Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

IoT secure-by-design guidance for manufacturers

First published: September 2020
Last updated: September 2023

Introduction

Malicious actors regularly target Australian Government data in an attempt to gain an economic or strategic advantage. As such, Internet of Things (IoT) devices, such as drones, security cameras, smart televisions, solar inverters and other 'smart' devices should have effective cybersecurity measures in place to defend against these threats.

This guidance has been produced for manufacturers in order to help them implement the thirteen secure-by-design principles from Australia's *AS ETSI EN 303 645* standard on cybersecurity for consumer IoT devices. In doing so, this guidance focuses on devices, not their associated backend servers. Associated backend servers should instead follow their own better practice security guidance.

The thirteen secure-by-design principles are:

- No duplicated default or weak passwords
- Implement a vulnerability disclosure policy
- Keep software securely updated
- Securely store credentials
- Ensure that personal data is protected
- Minimise exposed attack surfaces
- Ensure communication security
- Ensure software integrity
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

The thirteen secure-by-design principles

No duplicated default or weak passwords

Examples of good implementations

- Devices have a long, unique, unpredictable and complex password for setup and access. Where this isn't possible, devices prompt users to change the password during setup.

- Where users are prompted to set a password for devices or associated accounts, users are required to choose a password of at least the minimum length and complexity as specified within the *Information security manual*.
- All online accounts associated with devices use WebAuthn or multi-factor authentication.
- The Wi-Fi access point hosted by devices, and used for setup, requires users to authenticate.

Examples of bad implementations

- Devices have a weak default password that is unable to be changed.
- Devices share a common default password.
- Devices disclose their password by simply interacting with it them.

Implement a vulnerability disclosure policy

Examples of good implementations

- A clear and detailed vulnerability disclosure policy is available on manufacturers' websites.
- A point of contact specifically for reporting vulnerabilities is clearly identified by manufacturers.
- A security.txt file is hosted on manufacturers' websites to assist security researchers in locating vulnerability disclosure policies and points of contact for reporting vulnerabilities.
- Manufacturers have a bug bounty program to encourage people to report vulnerabilities.
- Vulnerabilities that are reported are acknowledged by manufacturers in a timely manner.
- Manufacturers have an appropriate timeframe for developing and distributing updates once vulnerabilities are identified.
- Manufacturers provide interim mitigation advice if a resolution for a vulnerability requires extensive engineering.
- Manufacturers conduct root cause analysis for reported vulnerabilities to determine if similar vulnerabilities could be prevented in the future.

Examples of bad implementations

- Manufacturers fail to acknowledge or remedy vulnerabilities reported in good faith.
- Manufacturers use lawyers to silence or prosecute people who report vulnerabilities in good faith.
- Manufacturers use non-disclosure agreements to supress information on vulnerabilities reported as part of bug bounty programs.

Keep software securely updated

Examples of good implementations

- Manufacturers provide updates for devices and any associated mobile applications.
- Devices check for updates daily.
- Manufacturers notify users of when updates will be applied and what they contain, such as via a change log.
- Manufacturers digitally sign updates.
- Manufacturers provide updates over secure communication protocols.
- Devices validate updates through cryptographically-secure mechanisms prior to their installation.
- Manufacturers prioritise remediating design weaknesses and vulnerabilities over introducing new features.
- Manufacturers maintain a software bill of materials for devices, and any associated mobile applications, and ensure all components are kept up-to-date.
- An end-of-life policy for devices is established and made available to users when devices are released.

Examples of bad implementations

- Devices, or any associated mobile applications, have vulnerabilities that manufacturers have claimed to have patched but are still present following an update.
- Users are required to pay a subscription fee for updates that remediate vulnerabilities.
- Updates makes changes to devices, or any associated mobile applications, that remove, reduce or break functionality making users hesitant to apply future updates.

Securely store credentials

Examples of good implementations

- Passwords stored on devices are encrypted using algorithms as specified within the *Information security manual*.
- All passwords and sensitive data exchanged during device setup are done so using cryptographically-secure mechanisms.

Examples of bad implementations

- Devices have hardcoded passwords that are contained within firmware and are common across devices.
- Devices have obfuscated (e.g. Base64 encoded) passwords that are stored in configuration settings or firmware rather than being encrypted using cryptographic algorithms.
- Devices store, share or extract passwords for Wi-Fi networks without suitable encryption or user interaction.
- Private key material is reused between multiple devices.

Ensure that personal data is protected

Examples of good implementations

- Manufacturers have a privacy policy that clearly describes the extent of personal data collected, how it will be used, how long it will be kept and how it will be protected.
- Only personal data that is absolutely necessary to operate devices is collected.
- Personally data is retained only for as long as absolutely necessary to operate devices.
- Encryption, as specified within the *Information security manual*, is used to protect personal data in transit and at rest, including that handled by any associated mobile applications.
- Metadata, and content associated with personal data, is encrypted.
- Manufacturers comply with relevant regulatory and statutory requirements (e.g. the *Australian Privacy Principles* and *Australian Consumer Law*).

Examples of bad implementations

- Users are required to provide non-essential personal data simply to use, or continue using, devices.
- Personal data is transmitted in cleartext.
- Manufacturers' privacy policies contradict elements of the *Australian Privacy Principles*.
- Manufacturers' terms and conditions contradict elements of *Australian Consumer Law*.
- Users are encouraged to connect with third parties for the purpose of sharing personal data without first being informed of the privacy and security implications of doing so.

Minimise exposed attack surfaces

Examples of good implementations

- A secure software development process that considers cyber supply chain security is used by manufacturers.
- Devices, and any associated mobile applications, are secure by design.
- Devices (where possible), and any associated mobile applications, use memory-safe programming languages.
- Devices, and any associated mobile applications, are secure by default.
- Devices, and any associated mobile applications, undergo regularly security testing.
- During device setup, devices only open required physical interfaces and network ports.
- After device setup, physical interfaces and network ports that were only required for device setup are closed.
- Physical interfaces and network ports are only exposed when users have configured such functionality.

- Web management interfaces are only accessible to local networks unless devices need to be managed remotely via the internet.
- Manufacturing and debug interfaces (e.g. JTAG and UART) are disabled by default on production hardware.
- Backups of configuration data are only available after authentication.

Examples of bad implementations

- Memory-safe programming languages are not used for any associated mobile applications.
- Devices are provided in an insecure state, such as to maximise functionality, with users being required to harden the configuration settings for devices themselves.
- Devices, including any associated mobile applications and their updates, do not undergo static and dynamic security testing before being released into production.
- Devices have unused network ports that are open and listening for connections after device setup.
- Bluetooth pairing stays active once devices have been setup despite no longer being used for any device functionality.
- Devices expose unencrypted protocols (e.g. Telnet) which are used to exchange usernames and passwords that provide access to devices.
- Devices have unused physical interfaces (e.g. USB ports) available to interact with.

Ensure communication security

Examples of good implementations

- Devices are either certified or qualified against the wireless communications standards they implement.
- Encryption, as specified within the *Information security manual*, is used to protect all data in transit.
- Logs detailing remote access to devices are kept and made freely available to users.

Examples of bad implementations

- Devices implement wireless communications standards in a non-standard or proprietary manner.
- Data communicated between devices, or between devices and any associated mobile applications, is sent in cleartext.
- Encoding, rather than encryption, is used to protect data in transit, such as usernames, passwords, authentication tokens and other forms of credentials.
- Wi-Fi network identifiers and passwords are sent in cleartext between devices and any associated mobile applications during setup.

Ensure software integrity

Examples of good implementations

- Manufacturers digitally sign updates.
- Manufacturers provide updates over secure communication protocols.
- Devices validate updates through cryptographically-secure mechanisms prior to their installation.
- Manufacturers include plugins and extensions for devices within the scope of their security testing.
- Devices only allow the use of signed plugins and extensions.
- Plugins and extensions only communicate with online resources using secure mechanisms that confirm the integrity of remote resources.

Make systems resilient to outages

Examples of good implementations

- Users are notified of devices going offline when network connectivity is lost.
- Devices reconnect to networks automatically following the loss of network connectivity and notify users once reconnected.
- Devices powered on prior to an unexpected loss of power automatically power on to their prior state, or a safe state, with the resumption of power.
- Battery backups are provided for relevant devices and activate on loss of power.
- Alternative secure communication mechanisms (e.g. Bluetooth) are provided in the event of loss of network connectivity.
- Devices maintain essential functionality when network connectivity is lost.

Monitor system telemetry data

Examples of good implementations

- Users are informed of whether diagnostic and telemetry data is collected from devices.
- Only diagnostic and telemetry data that is absolutely necessary to operate devices is collected.
- Users are required to opt-in to providing non-essential diagnostic and telemetry data related to the usage of devices.
- Diagnostic and telemetry data collected from devices is only used to improve device functionality, integrity or security.

Examples of bad implementations

- Diagnostic and telemetry data collected from devices is used for marketing purposes or selling additional subscription services to users.

Make it easy for consumers to delete personal data

Examples of good implementations

- Users can easily delete their personal data, at no cost, from both their devices and any associated online accounts.
- Processes for deleting personal data are clearly explained on manufacturers' websites.
- Devices have a user-friendly factory reset process that is clearly outlined in manuals, is easy to follow and includes the full removal of personal data and device configurations.
- Manufacturers allow users to delete single pieces of personal data while maintaining other personal data.
- All personal data is securely deleted upon removal of accounts.
- All device configuration data is securely deleted at the request of users.
- Confirmation of the deletion of personal data and device configurations from devices and any associated online accounts is provided.

Examples of bad implementations

- The only way to delete personal data is through ageing (i.e. waiting for a defined storage period to elapse).
- Users' personal data is maintained on devices even after users attempt to delete it, and subsequently believe it has been deleted.
- Users are required to contact manufacturers in order to delete personal data or device configuration data.

Make installation and maintenance of devices easy

Examples of good implementations

- Device documentation clearly describes how to install and configure devices using an easy to follow step-by-step process.
- Web management interfaces for configuring devices are easy for users to comprehend and navigate.
- Manufacturers explain how to check devices, and any associated mobile applications, are up-to-date (and apply updates as necessary) through short videos or interactive demos.
- Manufacturers explain how to use devices, and any associated mobile applications, through short videos or interactive demos.
- Device documentation clearly matches the actual user experience with devices.

- Where continuous battery operation is expected, devices notify users when batteries are running low.

Examples of bad implementations

- Device installation, configuration or updates cause issues that require a device factory reset to remedy them.
- Devices that experience issues when restarting during setup or update activities fail to notify users of such issues.
- Maintaining devices requires substantial investment in user training or education that does not align with the intended users or usage of devices.

Validate input data

Examples of good implementations

- Input of data by users requires authentication.
- Invalid and non-authorised input of data is rejected.
- Best practice advice is followed to reduce the attack surface of strings designed to encode or carry content beyond expected user input (e.g. rejects special characters, escape characters, non-ASCII or Unicode).
- Devices, and any associated mobile applications, defend themselves against common exploitation techniques, such as SQL injection.
- Both client-side validation and server-side validation are performed.

Example of bad implementations

- Devices, or any associated mobile applications, crash or become inoperable due to unexpected input.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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.

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

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate