Governments Must Promote Network-Level IoT Security at Scale
December 2021

Summary: To promote IoT security, policymakers must complement a focus on steps IoT device manufacturers should take with policies that promote network-level security at scale, detecting and stopping anomalous behavior by IoT devices using automation, machine learning, and the cloud. Networks can and should be a priority detection and enforcement point for IoT security, and technologies exist today that are appropriate to realize this goal. Network-level security addresses IoT security regardless of the type of device or its end-use, which is essential given that attacks on "consumer" IoT devices can have impact on businesses and throughout economies. This approach can create resilient networks ready-made for IoT and can be leveraged across businesses, governments, and homes.

Table of Contents

Introduction

Managing the security of the Internet of Things (IoT), the networks on which they operate, and the data they transmit and process is a challenge, particularly with the massive variation of device types and deployments. IoT adoption is growing rapidly across industry verticals and consumers worldwide, leading to a growing attack surface and new threat landscape. In turn, governments globally are exploring regulations or codes of practice to promote IoT security. However, many governments focus on promoting measures that IoT device manufacturers should take when building or maintaining devices[1] including ETSI EN 303 645[2], a standard for cybersecurity that establishes a baseline for Internet-connected consumer IoT devices by

[1] Particularly for consumer and healthcare IoT. Examples are Australia's Voluntary Code of Practice: Securing the Internet of Things for Consumers, Singapore's Cybersecurity Labelling Scheme for Consumer Smart Devices, the UK's Voluntary Code of Practice for Consumer IoT Security, and the U.S. National Institute of Standards and Technology (NIST) IoT Device Cybersecurity Guidance for the Federal Government Special Publication. Medical device examples are at https://www.orielstat.com/blog/fda-medical-device-cybersecurity-regulatory-requirements/

[2] ETSI EN 303 645 was issued in June 2020. See https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard

prohibiting universal default passwords, requiring that software is securely updated, and the like. Governments also are promoting device certifications or labelling schemes.

We commend governments' intentions to address IoT security. But while built-in IoT device security measures are important – and arguably manufacturers can make improvements – this approach does not account for or address the full picture of cybersecurity threats and risks to IoT devices, users, and networks. Further, this approach has technical constraints. Governments' understanding and policy approaches to improving IoT security must keep up with the evolution of IoT threats, many of which can only be stopped at the network level.

What is an "IoT" Device?
Although there is no one industry-wide consensus of how to define IoT, Palo Alto Networks definition of an IoT device is as follows: the device must be connected to a network, and the device must be purposefully used for a set function. The latter means that computers and tablets running an application that makes them have one set function-- like an iPad used as a point-of-sale device in a store -- would qualify as an IoT device, even if iPads generally would not (from our perspective). The definition of an IoT device can include non-traditional devices connected to a network, and devices that might not have a dedicated 1:1 user associated with them (such as security cameras or printers). IoT devices are unmanaged, in the sense they cannot have traditional security controls like anti-virus or enterprise endpoint-protection installed on them. Finally, IoT devices are unable to authenticate themselves on the network.

IoT Adoption is Growing, Particularly in Business and Industrial Settings

Many people equate IoT primarily with consumer uses, such as connected toys or smart appliances. However, businesses in healthcare, transportation, and many other sectors are deploying IoT, as are government agencies. IoT device usage has increased for these organizations as their employees have transitioned much of their work to their homes during the pandemic, as described in more detail in a later section. Many traditional consumer IoT devices—such as smart appliances and even consumer wearable devices—also are increasingly being connected to corporate networks. In 2021, 78% of IT decision-makers surveyed reported an increase in non-business IoT devices on corporate networks in the last year. [3] Smart light bulbs, heart rate monitors, connected gym equipment, coffee machines, game consoles, and even pet feeders were among the devices identified on such networks.

The utilization of the Internet of Medical Things (IoMT) in the healthcare market is growing rapidly. IoT is also widely deployed in industrial settings. Industrial IoT (IIoT) is the term for the use of IoT in processes (e.g. oil and gas, utilities) and discrete manufacturing (e.g. equipment manufacturing) to enable more efficiency and readability in operations through automation and optimization, as well as better visibility of logistics and supply chain. Examples include electric utilities leveraging IIoT to manage substations, water utilities operating valves that manage water flows, and port managers operating cranes and equipment to guide ships in and out of ports. Factory robots with embedded sensors can connect over the Internet to analytics platforms for data processing and analysis.

[3] Among those IT decision-makers whose organizations have IoT devices connected to their networks. https://www.paloaltonetworks.com/resources/research/connected-enterprise-iot-security-report-2021

Although statistics vary widely, the overwhelming consensus is that the number of IoT devices deployed is massive and growing rapidly. A report measuring enterprise and automotive IoT endpoints found 5.8 billion in use in 2020.[4] In 2020, Palo Alto Networks found that more than 30% of all network-connected endpoints are IoT devices (excluding mobile devices) at the average enterprise.[5] The number of IoT devices will likely eclipse IT devices soon. IoT adoption is transforming healthcare; in 2020, approximately 86% of healthcare delivery organizations reported using an IoT solution in most lines of business.[6] Finally, the Covid-19 pandemic has accelerated IoT adoption. As businesses slowly reopen, contactless IoT devices such as point of sale (POS) terminals and body temperature cameras have been widely adopted to keep business operations safe. Palo Alto Networks research shows 89% of IT decision-makers globally reported that the number of IoT devices on their organization's network increased over the last year, with 35% reporting a significant increase.[7]

Growing IoT Threat Landscape

Concurrently, the threats are growing. Many enterprises use IoT devices that process sensitive data that must be protected in transit and at rest. The secure operation of IoT devices in critical infrastructure keeps hospitals, society, and businesses running, and has life or death implications for patient health care. IoT devices are increasingly targeted in cybercrime.[8] High-profile, IoT-focused cyberattacks are forcing industries to recognize and manage IoT risks to protect their core business operations.

Types of IoT attacks include password attacks, port attacks, IoT worms, malware, botnets, and ransomware. When IoT devices are attacked, not only are devices impacted, but they can be steppingstones to other devices, corporate networks, and sensitive data. IoT devices can be configured to send traffic to known bad destinations such as command and control (C2) servers or they can spread malware to other devices on the same network. In 2020, Palo Alto Networks looked specifically at the rapidly increasing use of IoT devices in healthcare and found that over 98% of all IoT traffic was unencrypted and that 57% of all IoT devices were vulnerable to medium- or high-severity attacks.[9] Security changes are needed to protect corporate networks from non-business IoT devices. Organizations surveyed in 2021 reported that they need greater threat protection (59%), risk assessment (55%), IoT device context for security teams (55%), and device visibility and inventory (52%).[10]

[4] https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

[5] https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[6] https://www.gartner.com/en/documents/3979368/survey-analysis-healthcare-provider-iot-adoption-is-beco

[7] https://unit42.paloaltonetworks.com/iot-supply-chain/

[8] https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/

[9] https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[10] https://www.paloaltonetworks.com/resources/research/connected-enterprise-iot-security-report-2021

Combining IoT/IoMT/IIoT with the power of 5G has opened new areas of cybersecurity risk as cyber adversaries have new opportunities to infiltrate networks and gain access and control information and devices connected to these networks. There also are attacks on IoT supply chains, such as when criminals compromise software that will be installed in an IoT device (like a router or a camera), to hide malware, or modify hardware to change the device's behavior.

Examples of High-Profile IoT Cyberattacks

The Mirai botnet was one of the first incidents demonstrating major ramifications of IoT security at scale. Mirai gained notoriety in 2016 when over 600,000 CCTV cameras were remotely controlled and leveraged to create an immensely powerful botnet used in massive denial of service attacks and caused several network outages.[1] *Mirai developers continue to actively innovate: a growing array of IoT devices were targeted in 2018 and 2019, and four new Mirai variants were discovered in 2020.*[2] *The University of Berkeley found the economic cost of IoT insecurity can be extreme: a Mirai botnet operating at peak power can incur direct and indirect costs totaling over $68 million.*[3] *There have been an increasing number of attacks in which many IoT devices were impacted, such as the WannaCry and NotPetya attacks, both first seen in 2017. WannaCry continues to infect Internet of medical things (IoMT) devices and illuminate their susceptibility to ransomware attacks.*[4]

More recently is the March 2021 Verkada Inc. security camera breach, where an international hacker collective broke into a massive stockpile of live feeds from Verkada's web-based network of security cameras. The breach left sensitive and private video surveillance footage from its customers hacked and exposed; the perpetrators pivoted into separate corporate networks of some customer accounts.[5] *In May 2021, ransomware disabled the Irish Healthcare Service servers and affected IoMT devices. Medical imaging devices were particularly affected; software used for sharing X-rays and CT scans went down, making it impossible for most hospitals to send imagery between departments or to other hospitals. Doctors were forced to go in person to X-ray machines or else rely on written descriptions.*[6]

[1] *https://us-cert.cisa.gov/ncas/alerts/TA16-288A*

[2] *https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/ and https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/*

[3] *https://groups.ischool.berkeley.edu/riot/*

[4] *https://www.darkreading.com/risk/wannacry-has-iot-in-its-crosshairs*

[5] *https://www.paloaltonetworks.com/blog/network-security/are-your-security-cameras-safe-from-cyberattacks/*

[6] *https://abcnews.go.com/International/10-days-ransomware-attack-irish-health-system-struggling/story?id=77876092*

Work-From-Home is Exacerbating IoT Security Challenges

Over the past few years, the Covid-19 pandemic has exacerbated the IoT security challenges for enterprises and governments as their employees have transitioned much of their work to their homes. Homes are seeing new corporate-issued IoT devices beyond laptops and smartphones, such as voice-over IP (VOIP) phones, packages of professional-level audio and video collaboration and productivity tools (such as video cameras and microphones), digital white boards, gaming consoles for game developers, hardware prototypes for engineers, and the like. These devices are not always designed for "work from anywhere," as they cannot be configured with traditional enterprise security (such as agents[11] or virtual private networks (VPNs)) and therefore do not have adequate security posture built in at the device level. Even in

[11] An agent is endpoint security software.

cases when employees at home have a VPN on their laptops, that security is limited just to that device—if the laptop connects to an untrusted home network, it might be the target of a lateral threat movement from a connected, compromised IoT device that might then allow an attack to make its way into the corporate network.

In addition, highly sensitive work that was usually done only on corporate campuses or government networks is now happening at home. This includes executives preparing financial regulatory filings, engineers developing IP-sensitive source code and hardware, financial and legal departments conducting high-value business and contractual transactions, customer support teams collecting sensitive customer data on support calls, and government officials working with business confidential information of firms they regulate.

Combining this plethora of sensitive data used in the home with the fact that so many devices are now used in the home, IoT security for businesses and governments is even more imperative. When working on a corporate campus, employees could badge in, and IT departments could largely implement a uniform level of security for devices on that network. That is no longer always the case. Securing work-from-home equals securing the home, which requires bringing network-level security to all the IoT devices in the home.

Limitations to Relying Solely on Security Controls Embedded in Devices

Embedded device security is very important. Approaches that IoT device makers should take, such as prohibiting universal default passwords, keeping software securely updated, making systems resilient to outages, and others are important steps. Devices also must be secure so that their identities are not spoofed and their root of trust[12] stays intact -- this is imperative to an understanding of a device's baseline behavior and detection of anomalous behavior.

However, relying just on IoT device-based security is insufficient due to inherent limitations related to many IoT devices themselves, threats, and risks in the supply chains of IoT device manufacturers, and the threats and risks arising from real-world deployments of IoT devices.[13]

Security limitations related to IoT devices themselves

- It is impossible to embed security in certain IoT devices. Some IoT devices simply lack capacity for built-in security. For example, some devices do not have sufficient storage or processing power to support logging or cryptographic abilities to protect sensitive

[12] A root of trust (RoT) is a set of security functions (trusted boot, cryptography, attestation) that, if adequate, can mitigate cybercriminals from bricking IoT devices, using devices to form botnets, or introducing unauthorized code.

[13] NIST has highlighted the need to go further. The U.S. Internet of Things Cybersecurity Improvement Act was signed into law in December 2020 to address the IoT device procurement and security needs of the U.S. Federal Government and its agencies. Under the Act, NIST was asked to develop the IoT Device Cybersecurity Guidance for the Federal Government as a Special Publication (SP 800-213). NIST guidelines go beyond embedding IoT device security controls and recognize the heightened need for the security teams to have a comprehensive IoT risk management strategy that spans from plain device discovery to mitigation that should include threat detection, prevention and incident response. https://www.nist.gov/news-events/news/2020/12/defining-iot-cybersecurity-requirements-draft-guidance-federal-agencies-and

information being processed.[14] Sensors such as thermostats, smart lighting hardware, and smart blinds are examples of IoT devices that typically would not have sufficient capacity for built-in security. Many already deployed IoT devices are low cost, with no security embedded, making easy entry points for adversaries.

- Legacy devices are a challenge. Billions of already-deployed IoT devices globally cannot be retroactively (retrospectively) designed for security (nor can they be certified or labelled). For some devices, secure update mechanisms may be inadequate; some continuously operating, mission-critical devices (e.g., robotics, factory production line sensors, video surveillance, and IoMT devices) receive updates infrequently. Some already deployed devices may already have reached their end-of-life date or may never have had the functionality to update.
- Heterogeneous nature of devices makes a uniform built-in standard impossible. Too many different types of devices and manufacturers exist to expect a uniform standard for embedded device security.
- Lack of vendor action. Some vendors simply provide poor or nonexistent product security or patch support, even if required to do so.

Threats and risks in IoT device manufacturers' supply chains

Like all ICT manufacturers, IoT device manufacturers face threats impacting their supply chains. Even if an IoT device is built securely, weaknesses inserted into devices via a manufacturer's supply chain might not be visible when the device is shipped. Motivations for attacking an IoT supply chain could include cyberespionage (maintaining long-term, undetected access to confidential information and affected systems) and cybercrime (exploiting IoT devices to set up a botnet or DDoS service for hire, selling camera access to spy on someone, or developing and selling crypto jacking malware targeting IoT devices).[15]

Security challenges arising from real-world deployments

Again, even if an IoT device is built securely, external variables in real-world deployments can impact devices and their security in various ways, leading to different risk profiles.

- The same IoT device may be used in different environments. IoT devices and systems are used in a range of heterogeneous environments. For example, the same IoT sensor might be used to monitor agricultural activity as well as to track vehicles in the transportation industry. Some IoT devices can be used in both consumer and industrial settings (a connected lighting device could be used in a home and in a more high-stakes, industrial setting).
- The same IoT device may be used for different functions. An IoT device can have different functions or roles to play. For example, the same cameras in a hospital can be used by nurses to monitor patients and by security teams to monitor for intruders.
- There is often no central repository of all IoT devices. IoT devices are oftentimes purchased by different teams in an organization, resulting in no centralized device

[14] Drawn from: https://www.nist.gov/blogs/manufacturing-innovation-blog/whether-you-build-them-or-buy-them-iot-device-security-concerns

[15] https://unit42.paloaltonetworks.com/iot-supply-chain/

repository. For example, in healthcare delivery organizations, IoMT may be purchased by bio-medical teams without the knowledge of network security teams—who then therefore cannot secure those devices.

- IoT devices may be in physically nonsecure locations. Some IoT devices are deployed in nonsecure locations and left unattended, such as those used in power grids.
- Acumen of individuals operating IoT devices may differ. The individuals operating an IoT device or system may have varying cybersecurity skills or understanding of risk management.

In short, while security built into devices is an important piece of the puzzle, relying solely on this approach is only half of the answer and can bring a false sense of security. Organizations must also be able to detect and stop anomalous behavior by devices once deployed, as described below.

Network-Level IoT Security at Scale Must Complement Embedded Measures in Devices

Network-level[16] IoT security should include the approaches below, underpinned by a focus on prevention, automation, and Zero Trust. Machine learning and use of the cloud are essential.

- ***Visibility and dynamic identification of devices:*** Any organization needs visibility (a full inventory) of what IoT devices are on its network at any given time. More than simply identifying IP addresses, this requires understanding how many and what kinds of devices are connected. Visibility allows understanding of the “attack surface”[17] and important interdependencies: where IoT devices are, which applications they are using, and how they are interconnected. IoT devices must be identified and assessed for risk when they connect to the network; this should occur in real time because IoT devices frequently connect and disconnect from a network. Overall, device visibility and identification allow organizations to eliminate critical blind spots that attackers could otherwise access to infiltrate a network or IoT device.

- ***Continuous device and risk monitoring:*** Once visible, devices must be continuously monitored for anomalous behavior and threats. Because IoT devices are designed for a fixed set of functionalities, their intended behavior pattern is often predictable (e.g., actions of printers differ from those of medical devices or industrial sensors). Continuous monitoring shows what a device should and should not be doing, enabling detection of abnormal behaviors (a medical imaging machine should not be streaming videos on YouTube). Having complete visibility of devices connected to the network and getting notified when a device generates anomalous traffic is critical to defending infrastructure.

[16] A network-level security approach (complementing built-in security) is not unique to IoT devices: it is used to protect endpoints today. For example, enterprises deploy additional network security protocols such as firewalls, extended detection and response, and secure communication tunnels via VPNs to manage devices (such as laptops and servers) even though these managed endpoints come with in-built security controls such as antivirus and malware detection. The same thinking must be applied to IoT devices.

[17] https://www.paloaltonetworks.com/blog/security-operations/know-your-inventory/

- ***Security policy enforcement:*** Device/risk visibility and monitoring allows organizations to come up with security policies and take enforcement actions vis-a-vis IoT devices in real time to prevent cyberattacks and react to anomalous behavior. Network segmentation is a key enforcement measure for IoT security. Network segmentation creates “least access” [18] zones for IoT devices by function, so that particular device types can only converse with the network resources they need. This reduces risk and helps limit lateral movement of threats if an IoT device zone gets compromised. Quarantining (disabling or taking offline) an IoT device that has been infected or breached is another enforcement action. Technology can deliver security policy risk reduction recommendations automatically based on IoT device classification, crowdsourced IoT device data, and device posture, applications, and risk assessments.

  Basic network segmentation practices – let alone more secure micro-segmentation practices – are not yet widely followed within industry verticals with significant IoT usage.[19] In reality, IoT devices are often deployed on the same network segment as other devices and application servers. Palo Alto Networks 2020 IoT Threat Report found that 72% of healthcare virtual local area networks (VLAN)[20] house a mix of medical IoT devices, generic enterprise IoT devices, and IT devices, lowering the barrier for malware to spread laterally from IT devices to IoT devices (for example, an infected laptop can easily target surveillance cameras and medical imaging devices on the same network).

Prevention, workflow automation, and Zero Trust are also necessary. Preventing threats is crucial. Response to and recovery from incidents are important, but by then damage is done. Built-in prevention also reduces alerts for already fatigued security operations center (SOC) teams. Prevention must be both of known threats based on signatures and known behavior across crowdsourced data, as well as unknown (zero-day) threats.

Automation of workflows is essential across device discovery, risk monitoring, enforcement, and threat prevention to stay ahead of increasingly advanced and sophisticated attackers. Automation can prevent threats from becoming successful cyberattacks and must replace manual responses, which are time-consuming, costly and cannot scale against automated attacks.[21] IoT device visibility shared automatically with various network security tools such as IT security management (ITSM), enterprise endpoint protection (EPP), endpoint detection and

[18] Least-privileged access is a concept of careful delegation of access rights to a system for users, granting system permission to a user for only the necessary duration and scope for the actions needed and relinquishing privileges immediately after the user is finished accessing the resource.

[19] https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[20] A VLAN groups together and maps different network devices (computers, servers, IT devices, IoT devices) that behave as if they are connected to a single network segment.

[21] Automation can also free limited human resources from mundane tasks to allow people to pivot to focus on more sophisticated threat hunting.

response (EDR), and extended detection and response (XDR)[22] allows for more seamless security. Machine learning (ML)-powered behavior baselining can automate risk assessments. Other ML-powered capabilities essential to IoT security are described in the ML section below.

Finally, network-level IoT security must be based on the fundamental cybersecurity concept of Zero Trust Architecture (ZTA). Under the Zero Trust concept,[23] an organization should not automatically trust any unauthenticated activity inside or outside its network perimeters. Instead, anything and everything trying to connect to systems—including IoT devices—must be authenticated before access is granted.

Machine Learning Must Underpin Network-Level IoT Security

Recent advancements in ML have made it an essential tool for cybersecurity in the IoT context. In general, ML models leverage an extensive, data-driven understanding of any given IoT device's expected behavior and usage on a network to efficiently achieve real-time visibility and dynamic identification of devices, continuous device and risk monitoring, and enforcement.

The predictable patterns of IoT device behavior enable ML to easily learn patterns. And unlike humans, ML can pick up patterns at scale, in real time. This means ML and artificial intelligence (AI) can automate device identification, proactively detect malicious deviations in IoT devices' patterns of functionality, and automatically prevent attacks. This allows organizations to stay ahead of highly damaging attacks, avoiding the expense of lost information or production time. ML has advantages over signature-based monitoring and detection[24] which can only identify "known" things and thus cannot scale to identify all IoT devices, such as those new to the market. In contrast, ML can help with identifying unknown and never-seen-before devices.

Network-Level IoT Security Should Leverage the Cloud

Network-level IoT security also should leverage the cloud, for two reasons. First, many organizations around the world are extending their networks to hybrid (public/private) cloud models, including the networks to which IoT/IoMT/IIoT devices attach. Thus, securing these networks should be done in the cloud. Second, cloud security solutions enable updated controls to be delivered at the speed of innovation and can scale up and down based on computational needs, both of which are necessary to counter sophisticated, automated cyberattacks.

[22] XDR is a software-as-a-service (SaaS)-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system.

[23] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

[24] Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future.

Conclusion: How Government Policies Can Promote Network-Level IoT Security at Scale

Given the dynamic nature of IoT and the environment in which devices are deployed, it is critical to go beyond embedded device security and to have the capability to dynamically secure the entire network, extending from corporate settings to homes with hybrid work models, in real time and at any time. Networks can and should be a priority detection and enforcement point for IoT security, and technologies exist today, grounded in machine learning, that are appropriate to realize this goal.

As governments develop policies to promote greater IoT security in their economies, they must complement a focus on embedded IoT device security with policies that create and promote resilient networks that are ready-made for IoT. More specifically, governments should:

1. Promote use of the cloud and cloud-based security throughout economies.
2. Promote the adoption of automated approaches to cybersecurity, specifically those that leverage machine learning.
3. Encourage their businesses, government agencies and citizens to take steps to have a full inventory of all IoT devices on their networks, continuously monitor those devices for anomalous behavior and threats, and take automated security policy enforcement actions vis-a-vis their IoT devices in real time to prevent cyberattacks and react to anomalous behavior.