CableLabs® Micronets

A New Approach to Securing Home Networks

Prepared by:
Steve Goeringer
Principal Security Architect
s.goeringer@cablelabs.com

CableLabs Project Lead:
Darshak Thakore
Lead Security Architect
d.thakore@cablelabs.com

CableLabs Program Lead:
Michael Glenn
VP Security Technologies
m.glenn@cablelabs.com

FALL 2018

Contents

Executive Summary......3-5

Introduction......6-10

Use Cases......11-14

Architecture......14-16

Conclusion......17-18

Disclaimer......19

Executive Summary

Executive Summary

The increasing proliferation of Internet-connected devices—the Internet of Things (IoT)—has the potential to transform and enrich our lives and to enable increased efficiencies and productivity gains across the broader economy. However, IoT brings with it a new set of challenges around security, scalability, management and ease of use. These challenges pose critical security and privacy risks to consumers as well as risks to the basic functionality of the Internet. Existing consumer and small business networking technologies are not well suited to meet these challenges, threatening to undermine the promised benefits of IoT.

The IoT industry and the broader Internet ecosystem have a shared responsibility to address the security challenges posed by the proliferation of IoT endpoints—both through prevention of new vulnerabilities and mitigating those that are discovered. The IoT industry is working diligently to improve the security of IoT devices and services through standards efforts such as the Open Connectivity Foundation (OCF).

In this paper, we describe CableLabs Micronets, a new approach to securing increasingly complex home and small business networks. Micronets is a next-generation device and network management framework that helps address the challenges of IoT by organizing connected devices on the network into trust domains by creating separate micro networks, or "micronets." The Micronets framework provides dynamic and adaptive Software Defined Networking (SDN)–driven controls to deliver advanced, secure services to home and small business networks. Micronets enables dynamic and managed routing between trust domains and also allows detection and handling of compromised devices using advanced security techniques such as artificial intelligence (AI) and machine learning (ML).

Micronets brings the benefits of enterprise security to home networks, without the typical complexity associated with enterprise networks. Given the proliferation of connected devices in homes and small businesses, we have reached the point where a network with advanced capabilities, traditionally only possible in large enterprises, is necessary. To be viable in home or small business environments, networks must be automatically established and easily maintained. Consumers must have control of their networks and data. Micronets ensures that consumers maintain control of their devices in a simple and straightforward manner. Making security simple and transparent to the consumer is the key advantage of Micronets.

Perfect security is, of course, not obtainable. Micronets takes a unique approach to security by focusing on the user's experience. By automatically segregating the network into trust domains, when one device is compromised, other devices in different trust domains remain secure. Infected devices within a trust domain can be dynamically quarantined or restricted to minimize the impact of the infection for the consumer, third parties and the broader Internet ecosystem.

Micronets can also enable enhanced protection for high-value devices and services. For example, Micronets would enable a network operator to provision an end-to-end secure micro netswork between a medical device and the consumer's healthcare provider or manufacturer. Micronets provides a standardized approach to identifying and limiting the impact of infected devices while enabling consumer control. This eliminates the need for security vendors to deploy custom software on the gateway, enabling increased scale for vendors and a broad range of solutions for network operators.

> **"Consumers must have control of their networks and data. Micronets ensures that consumers maintain control of their devices in a simple and straightforward manner."**

Introduction

CableLabs Micronets is a platform to automatically organize connected devices on consumer and small business networks into trust domains and manage the connectivity of those trust domains. The platform applies adaptive use of addressing, fingerprinting and strong credentials—including public key infrastructure (PKI) certificates—to identify devices and dynamically segment them. SDN is used to both isolate traffic between various trust domains and manage the traffic flow.

Micronets leverages a variety of techniques to uniquely identify devices and authenticate each device that connects to the network. It applies appropriate policies and access control based on the device profile, credentials and traffic profiles.

1.1

Typical Home and Small Business Networks

With the increasing adoption of IoT devices, home or small business networks are seeing significantly more devices connecting to those networks compared to just a few years ago. A typical home or small business network consists of a cable operator–provided modem or gateway, either an integrated or standalone 802.11 Wi-Fi router or access point, and perhaps a few ethernet-connected devices. In most home and small business networks, the traffic from all connected devices (IoT, personal computers, smart phones, and tablets) transits a single network enabled by a residential or small office/home office (SOHO) gateway. This architecture of a single, flat network is ill suited to the rapidly evolving nature of these networks and poses several limitations:

- By connecting all devices through a single network, the compromise of one device can impact the security of all devices on the network, leaving the consumer with little to no ability to manage security risk across devices.
- These risks are further magnified by the complex and non-standard configuration and network management tools available today.
- Current home and small business network architectures inhibit the network operator's ability to assist consumers with security or other local network issues.

Micronets provides an approach to address the above challenges and provide consumers with a more secure and easy-to-manage home or small business network.

1.2

The CableLabs Micronets Experience

Micronets will completely redesign the user experience around network management and security:

Security and Security Management
Security is built into Micronets by design. The architecture supports devices with strong security controls and protects devices with weaker security controls. It takes a pragmatic approach to security. Not all devices will have the same security capabilities, and there will always be legacy devices in the network that may not be able to support stronger security controls. Micronets provides for easy onboarding and identification of legacy devices and configures them in an appropriate trust domain. For example, if a consumer buys an old smart TV at a garage sale that may have unpatched vulnerabilities, Micronets allows the user to still use the TV by provisioning it in a separate trust domain from which it would not be allowed to communicate with other connected devices in the home, such as the home security system, but may allow limited connectivity to authorized internet services.

Ease of Use and Transparency
Micronets automatically manages devices and continually fine-tunes security settings for the home or small business network without burdening the user with technical details. It focuses on executing the user's intent while providing a mechanism to ensure that consumers can review and audit Micronets' actions.

Simplification of Operator Services
By using SDN, Micronets can be employed to support many kinds of on-premises networks: homes and small businesses.

Equivalent Experience Using Wired and Wireless Connectivity
Devices on the on-premises network can connect over any mechanism and still receive the same services and security.

Mobility
With ubiquitous 4G/5G mobility, Micronets can provide an integrated connectivity experience to consumers and their devices. The Micronets platform allows services to work seamlessly across both mobile (5G) and fixed (WiFi) networks.

1.3

CableLabs Micronets Features and Capabilities

To enable the transformative user experience, Micronets will provide the following features and capabilities:

Network Segmentation (into micro networks)
Micronets allows the network on the customer's premises to be logically segmented based on a single device, a group of devices, or a service being delivered. The network segmentation is dynamic, supporting easy introduction of new devices, migration of devices between micronets (trust domains), or changing consumer requirements.

Separate Trust Domains
Micronets segmentation is policy-based and enables the creation of trust domains that are based on consumer needs. Micronets treats each network segment as a distinct trust domain. Each trust domain can have its own set of functional or business policies and associated security policies used for managing the connectivity to and from devices and trust domains.

Extended Secure Connectivity Beyond the "Home" Network
Micronets segmentation and trust domains may extend outside the on-premises network using SDN, Virtual Private Network (VPN), or other solutions. This allows the cable operator to connect specific devices to protected cloud services or be part of a larger software-defined networking in a wide area network (SD-WAN).

Leverage Artificial Intelligence and Machine Learning

Micronets provides the capability to integrate AI/ML systems and consume a set of rules or policies for each trust domain, guiding which devices and micro networks may be interconnected. Policies will dynamically evolve; adding, changing, or deleting rules based on consumer actions or network traffic behaviors as detected by AI/ML systems. This capability provides a number of additional capabilities:

- Identification of devices with strong credentials for automatic assignment to existing or new trust domains.
- Integration of fingerprinting solutions to permit adaptive identification of devices and their purpose/function, allowing trust domains to be created based on context and providing a baseline for normal device behavior.
- Identification of infected or compromised devices to dynamically separate them into their own trust domain, preventing or limiting their ability to connect to other devices on the local network and on the broader Internet.

Protecting Privacy

The Micronets platform provides the mechanisms to analyze readily visible attributes and patterns of network traffic to help identify anomalous device behavior, indicative of compromise or infection. It also allows quarantining of such devices, limiting their ability to exfiltrate sensitive data or otherwise harm the consumer. The Micronets platform can analyze the metadata of devices and network traffic such as IP addresses and MAC addresses. This provides the consumers with increased ability to manage and control their local networks, and the network operator to assist consumers with local network issues. Micronets does not and cannot examine the content of encrypted network traffic.

Dynamic Rules and Policy Management

Appling business rules and policies to specific devices or groups of devices allows specific service traffic to be treated more securely. These rules and policies start with a default configuration based on current practices but can evolve over time as consumer requirements change and services recognize device behaviors and anomalies. Moreover, as external threat and attack information becomes available, network operators may be able to provide new rules or policies to better protect consumers and their devices.

Identity of Each Device or Endpoint Connecting to the Network

Micronets allows each device to have a unique identity that is leveraged to connect to the network and allows for transparent, fine-grained control over network connectivity on a per-device basis. This may be certificate-based in the case of devices that participate in a PKI ecosystem. Dynamic certificates can be provisioned to devices that support this feature. Micronets also leverages and improves upon Wi-Fi Alliance (WFA) standards to provide frictionless onboarding of new devices by the consumer. Moreover, usage descriptors, such as Manufacturer Usage Description (an IETF draft RFC) may provide additional device information useful for knowing how devices should be connected. In the event that identity or usage descriptors are not created, a synthetic identity may be created to ensure that uniqueness of the device can be assured.

Standardized Interfaces

Many AI-based services are being developed for home networks. Dozens of vendors are providing a variety of capabilities, many of which require integration directly in a home gateway or cable modem. This approach does not scale, nor is it extensible. It limits the consumer and the operator to choosing one solution today that will need to be installed for a very long time before being changed. Micronets provides an alternative approach: leveraging flow-based switching capability in the gateway and providing a common, standardized interface that the network operator can leverage to enable a multitude of cloud-based capabilities from various AI vendors. This approach enables the possibility of providing a wide, technologically competitive mix of advanced services—such as advanced fingerprinting, anomaly detection, per-device granular walled garden malware management and more—across multiple vendors.

> “Micronets also leverages and improves upon Wi-Fi Alliance (WFA) standards to provide frictionless onboarding of new devices by the consumer.”

Use Cases

The following use case helps illustrate and provide a vision for how a cable operator may use Micronets to provide a more secure and easy to use consumer experience.

Emma is a busy mother of two children. She works full time as a mechanical engineer; her kids are active in sports and music. Her house is full of gadgets because Emma likes to tinker when she has time. She doesn't know it, but Micronets gives her time. All Emma knows is that her home network is easy to navigate and use.

Emma has a well-networked smart home. She has home automation IoT devices, a smart car, several mobile devices and even a device to send medical test results online. In addition, it is important to her to keep her children safe online.

Here are some simple stories about how Micronets makes Emma's life even more remarkable:

2.1

Organizing Emma's World | **CableLabs Micronets Segmentations**

Micronets automagically organizes Emma's world (her network) into trust domains. She has full visibility into how the network is set up, but she rarely has time to watch or manage her home network. She has a home automation network, home security network, and a network for updating her car; her 13-year-old son is on one network while her 6-year-old daughter is on another. The glucose tester for her daughter, which sends test results to her endocrinologist, is on a separate, secure network segment.

Segmenting Emma's network in this way is an important security feature found on well-designed enterprise networks. It allows rules to be applied against each network according to their needs and segments data and devices to minimize intrusions.

2.2

Protecting Emma's World | **CableLabs Micronets Network Security**

Last year, Emma got a notification from her Micronets app that her refrigerator was behaving strangely and she should consider fixing it. In the meantime, it had been temporarily placed in a special network to keep it from impacting other devices in her home automation network. Emma checked out the fridge's user interface and found a warning to perform a security update. She installed the update. A few days later, she updated the privacy rules for her daughter, Sarah. Emma noted that the fridge was back in the home automation network. "That's why the kitchen light was turning on again when she opened the fridge. Thanks, Micronets!"

2.3

Emma's Home Reaches Out into the World | **CableLabs Micronets Home Extension**

Emma's lifestyle is enhanced by a plethora of connected devices providing a wide range of services. Her smart car is maintained and updated remotely. Security monitoring keeps her family safe at home and keeps her home protected when they are away. Emma can remember the first time she tried a home automation product. She spent hours getting it on the network. A few months later, she upgraded her home router and had to do it again.

Micronets provides a much more direct, friendly experience. Partners work with Emma's cable operator to maintain a secure ecosystem that allows Emma's gateway to identify devices and automatically and securely connect them to their service providers. Emma has full control over which providers she works with (within the ecosystem) and what devices can connect with the home.

2.4

Helping Emma Care for her Family

Remote Patient Monitoring

Remote patient monitoring is a special case for home health care. Emma's daughter, Sarah, has severe diabetes that must be carefully monitored. Sarah's doctor prescribed an advanced networked glucose monitor. The monitor was provisioned at the doctor's office using an interface that integrated with her cable operator. Emma took the monitor home and immediately got a prompt from Micronets asking her to confirm that she wanted the device to connect to her home network. A secure channel enables the monitor to report medical test results three times per day. Using dynamic trusted identity, the device is fully authenticated, leveraging secure communications channels. Emma sleeps better knowing the doctor can proactively monitor and treat Sarah's diabetes.

2.5

Adaptable Security

Protecting Emma's Network

Security threats are continuously evolving. What was done yesterday to protect Emma's fridge may not work tomorrow. Unbeknownst to Emma, Micronets adapts security capabilities seamlessly as threats develop. Several technologies are employed to detect threats, identify compromised (infected) devices, and adaptively create "walled gardens" to ensure that compromises are contained. Identity management supporting multiple ecosystem certificates, manufacture usage descriptors and synthetic device profiles (fingerprinting) are used to determine network access and security permissions. Traffic capture and forwarding to high-performance scanners look for indicators of compromise or infections. Where useful, ML and neural network technologies are applied in the cloud to provide advanced intelligence to make all these capabilities as adaptable as possible. Hackers never had it tougher.

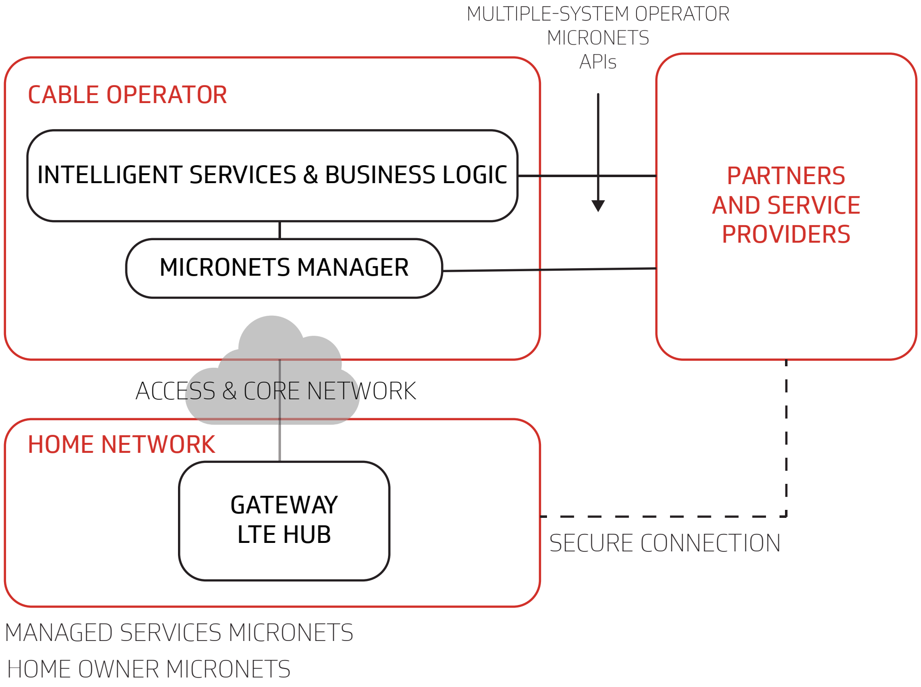
> **"A secure channel is enabled so the monitor can report test results three times per day."**

Architecture

Architecture

The Micronets architecture allows the establishment of micro networks to and in the home. Micro networks are subnetworks defined and managed by software-defined switching (e.g., flow-based). Rules can be based on frame or packet information at Layer 2 (MAC addresses or certificates and unique device credentials), Layer 3 (IP address, protocol, or network-level authentication), or higher (ports, device signatures). However, it is likely that most services will be based on Layer 2 and 3 flow rules. Using these flow rules, Micronets can interconnect devices or resources (such as virtualized storage or compute) within the home, the cable operators' infrastructure, or the internet.

Micronets can be viewed at a high level as having four distinct architectural components. The cable operator deploys the Micronets platform, which is composed of infrastructure-oriented micro services and an intelligence layer where intelligent services and business logic is applied. A Micronets Manager is the critical element that orchestrates all Micronets activities, most notably the creation of rules that manage device connectivity within the home and cable operator network to deliver services. A Micronets-enabled network is composed of trust domains that are used to deliver managed services to customer-owned and -managed devices and services. Managed services are automatically organized into appropriate network segments. Micro services interact with the network through a gateway, which may be a cable modem, router or LTE hub/femtocell. Operator partners and third-party service operators can interact with the Micronets Manager via APIs. See the figure and element descriptions below.



The four layers of CableLabs Micronets,

as shown in the Figure on page 15, are defined as follows:

- **Intelligent Services and Business Logic** – This layer acts as the interface for the Micronets platform to interact with the rest of the world. It functions as a receiver of the user's intent and business rules from the user's services and combines them into operational decisions that are handed over to the Micronets Manager for execution. It can host various advanced services that are enabled using cloud resources. It may receive information from various Micronets' micro services (such as the SDN controller) and in turn use that information to dynamically update the operational decisions. Example services include IoT fingerprinting that allows detection of devices in the network, third-party AI/ML–based systems that can be integrated at this layer for malware detection and abnormal behavior, and mobility service management.

- **Micronets Manager** – As the name suggests, the Micronets Manager coordinates the entire state of the Micronets-enabled on-premises network. It orchestrates the overall services delivery to the devices and ultimately to the user. Several micro services are engaged and managed by the Micronets Manager (e.g., SDN controller, DHCP, DNS, AAA/identity servers).

- **On-Premises Network** – The SDN switch is responsible for creating the micro networks. Customers do not need to worry about setting all this up. Instead, they will interact through a simplified interface such as a phone app to input their intentions, which the platform will implement.

    - **Managed Services** : Operators may leverage the Micronets platform to implement micro networks of devices for managed services. This may be done for their own organic service offerings (such as security services) or to support a third-party operator (such as a health care operator using remote patient monitoring). The customer controls what services are allowed/enabled.

    - **Customer Micro Networks** : Customers will acquire and connect their own devices. They may even integrate entire service-oriented networks, such as a smart home lighting system. Customer networked devices may be fingerprinted or authenticated using an ecosystem certificate and automatically placed into an appropriate micro network or a customer may request to create a new micro network.

- **Micronets Gateway** – The core networking component of Micronets is the gateway. The gateway implements a software-managed switch that is controlled using SDN paradigms. The gateway supports connectivity for both wired and wireless components.

- **Micronets APIs** – The Micronets API allows partners and service providers to interface with the customer's Micronets environment to provision and deliver specific services that the customer has requested.

Conclusion

CableLabs®

Conclusion

CableLabs is collaborating with its cable operator members and the vendor community to develop the Micronets architecture and interfaces. We are developing reference code that integrates into common gateway development kits (e.g., OpenWRT and RDK). In addition, we are working on porting SDN concepts and technology to address needs for on-premise networks. We are developing standardized APIs, with the requisite security controls, to allow intelligent services to interact with the gateways. For example, an API can be used to provide a standard approach to AI solution providers to deliver advanced services using ML and neural network capabilities in the cloud rather than requiring a dedicated, vendor-specific AI-enabled gateway. Finally, new APIs are being designed to allow third parties (such as health care providers) to securely interface with operators.

The introduction of SDN capabilities in the customer network enables a more secure and simple consumer experience. Leveraging strong identity management and heuristic-based analysis provides the core capability to automate the way subscriber networks are set up without sacrificing privacy or increasing complexity. This, in turn, allows the introduction of advanced machine learning or neural network capabilities without the need to deploy additional platforms.

“The introduction of SDN capabilities in the customer network enables a more secure and simple consumer experience.”

Disclaimer

This document is furnished on an "AS IS" basis, and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement or fitness for a particular purpose of this document, or any document referenced herein. Any use of or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason, including but not limited to changes in laws, regulations or standards promulgated by various entities, technology advances or changes in equipment design, manufacturing techniques or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards or recommendations.