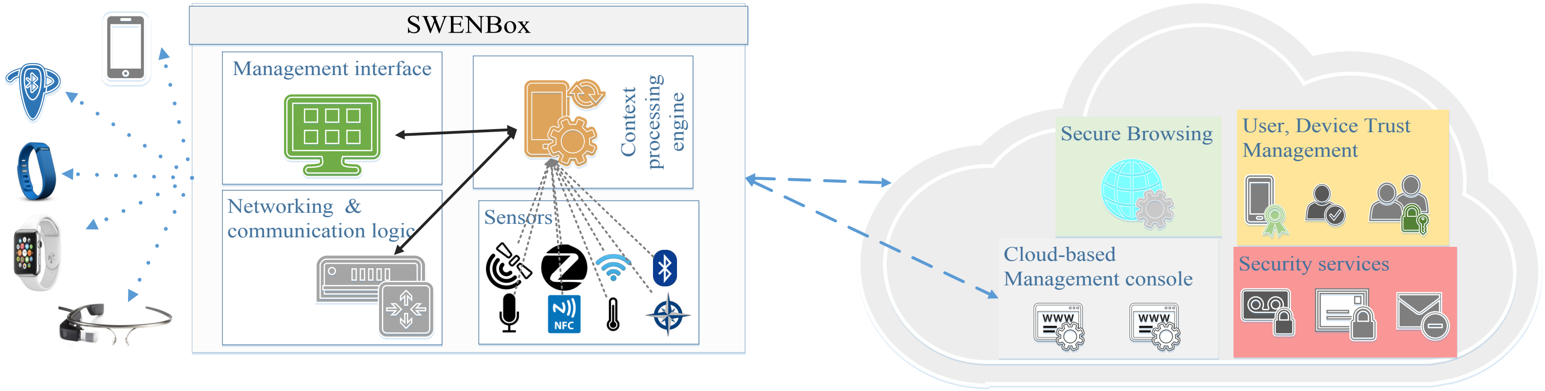
- Problem:
  - Leakage of shared PSK from compromised IoT device.
- Solution
  - Using device specific PSKs e.g. Private PSK, Dynamic PSK.
  - Still does not block device impersonation attacks.
- Securebox
  - Supports device specific PSK with dynamic access control and other security services.
  - Attacker using device impersonation will get limited access.

# Research
# Use cases

- Setting up Testbeds
  - Network models.
  - IoT Environments.
- Testing performance of malware, botnet, spam detection approaches.
- Develop and testing of software based middleboxes.

# SWENbox: Software-defined Wearable Network with Security Analysis

- Goals.
  - Big trust from little things.
  - Run-time secure pairing, device associations, resource sharing, secure D2D communications.
  - Secure sensing and privacy for wearable devices.


SWENBox
Management interface
Context processing engine
Networking & communication logic
Sensors
NFC
Secure Browsing
User, Device Trust Management
Cloud-based Management console
Security services
WWW
WWW

# SWENbox Features

- Software-defined networking for wearables.
  - Secure interactions with untrusted IoT devices.
  - Selective isolation of compromised devices.
- Using context-sensing for:
  - Second-factor authentication.
  - Trust ensemble using cloud analytics.
  - Contextual fencing
- Mitigate impersonation, replay attacks.w

# Progress

- Agenda
- Motivation
- Goals
- Platform:
  - Design, Architecture, Deployment, Implementation
- Use cases
- **Challenges & State of the Art**

# Challenges

- Latency
  - Traffic is analyzed remotely → Design choices (Policy database updates & local cache (Zipf's Law))
- Privacy
  - Remote analysis of user data → Use minimal data from user
- Attacks against the system
  - Rogue secureboxes launching DDoS → Logging & anomaly detection.
  - Request for falsified traffic queries → Human/ Automated supervision, feedback loop
- False positives
  - Threat and Malware analysis → Feedback loop, incentivized learning

# State of the Art

- **Remote deployment of middleboxes**.
  - J. Sherry et al. (SIGCOMM, 2012); C. Lan et al. (NSDI, 2016); SENSS (SIGCOMM, 2014)
- **Middlebox as a Service**.
  - Blackbox (SIGCOMM, 2015); DPI-as-a-Service (CoNEXT, 2014)
- **Improving Home Networks**.
  - N. Feamster (HomeNets, 2010); Tialong et al., (HotNets 2015); T. Zachariah (HotMobile, 2015); uCap (Ubicomp, 2012); SpaceHub (HotNets, 2015); Contextual Router (SOSR, 2016)
- **IoT Security**.
  - Z. K. Zhang et al. (ASIA-CCS, 2015); C. Liu et al. (Elsevier, 2014); E. Farnandes (SOSP, 2016)

# Products

Bitdefender Box $399
http://www.bitdefender.com/box/

F-Secure Sense
$199 (inc. 12 month membership)
https://sense.f-secure.com/

Google onHub $199
https://on.google.com/hub/

Dojo $99
https://www.dojo-labs.com/product/dojo/#

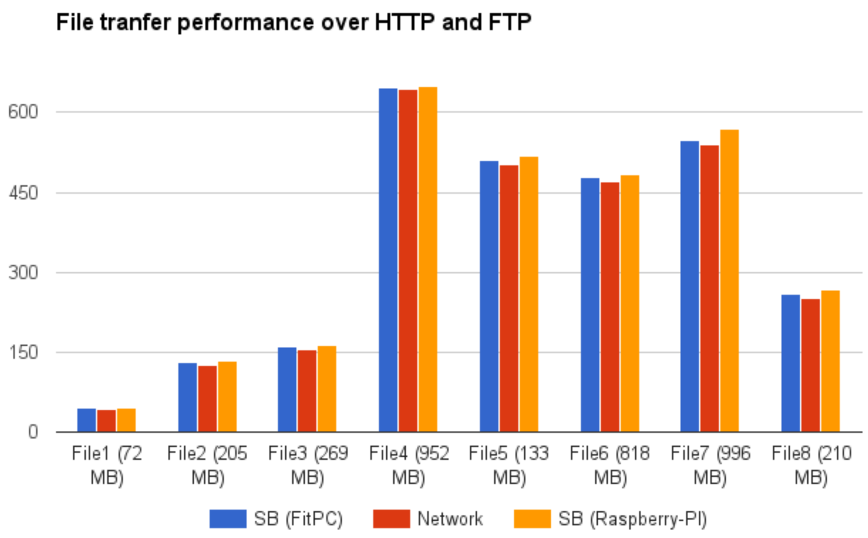
# Air gapped (isolated) networks weaknesses

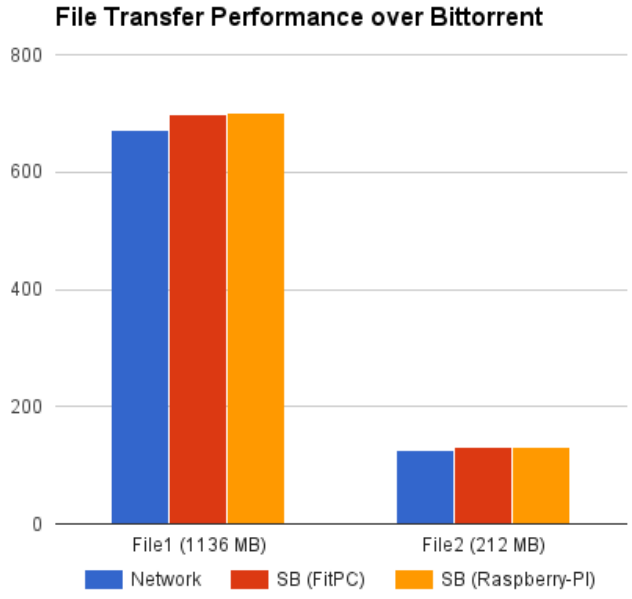
- Isolated and dedicated.
- Difficult to setup and maintain.
- What happens when the attacker is in the network?
    - Nothing ☹

# Thank You

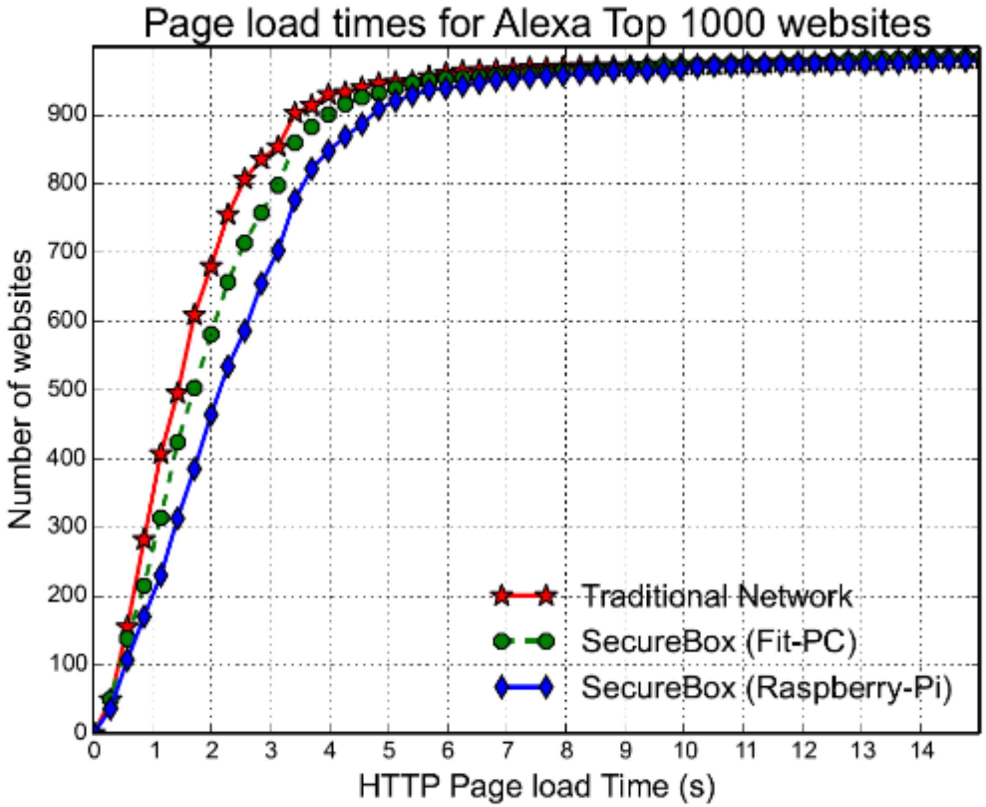
https://www.cs.helsinki.fi/group/close/secDemo/securebox.html
ibbad.hafeez@helsinki.fi

# Latency


File tranfer performance over HTTP and FTP
600
450
300
150
0
File1 (72 MB)
File2 (205 MB)
File3 (269 MB)
File4 (952 MB)
File5 (133 MB)
File6 (818 MB)
File7 (996 MB)
File8 (210 MB)
SB (FitPC)
Network
SB (Raspberry-PI)

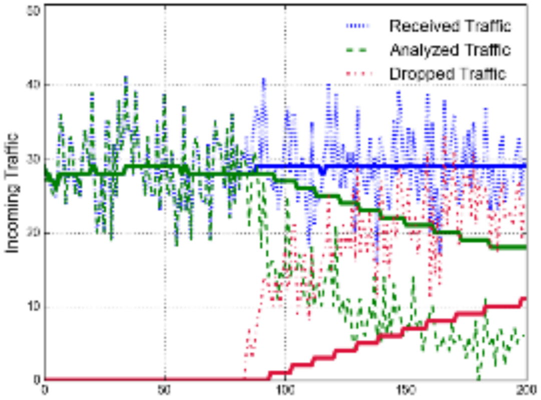

File Transfer Performance over Bittorrent
800
600
400
200
0
File1 (1136 MB)
File2 (212 MB)
Network
SB (FitPC)
SB (Raspberry-PI)

# Latency

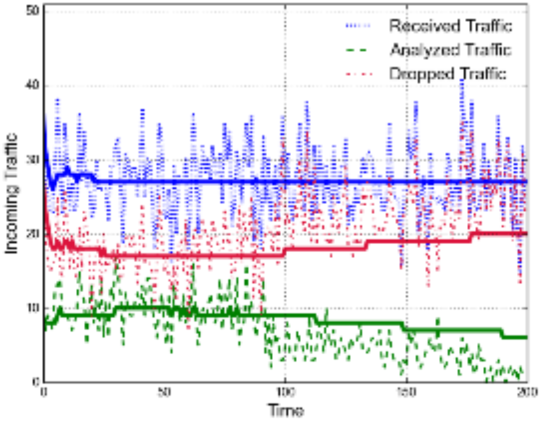

Page load times for Alexa Top 1000 websites
Number of websites
0
100
200
300
400
500
600
700
800
900
HTTP Page load Time (s)
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Traditional Network
SecureBox (Fit-PC)
SecureBox (Raspberry-Pi)

# No collaboration

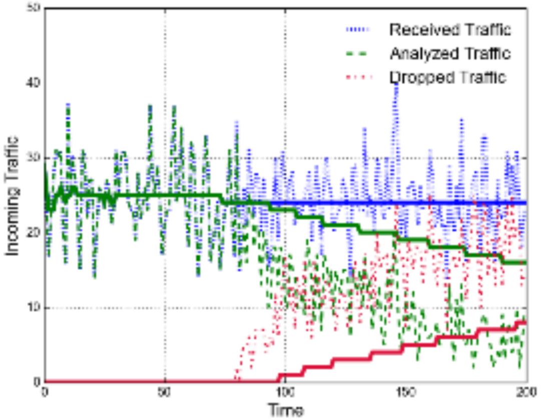
N1



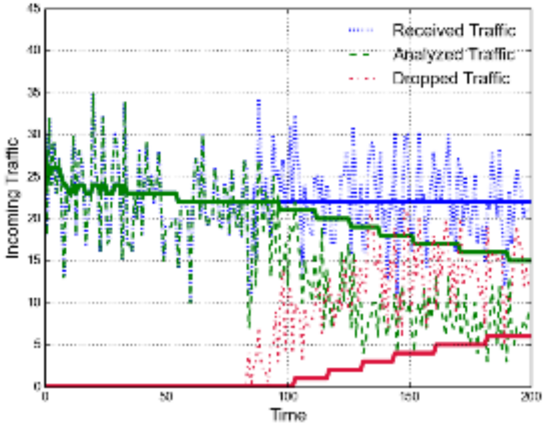
N2



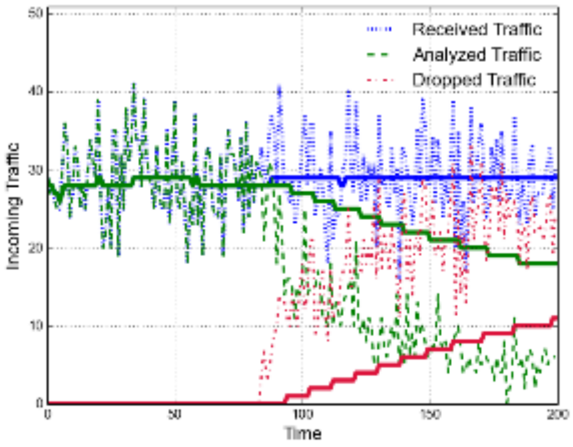
N3



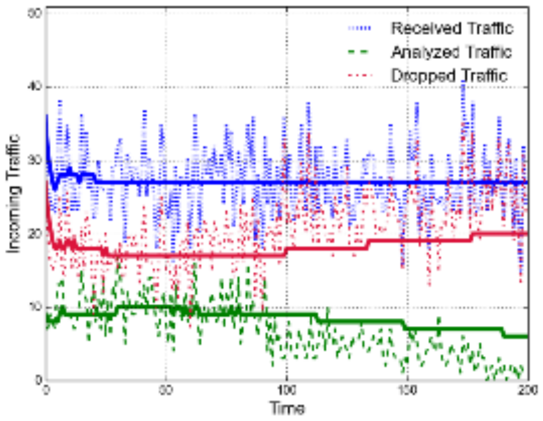
N4



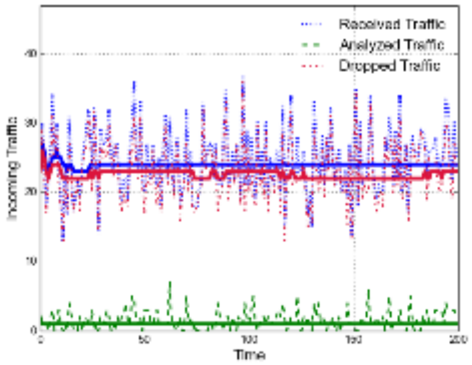
# Collaboration



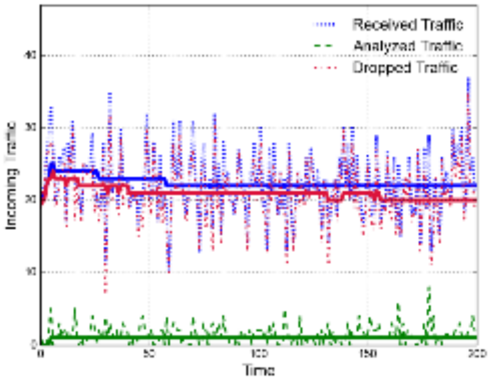
N1



N2



N3



N4

# Images

- https://upload.wikimedia.org/wikipedia/commons/thumb/c/c6/Botnet.svg/500px-Botnet.svg.png
- https://s3.amazonaws.com/ydtimages/~yourdai7/wp-content/uploads/2016/03/09094045/iot.jpg
- http://tlists.com/wp-content/uploads/2016/01/How-to-secure-your-home-network.png
- http://blogs.cisco.com/wp-content/uploads/wireless-network.png
- https://cdn.meme.am/instances/47510205.jpg