Microsoft

Evaluating Your IoT Security

How to approach the new threats and consequences facing your business with the Internet of Things

Published: March 2017

For the latest information, please see www.InternetofYourThings.com

Microsoft

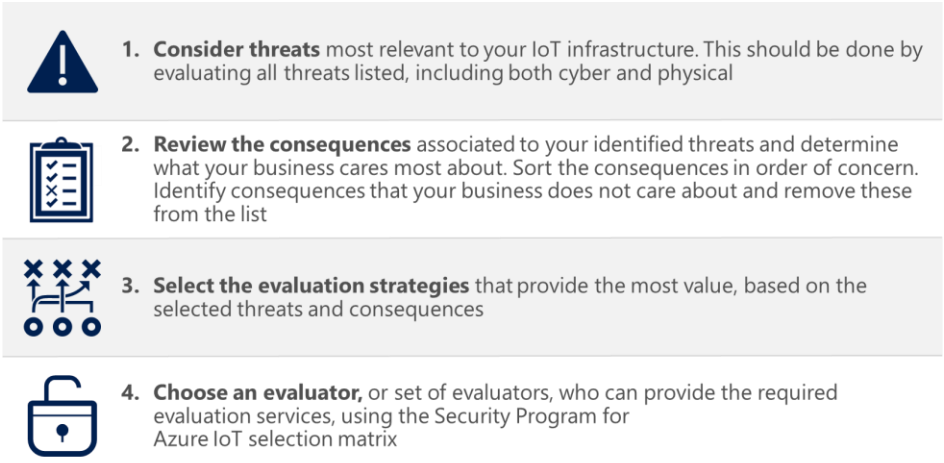
Executive Summary

Securing an end-to-end Internet of Things infrastructure is a challenging technical and logistical undertaking. Merging the cyber and the physical makes this task even more complex. This document provides a framework for the evaluation of IoT security in businesses. The *IoT Security Evaluation Framework* is a step-by-step guide for reasoning through threats affecting an IoT infrastructure using the existing threat models defined by the security community, linking these threats to consequences, and defining evaluation strategies which can detect flaws in IoT infrastructures.

The *IoT Security Evaluation Framework* is designed to be used by businesses who may already have an IoT infrastructure deployed or are in the process of designing or deploying one. Ideally, this framework is to be used by designers and developers who both understand their business and have a basic understanding of security threats and evaluation strategies.

The *IoT Security Evaluation Framework* is composed of two parts. The first defines the associations between specific threats, consequences, and evaluation strategies. The second links evaluation strategies with security evaluators enrolled in the Security Program for Azure IoT.

Figure 1: Microsoft's IoT Security Evaluation Framework summary



Microsoft

Contents

Microsoft

Introduction

The Internet of Things (IoT) is bringing together cyber infrastructure with the physical world. Cyber infrastructure includes Information Technology (IT) assets such as data storage, cloud services, operating systems, applications, various network technologies, backup services, monitoring, and security mechanisms like authentication, authorization, and auditing. The physical infrastructure includes devices and sensors of all shapes and form factors along with the control systems which ensure these elements function appropriately.

Securing the IT portion of an IoT infrastructure is necessary but insufficient. Even if an infrastructure is protected by advanced IT security techniques, any compromise of the physical devices and sensors may result in a compromised end-to-end IoT infrastructure. Such a compromised infrastructure could result in spoofed devices, and data generated from such devices may not be trustworthy. Similarly, if the control systems of an IoT infrastructure are compromised, the infrastructure could be used to inflict not just data breaches and unreliable operations but also physical harm to the facilities, or worse, to the humans operating in those facilities.

Securing an IoT infrastructure requires an end-to-end approach, from the physical devices and sensors to the services and data in the cloud. Articulation of this end-to-end IoT security requirement remains a challenge because an IoT infrastructure is usually designed, deployed, and operated by not only IT experts, but also designers, developers, and operators of physical devices and machines. These two paradigms may not have the same goals in mind. As an example, for IT infrastructure designers, security and privacy may be one of the more important functions of the system, together with functionality, usability, and cost. However, designers of physical machines may consider the safety of the machine, availability, and reliability to be more important. When these two designs merge to form an IoT infrastructure, the lack of end-to-end security design and oversight may result in a system with significant security flaws.

In this document, we provide a framework to evaluate IoT security end-to-end, with a view to improve both cyber security and physical implications of cyber security breaches. The approach of this document is to introduce common threats to the IoT infrastructure, identify the business consequences of these threats, and propose strategies and methodologies to conduct security evaluations regarding these consequences. These evaluations may require a member of the Security Program for Azure IoT, a group of security evaluators who possess the expertise, knowledge, and tools to conduct such evaluations.

Key Features of the IoT Security Evaluation Framework

This document provides a framework for an end-to-end security evaluation of an IoT infrastructure. Key features of this evaluation framework are described below:

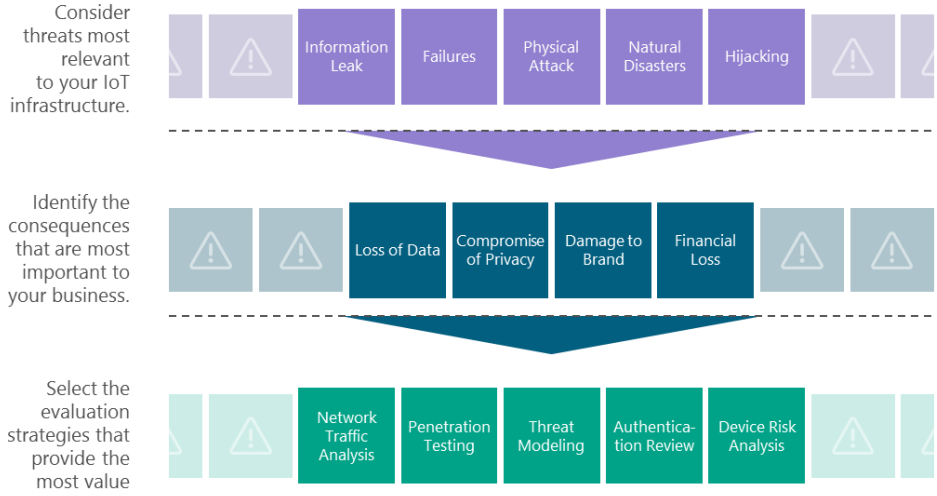
- **Real-world context** – This framework addresses real world threats, scenarios, and technologies. The outcome of the evaluation is directly applicable to the IoT infrastructure in question and is actionable.

- **Appropriate security guidance** – This framework provides security guidance appropriate to the scenario and use case. Security measures in consumer devices, for example, are not the same as those in business-critical infrastructure. Striking the right balance of security measures is important to keeping them actionable and practical.
- **Address IoT threats** – This framework addresses threats to both cyber security and physical infrastructure and recommends evaluation strategies accordingly.
- **Adaptable and extensible** – As the design of an IoT infrastructure evolves and as threats become more sophisticated and shift focus, this framework can be adapted to stay relevant in the long run.

Threats, consequences, and evaluation strategies

In this section, we provide details of threats to an IoT infrastructure, consequences of such threats to businesses and organizations, and evaluation strategies to detect and mitigate such threats.

Figure 2: Picking the right security evaluation strategy for your business.



Taxonomy of IoT threats

There are several existing threat models for defining threats to an IT infrastructure. Many of these models are being adapted to include IoT threats as well. Some of the more common ones include:

- **Microsoft's STRIDE threat model:** STRIDE is Microsoft's taxonomy of threats and their associated mitigation strategies. STRIDE stands for *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, and *Elevation of privilege*. In addition, Microsoft also offers tools based on the STRIDE model that capture and analyze architectural components, identify threats, and recommend actionable mitigations. You can learn more about how the STRIDE model has been adapted to address IoT threats here.
- **OWASP IoT Vulnerabilities Project:** The Open Web Application Security Project (OWASP) has defined IoT vulnerabilities, released in order of occurrence in specific timeframes. For each of the top IoT vulnerabilities, this model provides a summary and defines the associated attack surface.[1]
- **European Union Agency for Network and Information Security (ENISA) Threat Taxonomy:** This taxonomy provides a rich and multi-level definition of threats. The threat model includes threats to infrastructure from physical attack vectors such as natural disasters or legal actions.[2]

Note that the above is a small sample of threat models developed by security experts for analyzing IT and IoT environments. Businesses and organizations may develop or adapt these or other models to their own environments.

ENISA's taxonomy provides a library of threats related to a wide range of attack vectors, both cyber and physical. The following provides a summary of the ENISA taxonomy of threats and their effects on an IoT infrastructure. We will use this taxonomy for the rest of this document.

- **Nefarious activity and abuse** – This implies malicious abuse to infrastructure and results in some form of gain for the perpetrators of such attacks. In some cases, this may damage a business' or country's reputation. Identity fraud, denial of service, abuse of software or services, abuse of authorization, breach of personal data, and use of malware are just some examples of such threats. The distributed nature of IoT and the deployment of low-cost devices can make an infrastructure particularly vulnerable to these kinds of threats.
- **Eavesdropping, interception and hijacking** - This may also yield considerable gains for the perpetrators. Examples of these kinds of threats include communication interceptions, man-in-the-middle attacks, and repudiation of actions. In an IoT context, these threats can create much more harm than just a loss of data control. They may also lead to malicious control of devices, which introduces further risks to an organization's employees and property.
- **Outages** – The threat of outages in the IoT context can have significant consequences, such as lack of power, water, or cooling. Outages can also lead to system-wide failures, which may disrupt a company's services and infrastructure.

[1] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities
[2] https://www.enisa.europa.eu/publications/etl2015

- **Legal** – The threat of legal actions, such as court orders, regulations breaches, and compliance failures can have serious consequences for business, governments and other entities.
- **Physical attacks** – Physical attacks on an IoT infrastructure can lead to the loss of productivity and profit. Physical attacks can be of the form of theft, vandalism, collateral damage, or physical inaccessibility.
- **Unintentional damages** – Accidental damage to IoT infrastructure may be include information leaks, improper design, operations disruption due to carelessness.
- **Disasters** – Physical devices can make an IoT infrastructure particularly vulnerable to disasters. These may include natural disasters, such as storms, earthquakes, and floods or environmental disasters, such as pollution, dust, and corrosion.
- **Damage and loss of assets** – Device damage or the loss of physical assets may disrupt the data and operations within an IoT infrastructure.
- **Failure and malfunctions** – Failures and malfunctions in software systems can manifest as software bugs or design flaws. In a physical system, these may be caused by machine breakdowns, power outages, or services failures. Design flaws in physical devices may result in massive disruption to business operations.

Consequences of threats to IoT infrastructure

In order to better understand the IoT threat landscape and prioritize the right mitigations, it is important to correlate these threats with business consequences. The threats to an IoT infrastructure may impact normal operations resulting in a loss of productivity, visibility, operations and services. Some threats may result in financial damage to the operator or damage to brand.

Below is a list of consequences which may affect an IoT infrastructure.

- **Damage to brand (DB)** – This may have the most long-term impact to businesses, organizations, and governments. It may also lead to additional consequences, such as financial loss.
- **Financial loss (FL)** – This may include a direct financial loss due to theft or indirect loss due to losses in productivity or sales.
- **Loss of data (LD)** – As businesses become increasingly reliant on data, any loss of data or intellectual property can be costly.
- **Loss of control (LC)** – Many organizations depend on an IoT Infrastructure for their business control systems. A loss of control could be extremely detrimental to business operations.
- **Compromise of privacy (CP)** – Any breach of privacy for both individuals and businesses can have significant social implications, leading to further consequences like damage to brand and financial loss.
- **Loss of property (LP)** – This involves either physical damage to property or a loss of property. Both can create a financial loss for organizations.

- **Loss of life (LL)** – With IoT controlling physical devices such as cars, robotic arms, and critical infrastructure, injury to humans and the loss of life is a concern to prioritize.
- **Environmental damage (ED)** – Malicious activity or malfunctioning IoT infrastructure can cause catastrophic environmental damage. This concern is especially highlighted in industrial infrastructure, such as oil rigs.
- **Service disruption (SD)** – With an IoT infrastructure, disruption can affect both a business' physical services and services delivered to end-customers.

Evaluation strategies

The evaluation of an IoT infrastructure involves a broad range of processes, tools, and methodologies. Selecting the right evaluation strategies is an important step towards securing your end-to-end IoT infrastructure. This section provides guidance on when to apply these strategies during the lifecycle of an IoT infrastructure's design, development, deployment and operations.

Below are a few evaluation strategies:

- **Threat modeling** – This involves the analysis of infrastructure design to discover threats and define mitigations. There are several tools available to help with this evaluation, but one popular option is the STRIDE Threat Modeling tool.
- **Deployment reviews** – This involves a formal review and analysis of plans throughout the design, development, and deployment stages of an IoT infrastructure. Security processes for provisioning devices and maintaining fleets may be evaluated in this review. For an existing infrastructure, businesses may also evaluate audit logs and device configurations. A deployment review may include reviewing strategies for de-commissioning or changing ownership of IoT devices. These reviews are important to maintain both user and organizational privacy. Finally, deployment reviews may also be conducted on any planned or existing cloud services and gateways.
- **Authentication and access control review** – This review involves an end-to-end analysis of authentication and access control models used in an IoT deployment. This should involve a complete analysis of a device's operating system as well as any authentication scheme used in the cloud or the device, including certificate management. This also involves a review of existing password creation and change policies.
- **Device risk analysis** – IoT devices are designed and created by a variety of device manufacturers, who must adhere to various standards and regulations. A thorough analysis of device hardware and software provides a better understanding of the attack surface and threats associated with the device. This can also be used to discover any exploits of the device during its operation in order to ensure healthy operations.
- **Device firmware deployment review** – During the lifetime of an IoT device, new bugs will be discovered and the firmware will inevitably need to be updated. A review of the firmware deployment and re-deployment strategy provides a clear

understanding of gaps in this process. Some IoT devices and gateways may host more featured operating systems, which need to be updated frequently.

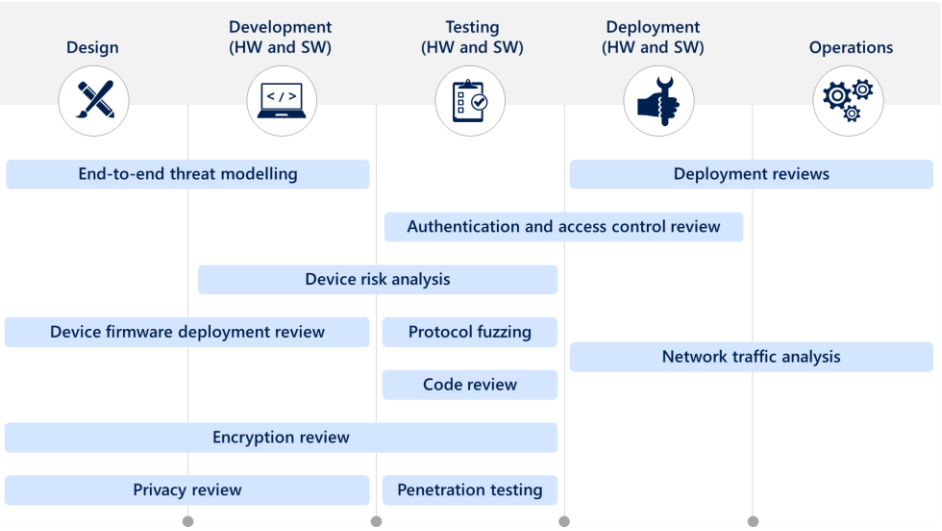
- **Protocol fuzzing** – Communications between devices, gateways, and cloud services are made possible by using various protocols. A standards-based approach allows greater compatibility and security. Minimizing the vulnerabilities in protocol design and implementation reduces the risk of protocols being exploited.
- **Network traffic analysis** – Many of the threats listed above exploit network topologies and traffic patterns. This exploit is exacerbated by specialized protocols such as Supervisory Control and Data Acquisition (SCADA)[3] which may not have been designed with an IoT architecture in mind. A thorough analysis of network traffic mitigates this risk.
- **Code Review** – A black and white box review of all code running on devices, gateways, and the cloud helps uncover vulnerabilities created during software development or integration.
- **Encryption review** – Reviewing the encryption algorithms using by both the devices and the cloud allow a better understanding of the attack surface.
- **Penetration testing** – Conducting an end-to-end penetration test of the solution can uncover risks in each component and at the interfaces of components.
- **Privacy Review** – This includes an end-to-end review of an IoT infrastructure design to evaluate if individual and organization privacy is maintained. This also includes the protection of an organization's IP.

Each of these techniques should result in an actionable report which can be used to improve the security of the IoT infrastructure.

The above-mentioned evaluation strategies are applicable at various stages of design, development, testing, deployment and operations of an IoT infrastructure. Figure 3 below offers a recommendation on when to use each evaluation strategy. Another important operations strategy may be to have a security incident response plan defining actions to be taken in case of security incidents.

[3] https://en.wikipedia.org/wiki/SCADA

Figure 3: Security evaluation strategies by IoT project lifecycle stage



Some evaluation strategies may span multiple phases. As an example, while network analysis may be conducted at the time of deployment, it may also be repeated regularly following deployment to detect any malicious activity. Similarly, end-to-end threat modeling is primarily performed in the design stage, but it may also be repeated in the development phases to confirm that any threats discovered during design are addressed. Encryption reviews may recur throughout the design, development, and testing phases to ensure the right algorithm is selected initially, implemented correctly, and validated thoroughly.

Security evaluation framework

Selecting an evaluation strategy that works in every IoT Infrastructure is a challenging exercise. While an ideal IoT deployment may benefit from applying all of the evaluation techniques listed above, it may not be practical to do so. For any security evaluation, it's important to balance the benefit with the cost in time and money.

Table 1 provides one way to think through this selection process by providing links between the threats, consequences, and evaluation strategies. Sometimes a single evaluation strategy may address multiple consequences.

Figure 4: Sample from IoT security evaluation framework (see Appendix for full table)

High-Level Threats	Threats	Primary Consequence	Evaluation strategy
Physical attack (deliberate/ intentional)	*Vandalism*	*Damage to brand*	*Deployment reviews*
	Theft (devices, storage media and documents)	*Financial loss*	*Deployment reviews*
	Information leakage/sharing	*Compromise of privacy*	*End-to-end threat modeling*
Unintentional damage / loss of information or IT assets	*Information leakage/sharing due to human error*	*Compromise of privacy*	*Encryption review*
	Erroneous use or administration of devices and systems	*Loss of data*	*Encryption review*
	Using information from an unreliable	*Loss of control*	*Threat modeling*

Microsoft

Azure IoT Security Program

For many businesses, securing both the cyber and physical aspects of their IoT infrastructure is complicated. It requires careful collaboration between device manufacturers, resellers, deployers, solution developers, cloud providers, and operators. The Security Program for Azure IoT addresses this need by providing security assessments, analyses, and recommendations for customers who are deploying an IoT solution.

The goal of this program is to provide our customers with an opportunity to find the best possible security evaluators for evaluating their end-to-end IoT infrastructure. This security evaluation can encompass a wide range of technologies, including IoT device manufacturing, hardware integration, solution development, solution deployment, cloud operations, data security, and privacy management. Some evaluators may have expertise in multiple, or even all of these areas.

We provide a list of all current security evaluators, along with their current expertise here.

Microsoft

Conclusion

The Internet of Things can deliver amazing value to organizations by reducing costs, increasing revenue, and transforming business. But these IoT transformations are incomplete and unsustainable without a secure infrastructure, one that is protected from the physical devices and sensors to the services and data in the cloud.

Microsoft and its partners have extensive experience with developing, deploying and evaluating secure software and devices and continue to be leaders in this new age of IoT. For more information, check out the resources listed below, and discover how we can help you secure the Internet of Your Things.

Learn More

- Explore Microsoft's IoT offerings at www.InternetofYourThings.com
- Find evaluator partners in the Security Program for Azure IoT
- Begin a trial solution of Azure IoT Suite

Microsoft

Appendix

Table 1: Evaluation framework for end-to-end IoT security evaluation

High-Level Threats	Threats	Primary Consequence	Evaluation strategy
Physical attack (deliberate/ intentional)	*Vandalism*	*Damage to brand*	*Deployment reviews*
	Theft (devices, storage media and documents)	*Financial loss*	*Deployment reviews*
	Information leakage/sharing	*Compromise of privacy*	*End-to-end threat modeling*
Unintentional damage / loss of information or IT assets	*Information leakage/sharing due to human error*	*Compromise of privacy*	*Encryption review*
	Erroneous use or administration of devices and systems	*Loss of data*	*Encryption review*
	Using information from an unreliable source	*Loss of control*	*Threat modeling*
	Unintentional change of data in an information system	*Loss of data*	*Authentication and access control review*
	Inadequate design and planning or improperly adaptation	*Loss of data*	*Privacy Review*
	Loss of information in the cloud	*Loss of data*	*Privacy Review*
	Loss of (integrity of) sensitive information	*Loss of data*	*Encryption review*
	Loss of devices, storage media and documents	*Loss of data*	*Threat modeling*
	Destruction of records	*Loss of data*	*Threat modeling*
Disaster (natural, environmental)	*Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)*	*Service disruption*	*Deployment reviews*
	Fire	*Service disruption*	*Deployment reviews*
	Pollution, dust, corrosion	*Service disruption*	*Deployment reviews*
	Thunder strike	*Loss of life*	*Deployment reviews*
	Water	*Loss of property*	*Deployment reviews*
	Explosion	*Loss of property*	*Deployment reviews*
	Dangerous radiation leak	*Loss of life*	*Deployment reviews*
	Unfavorable climatic conditions	*Loss of life*	*Deployment reviews*
	Major events in the environment	*Service disruption*	*Deployment reviews*
	Threats from space / Electromagnetic storm	*Loss of property*	*Deployment reviews*
Failures/ Malfunction	*Failure of devices or systems*	*Loss of control*	*Device risk analysis*
	Failure or disruption of main supply	*Loss of control*	*Deployment reviews*
	Failure or disruption of service providers (supply chain)	*Loss of control*	*Deployment reviews*
	Malfunction of equipment (devices or systems)	*Loss of control*	*Device risk analysis*
Outages	*Loss of resources*	*Loss of control*	*Deployment reviews*
	Internet outage	*Loss of control*	*Deployment reviews*
	Network outage	*Loss of control*	*Deployment reviews*

Microsoft

High Level Threats	Threats	Primary Consequence	Evaluation strategy
Eavesdropping/ Interception/ Hijacking	*Interception of information*	*Compromise of privacy*	*Privacy Review*
	Interfering radiation	*Service disruption*	*Deployment reviews*
	Replay of messages	*Loss of control*	*Protocol fuzzing*
	Network Reconnaissance, Network traffic manipulation and Information gathering	*Compromise of privacy*	*Penetration testing*
	Man in the middle/ Session hijacking	*Loss of data*	*Code Review*
Nefarious Activity/Abuse	*Identity theft (Identity Fraud/ Account)*	*Damage to brand*	*Threat modeling*
	Denial of service	*Loss of control*	*Threat modeling*
	Malicious code/ software/ activity	*Loss of data*	*Code Review*
	Social Engineering	*Compromise of privacy*	*Deployment reviews*
	Abuse of Information Leakage	*Loss of data*	*Network traffic analysis*
	Generation and use of rogue certificates	*Loss of data*	*Authentication and access control review*
	Manipulation of hardware and software	*Loss of control*	*Device risk analysis*
	Manipulation of information	*Loss of control*	*Penetration testing*
	Misuse of audit tools	*Compromise of privacy*	*Deployment reviews*
	Misuse of information/ information systems (including mobile apps)	*Compromise of privacy*	*Deployment reviews*
	Unauthorized activities	*Financial loss*	*Authentication and access control review*
	Unauthorized installation of software	*Service disruption*	*Penetration testing*
	Compromising confidential information (data breaches)	*Loss of data*	*Penetration testing*
	Remote activity (execution)	*Loss of control*	*Threat modeling*
	Targeted attacks (APTs etc.)	*Loss of control*	*Penetration testing*
	Brute force	*Loss of control*	*Penetration testing*
	Abuse of authorizations	*Compromise of privacy*	*Authentication and access control review*
Legal	*Violation of laws or regulations / Breach of legislation*	*Damage to brand*	*Threat modeling*
	Failure to meet contractual requirements	*Financial loss*	*Threat modeling*