Ensuring your IoT is secure

A provider's guide

IoT Alliance Australia

Proudly delivered via the generous funding of Accenture.

Taking responsibility for your users' IoT security, safety and privacy.

Foreword

A handy IoT security reference guide written for IoT providers ~ developers, manufacturers, suppliers, vendors and distributors of IoT products and services.

Welcome to the Internet of Things Provider's Security Awareness Guide. This guide provides tips and techniques for you to ensure your IoT products and services inherently deliver good practice security, safety and privacy to your clients.

For most of us, the internet has opened up new opportunities. We can shop, bank, research, work and connect when and where we want to. Unfortunately the online world also gives criminals opportunities to steal money, information or identities; we need to ensure our online environments and devices protect our safety and privacy. This is achieved by embedding security into IoT products and services.

So how do we reduce the risk of falling victim? The Internet of Things Alliance Australia (IoTAA) provides this information and service to help you ensure integration of good security practice in your business and your IoT products and services, helping your users stay safe when considering procuring devices that connect to the internet at their homes and workplaces. Protecting them properly means being aware and taking responsibility for your IoT products and base configuration.

Cyber security claims are becoming a requirement more often than not. This IoT Provider's Security Awareness Guide assists you to ensure those claims are met and any queries from users can be adequately addressed.

This guide has been delivered through the financial support of Accenture. The IoTAA would like to thank them for their generosity.

We hope you will find this guide useful and welcome any feedback you may have.

Matt Tett
Chair
IoTAA WSe3 – Cyber Security & Network Resilience

Security, safety & privacy

Security, safety & privacy

Producing IoT devices and systems is an exciting activity, however protecting an IoT product's security and your users' safety and privacy requires consideration. IoT devices are vulnerable to similar cyber-attacks that affect communications and computer systems. ICT security is reactive, IoT security needs to be embedded and proactive. It must be considered from the initial product design and underpin safety and privacy.

IoT Product Security is critical to User Safety & Privacy

Due to its pervasive nature in our day-to-day lives, vulnerable IoT introduces the additional risk of safety to human lives and wellbeing. IoT security needs to be incorporated by design, not added to products afterwards, to provide a secure platform for the delivery of safety. The increase in data results in more complexity to ensure privacy.

Security flaws in most computer systems are patched via regular updates. However, legacy IoT devices may not have been designed with the ability to easily, or automatically, patch their software, meaning that security vulnerabilities are going unaddressed. Users may also forget what IoT products they have connected to their networks and therefore not maintain their security leaving them open for attackers.

IoT devices generally have longer lives than other technologies, introducing a risk that the product will continue to live long after the provider's intended lifecycle where they discontinue support. These factors must be addressed when designing IoT device security.

- Know the IoT ecosystem your product is intended for – Map this using the IoT Reference Framework, and keep it up-to-date, enabling you to identify risks to users' safety and privacy.
- Be aware of the balance between IoT security, safety and privacy; each will take on different importance depending on the sector in which your product is deployed. Mapping identifies sectoral risks, compliance and regulatory requirements.

References: IoT Reference Framework Overview;
https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

State clear security claims

IoT providers are increasingly becoming aware of the risks to users' safety and privacy and are building products with good security, safety and privacy by design principles. A key to this for IoT device and service providers is to make clear security claims about their products. The IoT Security Trust Mark certification and labelling scheme exists for IoT providers to have their security claims independently validated and ensure their IoT products comply with baseline requirements related to global IoT security accepted good practice and derived from published recommendations, codes and standards.

IoT users save time and money, buying secure

There are a number of IoT associations, government departments/agencies and standards bodies globally who have produced recommendations, codes and standards that seek to ensure minimum levels of recommended security exist in IoT products.

IoT providers should be aware of these, and seek to produce products that follow them.

What to ensure when producing IoT products?

- Become familiar with the IoT security standards, recommendations and codes (covered later in this guide).
- Produce clear security claims about your IoT product.
- At a minimum;
  Ensure there are no default universal passwords.
  Ensure that software can be kept updated.
  Ensure you have a vulnerability disclosure program.
- Put your product through the IoT Security Trust Mark certification process. This will provide your organisation and your users with assurance that your product independently meets security claims and baseline requirements under the standards, recommendations and codes.

Further reading: IoT Security Trust Mark Certification & Labelling Scheme. www.iotsecuritytrustmark.com

Secure your business

IoT providers must lead by example, implementing good security practice in their products and services, but also in their own business, led from the top of the organisation down.

Ensuring good practices are in place assists the enterprise to identify risks and employ mitigation strategies, minimising loss and reputational damage should a breach occur.

The principles contained in ISO/IEC 27001 information security management standard are a very good starting place for structured organisational security policies and procedures:

- "Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis."[1]

What steps can you take to keep your business cyber-secure?

- Protect your networks, devices and accounts with strong passphrases.
- Never use the same passphrase across networks, devices or accounts.
- Seek vendors who offer multifactor authentication on products and enable it.
- Use a Virtual Private Network to connect remote devices to a work network.
- Control and limit who can access networks and devices to staff and verified parties.
- Ensure each user in your business has separate login accounts and credentials and logs out when not present.
- Install and update anti-malware software.
- Ensure all smartphones and similar devices are locked with PINs.
- Backup regularly, and keep the backup isolated from the network.

[1] https://en.wikipedia.org/wiki/ISO/IEC_27001

Embed security by design

Embed security by design

Security considerations must be applied from the very beginning of IoT product and service development ensuring safety and privacy are underpinned by a strong security foundation.

Actions to consider when embedding security by design

- Identify, review and adopt the applicable security standards and protocols for different technical components and regulatory compliance requirements for intended industry sectors and jurisdictions.
- Perform risk and threat analysis involving security experts at early stages of the device design process to discover the security features required. Document security claims.
- Security by design to follow system development lifecycle at each stage of producing smart devices, include effective (and ongoing) measurements and audits to demonstrate security maturity. Do not limit this just to the devices themselves, also include any sensors, application user interfaces and corresponding delivery of software/firmware patches.
- Defence in depth is a good mantra to follow – all layers, from physical to data layers.
- Strong IoT device and user identification through secure authentication and authorisation mechanisms, along with hashing and encryption incorporating access control lists for valid software/firmware updates.
- Implementing Network Layer Security with clear device guidelines for network setup configurations like network segmentation and perimeter firewall settings.
- Store sensitive application secrets in a secure storage medium.
- Address the secure transmission of information; for example, end points and network "hopping" points also.
- Design for encryption in data generation, transit, processing, storage, and display.

Additional reading; IoT Security Foundation Secure Design Best Practice Guides
https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

Implement good safety by design practices

Implementing good Safety by Design (SbD) principles is critical to the safety of IoT users.

"SbD is about taking a proactive approach to user safety, embedding a 'culture of safety' into product/service design, development and release. It encourages organisations to understand, and work to minimise, potential risks and to consider user safety at every stage. By including tools that empower users and designing services that do not enable, inflame or encourage illegal or harmful activity, organisations can build long-term trust and address regulatory, revenue and reputational risks."[2]

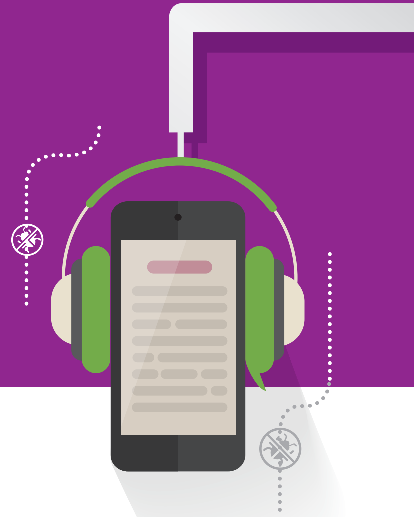
Actions to consider when embedding Safety by Design

- Nominate individuals, or teams accountable for user safety policy creation, evaluation, implementation and operations.
- Develop community standards, terms of service and moderation procedures that are fair and consistently implemented.
- Implement infrastructure that supports triaging, clear escalation paths and reporting on all user-safety concerns, alongside readily accessible mechanisms for users to flag and report concerns and violations at the point that they occur.
- Ensure there are clear internal protocols for engaging with law enforcement, support services and illegal content hotlines.
- Put processes in place to detect, surface, flag and remove illegal and harmful conduct, contact and content with the aim of preventing harms before they occur.
- Document risk management and impact assessments to assess and remediate any potential safety harms that could be enabled or facilitated by the product or service.
- Implement social contracts at the point of registration. These outline the duties and responsibilities of the service, user and third parties for the safety of all users.

[2] https://www.esafety.gov.au/about-us/safety-by-design

Embrace privacy by design

Embrace privacy by design



Privacy considerations must be applied from the very beginning of IoT product and service development and build upon a strong security foundation, including measures that are related to the privacy and protection of personal data.

These measures should be applied from the first stages of product development.

- Address privacy related issues based on applicable local and international regulations, such as privacy acts and privacy principles.
- Define the scope and objective for data processing by the IoT product, or service, during the design phase; avoid unnecessary provision or collection of sensitive data.
- Ensure personally identifiable information collected is used in fair and lawful ways.
- Establish a secure location for data storage and define data transfer guidelines between any organisations with restricted access of personal data limited to authorised individuals and include auditable access logs.
- Only use unique identifiers for devices, and individuals, for access to only carry out their functions efficiently and never use another organisations' unique identifiers.
- Separate data that can be used to identify an individual from other information and ensure it is secure at all times; for example, through the encryption of any personal data transferred within the IoT environment.
- A compliance function within the organisation should ensure that all existing, and new, systems comply with regulatory requirements.
- Transmit, store and retrieve personal information in line with good record keeping standards and security measures.
- Treat personal information as legislated and obtain individual's consent if transferring/sharing, the data.

Further reading; IoTAA Good Data Practice Guide: https://www.iot.org.au/wp/wp-content/uploads/2016/12/Good-Data-Practice-A-Guide-for-B2C-IoT-Services-for-Australia-Nov-2017.pdf

Third party security evaluations

Third party security evaluations and securing the supply chain

Security researchers are experts in their field, identifying weaknesses, before criminals do and enabling remediation. Ethical hacking and bug bounty programs deliver additional insight to your IoT products, services and organisation from a third-party perspective.

Consideration needs to be given to ensuring the suppliers to your organisation uphold the same security, safety and privacy practices that you do – this leads to robust, resilient, trustworthy supply chains. Attackers will target the weakest link in the chain and use that position to leverage their access to obtain access to the information of value to them.

Set the example and ask all suppliers in your chain to be accountable for good security practice.

- Identify and manage suppliers across the solution throughout the entire lifecycle.
- Perform due diligence on suppliers ensuring adequate security standards are implemented and being followed by actively participating in their security assessments and that the delivery of regular compliance audits and reports.
- There should be clear documentation on security, safety and privacy requirements, particularly technical specifications during tendering or procurement processes.
- Define the security and privacy requirements of any partnership with suppliers within the relevant agreements and contracts.
- Strictly control access of third parties to control or production layers. Avoid direct connection and only grant access to vetted and authorised individuals on demand, within a specified time window, for a specific purpose, and in the least privileged way.
- Define, plan and control third party access to the necessary selected functions, data entities and segments of any network.
- Ensure that security operational procedures are in place and abide to legal and government compliance rules and regulations.

Further reading; Bugcrowd, Crowd sourced bug bounty program. https://www.bugcrowd.com

IoT Security codes and standards

IoT Security codes, recommendations, and standards

There are a number of published IoT security codes of practice, recommendations, guidelines and standards that require consideration by IoT providers

Actions to consider;

- Define the end-of-life term and policy and provide to the user at time of purchase.
- Design and implement products to avoid duplicated default or weak passwords, no default administration credential or password.
- Plan for secure and automated software updates without disrupting functionality.
- Design and deliver the functionality of secure storage of credentials, certificates, keys and secrets. Avoid hard coding these, (i.e. administration access credentials).
- Implement authentication and access privileges that can be easily set up by users.
- Provide privileges for the user to disable unused features and ports on IoT products.
- Ensure capabilities are in place for data encryption from the source to the destination.
- Validate consistency and authenticity of data as it is delivered.
- Empower the user with audit privileges, (i.e. system, network and user logs).
- Provide the user with guidelines or steps to understand, report or resolve issues for any unprecedented incidents starting from situational awareness, problem confirmation, severity of the issue, and to isolate/rectify and eradicate the problem.
- IoT products should be designed to fail safe and secure, not fail open.

Further reading: ENISA Baseline Security Recommendations for IoT
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
ETSI EN 303 645 v2 Cyber Security for IoT: Baseline Requirements
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
NIST NISTIR 8259 Foundational Cyber Security Activities for IoT Device Manufacturers
https://csrc.nist.gov/publications/detail/nistir/8259/final

Codes of Practice for Consumer IoT Security
UK Government: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/77386/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
Australian Government: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

IoTA

IoT Alliance Australia

IoT Security Statistics

$$$

$520 billion

the combined IoT market size in 2021. Comprising a lot of valuable data that is attractive to attackers.

26·6 billion

active IoT devices August 2019. With 127 new IoT devices connecting to the web every second.

98%

of IoT device traffic is unencrypted due to the lack of IoT providers understanding of how to include such security by design.

Reference: https://leftronic.com/internet-of-things-statistics/

IoT Security Awareness Guide
Types of IoT Attacks

Eavesdropping

Unsecure or unencrypted IoT communication channels (e.g. from device to gateways/platform) network can be intercepted and information such as user names, passwords and configuration settings can be captured. Related attacks include man-in-the-middle, session hijacking, or message replay.

Privacy threats / data leakage

Confidential / sensitive data from devices may be captured by hackers during device communications, and disclosed intentionally or unintentionally. This could happen through back door access, and or by MITM attack.

Lack of authentication

IoT devices and system may lack an authentication mechanism and can not verify the authenticity of the SW or FW when updates are being made. An attacker can exploit this vulnerability, and can upload a malicious software package to the device.

Insecure network

Attackers exploit open and insecure network services (Shodan search engine shows HTTP, Telnet, SSH) and turn IoT devices into bots for DDOS attack (e.g., Mirai).

Malware

IoT devices can be infected with malware (virus, worm, trojan, etc.) designed to carry out unauthorised actions that could compromise the operation and integrity of the IoT system. The consequence could be data leakage, device hostage, DDOS attack, etc.

Firmware hijacking

Legitimate firmware could be hijacked when the owner of the IoT device tries to download firmware updates, believing the firmware comes from a legitimate source.

Ransomware

It is not unthinkable that ransomware hackers would naturally move on from encrypting files on computers to locking up smart devices, including industrial IoT devices, and demand a ransom to unlock them.

Machine phishing

Hackers could infiltrate IoT devices and command them to send fake signals that will cause the owners to take actions that could damage the operational network.

Trojan horse

Unsecured IoT devices are Trojan horses themselves. Once infected with malware, they can steal data, spy on people, elevate control functions, perform DDOS attack, and so on.

Cryptojacker

Cryptojacking malware is an emerging online threat that hides on a device and uses the machine's resources to "mine" forms of cryptocurrency, such as bitcoin. Cryptojacking causes high CPU and network usage and drains critical healthcare systems, potentially impacting life-saving capabilities.

Backdoor

Attackers gain access to endpoint devices and/ or system via backdoors such as hardware and software ports, including usb, cellular wireless access, etc. These ports are often used for device configuration and support purposes, but often left unmanaged, or forgotten.

Lack of encryption

An attacker can capture sensitive data if data is transmitted in clear text, i.e., without transport encryption.

Brute-force password attacks

Most (consumer) IoT devices have weak, or guessable default passwords, and brute-force attacks can be effectively used to gain access to the device.

Eavesdropping man-in-the-middle

An eavesdropping or man-in-the-middle attacker might be able to intercept network traffic and steal the sensitive information that IoT devices transmit over the communications channel.

Insecure ecosystem interfaces

Insecure web interfaces leave IoT management systems vulnerable to attacks such as SQL injection, cross-site scripting and cross-site request forgery.

Zombie/Botnet

IoT devices could be hijacked / and turned into botnets in large numbers for conducting DDOS attacks. They can cause chaos and denial of legitimate web servers of their services.

Waterhole / sinkhole

Sinkhole is a type of attack that creates a metaphorical sinkhole in a wireless sensor network node, that compromises the confidentiality of the IoT data and also denies any service to the sensor network. This is done by dropping packets instead of sending them to their destination.

Default settings

Unused SW/HW ports not disabled, and username and password left as default setting.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Internet of Things Supply Side Security Awareness Guide

IoT Alliance Australia

Disclaimer

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. This information has been prepared by Enex TestLab for the Internet of Things Alliance Australia (IoTAA).

Enex TestLab accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

ISBN: 978-0-9953944-4-5

Attribution

Use of all or part of this guide must include the following attribution: Enex TestLab 2020.

Ensuring your IoT is secure

A provider's guide

IoT Alliance Australia