Guide for Cellular IoT Security

EMnify

Introduction

IoT businesses that connect their devices via mobile networks are shaping our increasingly connected world, but enterprises must ensure that their devices, data and services, are protected from security threats. For hackers, IoT devices are a primary target, because many devices have the same configuration and they do not possess security measures such as virus scanners and software network firewalls. Attacking IoT devices has become an attractive business, with criminal organizations utilizing the devices for paid distributed denial-of-service attacks[1], mining of cryptocurrencies[2] and by making the IoT device useless unless the IoT business pays to regain access (ransomware)[3]. The complex nature of any IoT deployment exposes it to threats at multiple levels. Making it a major challenge to keep up with the latest security approaches – and choosing the best one for your business.

While there is no one-shield-fits-all solution, this guide will help you to make well-informed decisions about cellular IoT security technologies and best practices, and the type of solution that best suits your organization.

IoT attacks have become an attractive business

IoT attacks have been increasing steadily, with certain types of attacks[6] [7] increasing by as much as 900% in 2019[5]. This growth is attributable to two key factors: not only is IoT attracting the attention of more and more cyber criminals, but also most IoT companies lack the knowledge about IoT security best practices and technologies to adequately protect themselves.

25%
of respondents reported at least
$35 million
in IoT security related losses [4]

900%
Increase of Mirai attacks in 2019 [5]

Security problems in an IoT deployment cause far more than just financial losses, often severely damaging the reputation of the business and setting IoT profitability back by years. Companies that can demonstrate adequate security for their connected devices and applications can easily win customers' trust, gaining a huge competitive advantage in the process.

But IoT security is no simple task. Businesses have to answer questions like:

- How can I remotely control, manage and troubleshoot my devices without leaving a door open for attackers?
- How can I be sure that no attack is executed from my device?
- How can I securely transport data from the network to my application without attackers getting access?
- Are there new security options because my infrastructure is on one of the big cloud providers?
- How can I make my SIM more secure so that it cannot be misused in another device?
- Where should I store passwords, identities and certificates on the device?

This guide offers you an overview of the options and best practices in the market with respect to security in IoT.

Navigating the guide:

PG. 4 Attack Surfaces

PG. 4 Device Security

PG. 7 Connection Security

PG. 14 Application Security

PG. 16 Solution Monitoring

PG 19 Security Checklist

Back to top

1. Security is about attack surfaces

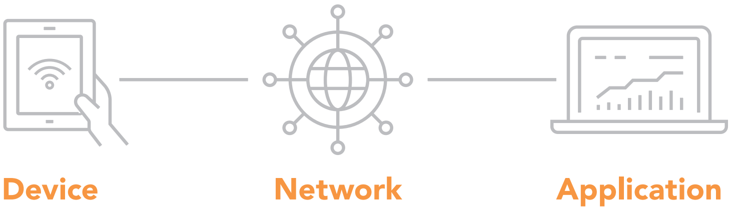
What is an attack surface?

An attack surface is any point or part of the system through which **an unauthorized user/attacker can try to get into the system.**

Within an IoT solution there are many attack surfaces – the device, wireless module, the data transmission from device to application, application infrastructure, and the application itself. Any of these can be used to impact access, misuse the system, or disclose/modify confidential information. One basic way to incorporate security into the design of your deployment is to **minimize the attack surface.**

The Open Web Application Security Project (OWASP) has gathered an extensive list of attack surface categories[8], which can be grouped under three broad heads: the device, the telecom service, and the application. Each attack surface requires its own specific security countermeasures. Let us examine them in detail.

Attack Surfaces:

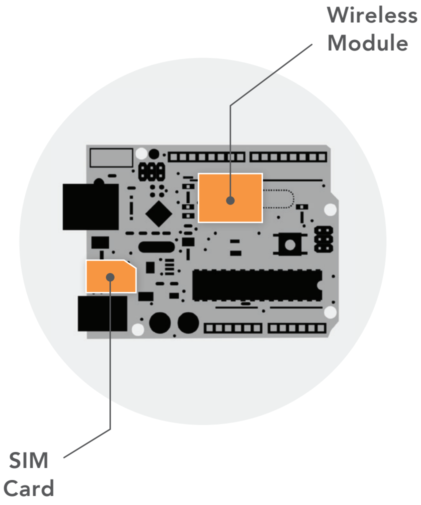


2. Device Security

The device is the end point of any IoT deployment: it could take any form factor from a sensor, GPS tracker, a car or edge gateway. **An IoT device connected by means of cellular connectivity, usually consists of three major components:**

- SIM card
- Device software
- Physical device (incl. processor, storage, OS, external interfaces)
- Cellular Wireless Module

Each of these components has a **Root of Trust (RoT):** an unchangeable source that is guaranteed to be correct. Many security processes, such as encrypting user data or validating data, are based on the Root of Trust.



Back to top

2.1 SIM Card

Mobile connectivity brings its own root of trust – the SIM card. Based on 30 years of evolution and standardization, SIM cards secure data transmission in the mobile network and ensure the proper identification of a connection's source.

The following information and algorithms are part of the RoT permanently stored and executed on the SIM card:

- **ICCID –** identifier of the SIM card
- **IMSI –** international mobile subscriber identity; used for authentication with a network
- **PIN1, PIN2 and PUK –** PIN Code. Less frequently used in IoT use cases as it requires unique device and/or screen configuration
- **Authentication key Ki –** unique key used together with IMSI for authentication in the GSM network
- **Security algorithms –** A3 for authentication, A8 for cipher key generation
- **ADM keys –** multiple keys that protect the editing of the SIM card with a SIM editing application

The SIM's unique identifiers play a central role in authenticating the device on the mobile network, granting or blocking permissions based on network policies, and transporting data securely within the network.

2.2 Physical Device

The fact that IoT devices are often deployed in remote locations (where the provider cannot control access) means that the physical device is the first attack surface. Attackers with physical access to a device could break into it and transfer the SIM to a different device, or attempt to gain access to the data on the device.

Best Practice #1 – *Device SIM Security*

Effective precautions to protect your device SIMs are:

- Using embedded SIMs that break when removed
- Activating an IMEI lock so the SIM can only be used in one device
- Using a cellular network firewall to control traffic to unauthorized destinations

Back to top

***Best Practice #2** – Device data security*

To protect data on a device, recommended precautions include:

- Using strong adhesive that will break the device when it is under physical stress
- Deactivation of physical interfaces (JTAG/Serial)
- Encryption of on-device storage
- The use of tamper-detection alerts that e.g. trigger remote data erasure

2.3 Device Software Security

The operating systems and software embedded on IoT devices are common attack surfaces due to software bugs or exploits. Therefore, software constantly needs to be updated to protect against constantly evolving threats and vulnerabilities. Given that IoT device fleets could be dispersed all over the world, they should be capable of being managed and updated remotely. **Two key capabilities are needed for this: remote device management, and remote access.**

Remote Device Management allows IoT businesses to remotely update the firmware or execute predefined commands on multiple devices. Usually, a centralized server prepares the software image or action, which the device downloads when it communicates with the server.

Remote Access allows a support engineer to log in directly to a device for troubleshooting. This could be to access the file system, execute commands, or analyze data that is not sent to the application. Remote Access does not require data to be sent from the device – only that a PDP context from the device is open.

***Best Practice #3** – Device Software Security*

- Conduct and verify remote firmware updates over a secure channel
- Allow firmware rollback in case firmware update fails
- No hardcoded credentials, clear-text usernames, password, or encryption keys on device
- Delete relevant information remotely when the device is placed out of service
- Use remote access over a secure channel
- Follow CI/CD and roll out latest security updates for used libraries in short time windows
- Ensure secure boot that verifies that the device firmware is correct

Back to top

3. Telecommunication Service Security

Figure 3 – Telecommunication Service for IoT

All telecommunication services (voice, SMS and data) provide an additional attack surface that can be exploited by criminals. Cellular providers with an IoT focus provide mechanisms to block or limit telecommunication services at the network level so attacks misusing the services can be prevented.

3.1 Voice services

Although voice is not widely adopted in the IoT domain there are still use cases that require voice capability. It is to be noted that not all 'voice' is 'voice': IoT solution providers often use Voice over Internet Protocol (VoIP) services instead of the regular telecommunication service, so they can use the same security mechanism used for their data services **(see Section 3.3)**.

If the voice service is active, attackers with physical access to the device or SIM can commit a variety of telecom frauds. For example, they can incur huge charges through fraudulent calls to premium-rate numbers, from which they gain a revenue share. The IoT solution provider is then liable for the incurred costs. Therefore it is recommended that the amount and duration of voice services allowed for a device are limited, as well as the numbers that can be called or can call the device.

Back to top

3.2 SMS

Recently, hackers are increasingly using SMS[9] as an attack surface. If SMS is part of a solution and cannot be deactivated, it should be blocked **from external devices** (also called person-to-person SMS) so attackers cannot reach the device directly. Not only does this prevent attacks, it also eliminates unwanted SMS charges from the network.

Instead of P2P SMS, cellular IoT connectivity providers typically offer an application programming interface (API) to communicate with a device via SMS. The API is secured by additional authentication mechanisms, restricting SMS access to specific users or applications.

Another best practice for IoT businesses is to ask the cellular connectivity provider to limit the amount of SMS that can be sent or received by a device. This prevents unwanted costs if the device malfunctions and sends an abnormal amount of SMS communications.

Best Practice #4 – *Voice and SMS Services*

- Allow the cellular provider to block unused services
- Use an API or provider portal to send and receive SMS programmatically instead of using external device-to-device SMS
- Limit the numbers that are reachable via voice
- Limit voice and SMS service consumption to a threshold that fits your use case

3.3 Data

Data services are the predominantly used telecommunication service in the IoT domain. Devices can send excessive amounts of data intentionally (due to misuse by an attacker) or unintentionally (due to a firmware or application error). To prevent unwanted costs, cellular IoT connectivity providers can limit the usage per SIM card, according to the expected behavior of the specific device or use case.

Over and above this, when it comes to data, the attack surface is large and there are several security mechanisms to be considered.

Back to top

3.3.1 IP addresses and Remote Access

Cellular connectivity providers generally offer both private and public IP addresses (IPv4 or IPv6) for devices using their SIM cards. IoT businesses need to choose carefully between private and public IP addresses, as this has a significant impact on attack surfaces for attackers. **There are four options**:

Type	Description	Remote Access
Dynamic Public IP	Each time the device opens a data session it may get a different public IP address, through which the device is reachable from any external point.	Only possible with an additional dynamic DNS service to resolve hostname to changing IPs.
Static Public IP	The device gets a single IP address through which it is reachable from external points.	Possible via a hostname or IP.
Dynamic Private IP	Each time a device opens a data session it gets a different private IP, which is not reachable from external points.	Requires additional applications on each device that open ports for remote access.
Static Private IP	The device gets a constant private IP address, which is not reachable from any external point.	Requires a VPN/IPSec or Secure Intra-Cloud Connection.

Private IP addresses significantly reduce the attack surface of devices, as they are not reachable from the public internet and attackers cannot directly route traffic towards the devices. Some cellular IoT providers require the setup of private Access Point Names (APNs) to manage private IP address spaces and the definition of a VPN/IPsec endpoint, while this is not needed by newer providers.

Although dynamic private IP addresses seem most secure, from a practical perspective it is recommended that private static IP addresses are used for IoT devices. This is because dynamic private IP addresses place severe limitations on remote access, which is essential to reconfigure, troubleshoot, and maintain connected devices. Remote commands can only be made with an additional remote access application on the device. However, these applications require additional costs, software maintenance, and device power.

Remote access to a device from cloud infrastructure using static private IP addresses has now been made even more secure with **intra-cloud connect.** The cellular connectivity provider manages the security of the complete path – from the device to the cloud infrastructure (Secure Intra-Cloud Connect). **Read more here**

***Best Practice #5** – IP Addresses*

- Use static private IP addresses to hide devices while retaining remote access to them
- Use a cellular cloud provider that offers intra-cloud connect, so that public IP addresses are not required for the application infrastructure

3.3.2 The Security Gap between Mobile Network and Application

Devices that connect to the cloud infrastructure via a cellular network will have a security gap between the mobile network and application. Here's a quick overview:

1. The communication from the device within the mobile network operator infrastructure is secured using the SIM card. Only SIM cards that can correctly authenticate their identity are authorized to connect to the network. Based on the identity, different policies like data volume limit, permitted networks, availability of voice or SMS service and so on can be enforced.
2. The communication path between the mobile network and cloud infrastructure is not secure. Data goes over the public internet, which creates attack surfaces for man-in-the-middle attacks, impersonation and DNS spoofing attacks.

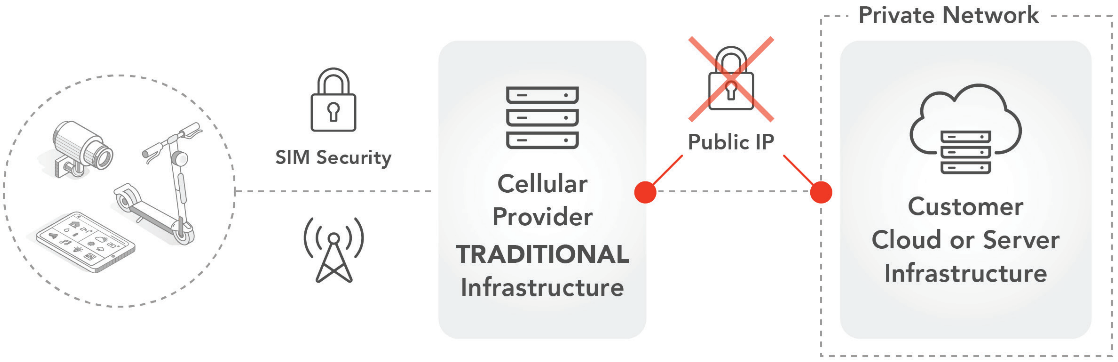
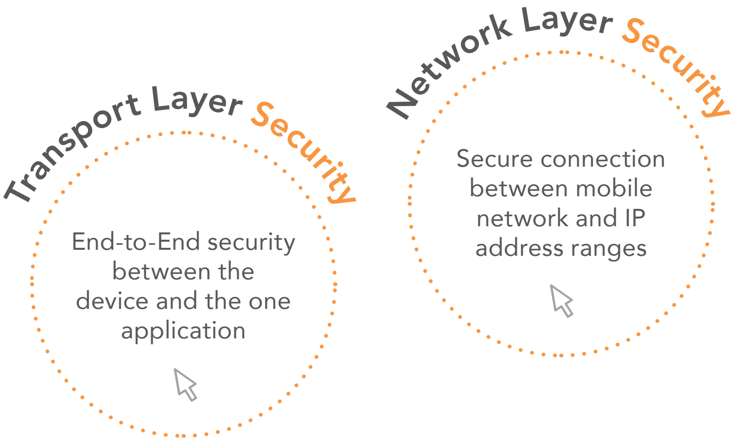

SIM Security
Cellular Provider
TRADITIONAL Infrastructure
Public IP
Private Network
Customer Cloud or Server Infrastructure

Figure 4 - Public Internet breakout in Cellular Connectivity

Back to top

There are **three major mechanisms** to prevent these types of attack:



Transport Layer Security

End-to-End security between the device and the one application

Network Layer Security

Secure connection between mobile network and IP address ranges

Intra-cloud Connect

Cellular cloud provider manages security from device to cloud provider

Transport Layer Security

Transport Layer Security (TLS) is commonly used within encrypted web pages (shown in a browser's address bar by the https prefix or a padlock). For web pages, only one side of the communication (i.e. the server) is authenticated. The client on the device can verify the security credentials of the web page and the hostname based on the certificate signature from a certificate authority.

In the case of an IoT device, authentication takes place on both sides. Based on the certificate from the server, the device also encrypts the data it sends with the server's public key. The server holds the matching private key, with which it can decrypt the data and therefore also confirm its identity. The data between device and server is then encrypted – preventing man-in-the-middle attacks and DNS spoofing.

There are two deployment models for using TLS in IoT:

1. **Application-side authentication only.** This ensures that the device is sending the data to the right application.
2. **Device- and application-side authentication.** In this case, generally considered best practice, the device also requires proof of identity. Cloud infrastructure providers like AWS, Azure and Google have dedicated IoT services that mandate bilateral certificate authentication. Based on device identity, granular policies (such as which data can be sent or read) can be enforced at the device level.

In cases where certificates are required on the device, **Roots of Trusts** (described in section 3, "Device Security") should be used. Several operators display secure certificate storage on their SIM cards. Just recently several operators started to store certificates in their SIM cards, following the GSMA IoT SAFE specifications[14]. IoT businesses can also use additional Hardware Secure Modules (HSM) for storing certificates, which provide the highest control and independence.

Back to top

Network Layer Security

While Transport Layer encryption is recommended to be used for securing the data path, there are several challenges.

Additional Device Processing & Power Consumption

For encrypting data

Only for one application

Devices connecting to multiple applications need a certificate for each

Additional data cost

TLS bloats transmitted data by up to 500%[10]

Network Path not Secure

Attackers can route traffic towards infrastructure

Older devices might not support the TLS version required by the application or cloud service. For example, TLS 1.2 encryption has become mandatory among cloud providers, leaving devices that only support TLS 1.1 unable to connect.

This is where Network Layer Security with virtual private networks (IPSec/VPN) is a recommended alternative, offering additional benefits on top of TLS.

IPSec/VPN provides a secure connection between the mobile network infrastructure and the cloud infrastructure – closing the security gap. The encryption is offloaded from the device, which simplifies setup while providing older devices with a high level of security. The additional data overhead for encryption is outside the mobile network, so it does not incur additional data costs from the mobile operator.

An additional benefit of Network Layer Security is that the **devices and infrastructure are within the same virtual private network.** For troubleshooting or configuration changes, devices can be remotely accessed with their private static IP address from the application infrastructure. What's more, IoT businesses can use their own private DNS server in their cloud infrastructure, eliminating another attack surface that is exploited with DNS spoofing attacks.

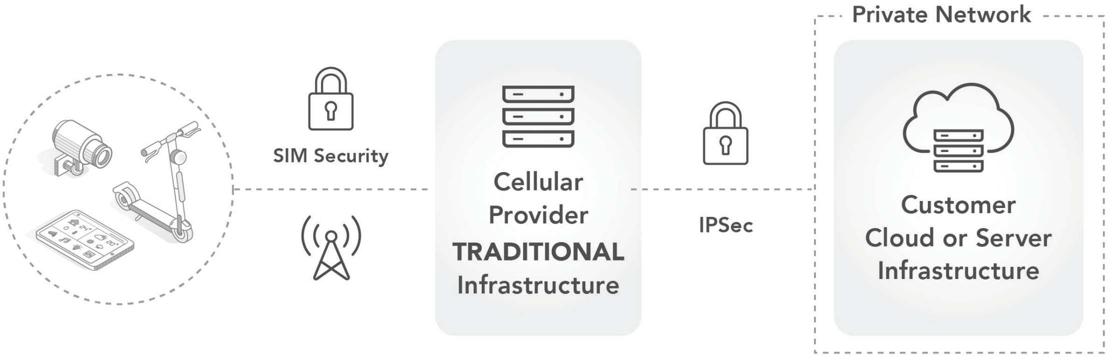

Private Network
SIM Security
Cellular Provider TRADITIONAL Infrastructure
IPSec
Customer Cloud or Server Infrastructure

Figure 5 - Network Layer Security between Mobile Network and Infrastructure

Secure Intra-Cloud Connect

Traditionally devices need to connect to the public IP addresses of the cloud infrastructure, which creates an attack surface even when using Transport Layer Security and IPSec / VPN.

However, with the advent of cellular cloud providers that have their mobile infrastructure already in the cloud, this can be addressed with **secure intra-cloud connect** (Figure 6). Under this security approach, data is securely brought into the cloud infrastructure by the cellular cloud provider. The connection to the customers' infrastructure is established via a secure intra-cloud connect service such as the AWS Transit Gateway. With this mechanism, public IP addresses are unnecessary, and devices and application infrastructure can be completely hidden from the outside. As a result, attackers cannot send any data to devices or the application infrastructure.

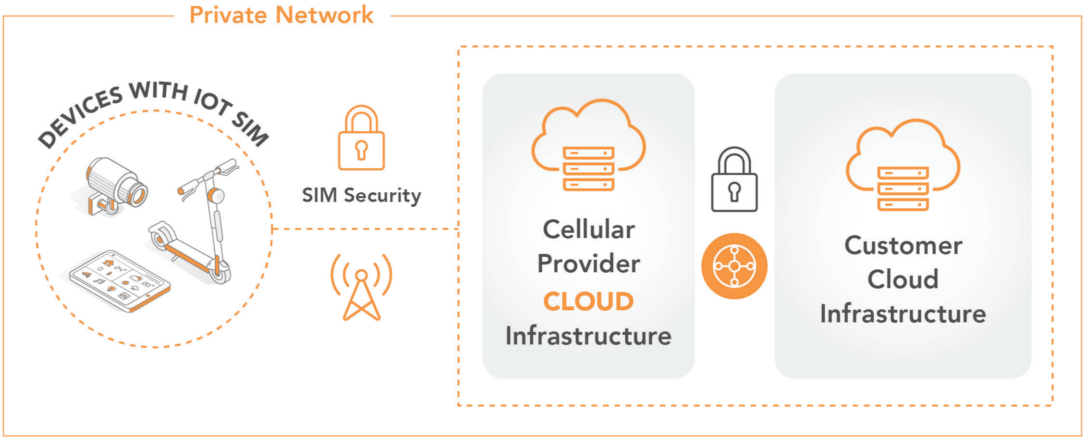

Private Network
DEVICES WITH IOT SIM
SIM Security
Cellular Provider CLOUD Infrastructure
Customer Cloud Infrastructure

Figure 6 - Cloud Native network security **click here for more information**

Benefits of intra-cloud connect include:

- All the connectivity-related security measures are managed by the cloud and connectivity provider. The cellular cloud provider is responsible for bringing data into the cloud infrastructure. The connection to the customer's infrastructure is established using a secure intra-cloud connect service such as AWS Transit Gateway
- Establishing a secure connection with the device does not involve an adjustment of the manufacturing process for certificate deployment or lengthy provisioning of private APNs
- Integration is automated, and the availability of the connection is based on the reputable standards of secure connectivity provided by the cloud service
- Public IP addresses are unnecessary. Devices and application infrastructure can be completely hidden from the outside
- Cloud service benefits such as no upfront investment, high service availability and intra-cloud connect availability in each region

Back to top

3.4 Cellular Network Firewall

If attackers gain control of a device (for example, through a Mirai attack), it may not be immediately obvious to the IoT business. As a result, the device may be able to create excessive data traffic by attacking a victim using the public network with a Distributed Denial of Service (DDOS) attack. To secure devices and SIM cards, a network firewall implemented by the cellular network provider is a very powerful security mechanism.

Cellular connectivity providers specializing in IoT provide network firewalls that limit the data service that a device / SIM card can access: so it is only able to send traffic to a specific IP address range. This limits the data service of the SIM card only to the applications purpose.

4. Application Security

IoT deployments can be protected at the application level, apart from at the device, software, and network security levels discussed in preceding sections.

The ecosystem behind any IoT deployment is extremely complex and diverse. Use cases are unique to every industry and the applications associated with them, and often use multiple open-source frameworks and libraries, each with their own maintainer. IoT businesses should apply an agile security approach that facilitates continuous integration and deployment of application software. This model minimizes the time between the detection of a bug or a security gap and the fix, limiting the impact of any potential threat.

Best Practice #6 – *Application Security*

- Follow security best practices, using secure and complex passwords that are changed periodically, multi-factor authentication, well-defined user roles and their permissions, and user audit trails
- To secure databases, use secure APIs that can only be executed by authenticated users
- Limit the API calls that can be executed per user, device or IP address to prevent attacks or errors that target the availability of the system
- Apply an approach that facilitates continuous integration and deployment of application software

Back to top

4.1 Application Infrastructure Security

One of the earliest decisions that an IoT business needs to make is on the infrastructure they use for their applications – on-premise, virtualized, private or public cloud providers. From the perspective of data privacy and security, the best option is to use a cloud-based infrastructure.

IoT businesses that host their own applications on virtual machines in the cloud will have to manage the security themselves. On the other hand, cloud providers AWS, Azure, and Google offer the highest levels of security, with infrastructure certified following international and national-approved norms and standards[11] [12] [13]. These providers generally take responsibility for the cloud infrastructure and services in case of security incidents. They therefore have a strong incentive to use the latest security and be innovation leaders in this field.

4.1.1 Infrastructure Network

While cloud infrastructure services such as AWS IoT, Azure IoT hub or Google IoT are publicly accessible by all devices, the security of these services is managed to extremely high standards and unwanted access completely restricted.

Cloud providers allow the definition of security groups for the virtual machines to limit the traffic into the infrastructure network on the protocol and port level.

4.1.2 Infrastructure Accounts and User Access

When deploying an IoT solution, the best practice is to logically separate services into multiple infrastructure accounts. The infrastructure is better isolated and the blast radius of human error or an attacker getting access to one account is limited.

Cloud platforms provide identity and access management services that allow authenticated and auditable access to all services. With this, user logs are stored which can be further analyzed for abnormal or malicious behavior.

Multi-factor authentication (MFA) provides an extra level of security by asking for additional security checks (besides normal login credentials) from users accessing the infrastructure.

Back to top

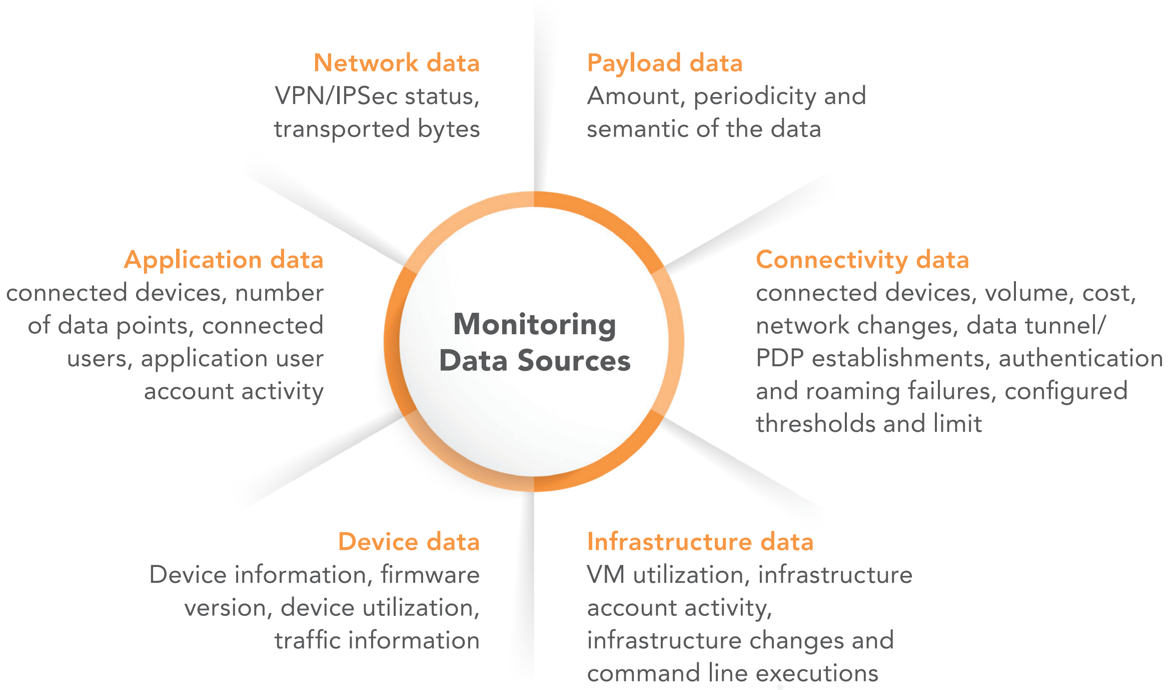
Best Practice #7 – Application Infrastructure Security

- Use cloud infrastructure like AWS, Azure, and Google to host IoT applications: these environments have been designed by domain knowledge experts to meet any level of sensitive security requirements
- When working with a cellular cloud provider, hide the virtual machine infrastructure in a private network using intra-cloud security to avert port scans, DDoS, and spam attacks
- Logically separate services into multiple infrastructure accounts, so that they are isolated, and damage is contained even if attackers manage to gain access to one account
- Use multi-factor authentication (MFA) for an extra level of security

5. Monitoring and Anomaly Detection

Monitoring the system is an integral part of keeping it secure. Establishing a monitoring system with well-defined alarms can reduce the response time to incidents and new security breaches.

Given the complexity of any typical IoT deployment, the system data that should be monitored is quite broad.



Monitoring Data Sources

Network data
VPN/IPSec status, transported bytes

Payload data
Amount, periodicity and semantic of the data

Application data
connected devices, number of data points, connected users, application user account activity

Connectivity data
connected devices, volume, cost, network changes, data tunnel/ PDP establishments, authentication and roaming failures, configured thresholds and limit

Device data
Device information, firmware version, device utilization, traffic information

Infrastructure data
VM utilization, infrastructure account activity, infrastructure changes and command line executions

Back to top

With regards to connectivity data, cellular providers focusing on IoT have APIs available that provide IoT businesses with insights into the data on the network. Some providers' APIs are not usable for anomaly detection because they are transactional rather than real-time, meaning the data for a device is delivered only on request. Other providers offer real-time delivery of all connectivity data – including data usage, costs, signaling and network events and errors, which are not only usable for abnormality detection but also to provide improved proactive customer support.

Cellular cloud providers also have the option to deliver connectivity data directly into the cloud infrastructure of the business. By providing connectivity data directly from the cellular cloud infrastructure to the IoT business cloud, **the connectivity data does not pass through the public internet,** and the data is reliable provided through managed cloud services.

To analyze and detect anomalies within the IoT system data there are cloud infrastructure-specific services, such as AWS Device Defender, Guard Duty or Azure IoT Hub Security and Advanced Threat Protection. Infrastructure independent services and monitoring solutions such as Threatstack and Grafana can be used to provide advanced protection.

The most effective approach is to decide on a few meaningful and manageable services that ideally provide a holistic overview of the data – making it unnecessary to jump between different tools and applications.

Best Practice #8 *– Monitoring and anomaly detection*

- Use cellular connectivity providers whose APIs are usable for real-time anomaly detection
- Deliver connectivity data directly into the cloud infrastructure
- Use a combination of cloud infrastructure-specific anomaly detection services and infrastructure-independent monitoring solutions, depending on the use case
- Use a selected few services that provide a holistic overview of the data

Back to top

6. Summary

With smart cities, connected health, smart wearables, industrial IoT, and other revolutionary developments, IoT businesses are reshaping the world today and making it more connected. However, keeping up with the latest security approaches and choosing the right one is a major challenge for any IoT business, large or small, anywhere in the world.

IoT attacks have become a serious business – where the attackers' target is to get control of all the connected devices and ultimately use the hacked device for cryptocurrency mining, for example, or to obtain valuable private and financial data from the devices.

By using the best practices and explanations of the different IoT security technologies in this guide, summarized within the exhaustive checklist below, IoT businesses can prevent common malicious attacks and make their business more secure.

Back to top

Cellular Connectivity Security Checklist

Device

Attack Surface	Countermeasure	Applied?
Physical Access to the device	Tampering Alerts / Storage Deletion Tamper resistant case Use of strong adhesive that break electronics on opening	
Exploits and Bugs in Device software or OS	Enable regular remote firmware updates	
External Interfaces of device	Deactivation of Serial / USB ports Use Fuse bit to protect from read/write access	
Client Certificate	Storage in Root of Trust such as HSM, SIM, Wireless Module	
Using of SIM card in another device	Use embedded SIMS (MFF2) Activate IMEI lock	
Device Software Bugs / New Security holes	Device Management capabilities that allow firmware updates that allow rollback	
Longevity of Device	Ensure remote information deletion at device end of life	
Password / Credentials	No hardcoding, randomization of default password	
Code Injection	Secure boot - the verification of the SW image	

Download Checklist as PDF

Back to top

Network

Attack Surface	Countermeasure	Applied?
Device IP Addresses	Use private IP addresses	
Infrastructure IP addresses	Usage of private IP addresses and intra-cloud connect security	
Use of public DNS servers	Use DNS over TLS or private DNS servers together with network layer security or intra-cloud connect	
Authentication of Device	Use of TLS and/or VPN/IPSec/intra-cloud connect security	
Remote Access to Devices	Use secure IPSec/VPN/Cloud-Native Security channel from the infrastructure	
SMS Service	Deactivate Service or use A2P SMS Limit amount of SMS per device	
Voice Service	Deactivate Service or Limit amount / available numbers	

Download Checklist as PDF

Back to top

Application and Infrastructure

Attack Surface	Countermeasure	Applied?
Infrastructure	Use cloud infrastructure that complies with latest security standards	
Exploits and Bugs in application or OS	Continuous Integration / Devops	
Infrastructure and Application User access	Identity management services Multi-Factor authentication User activity tracking	
Database access	Allow changes and access only through secure API	
Overuse of API	Limit API usage by using API gateways and management services	
Availability of the system	Utilize load-balancing, auto-scaling groups, network firewalls, access control list and overload protection algorithms to prevent over usage of the system	

Download Checklist as PDF

Monitoring and Anomaly Detection

Available Data Sources	Data Available?
Device Payload Data	
Device Data	
Cellular Connectivity Data	
Infrastructure Data	
Application Data	
Network Data	

Download Checklist as PDF

Back to top

References

[1] TrendMicro, „The Internet of Things in the Cybercrime Underground“, [Online]. https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf

[2] TrendMicro, „Cryptocurrency-Mining Malware Targeting IoT, Being Offered in the Underground“, [Online], https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-targeting-iot-being-offered-in-the-underground/

[3] Cyber Defence Magazine, „Ransomware and the Internet of Things“, [Online], https://www.cyberdefensemagazine.com/ransomware-and-the-internet-of-things/

[4] IotBusinessWire, “Research unveils corporate losses associated with iot related security missteps,” March 2019. [Online]. Available: https://iotbusinessnews.com/2019/03/25/10309-research-unveils-corporate-losses-associated-with-iot-related-security-missteps/.

[5] Darkreading, „IoT attacks up significantly in first half of 2019,“ [Online]. Available: https://www.darkreading.com/attacks-breaches/iot-attacks-up-significantly-in-first-half-of-2019/d/d-id/1336096.

[6] Wikipedia, „Mirai Malware,“ December 2019. [Online] Available: https://en.wikipedia.org/wiki/Mirai_(malware).

[7] KrebsonSecurity, “A deep dive on the recent widespread DNS hijacking attacks,” February 2019. [Online]. Available: https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

[8] O. W. A. S. P. (OWASP), „IoT Attack Surface Areas,“ [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas.

[9] “SIMjacker exploit,” September 2019. [Online]. Available: https://techxplore.com/news/2019-09-simjacker-exploit-independent-handset-sms.html.

[10] Nasko, „Netsekure - TLS overhead,“ March 2010. [Online]. Available: http://netsekure.org/2010/03/tls-overhead.

[11] Microsoft, „Azure Compliance List,“ [Online]. Available: https://azure.microsoft.com/en-in/overview/trusted-cloud/compliance/.

[12] AmazonWebServices, „AWS Compliance Program,“ [Online]. Available: https://aws.amazon.com/compliance/programs/.

[13] Google, „Google Cloud Compliance,“ [Online]. Available: https://cloud.google.com/security/compliance/offerings/#/.

[14] GSMA, “IoT SAFE. IoT SIM Applet for Secure End-to-End Communication”, [Online], https://www.gsma.com/iot/iot-safe/