TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of computer science

avast

Transparent Microsegmentation in Smart Home IoT Networks

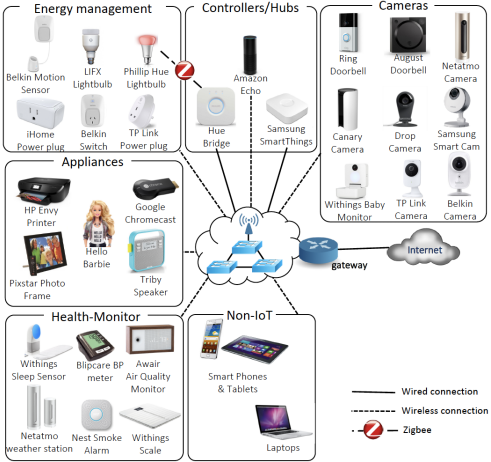
Amr Osman[1] Armin Wasicek[2] Stefan Köpsell[1] Thorsten Strufe[1]

[1]Chair of Privacy and Data Security
TU Dresden
firstname.lastname@tu-dresden.de
[2]*Avast Inc.*

HotEdge'20

Outline

Smart home IoT networks



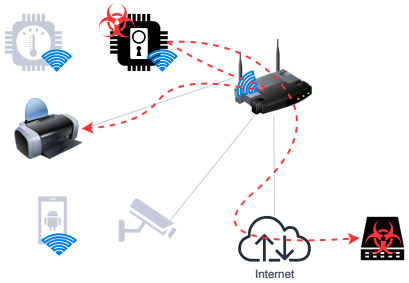
Problem statement

Communication setting:

- Mixed wired + wireless connectivity
- TCP/IP Protocol suite
- Ethernet as a L2 protocol (802.11 MAC addresses)

Threat model:

- Internal attacker
- Active
- Laterally moving
- Seeks: Reconnaissance, Data exfiltration, Unauthorized access, DoS, .. etc)



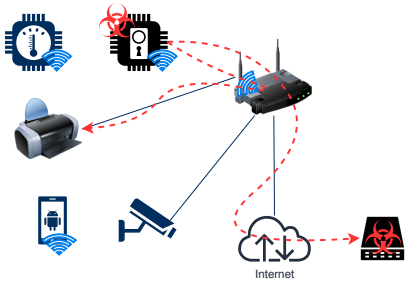
Problem statement

Communication setting:

- Mixed wired + wireless connectivity
- TCP/IP Protocol suite
- Ethernet as a L2 protocol (802.11 MAC addresses)

Threat model:

- Internal attacker
- Active
- Laterally moving
- Seeks: Reconnaissance, Data exfiltration, Unauthorized access, DoS, .. etc)



Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Requirements

- **Isolation**: controlling communication between devices within each microsegment, between microsegments, and external endpoints in the cloud or internet.
- **Scalability**: sustaining a large number of microsegments, IoT devices and home networks.
- **Edge-readiness**: virtual network functions in the edge cloud must seamlessly augment the home network.
- **Automatic segment allocation**: newly connected devices should be automatically recognized, identified and appropriately put into a microsegment.
- **Adaptability**: dynamically changing the current set of microsegments configuration at runtime as new devices are added to the smart home.
- **0-conf**: require no manual configurations for the residential gateway and the IoT end devices.

Existing solutions

Categories: Firewalls, VLANs, Overlays, Multiple APs, NAC-Servers, IP Subnets

Solution	Isolation	Scalability	Edge-ready?	Auto-alloc.	Adaptability	0-conf
Firewall	Can	No	No	No	Can	No
VLAN	Yes	4096	No	No	Can	No
VxLAN	Yes	2^{24}	No	No	Can	No
Multi-AP	Yes	~10	No	No	No	No
RADIUS	Can	No	No	No	Yes	No
Subnetsv4	Can	$\sim 2^{30} - 2$	No	No	No	No
MUD	Can	No	No	Yes	Can	No
Ours	*Yes*	2^{64}	*Yes*	*Yes*	*Yes*	*Yes*

Notes:

- VLANs are not well-suited for WLANs
- All existing solutions require complex manual configuration on the residential gateway, prior knowledge about the topology and are not transparent to the end user
- Some of the existing solutions require complex configurations for the IoT end devices and the infrastructure (e.g. RADIUS, Multi-AP, MUD)

Existing solutions

Categories: Firewalls, VLANs, Overlays, Multiple APs, NAC-Servers, IP Subnets

Solution	Isolation	Scalability	Edge-ready?	Auto-alloc.	Adaptability	0-conf
Firewall	Can	No	No	No	Can	No
VLAN	Yes	4096	No	No	Can	No
VxLAN	Yes	2^{24}	No	No	Can	No
Multi-AP	Yes	~10	No	No	No	No
RADIUS	Can	No	No	No	Yes	No
Subnetsv4	Can	$\sim 2^{30} - 2$	No	No	No	No
MUD	Can	No	No	Yes	Can	No
Ours	*Yes*	2^{64}	*Yes*	*Yes*	*Yes*	*Yes*

Notes:

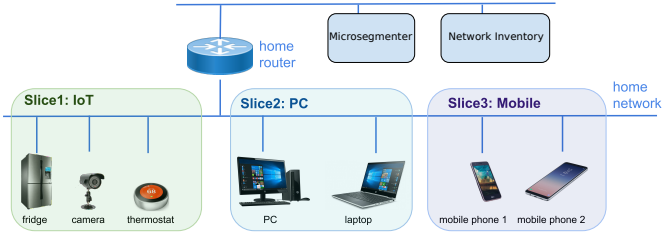
- VLANs are not well-suited for WLANs
- All existing solutions require complex manual configuration on the residential gateway, prior knowledge about the topology and are not transparent to the end user
- Some of the existing solutions require complex configurations for the IoT end devices and the infrastructure (e.g. RADIUS, Multi-AP, MUD)

Microsegmentation

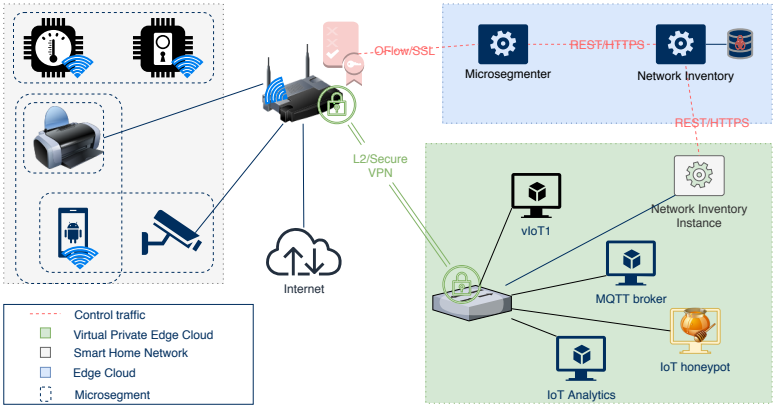
Two edge cloud VNFs are implemented: *Network Inventory* & *Microsegmenter*

- **Network Inventory**: Automatically fingerprints, scans and classifies devices based on functionality and security vulnerabilities
- **Microsegmenter**: Allocates devices to microsegments based on Network Inventory results

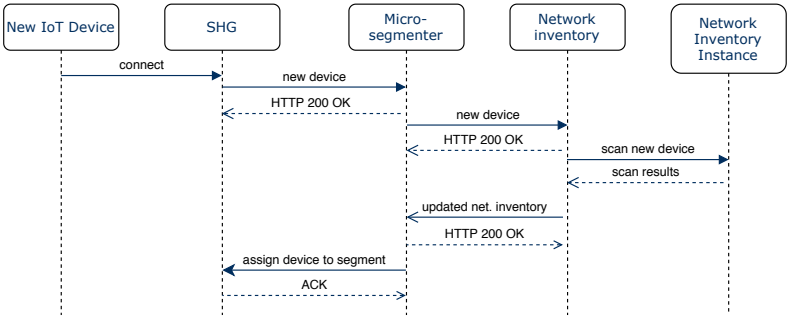
Strategy: Classify and isolate devices based on functionalities, i.e. Printers, Mobile Devices, Laptop/PCs, Cameras, ... etc)



System design

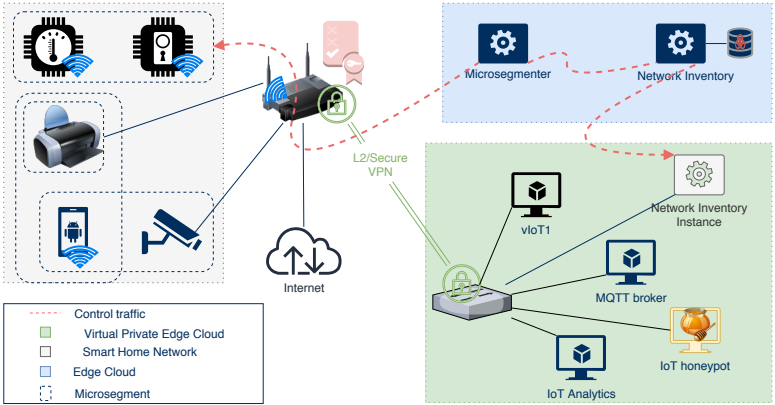


Transparent microsegmentation



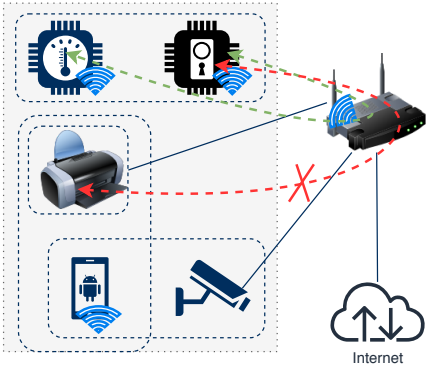
Automatic microsegment allocation

Transparent microsegmentation



Automatic microsegment allocation

Transparent microsegmentation



Network flows isolation inter- and intra- segments

Evaluation

- Used 3 different smart home network topologies with more than 28 different IoT devices from different vendors [1, 2, 3].
- Used well-known packet traces and IoT network vulnerability metrics from past literature.
- **Measured**: Scalability, Effectiveness, Impact on functionality
- **Case study**: Mirai infected webcam (65.85% attack surface reduction)

Evaluation

- Used 3 different smart home network topologies with more than 28 different IoT devices from different vendors [1, 2, 3].
- Used well-known packet traces and IoT network vulnerability metrics from past literature.
- **Measured**: Scalability, Effectiveness, Impact on functionality
- **Case study**: Mirai infected webcam (65.85% attack surface reduction)

Evaluation

- Used 3 different smart home network topologies with more than 28 different IoT devices from different vendors [1, 2, 3].
- Used well-known packet traces and IoT network vulnerability metrics from past literature.
- **Measured**: Scalability, Effectiveness, Impact on functionality
- **Case study**: Mirai infected webcam (65.85% attack surface reduction)

Evaluation

- Used 3 different smart home network topologies with more than 28 different IoT devices from different vendors [1, 2, 3].
- Used well-known packet traces and IoT network vulnerability metrics from past literature.
- **Measured**: Scalability, Effectiveness, Impact on functionality
- **Case study**: Mirai infected webcam (65.85% attack surface reduction)

Evaluation

- Used 3 different smart home network topologies with more than 28 different IoT devices from different vendors [1, 2, 3].
- Used well-known packet traces and IoT network vulnerability metrics from past literature.
- **Measured**: Scalability, Effectiveness, Impact on functionality
- **Case study**: Mirai infected webcam (65.85% attack surface reduction)

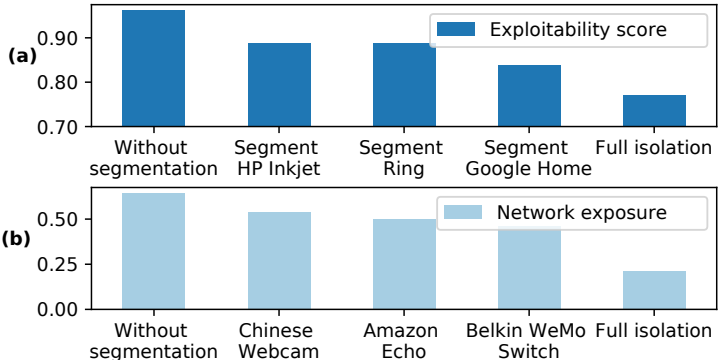
Scalability

Number of...	Count
Smart homes	2^{64}
Segments per home	2^{64}
Devices per segment	$2^{48} - 2$
OF rules required	$s[n(n+1) - 2] + 8$

Where:

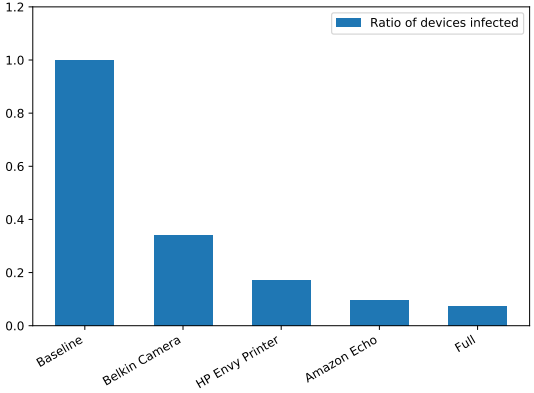
- s is the total number of segments
- n is the number of devices in a microsegment

Effectiveness



19% and **43%** reduction in exploitability score[2] and network exposure[3].

Case study: Mirai



65.85% attack surface reduction against an infected Belkin Camera

Transparency

From	To
HP Envy Printer	Laptop
Samsung Smart Cam	Belkin Motion Sensor
Samsung Smart Cam	Samsung Galaxy Tab
Belkin Motion Sensor	Samsung Smart Cam
Insteon Camera	Samsung Galaxy Tab
Samsung Galaxy Tab	Samsung Smart Cam

Only **2.16%** of the network flows were blocked due to functional microsegmentation

We also identified some flows in dataset that are *likely* malicious:

- HP Envy Printer → Laptop
- Insteon Camera → Samsung Galaxy Tab
- Belkin Motion Sensor ↔ Samsung Smart Cam (?)

Conclusion

- Introduced a novel edge cloud architecture to secure smarthome IoT networks against an internal adversary via microsegmentation.
- Implemented one transparent microsegmentation strategy according to functional groups.
- Evaluated our approach on 3 different topologies using different network exploitability metrics.
- **In the best case, we acheived a 65.85% attack surface reduction against a Mirai-infected webcam at the cost of blocking 2.16% of the otherwise-accepted flows in the network.**

Conclusion

- Introduced a novel edge cloud architecture to secure smarthome IoT networks against an internal adversary via microsegmentation.
- Implemented one transparent microsegmentation strategy according to functional groups.
- Evaluated our approach on 3 different topologies using different network exploitability metrics.
- **In the best case, we acheived a 65.85% attack surface reduction against a Mirai-infected webcam at the cost of blocking 2.16% of the otherwise-accepted flows in the network.**

Conclusion

- Introduced a novel edge cloud architecture to secure smarthome IoT networks against an internal adversary via microsegmentation.
- Implemented one transparent microsegmentation strategy according to functional groups.
- Evaluated our approach on 3 different topologies using different network exploitability metrics.
- In the best case, we acheived a 65.85% attack surface reduction against a Mirai-infected webcam at the cost of blocking 2.16% of the otherwise-accepted flows in the network.

Conclusion

- Introduced a novel edge cloud architecture to secure smarthome IoT networks against an internal adversary via microsegmentation.
- Implemented one transparent microsegmentation strategy according to functional groups.
- Evaluated our approach on 3 different topologies using different network exploitability metrics.
- In the best case, we acheived a 65.85% attack surface reduction against a Mirai-infected webcam at the cost of blocking 2.16% of the otherwise-accepted flows in the network.

Conclusion

- Introduced a novel edge cloud architecture to secure smarthome IoT networks against an internal adversary via microsegmentation.
- Implemented one transparent microsegmentation strategy according to functional groups.
- Evaluated our approach on 3 different topologies using different network exploitability metrics.
- **In the best case, we acheived a 65.85% attack surface reduction against a Mirai-infected webcam at the cost of blocking 2.16% of the otherwise-accepted flows in the network.**

References I


A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying IoT devices in smart environments using network traffic characteristics," *IEEE Trans. Mobile Comput.*, vol. 18, no. 8, 2019.


J. Payne, K. Budhraja, and A. Kundu, "How secure is your IoT network?" in *IEEE ICIOT*, jul 2019.


O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *IEEE S&P*, 2019.

Thanks!