IOT NOW REPORT:

HOW TO SECURE YOUR IoT DEVICES

Reproduced by IoT Now magazine

EUROTECH

Imagine. Build. Succeed.

How to secure your devices

The issue of IoT security has been prevalent since the first things were being connected. This special report by IoT Now's Antony Savvas considers how security technology has evolved and whether it is up to the job

The report looks at the market itself and what issues the industry has to address, including expert opinions on common security mistakes when planning and deploying an IoT project, IoT security best practices, IoT security by design, device-level and edge network security, communications security and cloud security.

The urgency needed to tackle problems is perhaps illustrated by a report from **SonicWall**, with the security vendor's Mid-Year Threat Report finding that worldwide IoT malware attacks were up 50% year-on-year in the first six months of 2020.

Reproduced by IoT Now magazine

"Currently, there is no globally accepted set of technical standards for IoT, especially in terms of communications,"

The market

The global Internet of Things (IoT) security market by value is expected to grow from US$12.5bn in 2020 to US$36.6bn by 2025, at a compound annual growth rate (CAGR) of 23.9%, according to research house **MarketsandMarkets**. This forecast - from July 2020 - sits somewhere in the middle of a variety of analyst forecasts for the IoT security market.

Technavio, in May 2020, said the market will actually grow by a whopping US$80.94bn during the period of 2020-2024, at a CAGR of almost 37%. Technavio said 2020 will see around 33% growth in IoT security spending when compared to 2019.

Both analysts say key factors driving IoT security growth are rising security concerns around critical infrastructure, increasing ransomware attacks on IoT devices, increasing data risk in IoT networks, growing IoT security regulations and the increasing adoption of cloud-based services. Industry players in the market are high in number, and range from hardware and software providers to system integrators and providers of professional deployment and security management services. Companies involved include **Cisco Systems**, **IBM**, **Intel**, **Infineon**, **Symantec**, **Siemens**, **Gemalto**, **Fortinet**, **Zingbox**, **Mocana**, **Centri**, **Armis**, **Forgerock**, **Newsky**, **Cyber X**, **Eurotech**, **Icon Labs**, **Digi International**, **SecureRF**, **Altran**, **CA Technologies**, **MagicCube**, **Thales**, **Qualys**, **Karamba Security**, **Claroty**, **Trustwave**, **Sectigo**, **Dragos Security** and **Broadcom**.

The challenges

A lack of standardisation for the security of IoT solutions is a major challenge. "Currently, there is no globally accepted set of technical standards for IoT, especially in terms of communications," says MarketsandMarkets. "With heterogeneous IoT networks and their protocols, it becomes difficult for devices connected in one IoT system to communicate with devices in another."

This, in turn, results in inefficient data management and reduced interoperability mechanisms, said the analyst. "The inability of such IoT networks to have a common platform, uniform standards and extensive authentication certificates can result in reduced security."

> "While IoT is one of the fastest growing markets in ICT. The ecosystem is a complex mix of technologies and service"

Antony Savvas
journalist and report author

Ben Carr
Qualys

Kevin Restivo, **IDC** research manager for European enterprise mobility, says: "While IoT is one of the fastest growing markets in ICT. The ecosystem is a complex mix of technologies and services: server, storage, analytics, IT services, security and a range of other technologies."

He confirmed that security fears lead when it comes to market inhibitors. Restivo adds: "A lack of coordination between operations and IT is very much an inhibitor to secure deployment. Everyone wants to protect their fiefdoms or they're simply not able or willing to cooperate.

"IT is often left behind during the project and security planning, budgeting and piloting. That lack of coordination can really stall the successful deployment of industrial Internet of Things initiatives."

On the compliance side there have been governmental initiatives in IoT security, but there are concerns that it is consumers that are being prioritised, not businesses, which doesn't address a joined up problem from past experience. For instance, in July 2020, UK digital infrastructure minister Matt Warman revealed that internet-connected gadgets will have to come pre-set with a unique password, or require the owner to set one before use, as part of plans for tighter UK cyber-security laws.

Peter Margaris, head of product marketing at **Skybox Security**, argues that while it's good to see a government prioritising security, warnings about IoT security risks and best practices should be extended to the business environment. He says: "In 2016, we saw the Mirai botnet take advantage of insecure IoT devices and turn its power against the internet itself. It didn't just affect select consumers, a single business or even a single sector - it disrupted the online world. Therefore, any new law must go beyond the consumer remit. A basic code of practice for all is the very minimum that should be put in place by governments to help prevent a repeat attack."

So let's look at the main issues and considerations around IoT security

Common security mistakes when planning an IoT project

In the rush to adopt an IoT strategy it is understandable that many organisations can get it wrong, particularly if there is a shortage of experts on the pay roll.

Deral Heiland, IoT research lead at cyber-security firm **Rapid7**, says: "Some of the biggest security issues around IoT are caused by not following manufacturer's guidelines or general security best practices during deployment."

This includes not changing administrator default passwords, exposing technology directly to the internet, and using weak account passwords or passwords that are identical to other systems and accounts.

"One of the most common issues is failure to properly segment networks – flat networks where every device can see every other device creates a serious risk to the organisation," said Heiland.

Common deployment mistakes:

- Use of hardware and software without built-in security and privacy features
- Allowing transmission of unencrypted data
- Lack of tools and processes to plan device updates
- Hard-coded credentials
- No integrity check of the software and OS installed
- API tokens not encrypted
- Lack of proper authentication and authorisation systems

"While asset management has been a core component of general IT, in many cases IoT devices have not been well accounted for"

Device-level and edge network security

Ben Carr, chief information security officer at **Qualys**, says: "Organisations and their partners have to ensure device-level security is optimised. At the most basic level it starts with knowing what devices you have in the environment and how they are configured."

"While asset management has been a core component of general IT, in many cases IoT devices have not been well accounted for," he adds. "For those building IoT devices they need to say clearly what the boundaries are for connectivity and communication from the device itself, and they need to implement security controls from the beginning."

There are three areas to consider, says Carr: how the devices behave normally; the security perspective, such as security controls and configuration; and third, the maintenance of the device and how updates can be applied securely and how they will affect the operational nature of the network.

By looking at these three elements, we can get a better picture of those IoT devices and how to manage their security. Sadly though, many devices, even today, are designed and deployed without any security planning or management in place.

Arthur Fontaine
RSA Security

Communications security

Strong encryption is critical to securing communication between devices, says Jerry Nicolas Ponvelil, director of technology at **Altran**. Data at rest and in transit should be secured using cryptographic algorithms. This includes the use of key lifecycle management.

"Protecting an IoT network includes ensuring port security, disabling port forwarding and never opening ports when not needed; using anti-malware, firewalls and intrusion detection/intrusion prevention; blocking unauthorised IP addresses; and ensuring systems are patched and up-to-date," says Ponvelil. "If this is not done properly, it may result in compromised security in the cloud network and applications."

Carolyn Crandall, chief deception officer at threat management and hacker deception vendor **Attivo Networks**, said: "Using secure communications protocols prevents eavesdropping and interception attacks. Using blockchain to store and validate transactions between devices can increase communications security as well. For organisations using patch management servers, it can be useful to interweave decoys and in-network hacker lures that can alert on attempts to discover or exploit these systems."

Alan Grau
Sectigo

Cloud security

We all know about the proliferation of the cloud and how it is increasingly connected to the edge where the majority of IoT devices are located, so how do we secure this interconnectivity?

Cloud security has a number of critical components, including access control; traffic filtering; security configurations; data protection; virus protection; and other incident monitoring, response and prevention elements.

Nigel Hawthorn, data privacy expert for cloud security at **McAfee**, says: "Cloud security threats are continually escalating, with our research recently revealing a 630% increase in external cloud attacks between January and April 2020. Cloud and data security should therefore be front and centre in informing any enterprise's cyber-security approach - even more so as increasing numbers of organisations adopt IoT devices and accelerate towards cloud only."

He adds: "A shared responsibility model of security has a key role to

"It is absolutely paramount that properly authenticated device identity is in-built into devices at the point of manufacture"

play here - cloud security requires a layered defence where businesses address each part of the stack of responsibility individually, yet they all interact together as a complete framework. From service providers to enterprises and individual users, everyone is accountable in some way, and with the shared responsibility model, businesses can ensure that everyone plays their part."

"A good way to illustrate this is to think about a family renting a car," he explains. "The manufacturer is responsible for the build quality and the airbags working, the rental company takes ownership of servicing and keeping the car roadworthy, while the driver is ultimately responsible for driving the car safely and carefully. Everyone does their bit."

Security by design

On IoT security by design, which has been promoted in the IoT industry for a number of years now, Altran's Ponvelil says: "IoT manufacturers - from product makers to semiconductor companies - should concentrate on building security in from the start, making hardware tamper-proof, ensuring secure upgrades, providing firmware updates/patches and performing dynamic testing. A focus should be on secure software development and secure integration. Hard-coded credentials should never be part of the design process. Organisations should require credentials to be updated by a user before the device functions."

He adds that public key infrastructure (PKI) and 509 digital certificates should play critical roles in providing the trust and control needed to secure data exchanges and verify identity.

Alan Grau, vice president of IoT/embedded solutions at **Sectigo**, said: "It is absolutely paramount that properly authenticated device identity is in-built into devices at the point of manufacture. In the absence of a clear legislative agenda, manufacturers have been able to churn out devices lacking authentication, with often only static credentials as a barrier for cybercriminals."

Grau says PKI needs to be in-built so it cannot be tampered with further along the supply chain by malicious actors. Only if the chipset is authenticated and protected by certificates from the foundry stage of manufacture, will it remain secure across the device lifecycle, he says.

Basic security design guidelines for manufacturers, developers, integrators and users have recently been published by both the US National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI), and are seen as a big advancement in promoting security by design.

The NIST guidelines are the NIST IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A) and the ETSI effort is ETSI European Standard (EN) 303 645.

The IoT Security Foundation, which is a global non-profit supported by the likes of **Samsung**, **Huawei**, **Vodafone**, **BT**, **Centrica** and **Arm**, has also published useful guidelines such as its Secure Design Best Practice Guides and the IoT Security Compliance Framework.

"Protecting access to and from devices is an important part of ensuring the overall operational integrity of the connected environment"

IoT security best practice

Arthur Fontaine, solution manager at **RSA Security**, says he has five rules for best practice:

1) Identification: "You should make sure that each individual endpoint can be discovered, identified and classified," he says. Security teams need to be able to see which endpoints are present at an IP address and then detect specific information about the device, such as where it was manufactured, its model and serial number and what version of firmware it runs.

"This can be achieved with modern edge platforms like the EdgeX Foundry, an open-source project hosted by the Linux Foundation," he says.

2) Conduct a thorough risk assessment: "It is not enough to simply get an IoT deployment up and running and then forget about it," says Fontaine. Risk assessments should be carried out continuously. The risk profile of IoT deployments changes over time, affected by activities such as adding and removing devices, changes to access policies, the discovery of new vulnerabilities and firmware and software updates applied to devices.

Third-party risks may also arise if IoT data needs to be shared between the enterprise and external service providers.

3) Make sure the integrity of data is protected. "Sensitive data such as production information or customer records is often processed via IoT devices," he says. This data is subject to the same privacy controls as other data but may be overlooked or even completely isolated from control systems, causing significant risk for organisations.

4) Understand who is accessing the devices. "Protecting access to and from devices is an important part of ensuring the overall operational integrity of the connected environment," said Fontaine. Businesses should authenticate all users to ensure they are who they say they are, can only access what they're allowed to, and that their credentials have not been compromised. Emerging standards such as FIDO IoT can be helpful in creating the appropriate IoT identity foundation.

5) Combine monitoring with access policies. Fontaine says: "The magnitude of IoT deployments is often an Achilles heel when it comes to security and risk, but this scale does offer one advantage – an abundance of operational data and use data about the devices." With this data, security teams can apply analytics and machine learning techniques to profile devices, baseline their normal behaviour, and detect and alert on anomalous activities.

It's clear that IoT is getting serious about security but approaches remain immature in contrast to the well-established security practices of mainstream IT. The risks are different in IoT and this is starting to be reflected in the solutions and approaches that are coming to market. These will accelerate over the coming years and IoT security will start to resemble the wild west less.

How to map out a wild west response to the threat of IoT security

To introduce our report on the evolving IoT security challenge, IoT Now's Antony Savvas spoke to Giuseppe Surace, chief product and marketing officer at Eurotech Group, a growing player in the IoT security market

The international company is headquartered in Italy and designs, develops and supplies edge computing and Internet of Things (IoT) solutions, including hardware, software and services. The most common customers of **Eurotech** are system integrators and enterprises, who want access to IoT building blocks that support edge gateways, high performance edge computers (HPEC) and artificial intelligence (AI) applications for the Industrial Internet of Things (IIoT).

With data security a leading factor in successful IoT deployment, Surace told IoT Now: "In the ecosystem in which we operate, to achieve IoT security we need to establish solid solutions for device discovery with secure identity, authentication and encrypted communications. Without this, the underlining protocols are increasingly subject to abuse."

With the proliferation of devices that already connect to our networks, says Surace, along with the take up of cloud and big data analytics, cyber-attacks have "blossomed in volume" along with their sophistication. That's confirmed by security vendor **SonicWall**, which reports that IoT malware attacks are currently up 50% year-on-year (see the following report). Organisations are also operating in borderless network environments making it increasingly more difficult to protect sensitive data.

Surace says: "The global Internet of Things security market value is growing at a compound annual growth rate (CAGR) of about 24% (see report), which is maybe not surprising considering the rising security concerns for critical infrastructure, increasing ransomware attacks on IoT devices and growing IoT security regulations."

Welcome to the wild west

He says: "One of the problems we face with the growth of IoT is the speed at which connected devices are being developed with a general lack of security standards or protocols. It's the new wild west for technology – and hackers are already loving it. Security pundits are predicting disastrous security results beyond what we are already experiencing in the market today."

He adds: "The following famous sentence is self-explanatory: "You call it 'Internet of Things; I call it Internet of Threats," - Eugene Kaspersky." ▶

Organisations are also operating in borderless network environments making it increasingly more difficult to protect sensitive data

Giuseppe Surace
Eurotech

Security mechanisms in the cloud ensure that authorised traffic is secure and authenticated and firewalls are used so all ports are secure – encrypted and authenticated.

Common IoT security mistakes:

- **Use of hardware and software without built-in security features to prevent root access**
- **Transmission of non-encrypted data**
- **Lack of tools to perform remote devices updates**
- **Hard-coded and inflexible credentials**
- **No integrity check of the software and OS installed on edge devices**
- **API tokens not encrypted**
- **No proper authentication and authorisation systems**

Best practice

"Best practices need to consider the specific aspects of distributed mobile systems and devices," says Surace. "We need a secure execution environment for all devices and the IoT integration platform, as well as secure software management distribution. Above all, connected devices and the IoT platform must have a validated identity."

To achieve this, companies must:

- **Build solutions based on open and industry standards**
- **Utilise proven security technology and partnerships**
- **Include security, scalability and resilience in the design from day one – security by design**
- **Identify each connected node and unique IDs and credentials**
- **Mutually authenticate nodes in the IoT infrastructure**
- **Encrypt all communication to protect data**
- **Implement controls for automatic revocation of certificates**
- **Digitally sign all communications over an encrypted channel**
- **Digitally sign software and configuration to ensure integrity and authenticity of systems**

www.eurotech.com

Device level security

Security mechanisms are an integral component of Eurotech's Everyware Software Framework (ESF) which are embedded in its IoT gateways. The ESF architecture is based on different software layers.

The OSGi (Open Services Gateway Initiative) layer provides a foundation for securely managing software components (signed bundles). And ESF ensures that strict Java and OSGi security policies are enforced at runtime, and verifies that only software signed by the approved authorities is installed and enabled.

The ESF Security layer encapsulates all the security features and it is supplemented by other measures like secure boot, appropriate hardware design and other measures, thereby ensuring proper protection of the solution at the edge. It also maintains a list of industry security guidelines to be followed when hardening a IoT device for a production deployment.

Secure communication

"Eurotech supports different protocols for secure communications, but we advocate the use of message queue telemetry transport (MQTT), which is a lightweight protocol optimised for IoT device communications," says Surace.

All MQTT traffic is originated from the gateway and encrypted over an SSL connection. Eurotech's systems also deliver all console access and REST API access over an encrypted HTTPS connection. And robust authentication is enabled by "strong, well-understood technologies" like X.509 certificates and encrypted credentials, Surace added.

Cloud security

Everyware Cloud, Eurotech's IoT integration platform unites the operational technology (OT) domain and the information technology (IT) domain, providing all the data, device and embedded application management required to deploy and maintain distributed intelligent systems in the field.

Security mechanisms in the cloud ensure that authorised traffic is secure and authenticated and firewalls are used so all ports are secure - encrypted and authenticated. In addition, device authentication uses strong username/password credentials or a per-device certificate. Each device can be automatically provisioned during first activation with a secure, randomised, device-specific password.

The device-level security, communication security and cloud security described here illustrate how Eurotech delivers security by design, says Surace.

Surace sums up what has to happen in the industry in the future: "Security for IoT needs to see everyone designing and deploying IoT devices, software and infrastructure that inspire confidence and which can be trusted. To do anything less will lead to market failure." ■

> ***The IoT ecosystem is composed of many standards, vendors using different hardware, software and third-party services and APIs***

An end-to-end approach to IoT security

The IoT ecosystem is composed of many standards, vendors using different hardware, software and third-party services and application programme interfaces (APIs). This huge fragmentation makes the ecosystem very vulnerable to all sorts of attacks, both at the edge and in the cloud. To achieve IoT security, we need to establish solid solutions for device discovery with secure identity, authentication and encrypted communications or the underline protocols are subject to abuse

The IoT ecosystem is composed of many standards, vendors using different hardware, software and third-party services and APIs. This huge fragmentation makes the ecosystem very vulnerable to all sorts of attacks, both at the edge and in the cloud.

Common mistakes when planning an IoT project

Often companies make important mistakes when planning IoT solutions, for example:

- Use of hardware and software without built-in security features to prevent root access
- Transmission of not encrypted data
- Lack of tools to perform devices updates (also remotely)
- Hard-coded credentials
- No integrity check of the software and OS installed on edge devices
- API tokens not encrypted
- No proper authentication and authorisation systems

To achieve IoT security, we need to establish solid solutions for device discovery with secure identity, authentication and encrypted communications or the underline protocols are subject to abuse.

IoT security best practices

Best practices need to consider the specific aspects of distributed mobile systems and devices. We need a secure execution environment for all devices and the IoT integration platform, as well as secure software man-agement distribution. Above all, connected devices and the IoT platform must have a validated identity. To achieve this, we must:

- Build solutions based on open and industry standard
- Utilise proven security technology and partnerships
- Include security, scalability and resilience in the design from day one
- Identify each connected node and unique ID and credentials ▶

- Mutually authenticate nodes in the IoT infrastructure
- Encrypt all communication to protect data
- Implement controls for automatic revocation of certificates
- Digitally sign all communications over an encrypted channel
- Digitally sign software and configuration to ensure integrity and authenticity of the systems
- Adopt Role-Based Access Control (RBAC)

Eurotech: security by design

As described earlier, IoT security must be designed from day one. The architecture of an IoT solution can be divided into three layers.

Device-level security

Security mechanisms are an integral component of the Everyware Software Framework (ESF), which in turn is embedded in the IoT Gateway.

The ESF architecture is based on different software layers. The OSGi (Open Services Gateway Initiative) layer provides a good foundation for securely man aging software components (signed bundles). ESF ensures that strict Java and OSGi security policies are enforced at runtime and verifies that only software signed by the approved authorities is installed and enabled.

The ESF Security layer encapsulates all the security features and it is supplemented by other measures like secure boot, appropriate hardware design and other measures, thereby ensuring proper protection of the solution on the Edge.

Moreover, maintains a list of security guidelines to be followed when hardening an IoT device for a production deployment. The guidelines are compiled following the recommendation of Industry Standards such the Center of Internet Security (CIS) and the IEC 62443.

Secure communication

Eurotech supports different protocols, but we advocate the use of message queue telemetry transport (MQTT), which is a lightweight protocol optmised for IoT device communications:

- All MQTT traffic is originated from the gateway and encrypted over an SSL connection
- All console accesses are exclusively available over an encrypted HTTPS connection
- All REST API accesses are exclusively available over an encrypted HTTPS connection
- Robust authentication is enabled by strong, well-understood tech-nologies like X.509 Certificates and encrypted credentials
- Device management messages published by the IoT platform are signed to guarantee authenticity and message integrity

IoT cloud security

Everyware Cloud unites the operational technology (OT) domain and the information technology (IT) domain, which means that it is the single, most important interface. A success attack would enable access to the enterprise environment. Everyware Cloud also functions as an M2M/IoT integration platform that acts like an operating system for the infrastructure.

On the operational technology side it provides all the data, device and embedded application management required to deploy and maintain distributed intelligent systems in the field.

- Security mechanisms in the cloud ensure that authorised traffic is secure and authenticated
- It employs firewalls, so all in-bound ports other than broker ports are closed and secure (encrypted and authenticated)
- Device authentication uses strong username/password credentials or a per device certificate
- Security mechanisms in the cloud ensure that authorised traffic is secure and authenticated
- It employs firewalls, so all in-bound ports other than broker ports are closed and secure (encrypted and authenticated)
- Device authentication uses strong username/password credentials or a per-device certificate
- Each device can be automatically provisioned during first activation with a secure, randomised, device-specific password. In addition, the device credentials can be strongly tied to a specific device so the IoT Integration Platform will refuse authentication requests with the same credentials from a different device.
- The device authorisation policy can further restrict the device data communication limiting the MQTT topics that the device can publish to and blocking device to device communication.
- Access control is centralised and authenticated via HTTPS/SSL
- Role-based access control is employed as well as user management and roles and permissions. A strict segregation of tenants down to a data level is another important element ensuring that other parties cannot access data and infrastructure.
- Logins to Everyware Console can be further protected using a Two Factor Authentication (2FA) ■

Best practices need to consider the specific aspects of distributed mobile systems and devices

www.eurotech.com