Consumer IoT Security Quick Guide:

SOFTWARE UPDATES

IoT Security Foundation

Keep Software Updated

New standards and regulation

Forty percent of consumers believe that keeping IoT products' firmware up to date is the responsibility of the software developer or device manager.[1] Now, new standards and upcoming regulations require IoT manufacturers, and some importers, to publish how long they will supply software updates (the product support period) in a clear and transparent way (e.g. on the outside of the box).

Standard ETSI EN 303 645[2] requires consumer IoT products to be able to support software updates. The UK Government's Code of Practice for Consumer IoT Security[3] and Australian Draft Code of Practice[4] set out similar requirements. Legislation in California[5] and Oregon[6] states require "reasonable security features". The UK government is preparing legislation which will require the product support period for security updates (i.e. the defined minimum length of time a manufacturer will provide updates) to be published in an accessible, clear and transparent way.[7]

Important security considerations

Software security updates are important because every IoT product is susceptible to vulnerabilities and will need to adapt to new security threats, vulerabilities or best practices. If security updates are not provided, the security of the product will diminish over time. The ability to update software is the major mechanism to resolve vulnerabilities or fix bugs in the product. Software update capabilities are also key to other IoT security best practices like coordinated vulnerability disclosure. See IoTSF's Quick Guide Manage Vulnerability Reports for more information.[8]

Additionally, software updates offer other benefits to the company. For example, features can be added to products after they leave the factory. This also allows for adapting to changes in the environment (such as third-party APIs), the evolution of business models, as well as enabling new functionalities and increasing the product lifespan.

Impact on consumer IoT manufacturers

Failure to comply with existing standards or regulation can result in significant reputational and financial damage to your company. Governments sometimes identify appropriate international standards, such as ETSI EN 303 645,[2] that companies can adopt to show compliance with regulation. A consumer IoT product which is not able to support updates or is not isolatable and replaceable will not be able to claim compliance with ESTI EN 303 645[2] and may have difficulty proving compliance with national legislation. Violation of forthcoming UK regulation will likely result in sanctions, such as fines or removal of products from the market.

Where to start?

Below are five key questions for managers to discuss among product development, security, and compliance teams which will help on the road to compliance with ESTI EN 303 645.[2]

- Does the product design support secure software updates?
- Do we have an update procedure?
- How do we securely install updates on our products?
- How long do we commit to providing security software updates for our product and where/how do we publish this information?
- Considering device components, how long can we provide software updates for?

Why it matters

- New security vulnerabilities are often discovered after product shipment.
- Not supporting security updates puts user safety, data, networks and devices at greater risk.
- Without updates, the product cannot evolve to respond to the changing security environment, and will become less secure.
- Security updates allow for vulnerabilities to be patched before public disclosure.
- Provisioning updates supports other best practices like coordinated vulnerability disclosure.
- Failure to comply with existing standards or regulation can result in reputational and financial damage.

Existing standards, regulation and guidance

- ETSI EN 303 645 Cyber Security for Consumer IoT (2020)[2]
- UK DCMS Code of Practice for Consumer IoT Security (2018)
- United States: California and Oregon state legislation
- Australia Draft Code of Practice: Securing the Internet of Things
- Upcoming UK Regulation for Consumer IoT Security (2021)

Dos and Don'ts: Guidance on complying with new standards and regulation

Dos

A guaranteed software update support period must be clear and transparent to customers at the time of purchase.

Have an update procedure in place

- The development team needs to be engaged in preparing for and rolling out updates.
- Updates should be available for automatic download and includes the ability to reset to older firmware if new features or updates do not work as intended.
- Automatic mechanisms should be used for software updates and enabled by default. If not, updates need to be easy to implement.
- When planning timelines to release updates, take into account relevant factors like criticality, vulnerabilities, necessity, and ease of fix.
- Consider factors that impact functionalities and the end user, such as length, timing, and reduced device capabilities for each update.
- Sometimes devices cannot be updated, for example if the device's communication capability is very constrained. Constrained devices that can't be updated are isolatable and hardware is replaceable. For example, until a product can be replaced, it must be quarantined from the internet.

Have communication channels with users in place

- You may need to communicate with users about the updates, for example if a security update is required and the risks mitigated by the update. Clear communications can help build user trust and confidence.
- Devices' basic functions should not be disrupted during the update process. If basic functions are disrupted or there are reduced capabilities the device should notify the user prior to rolling out updates.
- In most cases, users should have some control over when an update is installed. For example, when the product is not in use or performing critical functions.
- Configuration data should be restrained across an update.

Don'ts

- Do not provide updates that impact essential device functions or configurations. For example, a smart door lock must be able to manually lock/unlock during the update process.
- Do not offer consumer IoT products that cannot be updated unless they are isolatable and hardware is replaceable.
- Do not shorten the defined support period after purchase. Updates must be provided for the defined support period.

5 minutes -

average amount of time it takes for a newly connected IoT device to be attacked

Support secure updates

- The device should verify the authenticity and integrity of software updates.
- If the update is delivered over a network, verify the update via a trust relationship. Three examples from ESTI EN 303 645[2] are authenticated communication channels, digital signature based verification of the update, or confirmation by the user.
- Use industry best practices in cryptography to support secure updates.

Things to think about going forward

In addition to the basic dos and don'ts, here are a few more areas that need to be considered when supporting software updates.

- Build clear and timely communications channels with your supply chain about software updates.
- Consider how you might collect and use update telemetry. If you are collecting information , ensure that privacy is respected and your company complies with data protection regulations.
- Implement a plan to stage updates and stagger releases of updates to prevent everyone from updating, and potentially failing, at the same time.
- If problems with updates or features are reported, open a bug report and work to resolve the issue.
- Have mechanisms in place that would facilitate rollback of the updated if needed.

Where to go for more information?

From the IoT Security Foundation

- IoTSF Best Practice Guides[9]
- IoTSF consumer IoT security resources[7]
- IoT Security Compliance Framework, particularly section 2.4.5, Device Software[10]

From other bodies

- ENISA Good Practices for Security of IoT[11]
- US National Telecommunication and Information Administration (NTIA) Stakeholder-Drafted Documents on IoT Security[12]
- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers[13]

Who should see this:

It is critical that people with different roles and responsibilities are aware of software update standards and regulation, and how they impact the organization. Examples of who should see this include:

Product Manager: The software update mechanism is the primary mechanism that the product manager will have to stage their efforts.

Product Development Manager: Product development will have to implement the mechanism(s), but also will be users of the mechanism themselves as they test their code.

Supply Chain Manager: The supply chain manager can help identify who in the supply chain should be notified of software updates and help manage relations.

Software Release Team: This group will be creating the updates.

Head of Design: Software updates require planning throughout the device design lifetime; choices in hardware have profound effects on how easily they can be done.

Product security team: This team will be the primary user of the software update mechanism, and their needs must be accounted for in planning.

Compliance officer: Will be responsible for how the organization respects the principals in this guide and the code or practice and related quality assurance.

Head of Marketing: The hardware design choices affect the marginal cost of the product. A more expensive Bill of Materials (BOM) may be required to permit smooth upgrades. At the same time, this may open opportunities for improved functionality over time keep the same product in the market longer and reduce non-recurring engineering (NRE). Without updates there can be no useful response to disclosed vulnerabilities.

What are the Consumer IoT Security Quick Guides?

The "Consumer IoT Security Quick Guides" identify best practices to help organizations around the world understand and comply with new international standards, regulations and national guidance on consumer IoT security. These Quick Guides demystify high level language, point to additional information, and provide different ways of thinking about or alternative approaches to consumer IoT security.

The Quick Guides build upon the ETSI EN 303 645[2] specification on consumer IoT cybersecurity. It is the first international standard of its kind. Based upon it, governments are publishing Codes of Practice[14] and are preparing legislation[15] that impact companies developing, manufacturing or providing consumer IoT products. The Quick Guide series focuses on the top 3 issues identified in standards and guidance: passwords, vulnerability disclosure, and software updates.[3]

Footnotes

1. https://pages.ubuntu.com/IoT-Security-whitepaper.html
2. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
4. https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf
5. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
6. https://olis.leg.state.or.us/liz/2019R1/Measures/Overview/HB2395
7. The regulatory proposals are currently subject to a public call for views and might change as a result.
8. https://www.iotsecurityfoundation.org/consumer-iot
9. https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf
10. https://www.iotsecurityfoundation.org/wp-content/uploads/2020/05/IoTSF-IoT-Security-Compliance-Framework-Questionnaire-Release-2.1.zip
11. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
12. https://www.ntia.doc.gov/IoTSecurity
13. https://csrc.nist.gov/publications/detail/nistir/8259/final
14. For example, the UK and Australia
15. For example, US states Oregon and California, and the UK.

Acknowledgements

This guidance was commissioned by the Department for Digital, Culture, Media & Sport (DCMS) and delivered by the IoT Security foundation in partnership with Oxford Information Labs.

We wish to acknowledge significant contributions from IoTSF members to this version of the document

Stacie Hoffmann and Patrick Taylor, Oxford Information Labs
Michael Richardson, Sandelman Software Works

Peer reviewers:
Roger Shepherd, Chipless
Trevor Hall, DisplayLink
Richard Marshall, Xitex Ltd
Claire Milne, independent consultant

Plus others – you know who you are!

IoT Security Foundation

Department for Digital, Culture, Media & Sport

In partnership with OXFORD INFORMATION LABS