IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Check Point

As the Internet of Things (IoT) and operational technology (OT) begin to deliver value, the adoption and proliferation of IoT capabilities also bring new risks. Security is paramount to many organizations as they realize how usage scenarios may be affected by compromises to the confidentiality, integrity, and availability of data.

IoT Security Guide: Challenges and Solutions

March 2021

Written by: Frank Dickson, Chris Rodriguez, Pete Finalle, and Robyn Westervelt

Introduction

Despite its name, the Internet of Things (IoT) is not a single monolithic structure but an umbrella category of thousands of digitally transformed solutions that create value by connecting "things" that were once not connected. The ability to connect these devices is the first step to unleash or reveal new business models. Distributed technical architectures that combine sensors, intelligent systems, connectivity, platforms, and analytical capabilities are evolving into fully formed use cases for remote health monitoring, connected cars, and smart utilities, among others, that are poised to deliver great value and create new markets.

IDC defines an IoT solution as "a network of networks of uniquely identifiable endpoints (or things) that communicate without human interaction using IP connectivity — whether locally or globally. IoT brings meaning to the concept of ubiquitous connectivity for businesses, governments, and consumers with its innate management, monitoring, and analytics."

AT A GLANCE

KEY TAKEAWAYS

- Cyberattacks against IoT systems hold the potential for serious real-world consequences.
- To deliver security and trust to the IoT, organizations must focus on connectivity, hardware, software, and the environment.
- IoT security may be required at various parts of the ecosystem based on the technical architecture and particular use cases.
- Not all device manufacturers or their users will accommodate agent installations. Alternative approaches will be required.

The scope of the definition is not limited to traditional consumer devices but extends to the almost unlimited use cases within the industrial IoT (IIoT) and operational technology (OT) as the future of operations emerges. That future encompasses the transformation of an operation from being strictly cost and efficiency driven to being customer or market driven. The currency of this transformation is data, transforming an organization that is measured on reporting and compliance to an organization that is built on resilient decision making. Traditional models rely on a tedious process of information gathering direct from devices, leading to centralized decision making, formulating a plan of action, and enforcing the necessary changes to the devices or network. Increasingly, data must be ingested from and decisions made at the point of activity with the help of artificial intelligence (AI).

While IoT and OT technologies promise to deliver great value, the adoption and proliferation of IoT capabilities also bear new risks. Security is paramount to many organizations as they realize how usage scenarios may be affected by compromises to the confidentiality, integrity, and availability of the data as well as the productivity and propriety of the devices themselves.

Proof-of-concept exploits as well as real-world compromises highlight some of these risks. Simple methods for surreptitiously sniffing RFID, Bluetooth, and NFC communications have been seen for years. Physical items such as digital picture frames have been mistakenly shipped with embedded malware. Compromises of ATM machines, insulin pumps, heart pumps, and cars have been demonstrated. Cyberattacks against SCADA systems hold the potential for serious real-world consequences, as shown by industrial cyberattacks in countries such as Ukraine, Germany, and Iran.

The IoT can be susceptible to various attacks including botnets, distributed denial of service, crypto miner, Mirai, or ransomware. Consider this scenario: An unknown IoT device is placed into an enterprise network, behind perimeter defenses such as firewalls, intrusion prevention systems (IPS), and other IT infrastructure so that the device has unfettered access to all corporate network resources. A web server is embedded into the device to maximize the its functionality. All the ports will be set as "open" by default and enable as much as a gigabit of Ethernet connectivity, which will make the device accessible. The device will have a rich operating system (OS) such as Linux to maximize functionality. It will not be examined on an ongoing basis using the enterprise's vulnerability scanner as the embedded web server will likely light up the organization's security information and event management (SIEM) tools like a Christmas tree with false positives. The vulnerability scanner will be configured to ignore the device, meaning that it will not be updated, maintained, or patched over the five- or sometimes 10-year useful life of the device. Device protection will consist of a default password, and unvetted third parties will maintain the device. It will be core to organizational productivity, so there will be one device for every 10 employees. Some might call this a nightmare; some might call this a printer.

As organizations seek to deliver security and trust to the IoT, they must focus on the following architectural components:

- Connectivity, including service enablement
- Hardware, including IoT modules/sensors, security, servers, storage, and other hardware
- Software, including analytics, applications, IoT purpose-built platforms, and security software
- Environment, including unique requirements driven by operational technologies

Protecting each of these elements and their corresponding interactions with other components may require security at various parts of the ecosystem based on the technical architecture and particular use cases.

Evaluating Objectives

The practice of protecting any set of computing assets — information or data, executable software, and physical devices — must begin with a set of objectives. In technology risk management, the following information traits have long been objectives:

- **Confidentiality** — ensuring that the information can be read only by appropriate parties
- **Integrity** — ensuring that the information retains its distinct content and that any changes can be identified
- **Availability** — ensuring that information is available for use by people or resources that require it

These first three control objectives — often referred to as the "CIA triangle" — arose through research and common agreement within the information security field. However, IoT and OT span both digital and physical worlds. The proliferation of computing resources in the form of devices that provide some function other than processing information requires further extension of the set of objectives, so we can add two more:

- **Productivity** — ensuring the use of computing resources that do not process sensitive information or data and yet provide value through their functionality, such as systems used to run manufacturing machines or components of the energy grid
- **Propriety** — protecting against the abuse of computing resources for inappropriate or otherwise unauthorized activities such as surreptitiously mining for bitcoins or secretly operating an audio/visual torrent

With possible control objectives in mind, an organization can evaluate its need for each IoT component in a scenario, consider its corresponding set of communicating inputs and outputs, and look for ways that the control objectives will be left unmet. Consider whether an attacker can:

- Interrogate a component of the IoT and collect data or other types of files? (Confidentiality)
- Intercept the traffic between or among components? (Confidentiality)
- Alter the data or binary files of a device? (Integrity)
- Modify communications between or among two components? (Integrity)
- Insert or inject inappropriate packets into a transmission either directly or by impersonating the transmitting component of the architecture? (Integrity)
- Corrupt a component or one of its key parts to render it unusable? (Availability and productivity)
- Disrupt communications to render the system unusable? (Productivity)
- Abuse the components of the system for other purposes? (Propriety)

It is crucial to evaluate the specific risks of any use case scenario while applying control objectives. The risk assessment involves estimating the probability that some bad thing will happen, along with the potential impact of that unwanted activity, often but not always described in terms of increased costs or reduced revenue.

As IoT scenarios and use cases play out, more unique needs of the security program will arise based on changing threat models. The clearest way to manage risk is to identify the functional control components, particularly into inline and management offerings, that may be organized and aligned into new products that more directly support IoT.

Looking Forward

IDC has defined an IoT taxonomy to describe the architectures and systems that may be used in furthering the development of the 3rd Platform (the foundational technologies of cloud, mobile, analytics, and social). An application of the model and catalog leads to the observations, for each component in the IoT taxonomy, that are discussed in the following subsections.

Hardware: IoT Modules

Devices in the IoT context include sensors, RFID tags, or other such wired or wirelessly enabled devices that are managed by intelligent systems. Intelligent systems are defined as securely managed electronic systems that run a high-level operating system (HLOS) and autonomously connect to the internet, execute native or cloud-based applications, and analyze data collected. Such systems possess greater programmability and performance, integral connectivity, and the potential to capture, analyze, and forward data to and from other systems.

An attacker scrutinizing the (typically wireless) communications among various sensors and devices and their proximally located intelligent systems manager may be able to do the following.

- To the objects:
  - Read sensor and/or system data
  - Manipulate or corrupt sensor and/or system data
  - Delete sensor and/or system data
  - Abuse the sensors or devices
  - Destroy the sensors or devices
- To the local communications:
  - Sniff communications among sensors, devices, and intelligent systems
  - Modify communications by injecting transmissions directly into component activity, by spoofing devices (impersonation), or by replaying legitimate activity
  - Jam communications by overloading the receivers with traffic or injecting noise into the communication stream

The IoT modules/sensors may operate as a "final mile" receiver of content, data, or compute instructions but are more likely to be the "first mile" initiator of data collection and transmission. This IoT component level is likely to be most dynamic, with sensors communicating with the intelligent system or devices communicating with each other, or some combination of the two.

Protection capabilities to identify and authenticate the components of a system are likely to be built in by the manufacturer. Care must be taken to protect any sensitive data on the components of the system, by leveraging encryption, utilizing on-device runtime protection, or simply separating the information and keeping it on another system.

The most likely security solutions at this level include:

- **Data encryption solutions** to ensure any data that is retained on the intelligent system is protected from an attacker. This capability is likely to be an extension of existing encryption solutions.
- **Wireless monitoring solutions** to discover devices, determine whether they are legitimate or rogue, and then track them within a specified location.
- **Embedded security solutions** built into the device firmware to ensure the integrity and security of the IoT device through real-time on-device runtime protection, protecting the device against hijacking, rogue monitoring, and destruction (e.g., memory corruption, device hijacking, control flow hijacking).

Hardware: Servers and Storage

Server and storage components can vary greatly depending on the use case. These components may also be local, in datacenters, or at a service provider location. While the IoT taxonomy places infrastructure as a service in its services category, from an architectural threat modeling perspective, the use cases are the same. Each component in the architecture maintains some level of control over the data and programming flow and should be separately assessed.

Attackers often attack the aggregator components, such as servers and storage, because the information available tends to be more voluminous and therefore valuable. The Willie Sutton principle of robbing the vault because that's where the money is applies here. Attackers may attempt to do the following:

- To the objects:
  - Read the aggregated/stored sensor and/or system data in data repositories
  - Manipulate or corrupt data repositories or programming instructions
  - Delete information or program data
  - Destroy the components
- To the local communications among servers and storage:
  - Sniff communications among servers and storage
  - Modify communications by injecting transmissions directly into component activity, by spoofing devices (impersonation), or by replaying legitimate activity
  - Jam communications by overloading the receivers with traffic or injecting noise into the communication stream

Protection capabilities to identify and authenticate the server and storage components of a system should be built in by the manufacturer. Protection is needed for any sensitive data on the system's components, either by leveraging encryption or by simply separating the information and keeping it on another system.

The most likely security solutions at this level include:

- **Application control solutions** to "harden" servers and storage solutions and minimize the attack surface. These solutions apply to systems that are receiving the data from sensors and devices at the local level and possibly remotely via the internet. This capability is likely to be an extension of an existing security product category that may need to add support for unique operating systems and/or applications.
- **Data encryption solutions** to ensure that data retained on the intelligent system is protected from an attacker. This capability is likely to be an extension of existing encryption solutions.
- **Wireless monitoring solutions** to discover the things, determine whether they are legitimate or rogue, and then track them within a specified location.
- **Edge firewall solutions** to manage communications between an intelligent system and its upstream components on the internet.

Connectivity/Service Enablement

Service providers enable connectivity by deploying networks and operating in a similar manner to the internet, phone, and cable services today. As a part of this enablement, they may incorporate security solutions and services to manage the risks.

At this level, an attacker may be able to:

- Read or sniff communications between the intelligent system and a management server in another location.
- Disrupt control channel communications between the intelligent system and a management server in another location.
- Interfere with the ability to add or remove sensors and devices within a system.
- Steal or manipulate data or programs used in the management process.

The most likely security solutions at this level include:

- **IoT intrusion detection solutions** to monitor the local communications among system components and identify inappropriate devices or sensors. These solutions may maintain state tables to track devices as well as look for anomalous communications. They may require custom devices that can decode protocols and analyze the network traffic accordingly.
- **Communications encryption solutions** to protect the communications between the intelligent systems and the management systems. Often, these communications are more sensitive since they might include aggregated information, sensitive management reports, or control channel data.
- **IoT security gateway solutions** to provide combined security capabilities such as filters, detection, segmentation, and encryption to local systems.

The area of connectivity and service enablement is most likely to see significant innovation as it provides the "sweet spot" of connectivity between the things and some broader management capability. Almost no breach of IoT or OT environments has ever happened without first passing through IT. Providers may consider adding various types of deception services — frequency hopping, jamming, or decoys — to the security program as risks increase, although doing so may be impractical in some cases.

Software: Platforms

At the platform level, service providers may offer management-level controls as part of a use case or an add-on to a general-purpose environment. Since platforms are related more directly to outsourcing and third-party management, the threats themselves become more functional — the need to maintain a properly managed solution. In addition to anticipated security benefits, managed platforms typically yield improvements in efficiency and effectiveness. A variety of solutions are available:

- **Provisioning (and deprovisioning) solutions** can incorporate the need to deploy new sensors or devices and properly identify the applicable components. In addition, since some components may possess legacy components or components with closed operating systems, the ability to rapidly deprovision any pertinent components can be very important.

- **Patch management solutions** may be necessary within the same local environment or strategic geographic locations to provide real-time updates to sensors, devices, and systems that may be ephemeral or dynamic within their systems, as these qualities make it difficult to control and manage the patches directly.
- **Compliance solutions** are necessary to address the regulatory and policy needs of a controlling organization. These solutions may be manual but are more likely to cross into the realm of automated data collection and organization. As the results are aggregated, they can then be mapped to regulations to ensure the prescribed control environment is in place and functioning as intended.
- **Discovery solutions** add versatility and ease of use through a combination of network monitoring and network probing techniques to discover, identify, classify, and assess endpoints leveraging 802.1x infrastructure without requiring network infrastructure changes or endpoint agents in many cases. Although device identification, classification, and status result in important data from a security standpoint, their usefulness extends beyond that of strengthening the on-premises security ecosystem. Modern discovery solutions are experiencing an increasing role as a basic asset management solution to monitor and track devices on a network. This is increasingly becoming an important feature as IoT and OT devices are difficult to discover and monitor through traditional methods.
- **Network segmentation** is enabled through visibility. Device discovery and transparency enable risk assessment and scoring, which in turn allows for policy standards to automatically segment devices on the network.

Software: Analytics/Social Business

When IoT data is aggregated, it may provide the most strategic information within a system. The context and volume of data can paint a significantly detailed picture through pattern analysis and anomaly detection and by using custom algorithms.

This data must be properly protected based on the ease of loss and the value of the data, and the inputs and outputs should be validated, such as sources of data, solutions accessing the data, queries and algorithms used to access the data, and reports or dynamic dashboards used for decision making.

An attacker working at this level may be able to:

- Read, modify, or otherwise disrupt communications (as with the previous levels).
- Steal or manipulate data or programs used in the analysis process.
- Conduct inference attacks against disparate pieces of data to create sensitive information about a target.

From a security perspective, the comparable services at this level are:

- Security monitoring services that observe aggregated traffic. In the tradition of managed security services in use to monitor datacenter activity, branch offices, and enterprises, these solutions may be useful to manage collections of assets, geographic locations, or other elements of the system being evaluated.
- Threat intelligence services that may be leveraged to continually identify intelligent adversaries focused on the specific IoT use cases.

Considering Check Point Software Technologies

Check Point Software Technologies provides governments and enterprises with cybersecurity solutions that are designed to protect against malware, ransomware, and phishing. The company is focused on the following IoT sectors:

- Enterprise smart offices and smart buildings
- Medical devices
- Industrial devices
- IoT manufacturers

Check Point's IoT Protect security solution is built on three tenets:

- **IoT discovery and risk analysis.** Leveraging a discovery engine, Check Point's IoT Protect can identify, classify, and analyze IoT devices, providing identity details such as device type, vendor, model operating system, and OS version. In addition, it will analyze the risk that the device poses in the network based on indicators such as known vulnerabilities and connection types.
- **IoT zero-trust segmentation.** The solution enables customers to configure an access policy for each device based on attributes. Leveraging Check Point's application control service enables policy definition based on application, protocol, or specific command.
- **IoT threat prevention.** Check Point's IoT Protect threat prevention engines such as IPS and Anti-Bot are activated inside the security gateways to identify and block malicious traffic using deep packet inspection technology.

Enterprises typically begin IoT projects with the need for discovery capabilities to map at-risk devices in their environments. For IoT risk analysis, Check Point's IoT Protect discovers devices, assigning each one to a descriptive category (e.g., device type and manufacturer) and mapping its current relationship in the customer's environment.

Check Point's IoT Protect capabilities are actively evolving, as the solution utilizes visibility, network behavior, and segmentation data from many of the company's customers to drive the efficiency and effectiveness of policy creation and enforcement.

Check Point IoT Device Security for Manufacturers

Check Point contends that IoT threat prevention must be conducted within devices and during runtime. To support this goal, the company is utilizing what it calls a Nano Agent, small snippets of code tailored for specific devices. Working with device manufacturers, the Check Point Nano Agent can be installed during the device manufacturing process or added as a software update later on. Once deployed in the customer environment, the Nano Agent sends device information to the Check Point Infinity Cloud. In return, a larger application for each device is sent by Infinity Cloud and installed next to the device's firmware for tailored threat prevention.

Challenges

The market for IoT risk analysis products includes traditional network access control solutions. However, an emerging group of security start-ups are specializing in offering innovative embedded security solutions, such as on-device runtime protection that brings security closer to the device. These new solutions are, in effect, built into the device during the development life cycle and before mass production, enabling the newest evolution in IoT security — devices designed to be secure right out of the box. As devices connect directly to the internet (accelerated by 5G networks), this capability enables real-time threat prevention against sophisticated attacks in enterprise networks or sensitive air-gapped environments (where no connection to the public internet is available, such as defense or healthcare environments). Check Point anticipated this challenge with its December 2019 acquisition of Cymplify, which specializes in device firmware protection.

However, not all device manufacturers or their users will accommodate agent installations (e.g., medical devices already manufactured and deployed). Consequently, alternative approaches such as network-level security will be required, which could add to the cost and complexity of designing and managing IoT security and subsequently restrain market demand. Check Point is positioned to meet this challenge through the combination of its partner integrations in device discovery, extensive threat intelligence engine, and gateways from which to enforce policies and apply virtual patches.

Conclusion

IoT and OT technologies are delivering great value. However, the adoption and proliferation of IoT capabilities also bear new risks.

The IoT is that special environment in which networks, applications, data, and identity need to be addressed in a single offering many times. Therefore, it is crucial to evaluate the specific risks of any use case scenario. The risk assessment involves estimating the probability that some bad thing will happen, along with the potential impact of that unwanted activity, often but not always described in terms of increased costs or reduced revenue.

As IoT scenarios and use cases play out, IDC believes the market for IoT security will continue to grow in importance. To the extent that Check Point can address the challenges described in this paper, the company has a significant opportunity for success, as more unique needs of the security program will arise based on changing threat models.

About the Analysts

Frank Dickson, *Program Vice President, Cybersecurity Products*

Frank Dickson is a Program Vice President within IDC's Cybersecurity Products research practice. In this role, he leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response and Orchestration (AIRO); Identity and Digital Trust; Legal, Risk and Compliance; Data Security; IoT Security; and Cloud Security.

Chris Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Network Security Products and Strategies program covering technologies designed to secure today's complex enterprise networks. The IDC Network Security Products and Strategies practice covers specific functions including firewall/UTM, IDS/IPS, VPN, DDoS mitigation products, cloud security gateway, messaging security, web security, and web application firewall.

Pete Finalle, *Senior Research Analyst, Security*

Pete Finalle is a Senior Analyst for IDC's Security team, currently responsible for the appliance tracker. Mr. Finalle's core research coverage area is currently focused on security hardware base year/market share quantitative information, forecasting, and qualitative analysis.

Robyn Westervelt, *Research Director, Security and Trust*

Robyn Westervelt is a Research Director within IDC's Security and Trust group. She leads IDC's data security practice and provides insight and thought leadership in the areas of encryption, tokenization, data loss prevention, and other data protection, risk mitigation, and compliance technologies. She also contributes thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT).

MESSAGE FROM THE SPONSOR

About Check Point Software

Check Point Software Technologies Ltd. (***www.checkpoint.com***) is a leading provider of cybersecurity solutions to governments and corporate enterprises globally. Its solutions protect customers from sophisticated 5th generation cyberattacks with an industry-leading catch rate of malware, ransomware, and other types of attacks. Check Point offers its multilevel security architecture, Infinity Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Determine your IoT security risk through a Free IoT Security Check Up and Device Firmware assessment. Sign up today at ***https://www.checkpoint.com/products/iot-security/***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com