

# IoT Security Reference Architecture

Reference Architecture Series



# IoT Security Reference Architecture for the Enterprise

September 2018

## Executive Summary

The appetite for IoT devices has grown rapidly in recent years as consumers and enterprises look to take advantage of the seamless connections between people, devices, networks, and physical services. The influx of IoT devices, however, has opened up new entry points into enterprise networks that cyber criminals can exploit. Current IoT security management standards and regulations are proving to be inadequate and overly confusing in the face of enterprises' efforts to secure a diverse ecosystem of legacy and new devices.

Kudelski Security acknowledges that enterprises, whether by design or by default – have already become major consumers of IoT solutions. We also accept that the extent of the business impact of IoT will largely depend on their ability to overcome the challenges inherent to securing IoT devices. Building on 30 years of experience in helping organizations to design, run, and sustain comprehensive security programs, Kudelski Security has devised the IoT Security Reference Architecture to guide enterprises in protecting their IoT ecosystems.

This paper presents a comprehensive review of the IoT architecture, security threats, and challenges as well as a set of recommendations and highlighted vendor solutions, which aid organizations in securing their IoT ecosystems through people, process, policy, and technical measures.

The approach described is primarily targeted at addressing the cybersecurity risks of organizations that have already deployed a large number of IoT devices. For those considering greenfield or next-generation IoT device implementations, we strongly recommend taking a “security by design” approach. This embeds a strong root of trust into each device or endpoint, enabling a wide range of robust device, data, and access protections designed to actively secure the entire device lifecycle. The “security by design” approach – though outside the scope of this paper – is briefly described in Appendix A, which introduces the Kudelski IoT Security Suite designed for precisely that purpose.

## Table of Contents

Executive Summary .....	2
Introduction.....	4
The 4 Layers of IoT Architecture.....	5
IoT Security Threats, Impacts, and Challenges .....	6
Threats.....	6
Impacts .....	10
IoT Security Impact: A Case Study – Unleashing Mirai.....	11
Security Challenges .....	12
IoT Security Reference Architecture .....	14
People, Policy, and Procedures .....	15
Technical Measures .....	21
Conclusion.....	32
Appendix A: Kudelski Security’s IoT Security Suite .....	33
Appendix B: Questions to ask IoT Vendors (During Procurement) .....	37
Appendix C: Common Cybersecurity Standards and Regulations .....	41
About the Author .....	46
About Kudelski Security .....	47

## Introduction

### IoT Solution Implementation

- **In their 2018 State of IT report, [Spiceworks](#) claims that 29% of enterprises have already implemented IoT solutions, and this is expected to surge to 48% by year end, as businesses are increasingly sold on the cost-savings and the productivity-enhancing benefits of IoT.**

IoT devices have become pervasive, and even essential, in many aspects of our day-to-day life; from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to enterprises and homes. While the benefits of IoT devices are undeniable, so too is the reality that security is not keeping pace with innovation.

In 2015, researchers demonstrated how Jeep vehicles could be remotely hijacked. In 2016, Mirai wreaked havoc on the OVH hosting provider and on the DNS provider, Dyn, resulting in denial of access to several popular websites such as Netflix and PayPal. In 2017, BrickerBot incapacitated poorly secured IoT devices, and in 2018, researchers discovered the Z-downgrade attack, which left 100 million IoT devices open to unauthorized access. It is estimated that by 2020, 25 percent of cyberattacks will target IoT devices.<sup>1</sup>

Where the business typically sees opportunity, security professionals have, rightly, taken note of the IoT-related risks. When enterprise security professionals were asked to name the two threat vectors that pose the largest risk to enterprise network security, 44.3 percent mentioned IoT devices, second only to email, which topped the list at 44.8 percent. Taking it a step further, 99 percent of those surveyed said Amazon Echo and other chatbot devices pose a security risk to the enterprise, and a majority (62.1 percent) believed they should be banned from work environments.<sup>2</sup>

While there seems to be overwhelming consensus in the security community that these web-enabled devices pose a threat, it is unrealistic to assume an outright ban would work. Efforts should rather focus on developing a dedicated plan to secure the IoT devices, especially given how an IoT architecture – with its disparate protocols, software, and hardware – differs from the traditional enterprise network. Integrating IoT devices into enterprise networks will require new risk management strategies and updated operational security strategies with the level of protection for a given asset greatly depending on its use case and the

### Common Questions to Assess IoT Security Level

- **Do you have full visibility into your IoT assets?**
- **Do you know what sensitive data they collect and what they connect to?**
- **Are all your IoT assets securely configured and managed?**
- **What are the most common vulnerabilities and effective attacks against your IoT assets?**
- **Can you contain and analyze an IoT attack?**

<sup>1</sup> <https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf>

<sup>2</sup> <https://www.helpnetsecurity.com/2018/05/25/future-cryptocurrencies-cryptomining/>

criticality of the application it supports.

To that end, the following sections of this paper will detail the unique components of an IoT architecture and the IoT security threats, impacts, and challenges. This provides a structure around which we have determined a set of recommendations on privacy and security controls that address IoT cybersecurity risks to enterprises that have already deployed IoT solutions in their environment. The paper however, does not address the cybersecurity risks associated with OT or IIoT, but related information can be obtained from our whitepaper, *Operation Technology: The next cyber battlefield*<sup>3</sup>.

## The 4 Layers of IoT Architecture

The fundamentals of an IoT architecture are quite similar to that of traditional IT architecture with multiple endpoints. The main difference is the scale and diversity of the IoT endpoints. Enterprises cannot always guarantee the security of the IoT device, and therefore, understanding and properly setting up each of the four layers in the IoT architecture is critical to preventing compromise.

### Device Layer

The device layer is where the digital world meets the "real world." This layer consists of IoT hardware, software, sensors, and actuators. IoT devices are susceptible to spoofing, tampering, theft, elevation of privilege, information disclosure, and repudiation threats. Compromise of IoT devices can lead to data breach, mass service interruptions, privacy violation, extortion, and reputational damage to enterprises.

### Communication Layer

The communication layer defines the communication protocols, network technologies, and communications service providers (CSPs) necessary for the IoT system. It may also define the necessary security protocols (e.g. data transport layer security DTLS) or other security mechanisms (e.g. X.509 certificates). In general, this layer is susceptible to eavesdropping, tampering, information disclosure, spoofing, and denial of service. Compromise of the communication layer can result in service

---

<sup>3</sup> <https://resources.kudelskisecurity.com/en/operational-technology-whitepaper>

interruptions, data breach, and eventual reputational and operational damage.

## Cloud Platform Layer

The cloud platform layer is the layer that ensures end-to-end semantic consistency of data objects throughout the distributed IoT system. It describes how data flows into, out of, and through the system, as well as how it is transformed and stored. It also contains the features and intelligence that gives an organization its competitive advantage. It provides stream processing, event processing, dispatching, orchestration, analytics, algorithms, and machine learning necessary to meet the needs of the business.

This layer includes all web-based services and cloud infrastructure and is susceptible to threats like tampering, information disclosure, elevation of privilege, theft, and denial of service. A compromise of a cloud platform can be devastating to an enterprise. It could lead to data breaches, extortion, prolonged service interruptions, privacy violations, reputational, and operational damages.

## Process Layer

The process layer focuses on how the organization will integrate IoT projects with governance, operations, and management processes, and line-of-business systems. The weakest link in a cybersecurity architecture is people. Their negligence in understanding and implementing cybersecurity practices and policies can render the entire ecosystem vulnerable to debilitating cyberattacks. These attacks include repudiation and theft of sensitive information, such as intellectual property, and could result in reputational damages and lawsuits.

## IoT Security Threats, Impacts, and Challenges

### Threats

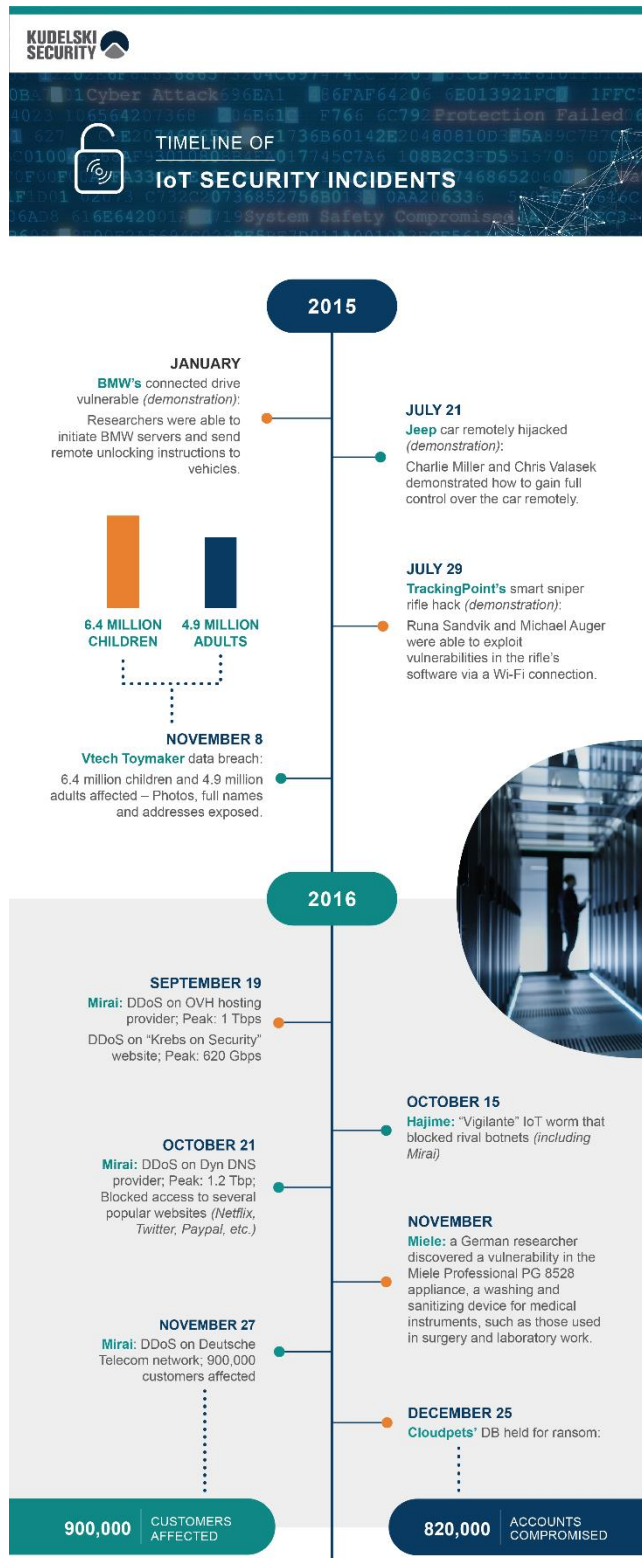
The sophistication of cyberattacks directed at IoT devices is unceasing and on the rise. Where 2015 saw the rise of remote hacks on internet-connected vehicles, 2016 saw the emergence of an IoT-based botnet that almost crippled the internet. Similarly, 2017 and 2018 witnessed the growth of IoT-based botnet variants, malwares, and cryptominers alike. The figure below illustrates relevant IoT security incidents that have

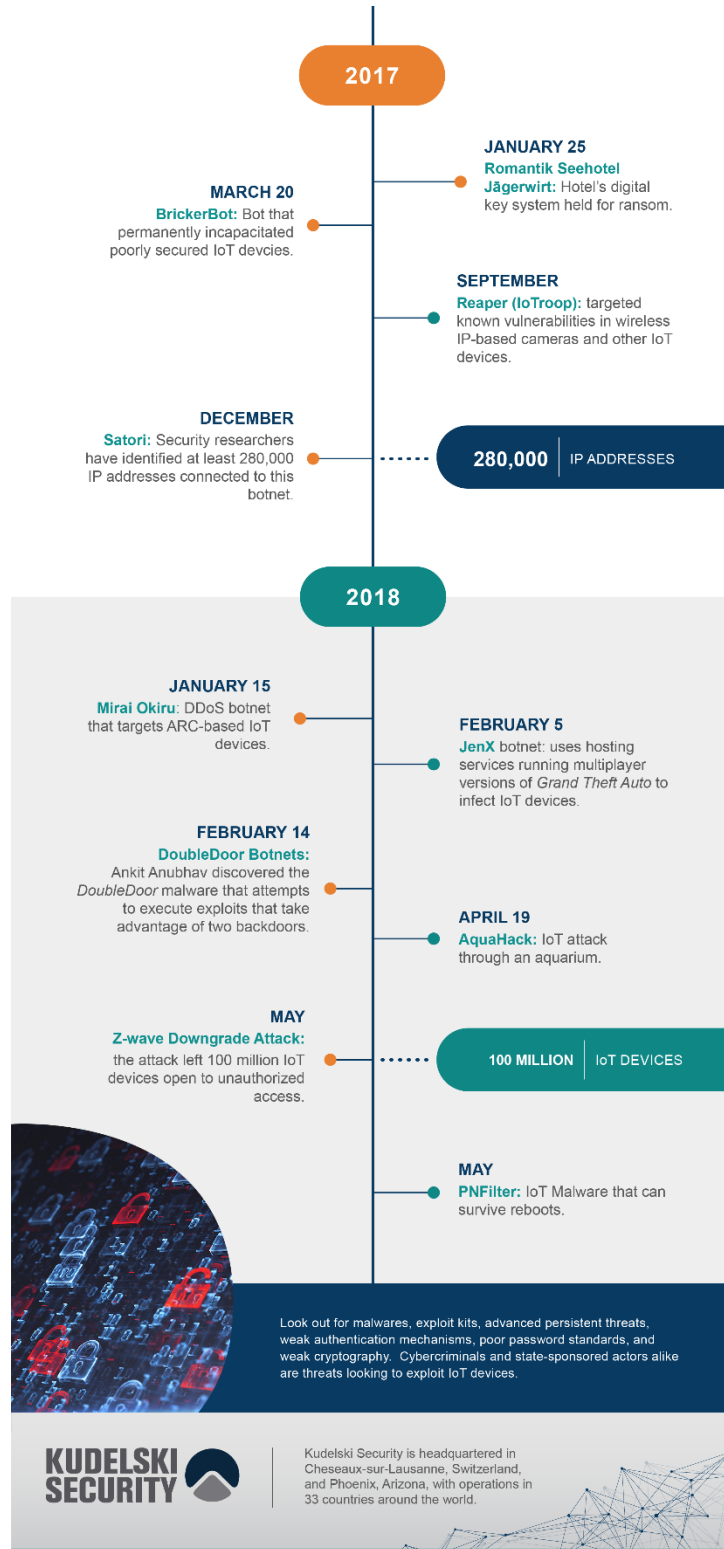
IoT Security is considered a Commodity

**There is a fundamental disconnect between the desire for security and the willingness to pay for it among its users. It was found that 31 percent of semiconductor leaders claimed that their manufacturing customers want to try to avoid all security breaches at any cost; but only 15 percent of respondents believed that their customers would be willing to pay a premium higher than 20 percent for the next tier of enhanced chip security. Customers either are unwilling to pay any premium or expect security costs to decline.**



shaped the IoT threat landscape over the years. From this, it is evident that IoT threats are widespread, varied, and quickly evolving.







It would be difficult to comprehensively list the threats posed to an IoT ecosystem; however, some of the most notorious and notable risks include: malware (e.g. Mirai, Satori, Brickerbot, and VPNFilter), exploit kits (e.g. RIG), advanced persistent threats (e.g. Stuxnet), weak authentication mechanisms, poor password standards, weak cryptography that enables man-in-the middle attacks, session hijacking, and protocol hijacking. Cybercriminals and state-sponsored actors also pose threats as they seek to exploit IoT devices in order to eavesdrop, collate information, steal sensitive data, extort, or instill operational or reputational damage by causing service interruptions.

For the purpose of illustrating the IoT threat landscape, we are using the Microsoft's threat model, STRIDE and the IoT threat model as defined by Microsoft<sup>4</sup>:

**Spoofing:** A spoofing attack occurs when an attacker pretends to be someone they're not. An attacker may extract cryptographic key material from a device, either at the software or hardware level, and subsequently access the system with a different physical or virtual device under the identity of the device the key material has been taken from. A good illustration is a remote control that can turn on any TV. This also involves identity theft to authenticate user accesses.

**Denial of Service:** Denial of service threats occur when an attacker can degrade or deny service to users. A device can be rendered incapable of functioning or communicating by interfering with radio frequencies or cutting wires. For example, a surveillance camera that had its power or network connection intentionally knocked out cannot report data at all. And, as we saw with Mirai, a network of those same network-connected cameras and other poorly-secured IoT devices can be compromised and serve as the source of an Internet-scale denial of service attack.

**Tampering:** An attacker may partially or wholly replace the software running on the device, potentially allowing the replaced software to leverage the genuine identity of the device if the key material or the cryptographic facilities holding key materials were available to the illicit program. For example, an attacker may leverage extracted key material to intercept and suppress data from the device on the communication path and replace it with false data that is authenticated with the stolen

---

<sup>4</sup> <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture>

key material. This also involves manipulation of data in servers and clients.

**Repudiation:** This occurs when someone performs an action and then claims that they did not actually do it. It primarily shows up on operations like credit card transactions. A user purchases something and then claims that they didn't actually make the purchase. Email is another example. If I receive an email from you, you can claim that you never sent it.

**Information Disclosure:** If the device is running manipulated software, it could potentially leak data to unauthorized parties. For example, an attacker may leverage extracted key material to inject itself into the communication path between the device and a controller, field gateway, or cloud gateway to siphon off information.

**Elevation of Privilege:** This happens when a device that has a specific function can be forced to do something else. For example, a valve that is programmed to open half way can be tricked to open all the way.

**Theft:** This involves physically stealing the device, intellectual property, or stealing data while in transit or at rest through eavesdropping.

### Impacts

To grasp the full extent of IoT threat landscape, the table below (IoT Threat Landscape) illustrates the threats associated at each layer of an IoT Architecture and its corresponding impact on enterprises. Understanding what needs to be secured and from which threats, is the first step in developing comprehensive security measures to protect an IoT ecosystem and, hence, the enterprise as a whole.

Layer	Threats	Impact
Process Layer	Theft, Repudiation	Intellectual Property theft, Lawsuits, Reputational Damage
Cloud Platform Layer	Tampering, Information Disclosure, Elevation of Privilege, Theft, Denial of Service	Data Breach, Extortion, Service Interruption, Privacy Violation, Reputational damage
Communication Layer	Tampering, Information Disclosure, Denial of Service, Spoofing	Data Breach, Service Interruption, Privacy Violation, Reputational damage, Fraud
Device Layer	Spoofing, Denial of Service, Tampering, Information Disclosure, Elevation of Privilege, Theft, Repudiation	Fraud, Service Interruption, Data Breach, Privacy Violation, Fraud, Extortion, Reputational damage
<b>IoT Threat Landscape</b>		

## IoT Security Impact: A Case Study – Unleashing Mirai

Mirai is the infamous IoT botnet that took down major websites via a massive distributed denial-of-service attack using hundreds of thousands of compromised IoT devices. Mirai's first big wave of attacks came in September 2016 against the Krebs on Security website, followed by an attack on the French hosting provider, OVH. Simultaneously, the author of the malware leaked the code of the malware online, resulting in copycats attacking the Dyn DNS provider (an attack that crippled major websites like Amazon, Twitter, and PayPal) and Deutsche Telekom, a German Internet provider (affecting more than 900,000 of its customers). Investigation into these attacks uncovered 49,657 unique IP addresses, assigned mostly to CCTV cameras, in more than 164 countries.<sup>5</sup>

**The Impact:** The Mirai botnet attack took managed DNS services from New Hampshire-based Dyn offline in October 2016, causing short-lived pain for Internet users trying to reach popular web sites like PayPal, Twitter, Reddit, Amazon, Netflix, and Spotify. However, the attacks had more lasting implications for Dyn and other Internet companies like it. A report from BitSight found that around eight percent of the web domains relying on Dyn's managed DNS service dropped the service in the immediate aftermath of the attack, and approximately 14,500 web domains that used Dyn's managed DNS services prior to the Mirai attack also stopped using them immediately following the attack.<sup>6</sup>

In a highly competitive market, network or website service availability is crucial to maintaining customer trust and satisfaction and to acquiring new customers. Hence, the botnet attack impacted companies that exclusively used Dyn's services the most severely. Additionally, enterprises who lay victim to a successful DDoS attack can now expect a financial impact of \$2.5 million per attack. Even the mere threat of a DDoS attack can cause businesses to sweat, handing over big money to cybercriminals who threaten a company with a future attack unless they pay protection fees.<sup>7</sup>

---

<sup>5</sup> <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>

<sup>6</sup> <https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/>

<sup>7</sup> <https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/>

## Security Challenges

With familiar attacks to manage, securing the IoT ecosystem seems like a no brainer for enterprises. However, security teams face some significant challenges in making this happen.

**The IoT ecosystem is complex.** An IoT ecosystem is an amalgamation of diverse, dynamic, independent, and legacy devices that intertwine communication protocols, interfaces, and people. At first glance, the environment may resemble that of a traditional IT ecosystem, but the sheer quantity and diversity of IoT devices magnifies the attack surface and stifles the efforts to integrate security.

The complexity of the ecosystem hampers the ability of IT security professionals to exercise basic cyber hygiene, such as keeping an inventory of hardware and software components on the company network, identifying and disabling vulnerable applications that are no longer in use, consistently backing up data and keeping multiple copies, patching all applications immediately and regularly (unpatched systems are one of the biggest risk factors for most enterprises), and upgrading aging infrastructure and systems.

The variability of risks associated with every deployed IoT system further creates new challenges for IT security professionals who have been tasked with addressing those risks. Conflicting viewpoints and requirements from involved stakeholders also make securing the IoT ecosystem a formidable task.

**IoT ecosystems are difficult to monitor and manage.** The more complex an environment is, the more likely it is that IT administrators lack visibility, access, and control over one or more of its components. Deployment of IoT devices on legacy infrastructures and non-IP based devices also exacerbate the IT administrators' inability to monitor and control these devices.

Additionally, IoT systems can be inflexible and opaque, which creates a lack of basic management functionalities that are available in traditional IT systems. For instance, a system administrator cannot directly access an IoT system's operating system and reconfigure it to disable unwarranted hardware and software capabilities. This action could completely break an IoT device or hinder its intended functionality.

IT administrators are also challenged by employees who do not exercise

basic security practices, such as not connecting personal IoT devices to the IT network, not visiting malicious websites while on the company network, or not keeping their devices up-to-date.

#### The Curse of the Minimum Viable Product

**Security researcher David Tentler told Ars Technica UK that webcam manufacturers are in a race to the bottom, developing products with the required functionality while trading-off security measures to slash costs and maximize their profit. Many webcams now sell for as little as £15 or \$20 with no apt security functionalities.**

**IoT ecosystems can be inherently insecure.** Multiple factors – lack of security-by-design expertise, paucity of incentives to develop security controls, or poor implementation – render IoT devices vulnerable and defenseless against cyberattacks. IoT devices are known to have little to no encryption for securing the data at rest or in transit. They lack mechanisms to ensure that the software they host is protected from malicious modifications. They have poor or no authentication mechanisms, poor and insecure update mechanisms, and substandard physical security mechanisms, all of which work in favor of an attacker. Furthermore, legacy devices are inflexible to change or are no longer supported by manufacturers, making them all the more vulnerable to cyberattacks.

**IoT standards and regulations are obscure.** A lack of mature security frameworks as well as a breadth of security considerations are big barriers for the improvement of IoT security. Currently, there is no common approach to cybersecurity in IoT, nor is there a common multi-stakeholder model on cybersecurity. Therefore, most companies and manufacturers are taking their own approach when implementing security for IoT, resulting in undeveloped or underdeveloped standards to guide adoption of IoT security measures and best practices.

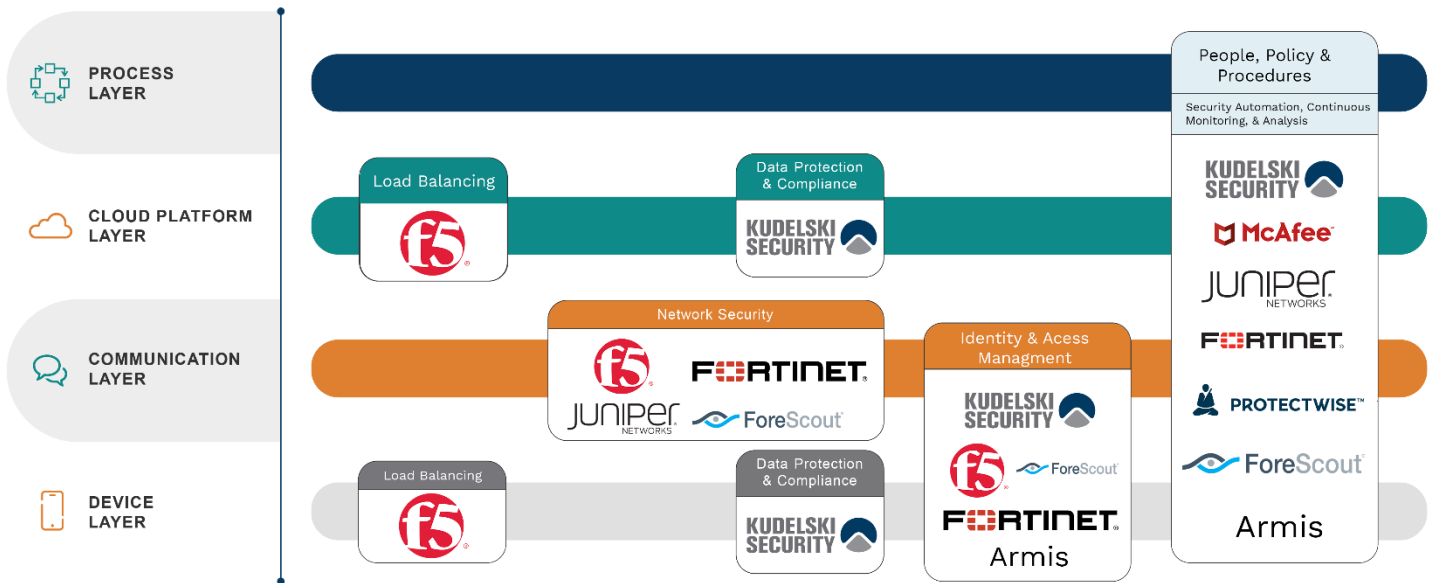
Fragmentation of regulations also pose a barrier to security, because there is no regulation that forces security measures and protocols at each of the levels of an IoT architecture, including the devices, the network, etc.

Unclear liabilities are another significant problem. There is a barrier of non-responsibility among the stakeholders involved, both moral and legal, in the event of a security incident. Lack of opportunity to enforce a perfect isolation between the different elements of an IoT ecosystem unavoidably results in condemnation of different parties involved in the ecosystem. In this context, there is a need to clarify the liability of each actor in case of a security event.

**There is a lack of IoT security awareness and knowledge.** There is an overall lack of awareness when it comes to security of IoT devices. Even more worrisome is the lack of knowledge regarding the threats they

are exposed to. Most IoT consumers do not have a basic understanding of their IoT devices and the impact on their network environment. This may result in devices not being updated and a subsequent breach of security.

## IoT Security Reference Architecture



Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland and Phoenix, Arizona.

The IoT Security Reference Architecture details the best practices and security controls for mitigating the threats, vulnerabilities, and risks identified in an IoT environment. The recommendations include people, policies, and processes that IoT enterprises should have in place as well as more specific technical measures.


The reference architecture considers numerous security guidelines and standards, with the two primary sources of inspiration being ENISA's *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* and the Industrial Internet Consortium's *Industrial Internet of Things Volume G4: Security Framework*.



Additionally, NIST’s *Framework for Improving Critical Infrastructure, Cybersecurity* also provided guidance for “aligning and prioritizing enterprise cybersecurity activities with its business/mission requirements, risk tolerances, and resources.” The CIP 003-3 provision in the North American Electric Reliability Corporation (NERC)’s cyber-security specifications for power systems in US electrical supply was also relevant in determining the security controls.<sup>8</sup> For a robust list of guideline and standard references, refer to Appendix C.

These recommendations are intended for enterprises that have already deployed IoT devices in their environment. Enterprises can compare the recommendations with their current security posture to identify security gaps and other complementary technology solutions that would enhance their security efforts. For those considering greenfield or next-generation IoT device implementations, it is advisable to take the “security by design” approach detailed in Appendix A.

## People, Policy, and Procedures

Layers Covered	Threats Addressed	NIST CSF	Kudelski Security Technology Recommendations
People, Policy, and Procedures			
All	All	Identify, Detect, Respond, Protect, Recover	

Because people are the weakest link in any cybersecurity effort, it is paramount to establish comprehensive and consistent policies and procedures for secure IoT deployment. These are guiding principles for good IoT security practices that also recognize that technological

<sup>8</sup> <https://www.iboss.com/resources/blog/iot-security-standards-and-frameworks-comparative-review>

### Common IoT Security Administrative Questions

**Is there a person or role, typically a board-level executive, who takes ownership of and is responsible for product, service and business level security?**

**Is there a person or role who takes ownership for adherence to a compliance checklist process?**

**Is there a documented business process in place for security?**

**Is there a security policy that has been established for addressing changes such as vulnerabilities that could impact security?**

**Is there a process in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements?**

**Is there a policy that has been established for dealing with both internal and third-party security research on products or services?**

**Has a security threat and risk assessment been carried out using a standard methodology such as Octave, NIST RMF or NCSC to determine the risks and evolving threats?**

**Do all the related servers and network elements prevent the use of null or blank passwords?**

**Do all the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts?**

**If run as a cloud service, does the service meet industry standard cloud security principles such as the Cloud Security Alliance, NIST or UK Government Cloud Security Principles?**

expertise does not necessarily equate to security expertise.

Kudelski Security's Advisory Services recognizes this, and guides organizations to define policies and procedures in key areas of IoT security, including change management, business continuity, compliance, and data governance. Nonetheless, enterprises that deploy IoT solutions, at the core, need to employ the following security management practices.

### Risk Identification, Management, and Assessment (NIST CSF: Identify)

Enterprises must adjust their existing risk management strategies and processes, including risk assessment and supply chain risk management processes, to take IoT into account. Enterprises can use frameworks provided by NIST (RMF), ISO/IEC 27000, Octave, and NCSC to plan, manage, review, and document their existing security practices.

A periodic risk assessment is core to providing an accurate picture of the evolving IoT threat landscape and an opportunity to work closely with stakeholders across lines of business, operational technology, and information technology to prioritize these risks and develop robust security measures based on potential impacts (business disruption, breach, or malicious activity).

### Incident Response Management (NIST CSF: Detect, Respond, Recover)

Enterprises require established procedures for analyzing and handling security incidents in the event of an IoT security breach. An incident response plan with roles and responsibilities must be in place prior to an incident and tested and updated at specified times or as needed. There are many standards for cyber incident management that cover cyber incident identification, handling, and remediation. Many of these standards are applicable to IoT systems as well. Some of the standards include:

- ISO/IEC 27035:2016, Information technology – Security techniques – Information security incident management – Part 1 and 2
- HITRUST CSF v9 for reporting information security incidents and weaknesses
- ITU-T X.1056, Security incident management guidelines for

telecommunications organizations

- Payment Card Industry (PCI) Data Security Standard (DSS) v3
- OpenFog RA (February 2017) for tamper response

We also advise enterprises to participate in information-sharing platforms as a way to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. The US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, and provide information about vulnerabilities and mitigation techniques. Also, there may be instances where certain measures would not be applicable to IoT devices. In such situations, we recommend that enterprises identify compensatory controls to mitigate the risk or the incident.

### **Security Training and Awareness** *(NIST CSF: Protect, Respond)*

Enterprises must ensure that their employees are well enabled to practice and promote security and privacy. It is the responsibility of the enterprise executives to establish clear cybersecurity roles and responsibilities for all their workforce. This can be achieved by training employees on good privacy and security practices while documenting and monitoring their training activities.

### **Asset Management** *(NIST CSF: Identify)*

Increased awareness will assist enterprises in identifying where and how to apply security measures or build in redundancies. Hence, we recommend that enterprises identify and catalog all IoT devices deployed in their environment with their corresponding external information systems if any (cloud systems for instance), map IoT communication and data flows, monitor their performance, patch known vulnerabilities up until the “end-of-support period of a product’s lifecycle,” and develop an end-of-life strategy for their IoT products. It is also crucial that enterprises identify and remain aware of data collected and processed by third parties and subsequently protect themselves via a data processing agreement if need be.

Asset management also involves having strong policies that manage

devices remotely via mobile phones and restricting employees from connecting their personal IoT devices to the corporate networks.

### **Credential Management** *(NIST CSF: Protect)*

According to OWASP, weak credential policies, weak passwords, and default passwords are the top vulnerabilities for most IT and IoT systems. Therefore, to limit the risk of compromise, credentials should be replaced at a specific frequency as defined in the organization's credential rotation policy. In some cases, it is possible to renew credentials, rather than to replace them, in order to extend their useful lifespan.

At the end of its lifecycle, the credential must be appropriately removed from service. When a credential is identified for suspension, it must be temporarily blocked from being used for authentication. This applies to any credential or generation process that is suspected of potential compromise in a system. If the compromise is likely for the credential or the generation process, then the credential must be revoked.

Furthermore, credential storage must also meet strict criteria on certain endpoints, cloud platforms, and services that have a high level of criticality. There may be organizational policy requirements that stipulate that highly critical entities with strong authentication and credential storage do not trust entities with insufficient authentication and credential protection.

### **Change Management** *(NIST CSF: Identify, Protect)*

Although security is included at the design stage, vulnerabilities that creep into systems after deployment can be mitigated through patching, security updates, and vulnerability management strategies. Furthermore, changes to regulatory policy, industry standards, and new directives should also trigger review of the security model.

Any update affects the organization's policy hierarchy. For example, when regulatory policy strengthens network access controls, these changes must be reflected in the organizational policy by setting access rights to certain networks to match the directives from the regulatory policy. Changes in organizational security policy similarly require adjustment to the machine policy for security control settings,

#### OWASP Top 10 IoT Vulnerabilities

**Insecure Web Interface: Default and weak credentials, susceptible to XSS, SQLi or CSRF**

**Insufficient Authentication/Authorization: Weak password and password recovery mechanisms, predictable tokens, etc.**

**Insecure Network Services: Unwarranted exposure of ports and services to the internet**

**Lack of Transport Encryption: Lack of SSL and TLS while transmitting data, poor implementation of encryption protocols**

**Privacy Concerns: Collection of unnecessary personal data, lack of transport encryption and storage of data in encrypted format**

**Insecure Cloud Interface: Insufficient and inefficient authentication and authorization mechanisms, lack of transport encryption, weak configurations, etc.**

**Insecure Mobile Interface: Insufficient and inefficient authentication and authorization mechanisms, lack of transport encryption, weak configurations, etc.**

**Insufficient Security Configurability: Lack of granular ability to configure authorizations, weak or inefficient credentials**

**Insecure Software/Firmware: Lack of firmware/software verification, unencrypted software/firmware**

**Poor Physical Security: Inadequate physical barriers to protect devices from unauthorized USB/cable insertions, lack of tamper-resistant/tamper-detection mechanisms**

configurations, and controls. All policy updates must be carefully controlled and tracked with an audit trail.

### **Privacy and Data Management** ***(NIST CSF: Identify, Protect)***

Security metadata such as connection status and characteristics (encrypted or authenticated) as well as the state of security controls on the device should be gathered and shared with operational management systems so they can be tracked and audited as required. The security metadata should be sent on a separate communication channel from the operational application data, and, in some cases, security management data should be sent on a separate physical network adapter, such as what may be found on a gateway device or a larger device with multiple physical adapters.

Security data should also conform to the requirements of the specific network. For example, if the network is bandwidth-constrained by operational technology data, then the security metadata may need to be bandwidth-limited through the connection, or it may need to be transmitted in bursts at intervals when network load is lower. Control of the frequency, throughput, volume, and duration of metadata updates to the management server is desirable.

Furthermore, privacy-sensitive data should be documented to ensure that there is adequate awareness of it. It should be managed based on policies governing access rights, consent/revocation, and third-party sharing. It is advisable to factor in privacy during the security architecting phase. Consider anonymizing the sensitive data and controlling its retention period and storage location, while ensuring that it is properly deleted as the need so arises. Careful management over the ownership of data is also required to keep the data safe from unintended modification.

### **Disaster Recovery Management** ***(NIST CSF: Recover)***

Disaster recovery management requires establishing security measures regarding business continuity management and crisis management. This also includes backup and restore procedures that are to be followed in the event of a compromise. These policies ensure essential features continue to work without loss in communication and without experiencing negative impacts from compromised devices or cloud-based systems.

## **Logging and Auditing**

***(NIST CSF: Identify, Detect, Respond)***

Enterprises must record all relevant activities and events related to user authentication, authorization, access rights, configuration changes, network traffic, and accounts management. All incidents, their corresponding impacts, and losses must be documented for future reference as well. Logs must be preserved on durable storage and retrievable via authenticated connections. Periodic audits and reviews of logs and security controls ensure the implemented controls are current and effective. Penetration tests performed biannually help mitigate vulnerabilities. Logging also aids forensic investigations in the event of a breach. Moreover, the audit data should be retained for a period of time defined by the organizational data retention policy, and its integrity should be assured, attestable, and treated as confidential. Kudelski Security's consultants perform technology assessments that include vulnerability, security, and audit assessments.

Furthermore, there must be accountability across the system that involves tracking employees and contractors in the IoT process as well. Privacy concerns arise whenever personal information is tracked. Hence, when customer, partner, and other data is tracked, care must be taken to protect personally identifiable information and other sensitive data.

## **Assess Security Programs**

***(NIST CSF: Protect, Recover)***

Several methods exist to assess security programs, the security posture, and the process for secure maintenance of their products. These include the Cyber-Security Capability Maturity Model (C2M2) and its vertical-specific variants (ES-C2M2 and ONG-C2M2 for energy and oil and gas subsectors, respectively), the tiers of the NIST framework focused on critical infrastructures, the CERT Resilience Management Model (CERT-RMM) focused on operational resilience management, and the Building Security In Maturity Model (BSIMM) focused on secure software development. They work best, however, when tailored to the organization.



## Technical Measures

Technical measures are necessary to preserve and protect the security of an IoT ecosystem. Technical measures must consider the particularities of the IoT ecosystem such as scalability, variability, and heterogeneity and implement the controls at the level of specialized architectural components (e.g. gateways) if required. Some measures to consider include:

### Security Configuration and Operational Management

Security configuration and operational management requires controls that ensure the integrity and confidentiality of configurations made to operational elements of the system including endpoints, communications, monitoring, and management systems. Most technologies offer a variety of features which when enabled/disabled can increase convenience or functionality, but they can leave enterprises more vulnerable to an attack. This is especially true with features that enable remote debugging or testing capabilities.

Therefore, it is critical that enterprises examine these settings at all layers, particularly security settings, and select options that meet their needs without putting them at an increased risk. Enterprises must also be mindful of unwarranted ports and interfaces and disable them. They must ensure that default passwords and usernames are changed during the initial setup, and that weak, null, or blank passwords are not allowed. If the web application has firewall and secure communication such as HTTPS option, enable it. Also, if the system has account lockout functionality, ensure that is enabled.

In the event that certain vulnerable features cannot be disabled, it is advisable that enterprises implement compensatory controls to mitigate the risk. For instance, if a certain port needs to be kept open at all times on the device, and the device is connected to the Internet, the device should be protected with a strong password policy. Additionally, the port can be monitored, and applications connecting to that particular port can be whitelisted on the firewalls. Network monitoring tools can greatly enable enterprises to achieve this.

Examining these settings periodically is equally essential. Patches or new versions of IoT software can come with additional features, forcing enterprises to reevaluate their settings to meet an appropriate level of risk.

#### Questions to Assess IoT Security Technical Measures

**Are all products' unused ports closed?**

**If a connection requires a password, passcode, or passkey for connection authentication, is the default password or factory reset password unique to each device?**

**For a Wi-Fi connection, are insecure protocols such as WPA and TKIP disabled?**

**Do all the product related cloud and network elements have the latest operating system(s) security patches?**


**Do the product-related web servers have their webserver identification options (e.g. Apache or Linux) switched off?**

**Do all the product-related web servers have their web servers have their webserver HTTP trace and trace methods disabled?**

**Are all the product-related web servers' TLS certificate(s) signed by trusted certificate authorities, are within their validity period, and processes are in place for their renewal?**

Moreover, to change the configuration of security controls, the security model should be transformed into actionable settings in the security policy, including identification and configuration of endpoints and their connectivity. This level of granularity varies depending on the systems and trust requirements captured in the system security model and policy.

### Data Protection and Compliance

Layers Covered	Threats Addressed	NIST CSF	Solutions
Data Protection and Compliance			
Cloud platform, Device	All (except DDoS, software/hardware vulnerabilities, device modification, and natural disaster)	Protect	

Data protection and compliance involves scanning data repositories and resources to identify existing sensitive data, classifying it appropriately in order to identify compliance issues, applying the right security controls, and making decisions about storage optimization, deletion, archiving, legal holds, and other data governance matters. Enterprises must also have the means to provide visibility into what sensitive data exists and where as well as monitor and log data access permissions and activities.

Managing customer and employee consent and enforcing their rights over the personal data that they share – access, erasure, rectification, data portability, etc. – is critical to remain in compliance with certain regulations such as GDPR. Furthermore, enterprises must consider using encryption and other obfuscation techniques to obscure data in relational databases and the distributed computing architectures of big data platforms in order to protect personal privacy, achieve compliance, and reduce the impact of cyberattacks and accidental data leaks.

Enterprises must also ensure data loss prevention strategies are well documented and accessible. Kudelski Security’s solution implementation and migration capabilities can help enterprises design/redesign their data centers, implement required hardware for database encryption, and provide an automation and orchestration service that will streamline enterprise’s infrastructure operations and security activities to make them more efficient and cost effective.

## Identity and Access Management

Layers Covered	Threats Addressed	NIST CSF	Kudelski Security Technology Recommendations
Identity and Access Management			
Cloud platform, Device, Communication	All (except DDoS and natural disaster)	Protected	   Armis

Authentication and authorization schemes (unique for each device) must be based on system-level and cloud threat models. Identity and access management and related standards enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management include identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, un-linkability, and un-traceability, ensure data minimization, and gain explicit user consent as to when attribute information may be shared among entities.

Some identity management standards and recommendations in place today include:

- *Entity Authentication Assurance Framework (EAAF)* in ISO/IEC 29115 – an authentication standard describing the life cycle for credentials and authenticating entities
- NIST 800-57, *Recommendation for Key Management* – applies similar approaches to the management of credentials and identity material

- *Functional Model Representation of the Identity Ecosystem* – a model for identity solutions, including the various components and interactions

**Authentication:** Entities should be categorized by criticality. Each level of criticality should be associated with a level of authentication that defines the level of trust to place in a successful authentication. The level of authentication also defines what controls must be in place to minimize the risk of false attestation or impersonation. For example, in very low criticality endpoints, it may be acceptable to authenticate with a plaintext credential, using the IP address or MAC address as the identity.

For slightly more critical entities, multifactor authentication may be needed to protect against attacks on stored and transmitted credentials. In the higher criticality entities, authentication should be cryptographically protected, and tamper-resistant hardware should be used to store all sensitive data and credentials at rest and in use. Furthermore, mechanisms must be in place to protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.

Note that throughout the enrollment phase, an audit trail should be created to track the steps as they are executed. The audit data should be retained for a time as defined by policy. The audit trail data integrity should be assured, attestable, and treated as confidential.






**Authorization:** Limit the actions allowed for a given system by implementing fine-grained authorization mechanisms. Using the Principle of Least Privilege (POLP), applications must operate at the lowest privilege level possible. Credential storage must be implemented to the level required by the organizational policy based on the level of authorization for a particular endpoint. The higher the level of authorization required, the more stringent the credential storage requirements must be. The level of authorization should be enforced in the communications policy so that endpoints that do not have strong enough credential storage are not allowed to connect to the endpoint.

**Access Control:** Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy. The access control must be enforced on the endpoint and cloud platform, such as in the configuration on a device or

in the database of the management server, and in the communications between endpoints. Enterprises should also adopt context-based security and privacy that reflects different levels of importance and deploy measures for tamper protection and detection. Physical security controls such as meshes also ensure that the device cannot be easily disassembled.

Standards to enforce access policies, share attributes, preserve anonymity, minimize data release, and consent are still immature, difficult to deploy, and not available from a large majority of software-as-a-service providers and traditional enterprise product vendors, which additionally hampers adoption

### Security Automation, Continuous Monitoring, and Analysis

Layers Covered	Threats Addressed	NIST CSF	Solutions
Security Automation, Continuous Monitoring, and Analysis			
All	All	Identify, Detect, Respond	Armis     

Visibility into the current status of all IoT devices in the network provides an accurate picture of the security posture of the enterprise. Continuous monitoring verifies device behavior and assists in detecting malware, security policy violations, failed authentication requests, tamper sensor alerts, and integrity errors. In forensic investigations, they help determine which device and data was affected by a compromise and the specific sequence of events leading up to it. Analysis on the collated data can also identify trends suggesting that new attacks are about to occur or that IoT systems have changed in ways that might make them more susceptible to future attacks.

Security monitoring gathers security-related event data, then aggregates, correlates, and analyzes it. It should be able to monitor and control the various endpoints and communications in a generic and consistent way. Network and host information that may be monitored includes:

- Full network traffic recordings that store every bit in every packet for a period of time
- Host execution activity and audit recordings that store every significant action taken by a CPU
- Process or software components such as reading a value from a physical process, controlling some aspect of the process, or accessing sensitive information such as personally identifiable information or a private encryption key
- Network statistics, including connection setup and tear-down events
- Communication volume statistics for different kinds of data content and connections
- Data from security analysis systems that should also be treated as security data and made available to analysis engines for further correlation.

Additionally, all security monitoring designs must consider the risk that a successful intruder can erase all evidence of their activities. Transmitting the most important security monitoring data to external monitoring systems in a secure and timely manner mitigates this risk. Endpoints must log data based on both local endpoint events and communications events. Logging to a network log system can also mitigate attempts of intruders to interfere with the integrity of log data.

Furthermore, there are several approved and draft Security Automation and Continuous Monitoring (SACM) standards that are specifically relevant to IoT systems. These include:

- IEC TR 62443-2-3:2015 - requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program
- IETF RFC 7632 - use cases for securely aggregating configuration and operational data and evaluating that data to determine an organization's security posture
- IETF Active Internet Drafts: The Resource Oriented Lightweight Information Exchange (ROLIE) Definition of the ROLIE Software



Descriptor Extension, Concise Software Identifiers, Endpoint Compliance Profile, Software Inventory Message and Attributes (SWIMA) for PA-TNC, and Security Automation and Continuous Monitoring (SACM) Terminology

However, resource limitations of IoT devices (memory, processor, power) can make it difficult to implement agent-based approaches to continuous monitoring. But, certain network monitoring and alerting tools like IDS/IPS, firewalls, ICMP, SNMP, and Syslog can be used to monitor the health of the IoT infrastructure/ecosystem. The deterministic nature of IoT networks allows the system to be baselined and deviations quickly identified.

### Network Security

Layers Covered	Threats Addressed	NIST CSF	Solutions
Network Security			
Communication	All (except software/hardware vulnerabilities and natural disaster)	Detect, Respond, Protect, Recover	

### Network Segmentation

Networks cannot be interconnected indiscriminately. Industrial security standards such as SA/IEC 62443-1-1, ISA/IEC 62443-3-3, ANSSI, NIST 800-82, CIS (Control #18 – Boundary Defense), *inter alia* recommend separating networks into segments, with each segment containing assets with similar security policies and communications requirements. These industry security standards also recommend assigning each network segment a trust level and recommend protecting communications and connectivity through the perimeters of networks, especially between segments at different trust levels. Enterprises should also adopt risk-based segmentation – splitting network elements into separate

components to help isolate security breaches and minimize the overall risk.

Network segmentation can be fine-grained or coarse-grained. Candidates for segmentation include public networks (such as the Internet), business networks, operations networks, plant-wide networks, control networks, device networks, protection networks, and safety networks. Security and device management networks are often candidates for segmentation. The separation can be done using VLANs, routing, or creating separate networks for the devices to run on. Gateways with filters can also be used to implement network segmentation by controlling the flows of information passing between network segments.

This guidance corresponds not to the perimeter of the organization, but to internal boundaries between and among internal networks.<sup>9</sup>

## Network Filters

The Industrial Internet Reference Architecture suggests use of gateways with filters to integrate multiple connectivity technologies. An IoT gateway enacts proxies to one or more legacy endpoints and prevents exposure of legacy endpoint attack surfaces to networks. Examples of important IoT filtering technologies include:

- **Air Gaps** – Network segments with no online connection, wired or wireless, to any external network. Air gaps are the strongest form of filtering but provide none of the connectivity benefits.
- **Layer 2 Filters** – Separate physical network signaling systems, but forward Open Systems Interconnection (OSI) Layer 2 network frames. Managed switches and bridging firewalls are examples of technologies that filter messages based on Ethernet Media Access Control (MAC) addresses or other device-level addressing.
- **Layer 3/4 Filtering** – The most commonly used IoT message filters are firewalls able to filter messages based on network addresses, port numbers, and connection state. Such filtering technologies are known as packet filters and stateful inspection.

---

<sup>9</sup> <https://www.sans.org/reading-room/whitepapers/analyst/stopping-iot-based-attacks-enterprise-networks-38470>

- **Application and Middleware Layer Content Filtering** – Some firewalls and other message filters understand specific communications protocols and are able to filter messages based on application content. For example, an application layer filter might permit device register read requests, but block write requests. Other filters might permit messages from a particular user, but not other users. This is called deep packet inspection.
- **Message Rewriting** – Some message filters modify messages as they pass through the filter. For example, network address translation (NAT) filters change IP addresses and port numbers, and virtual private network (VPN) servers encrypt and decrypt message streams. VPNs are often deployed in IoT systems to help protect interactive remote access mechanisms and to encapsulate and protect plain-text device communications protocols as they pass across WAN.
- **Proxies** – Application-layer message filtering with message-rewriting capabilities.
- **Server Replication** – Server replication maintains a real-time copy of part or all of a protected server on a less-trusted network segment, most commonly at IT/OT network perimeters. For example, a plant historian server may be replicated through an IT/OT firewall. The replication mechanism can act as a filter by replicating only a subset of historical data points out to the corporate network.
- **Virtual Networks** – May implement message filters in hypervisors or virtual firewall hosts.

Most of these message filters can be implemented in gateway host or device software or as real or virtual network appliances. In hosts or devices, these filters control messages and information exchanges for a single endpoint. As real or virtual network appliances, gateways with filters can control messages and information flows for entire network segments.

## Secure and Trusted Communications

Enterprises should make only intentional connections and prevent unauthorized connections to its network while disabling specific ports and/or network connections for selective connectivity. Enterprises must develop policy and procedures for BYO-IoT and use rate limiting to control the traffic sent or received by a network to reduce the risk of automated attacks.

It is highly recommended that end-to-end encryption, if available and applicable, be deployed to protect data as it crosses the network as well as while it's stored on a back-end server or on the device. If the embedded IoT devices cannot perform encryption natively, an enterprise can leverage infrastructure techniques such as encrypted tunnels to properly secure data.<sup>10</sup>

Furthermore, enterprises must determine if the devices need to be continuously connected to the network. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device and systems. For example, in nuclear reactors, a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.<sup>11</sup>

### Load Balancing

Layers Covered	Threats Addressed	NIST CSF	Solutions
Load Balancing and Secure Updates			
Cloud Platform, Device	All (except software/hardware vulnerabilities and natural disaster)	Defend, Recover, Protect	

Implementing a DDoS-resistant and load-balancing infrastructure that inherently does not trust data received and always verifies any interconnections is recommended.

<sup>10</sup> <https://blog.leanix.net/en/9-steps-to-iot-security-in-the-enterprise>

<sup>11</sup>

[https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL\\_v2-dg11.pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf)

## Implement Microservices (If Applicable)

The inevitable implementation of IoT will create a challenge for enterprise architects. It will be important to determine how device networks will communicate, how data will be processed, which applications or systems to invest in to process the surge in data, and which team members will oversee IoT endeavors. Running IoT applications as microservices will help for quick deployment, maintenance, and account for the inflation of volumes of data.<sup>12</sup>

## Physical Security

Any physical device is liable to be tampered with in a way not intended by the manufacturer or retailer. IT devices in particular are a target for those people who are just plain curious, hackers seeking a new challenge to their technical skills, people trying to steal corporate knowledge about products and services, those seeking financial gain, and a multitude of others pursuing an assortment of malicious intent.

Hence, we recommend that enterprises lock up their server rooms, authorize only intended users with least privilege access and log and monitor their access via video surveillance, and prevent portables from connecting to the devices. Other strategies require basic "handyman" skills to install simple equipment (e.g. key locks, fire extinguishers, and surge protectors), while others demand the services of consultants or contractors with special expertise (e.g. window bars, automatic fire equipment, and alarm systems).

---

<sup>12</sup> <https://blog.leanix.net/en/9-steps-to-iot-security-in-the-enterprise>

## Conclusion

**Research from management consultant Capgemini found that only 33% of organizations believe their IoT products are “highly resilient” against future cybersecurity threats, and 48% of companies focus on securing their IoT products from the beginning of the product development phase.**

In an IoT ecosystem, products and services may intentionally or unintentionally be used in different applications by their users. When used outside the expected context, the security may not be adequate. This challenges the notion of listed security practices, as the intended use case influences the appropriate security mechanisms. Furthermore, enterprises must accept that residual risk is unavoidable, no matter how thoroughly the device is hardened.

It is therefore critical for enterprises to establish a clear vision of the business need for IoT devices, validate the solution with stakeholders (including security professionals), assess the risks, deepen their technical understanding of how the IoT system really works, and validate system operations and feasibility.

Moreover, IoT security is a shared responsibility. Many security incidents could be avoided if developers and manufacturers were aware of the risks they face on a daily basis, considering not just those that affect IoT devices but also those that affect the IoT environment as a whole and develop products accordingly. But, connected devices are typically designed to be low-cost and built for a single purpose – not with security at the forefront. They often have limited memory and computing power, which means they can't be protected by traditional endpoint security. Therefore, enterprises must fully vet new IoT devices to understand how much security is built in. For example, the device may have strong embedded encryption, or it may have a USB port. The administrative password might be “password,” providing an open invitation for misuse and abuse. For a checklist of security-related questions to ask an IoT device vendor before making a purchase, refer to Appendix B.

Finally, it should be noted that IoT security is a continuum and not a Boolean expression, something that simply “is” or “is not”. It is always impossible for every IoT system to behave securely within every context. A good rule of thumb and a sound approach for enterprises, therefore, is to always adopt an evolving security posture.

*If you'd like to get in touch for a discussion about IoT security and risk reduction options tailored to your unique business requirements, please email [info@kudelskisecurity.com](mailto:info@kudelskisecurity.com)*

## Appendix A: Kudelski Security's IoT Security Suite

Like many of the world's leading companies, you are investing money and effort in IoT projects, devices and services to transform your business. You expect that this will enable new business models, new features, greater operational efficiencies and data to drive quicker, smarter decision making. But to enable these new benefits, you also need to protect the pillars of your business, including monetization, safety, privacy, intellectual property, regulatory compliance and reputation.

As you develop your IoT security strategy, you must decide whether to go it alone or to get help. Does your organization have the expertise, the resources and the desire to do this by yourself? Or would you be more successful reaching your IoT goals by working with a trusted IoT security partner to guide you through the process of designing, implementing and managing IoT security throughout the entire lifecycle of your product?

### **A Trusted, Strategic Security Partner**

Through its activities in Content Security, Public Access and Cybersecurity, the Kudelski Group has spent more than 30 years securing its customers' business data, devices and high-value business models. It is our singular mission to make your IoT projects and assets secure and sustainable for the long term, so you can reap the full benefits you expect to gain from connecting your business.

### **Kudelski IoT Security Suite – We Make IoT Security Easy**

The Kudelski IoT Security Suite provides you with everything you need to guide you through the process of establishing trust, integrity and control between you, your devices and your data, and ensures that trust is maintained during all phases of your product's lifecycle. We address IoT security using a unique, holistic approach by helping you design, run and sustain the security of your IoT ecosystem over time: IoT Security Platform: Trust & Integrity Management

Our IoT Security Platform makes IoT security easy to embrace by securing the chain of trust between you, your devices and your data. We give you all the tools you need to integrate security into your devices, control access to them, and actively secure them over time. This allows you to create and operate a wide variety of security use cases to support



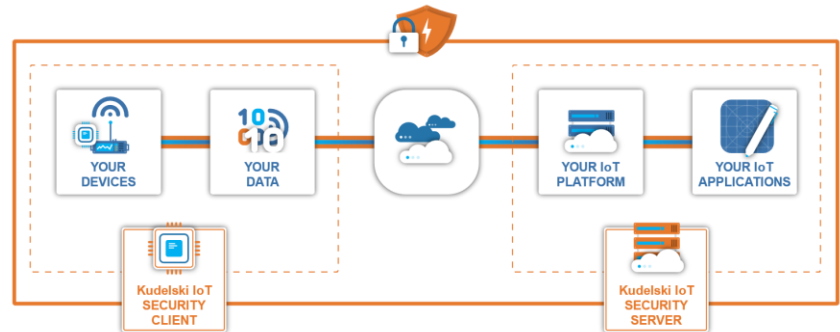
your connected business.

### Kudelski IoT Security Platform - Trust, Integrity and Control

The success of your IoT projects depends on your ability to establish robust and sustainable trust between your IoT devices and your backend platforms. The Kudelski IoT Security Platform protects your investments and secures your connected business with a pre-integrated, end-to-end solution that makes IoT security easy.

Integrate our IoT Security Client into your devices and our IoT Security Server with your IoT platform and applications, and you will have a powerful solution for protecting any IoT use case you wish to secure. The IoT Security Server can be delivered on premises or as a cloud-based service and its patented key management system is bandwidth-optimized for Cellular and Narrow-Band IoT networks.

Once our Security Client with Root of Trust is integrated with your device, The Kudelski IoT Security Platform provides:



- **Device Security**

Your devices are protected from attack and you can trust and control them

- Identity
- Authenticity
- Firmware protection

We enable you to seamlessly manage device provisioning, trusted device identity, mutual device and cloud authentication and verify that your devices are running the correct software. Using a simple API, your IoT platform and applications can then get a list of devices and their status, claim device ownership and manage software patches. We can

also help you implement secure boot, download and incremental patch mechanisms that keep your devices secure and updated.

- **Data Security**

The privacy of your data is protected from your devices to the cloud

- Confidentiality
- Integrity
- Authenticity

Our platform enables your devices and applications to encrypt and decrypt sensitive data between them so that it is secure both at rest and in motion. It also guarantees the data is authentic and cryptographically linked to the device it came from. Your devices and platform applications just connect to our Security Client and our Security Server and automatically apply the default data policies you've established, privacy protection easy and effective.

- **Access Management**

You have control over who has access to your devices, data & features

- Device policies
- Data policies
- Features authorization

We give you complete control over your assets by providing application APIs that securely manage device, data and feature access within our Secure Client. Policies defined by your platform are enforced within our secure processing area on your devices. We can also help you define and implement end-to-end trusted functions like secure feature activation or anything else you need to maintain dominion over your physical or virtual assets.

- **Active Security**

Your IoT ecosystem is robust, smart and secure for the long term

- Detection/Response
- Local decision making
- Secure processing

We evolve and adapt your platform to constantly changing threat models

by delivering you security updates and countermeasures; proactively or reactively in response to specific incidents. We also enable secure local decision-making functions at the edge for use cases where the device isn't always connected, executed in our secure processing environment. And our experts can also help you implement any of these secure functions in a way that works best for your technical architecture and business.

### **IoT Managed Security Services: Security Lifecycle Management**

Our IoT Managed Security Services monitor and analyze the security data from your devices to give you a global view of your devices and of the network as a whole. Our expert security analysts detect potential threats and provide quick prevention and response services to ensure your business is protected. We can also run and manage the Kudelski IoT Security Platform for you.

### *Other Kudelski Security Services*

#### Advisory

Our advisory services engage clients through our strategic cyber program-based approach to cybersecurity. As program focus areas are identified, our consultants leverage industry proven models, methodologies, and best practices to identify gaps in your security program, helping prioritize strategies for improved processes, management, and technology. This program-based strategy allows CISOs and senior leadership to plan, manage, and measure program areas that minimize business risk and strengthen cyber resiliency.

#### Technology Consulting

Kudelski Security technology delivery teams provide end-to-end professional services to support enterprise security architecture development and technology installation. Our network engineers extend your internal capabilities, leveraging extensive field experience to deliver business-enabling service and support. The team includes senior engineers and senior solution architects with the skill sets to help you design and deploy an optimal IT security architecture.

Our services are built on a tried and tested methodology that delivers planning workshops and IT architecture and technology assessments, and full, onsite support for technology installation and integration. Our

goal is simple: to ensure your network environment is always secure, available, accessible and matched to your business needs.

### *Strategic Cyber Staffing*

Strategic cyber staffing fills long-term or temporary knowledge resource needs with highly experienced and qualified professionals. Our expansive Cybersecurity Alliance Ecosystem (CAE) allows our clients to gain access to cyber expertise, spanning from strategic vCISOs to deep engineering and technical resources. These IT staffing resources help corporate security leaders ensure they can always operate their security programs efficiently.

## Appendix B: Questions to ask IoT Vendors (During Procurement)

Enterprises must use a device with security incorporated into the hardware. For example, specialized security chips and co-processors that integrate security at the transistor level provide trusted storage for device identity and authentication means, protect keys at rest and in use, and prevent unprivileged access to sensitive code. Protection against local and physical attacks can also be covered via functional security. However, when in doubt, it is highly recommended to seek out third party assessment of the IoT device that an enterprise intends to purchase. Nonetheless, below is a questionnaire an IoT consumer can use to assess the security of an IoT device

### *Trust & Integrity Management*

**Have the operating system and firmware been updated to the latest version?** Are there any known vulnerabilities present in them? IoT products are often sold with old and unpatched embedded operating systems and software. Ensure at the time of purchase that they are of the latest version and that there are no known software vulnerabilities in the product.

**Is secure boot or root of trust mechanism available in the device?**

Trust must be established in the boot environment before trust in any other software or executable program can be claimed. Run-time protection and secure execution monitoring must be implemented to make sure malicious attacks do not overwrite code after it is loaded.

**Can the devices be authenticated? Is the device password hardcoded? Is it unique to per device? Can it be changed regularly?**

Devices must be authenticated while being added to the enterprise network. Manufacturers must provide some form of authentication via the device interface, web, mobile, or cloud interfaces. If for reasons, a device has hardcoded passwords, ensure that is not the same across all manufactured devices and that it cannot be changed, else an attacker could easily compromise the device. Also, ensure that the manufacturer provides strong password policies regarding password length and complexity.

**Does the device have strong password policy in place? Are there mechanisms to lock down device after “n” number of attempts? If this is possible, would it hamper the normal function of the device?**

**Does the manufacturer have a transparent privacy policy?** To protect consumers from potential data privacy breaches, manufacturers need to develop privacy policies that clearly detail how the data collected from IoT products will be used, and these policies should be easily accessible to enterprises.<sup>13</sup>

**Does the device have any anti-tamper techniques deployed?** As the name suggests, this is a nice-to-have feature that prevents unauthorized access to the device. However, if this feature is not available, a consumer could deploy tamper detection and prevention techniques aftermarket.

**Does the web/mobile/cloud interface have data sanitization techniques enabled?**

Data input validation ensures that data is safe prior to use and output filtering ensures that the data omitted by the device doesn't reveal sensitive information. Consumers must ensure that the manufacturer has done due diligence regarding this.

*Secure Communication*

Cryptographic techniques, if used appropriately, can guarantee the

---

<sup>13</sup> <https://www.computerweekly.com/opinion/How-to-secure-the-internet-of-things>

different security aspects -confidentiality (privacy), integrity, availability and authenticity - of the information in transit on the networks or stored in the IoT application or in the cloud. Some questions an enterprise can ask related to secure communication include:

**Are the communication protocols secure?** A device should use standard protocols for communication. If a device uses proprietary protocol, ensure the manufacturer has vetted the protocol for known attacks and are able to represent and manage trust and trust relationships.

**Are cryptographic mechanisms used in the device?** Ensure that the device has a proper selection of strong, standard encryption algorithms and strong keys to protect the confidentiality, authenticity, and integrity of data and information (including control messages) in transit and in rest. If possible, verify the robustness of the implementation via a third party.

**Are cryptographic keys and/or certificates securely managed?** Devices must store the keys and/or certificates in a secure element if possible. Consumers must ensure the manufacturer has provided options to rotate keys at will or revive, renew, and disable certificates as required.

**Is the device communication secure (from device to gateway, and from gateway to cloud)?**

IoT devices should be restrictive rather than permissive in communicating. Consumers must ensure that secure communication is provided in the device using state-of-the-art, standardized security protocols, such as TLS. This ensures and guarantees data authenticity with reliable exchanges from data emission to data reception. Also, data must be signed whenever and wherever it is captured and stored.

**Does the device use the same secret key in the entire product family?** Manufacturers must avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family. Consumers must make a note of this when purchasing new products.

**Do the web interfaces fully encrypt the user session?** Manufacturers must ensure that the sessions from the device to the backend services are encrypted and that they are not susceptible to XSS, CSRF, SQL injection, etc.

## *Vulnerability & Incident Management*

**Does the manufacturer have a robust vulnerability and patch management program?** It is crucial that manufacturers have the capabilities to address unknown vulnerabilities in a timely manner.

**Does the device have secure update mechanisms enabled? Are secure code signatures made available?** Vulnerabilities will likely be discovered after the consumer has deployed the connected devices, IoT gateways, and other systems in the field. Manufacturers must provide a way to patch devices or push out security updates. If the device cannot be updated, the consumer's risk of being compromised at a large-scale increase. Also, merely updating the devices is not sufficient, preventing unauthenticated software and files from being loaded onto the device during updates is essential to safeguard IoT devices from malicious takeover as well. Hence, ensure that the device has a mechanism to verify the code/firmware made available to the device. Cryptographically signed codes ensure that the code itself has not been tampered with and it is safe to install it on the device.

**Does the device have restore capabilities?** This feature enables a system to return to a state that was known to be secure after a security breach has occurred or if an upgrade has not been successful. Mechanisms for self-diagnosis and self-repair to recover from failure, malfunction or a compromised state are a necessity for continued business operations.

## *Logging*

**Does the device or application have logging features?** Logging enables consumers to document and review device activities for troubleshooting and general management. Consumers must also ensure that the logs do not hold any sensitive data, if they do, they must be in an obfuscated manner.

**Does the device have any alert or notification capabilities?** In the event of failure or compromise of the device, the device must be capable of sending alerts to authorized person to indicate its state.



## Appendix C: Common Cybersecurity Standards and Regulations

### *Information security management system (ISMS)*

Information security management system (ISMS) standards provide a set of processes and corresponding security controls to establish a governance, risk, and compliance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. There are several ISMS standards with market acceptance that are generally applicable to IoT systems or specific IoT applications. These include:

- The ISA/IEC 62443 series includes security management requirements for Industrial Automation and Control Systems (IACS).
- ISO 13485:2016 Provides management requirements for medical devices and related services.
- ISO 27799:2016 covers information security management in health using ISO/IEC 27002.
- ISO/IEC 20243:2015 identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains.
- And, ISO/IEC 27002:2013 is being widely used as a reference for selecting security controls when implementing an Information Security Management System (ISMS).
- The ISO/IEC 27000 series provides best practice recommendations on information security management, risks, and controls within the context of an overall information security management system.

### *Hardware Assurance*

Hardware Assurance is an activity to ensure a level of confidence that microelectronics function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.

Existing standards include:

- ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security (three parts);
- ISO/IEC 20243:2015 Information technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains;
- ISO/IEC 27036 Information technology – Security techniques – Information security for supplier relationships (three parts);
- SAE International AS5553B-2016 Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria; and
- SAE International AS6081-2012 Counterfeit Electronic Parts; Avoidance Protocol, and

NISTIR 8200 (DRAFT) STATUS OF INTERNATIONAL CYBERSECURITY STANDARDIZATION FOR IOT

### *The National Institute of Standards and Technology (NIST)*

The National Institute of Standards and Technology (NIST) has published NIST SP 800-82 'revision 2'. It provides guidance on improving security in Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Performance, reliability and safety requirements are also considered. Comprehensive security controls, presented in this document, map to additional NIST recommendations such as those listed in SP 800-53, 'Recommended Security Controls for Federal Information Systems and Organizations.' A framework for considering networks of things is described in NIST SP 800-183.

### *NIST IR 7628, 'Guidelines for Smart Grid Cyber Security, Volume 1'*

NIST IR 7628, 'Guidelines for Smart Grid Cyber Security, Volume 1', is a recommendation for addressing security concerns across the electric smart grid. It is a three-volume compendium that contains sections that

describe risk assessment and vulnerability analysis and analyzes secure information exchange for electric grid systems. NIST has also published Considerations for Managing IoT Cybersecurity & Privacy Risk and is working on a “NIST Cybersecurity Framework application to IoT” publication.

### *NERC CIP Standards*

NERC CIP Standards, published by the North American Electric Reliability Corporation (NERC), aim at improving the security and reliability of the electric industry by defining auditable requirements for critical infrastructure protection (CIP).

### *Industrial Internet Consortium*

The guidance from the Industrial Internet Consortium details how to protect IoT devices against threats and vulnerabilities using physical security, secure architectures, and identity and access controls (and many other methods). Though the framework targets Industrial IoT, stakeholders should find it useful for securing other connected hardware.

### *The OWASP's IoT Security Guidance*

The OWASP's IoT Security Guidance conveniently lists specific steps in securing IoT environments. Tips cover authentication, passwords, encryption, and secure interfaces (and much more).

### *Other Industry Frameworks and Recommendations*

AT&T: The CEO's Guide to Securing the Internet of Things

<https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf>

Broadband Internet Technical Advisory Group (BITAG):

[http://www.bitag.org/documents/BITAG\\_Report\\_-\\_Internet\\_of\\_Things\\_\(IoT\)\\_Security\\_and\\_Privacy\\_Recommendations.pdf](http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf)

European Union Agency for Network and Information Security (ENISA):

GSM Association (GSMA): IoT Security -

<http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/>

GSM Association (GSMA): IoT security checklist for self-assessment:

<http://www.gsma.com/connectedliving/iot-security-self-assessment/>

I Am The Cavalry: Five Star Automotive Cyber Safety Framework And Hippocratic Oath for Connected Medical Devices

IETF: <https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf>

Industrial Internet Consortium: Industrial Internet Security Framework: <http://www.iiconsortium.org/IISF.htm>

IoT Alliance Australia: IoT Security Guideline <http://www.iot.org.au/wp/wp-content/uploads/2016/12/loTAA-Security-Guideline-V1.0.pdf>

IoT Security Foundation: Whitepaper: Establishing Principles for IoT Security: <https://iotsecurityfoundation.org/wp-content/uploads/2015/09/loTSF-Establishing-Principles-for-IoT-Security-Download.pdf>

IoT Security Foundation: IoT Security Compliance Framework: <https://iotsecurityfoundation.org/best-practice-guidelines/>

IoT Security Foundation: Connected Consumer Best Practice Guidelines: <https://iotsecurityfoundation.org/best-practice-guidelines/>

IoT Security Foundation: Vulnerability Disclosure Best Practice Guidelines: <https://iotsecurityfoundation.org/best-practice-guidelines/>

IoT Security Foundation: Best Practice User Mark: <https://iotsecurityfoundation.org/best-practice-user-mark/>

IoT Security Foundation: IoT security training: <https://iotsecurityfoundation.org/iot-security-training>

Microsoft: Internet of Things security best practices <https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices>

Microsoft: The Seven Properties of Highly Secure Devices <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf>

NIST: Systems Security Engineering 800.160: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>

OneM2M: Security Technical Report

[http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2\\_0\\_0.pdf](http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf)

Online Trust Alliance: IoT Security & Privacy Trust Framework

[https://otalliance.org/system/files/files/initiative/documents/iot\\_trust\\_framework6-22.pdf](https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf)

Symantec: An Internet of Things Security Reference Architecture

<https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf>

UK Government: Principles of cyber security for connected and automated vehicles

<https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

UK Government: Walport Report

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/409774/14-1230-internet-of-things-review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf)

US Department of Homeland Security: Strategic Principles for Securing the Internet of Things

[https://www.dhs.gov/sites/default/files/publications/Strategic\\_Principles\\_for\\_Securing\\_the\\_Internet\\_of\\_Things-2016-1115-FINAL\\_v2-dg11.pdf](https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf)

W3C: <https://www.w3.org/standards/>

## About the Author

### **Vishruta Rudresh**

Vishruta Rudresh is a Senior Cybersecurity Researcher at Kudelski Security focusing on fundamental new approaches to IoT and OT environment security, including but not limited to machine learning, edge device decision making, and low power environment security. She has been working in the Information Technology industry since 2011 specializing in IoT security, malware reverse engineering, system and application administration, incident response, digital forensics and mobile security and has a master's degree in Information Technology-Information Security from Carnegie Mellon University.

## About Kudelski Security

Kudelski Security is an independent provider of tailored cybersecurity solutions to enterprises and public sector institutions, delivering workable solutions to the toughest security challenges they face.

As part of the Kudelski Group, Kudelski Security embodies the same innovative spirit that has inspired the company since its creation in 1951. Our innovation is purposeful; we strive to create and deliver cybersecurity solutions that answer real problems. We help our clients in their journey to design, deploy, and manage effective cybersecurity through a combination of advisory services, technology deployments, managed security services, and custom research and development.

We build on the concrete expertise of the Kudelski Group and their creation of ground-breaking technology that has shaped the evolution of the digital content ecosystem. Together with the Group, we hold thousands of patents and apply the rich engineering expertise of 3,900+ employees worldwide to the solutions we create and deliver in the cybersecurity marketplace.

Our global reach and comprehensive cyber solutions focus is reinforced by key international partnerships. These include alliances with the world's leading security technology firms as well as with experts in specialized services, so clients have access to all the tools and talent they need in order to plan, deploy, and run effective cybersecurity programs.

### Disclaimer

The information in this document provides guidance on relevant technologies serving a specific enterprise security challenge. As each client environment and business need is unique, we do not warrant that these recommendations are appropriate in every instance. To clarify the appropriateness of a strategy or test the impact of a specific vendor, we recommend clients engage our presales solutions team for a more detailed analysis.