Online Trust Alliance

IoT Trust Framework – Resource Guide
Updated January 5, 2017

PURPOSE

This Guide is a companion to the OTA IoT Trust Framework (Framework), a set of required and recommended strategic principles necessary to help secure IOT devices and their data when shipped, and throughout their entire life-cycle. The Guide is designed to give added context, consideration and resources, providing developers and manufactures practical advice to help secure their devices and data and adopt responsible privacy practices. The purpose of the Guide is to aid in the adoption and implementation of the Framework and the Guide will evolve based on industry and academic research and evolving standards and best practices.

As the Framework is a summary of baseline requirements, it does not override regulatory requirements nor does adoption necessarily guarantee compliance with the law and/or regulations. The underlying recommendations are based on the Fair Information Practice Principles (FIPPs), building on security and privacy best practices advocated by the OTA, industry organizations and governmental agencies. [1, 2, 3] Readers are encouraged to review their practices against published guidance from regulatory agencies, standards bodies and industry associations to help ensure use of the most current practices including but not limited to the EU Privacy Shield and the General Data Protection Regulation (GDPR)[4].

BACKGROUND

The Internet of Things is transforming the way we live, work and communicate. IoT connected devices bring substantial benefits, yet as they proliferate, their security and privacy risks are amplified. Simultaneous compromise of a multitude of devices could cause disruption of critical infrastructure and services. Addressing mounting concerns, in January 2015 the Online Trust Alliance established the IoT Trustworthy Working Group (ITWG), a multi-stakeholder initiative. For purposes of this Guide, the term IoT refers to "things" such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Through a multi-stakeholder efforts including public call for comments, version 1.0 of the Framework was formally adopted and released in March 2016. Use of the Framework "in the field" through 2016 brought updates with version 2.0 released January 5, 2017.[5]

---

[1] FIPPs are the widely accepted framework of defining principles for evaluation of programs that affect individual privacy. They are mirrored in the laws of many U.S. states, many foreign nations and international organizations.

[2] Start With Security: A Guide for Business (lessons learned from FTC cases): https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

[3] OWASP Project: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[4] EU GDPR http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[5] OTA Releases v2.0 of Trust Framework https://otalliance.org/news-events/press-releases/coalition-embraces-iot-security-privacy-trust-framework

While members of the working group support the objectives of the Framework, individual contributors and their respective organization may not support every criteria. The ITWG acknowledges technical limitations of devices with embedded firmware, and that some requirements today may not be applicable to every product, or feasible based on current design parameters, but should be the basis for future product development. The ITWG recognizes that "security and privacy by design" must be a priority from the onset of product development and be addressed holistically. Devices and applications should be built with privacy and security protections that are commensurate with the risk posed to all parties including the end user.

INITIAL SCOPE AND INTENT

The initial scope of the Framework includes key criteria identified for connected home, work and wearable technologies including toys and fitness devices. The Framework outlines mandatory requirements including comprehensive disclosures which must be provided prior to product purchase articulating policies regarding data collection, usage and sharing, as well as the terms and condition of security patching post warranty. The Framework today serves as a voluntary code of conduct and as minimum baseline requirements for IoT certification programs. Its principles are grouped as follows:

- **Security Principles** (1-9) – Applicable to any device or sensor and all applications and back end cloud services. These range from the application of a rigorous software development security process to adhering to data security principles for data stored and transmitted by the device, to supply chain management, penetration testing and vulnerability reporting programs. Further principles outline requirements for life-cycle security patching.
- **User Access & Credentials** (10-14) – Requirement of encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password re-set processes and integration of mechanisms to help prevent "brute" force login attempts.
- **Privacy, Disclosures & Transparency** (15-30) – Requirements consistent with generally accepted privacy principles including prominent disclosures on packaging, point of sale and/or posted on line, capability for users to having the ability to reset devices to factory settings and compliance with applicable regulatory requirements including the EU GDPR and children's privacy regulations. Required disclosures include the impact to product features or functionality if connectivity is disabled.
- **Notifications & Related Best Practices** (31-37) - Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required. Principles include requiring email authentication for security notifications and that messages must be communicated clearly for users of all reading levels. In addition, tamper-proof packaging and accessibility requirements are recommended.

The OTA and the ITWG recognize that there is no perfect security or privacy state; organizations should adopt such protections as are commensurate with the risk posed to themselves and the end users, including a defense-in-depth strategy for all systems and a complete audit of the practices of their third party service providers.

Updates to this document and related resources are posted at https://otalliance.org/IoT

SECURITY – Device, Apps and Cloud Services

1. Ensure devices and associated applications support current generally accepted security cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, and Bluetooth connections. IoT introduces several data flows including: from a device to a mobile application to a back-end cloud hosting service. Industry must look to encrypt all data including data in motion and at rest. Companies should review acceptable best practices applicable to their respective industry segment.

   It is understood that the definition of Personally Identifiable Information (PII) is rapidly changing, but typically includes data relating to an identified or identifiable person. Currently, the US has no single regulatory definition. Companies are encouraged to take a cautious view in protecting all data which can be attributed to a specific user or home. Metadata should be considered personal data by default since these are subject to the same threats. For example with some devices such as smart lighting systems, mere data traffic patterns alone or "digital fingerprints", even if encrypted, could reveal user information such as presence in or absence from a home.

   As organizations and IoT solution providers increasing rely on service providers and third party platforms, they need to understand and assess end-to-end risk and vulnerabilities of IoT applications. It is recognized in some scenarios, such as mobile device platforms, companies may not have direct control of all device communication protocols for data stored on mobile devices or in transit to their cloud service platform but need to be aware of the risks incurred by lack of controls in this area.

   - Standards and guidance on a wide range of cryptographic technologies: NIST Cryptographic Toolkit http://csrc.nist.gov/groups/ST/toolkit/index.html
   - FTC Staff Report covering risks, principles, legislation and recommendations on IoT privacy and security: FTC Privacy & Security in a Connected World - January 2015 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
   - PCI Security Standards Council standards and extensive library of resources developed for the payment card industry but applicable to environments managing sensitive personal data: https://www.pcisecuritystandards.org/index.php

2. All IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications. SSL/TLS (also referred to as HTTPS and HTTPS everywhere), delivers website and server identity authentication as well as encryption of data in transit. Historically some organizations have utilized the SSL/TLS protocol to encrypt the authentication process when users log in to a website and shopping carts, but do not encrypt subsequent pages during the user's session. Unfortunately this intermittent use of SSL protection is no longer adequate. Today, cybercriminals have employed what is known as sitejacking or session hijacking, (also known as cookie hijacking) to exploit a valid computer session— to gain unauthorized access to information or services in a computer system. It has particular relevance to

web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

AOSSL utilizes SSL/TLS across your entire website to protect users with persistent security, from arrival to login to logout and is a proven, practical security measure that should be implemented on all websites where users share or view sensitive information. Leading sites include Google, Twitter, Facebook, Bank of America, Alaska Airlines and others have migrated their entire sites to be encrypted. This practice not only enhances website privacy from sitejacking or session snooping, but overall security (including countering man-in-the-middle attacks) as the entire user string and search requests are encrypted.

- OTA resources for Always On SSL https://otalliance.org/AOSSL
- OTA SSL best practices: https://otalliance.org/resources/ssl-best-practices
- Google is supporting HTTPS by prioritizing it in search result rankings:
  - https://webmasters.googleblog.com/2015/12/indexing-https-pages-by-default.html
  - http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html
- U.S. Office of Management and Budget memorandum on secure connection guidance: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf
- CA/Browser Forum - https://cabforum.org/

3. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least annually. A leading cause of data breaches and data loss incidents is from misconfigured and outdated server configurations. Research indicates that frequent scans of sites can identify weaknesses – for example, outdated protocol support, inadequate key strength, weak cipher suites and lack of Perfect Forward Secrecy (PFS) – in advance of attacks . It is recommended to:

   a) Conduct regular penetration tests and vulnerability scans of both your and your service provider's infrastructure to identify and mitigate vulnerabilities and thwart potential attack vectors. Penetration testing by an independent third party should be conducted regularly.

   b) Regularly scan your cloud providers' access points and look for potential vulnerabilities and risks of IoT application data loss or theft.

   c) Deploy solutions to detect anomalous flows of data which will help detect attackers staging data for exfiltration.

   d) Continuously monitor the real-time security of your organization's infrastructure by collecting and analyzing all network traffic, and analyzing logs and network statistics (including firewall, IDS/IPS, VPN and AV) using log management tools. Identify anomalous activity, investigate, and incorporate new learnings of threats accordingly.

   e) Upgrade from Domain Validated (DV) certificates to Organizationally Validated (OV) or Extended Validation (EV) SSL certificates. The subject organization of OV and EV SSL certificates are both validated by a Certificate Authority issuer at an increasing degree to create public trust of the identity of the applicant. EV SSL certificates offer the highest level of

authentication and verification of a website provider. EV SSL certificates displays this higher level of assurance by presenting the user a green trust indicator in a browser's address bar.

- See OTA Online Trust Audit https://otalliance.org/HonorRoll
- High-Tech Bridge SSL Service Test – Testing tool includes compliance against NIST guidelines and PCI DSS requirements. https://www.htbridge.com/ssl-check/
- Qualys SSL Labs test tools https://ota.ssllabs.com

4. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). Consider "bug bounty" programs, and crowdsourcing methods to help identify vulnerabilities that companies' own internal security teams may not catch or identify. The majority of vulnerability discoveries come for external sources including researchers, users and law enforcement, yet responsible disclosure of such information can be difficult. To effectively use this intelligence, companies must put in place responsive reporting processes including establishment of a monitored reporting vehicle, tracking and a replying mechanism for all such reports. Additionally, companies may consider a "bug bounty" program as an incentive for responsible disclosures.

   Developers often require time and resources to investigate such reports and to test remedies. This time period may vary between a few days and several months depending on issues such as the potential impact of the vulnerability, the complexity of developing an emergency fix or workaround, the time to implement such remedies and other factors. Companies need to create a system for tracking, archiving and responding to such threats. The absence of such a program opens an organization up to legal exposure and reputational damage (such as the breach of user data from Snapchat, a brand whose reputation is specifically designed around security and not leaving a trail).

   - NTIA Vulnerability Disclosure Process http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities
   - ISO International Standards on vulnerability disclosure (nominal download fee) http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170
   - An example Disclosure Policy from CERT: https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm
   - Electronic Frontier Foundation Coders Rights Project Vulnerability Reporting https://www.eff.org/issues/coders/vulnerability-reporting-faq
   - Bug Bounty Programs Overview https://en.wikipedia.org/wiki/Bug_bounty_program
   - The Bug Bounty Model: 21 Years & Counting (Dark Reading 1/3/2017)

5. Must have a mechanism for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Automated (vs automated) updates provide users the ability to approve, authorize or reject updates. Increasingly IoT devices need frequent updates to their application software and firmware. With the growing popularity of such devices, cybercriminals are increasingly targeting spear phishing campaigns to device users through the device code itself. Code signing processes ensures that code has not been tampered with after manufacturer release. Trusted sources could include certified installers, field support technicians or help desks at consumer electronics and office supply retailers. As experienced with a major TV manufacturer, self-signed or unverified patches can compromise devices by rendering them inoperable or installing malware and ransomware.

    - Code Signing Certificates: https://en.wikipedia.org/wiki/Code_signing
    - Example of poor validation via 'self-signing': http://wtnnews.com/articles/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits/
    - Further discussion of MitM attack on smart TV : http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it

6. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process and methodologies including unit, system, acceptance, regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components utilized. Employ generally accepted code and system hardening techniques, across a range of typical use case scenarios and configurations, including preventing any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. Devices should ship with reasonably current software and/or on first boot push automatic updates to address any known critical vulnerabilities. The development lifecycle must involve alertness to potential risks, and assessments of strength against such risks, from the beginning phases through the end product/service testing. The process should integrate rigorous assessment of potential risk and testing of defenses throughout with hardening to reduce the attack surface of the product or device which includes removing development services or interfaces not needed in production as well as protections against malware attacks.

    - SANS whitepaper: https://www.sans.org/reading-room/whitepapers/analyst/integrating-security-development-pain-required-35060
    - Microsoft Secure Software Development Lifecycle (SDL): http://www.microsoft.com/en-us/sdl/default.aspx
    - The Common Vulnerabilities and Exposures is sponsored by US-CERT and provides an international reference for known vulnerabilities: https://cve.mitre.org/

7. Conduct security, and compliance risk assessments for all service and cloud providers. Risk assessments are critical for every organization. Increasingly, organizations and their executives are being held accountable and facing lawsuits for the failure to uphold fiduciary duties as they apply to data security and governance. Assessment of third-parties' security and privacy practices should be part of the vendor selection process and requires a commitment of both time and resources. Assessments and audits of third-party capabilities need to continue after a vendor is on-boarded to help identify potential lapses in security and privacy practices as well as ascertain the adoption of new technologies and standards. Companies should consider penetration testing, scan vendor sites, and review vendor privacy policies regularly for vulnerabilities and insecure configurations.

    - OTA Cyber Incident & Breach Response Guide (with Risk Assessment checklists): https://otalliance.org/incident

8. Develop and maintain a "bill of materials" including software, firmware, hardware and third party software libraries (including open source modules and plug-ins). This would apply to the device, mobile and cloud services to help quickly remediate disclosed vendor or open source vulnerabilities. A Bill of Materials (BOM) is a list of components and code libraries used in an application or service. Software vendors often create products by assembling open source and commercial software components. The BOM describes the components in a product. It is analogous to a list of ingredients on food packaging. The concept of a BOM is well-established in traditional manufacturing as part of supply chain management. A manufacturer uses a BOM to track the parts it uses to create a product. If defects are later found in a specific part, the BOM makes it easy to locate affected products. (Source Wikipedia)

9. Design devices to minimum requirements necessary required for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.

USER ACCESS & CREDENTIALS

10. Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets. A common practice of device and software developers is to provide a default user name and password "out of box" or upon initialization with no user requirement to change this default configuration. Best practices require a unique initial password (ideally printed on a label affixed to the device) and/or forcing the user to create a unique password on initial set up or whenever a device is restored to factory configuration. Alternative credentials could include biometrics, two factor and fingerprint readers.

    Organizations should consider federated identity systems including those being supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC helps individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation.

    - NSTIC overview http://www.nist.gov/nstic/
    - FIDO Alliance https://fidoalliance.org
    - Kantara Initiative https://kantarainitiative.org/

11. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential re-set using multi-factor verification and authentication (email and phone, etc.) where no user password exists. Developers should anticipate that consumers will lose, forget or need to reset passwords. In reestablishing access for authorized users, best practices include two factor authentication such as sending a onetime passcode to a mobile device or email address on file.

    - Two Factor Authentication: http://searchsecurity.techtarget.com/definition/two-factor-authentication
    - Microsoft Password Best Practices https://technet.microsoft.com/en-us/library/cc784090(v=ws.10).aspx
    - Fishnet Security https://www.fishnetsecurity.com/6labs/resource-library/white-paper/best-practices-secure-forgot-password-feature
    - Best Practice for Secure Forgot Password Feature https://www.fishnetsecurity.com/6labs/resource-library/white-paper/best-practices-secure-forgot-password-feature

12. Take steps to protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts. Establishing a procedure to lock-out or disable after repeated failed logins is crucial to preventing brute force attacks by automated bots. Possible protections against abusive login attacks could include techniques such as use of CAPTCHA or similar mechanisms, two-factor authentication to re-authorize after lock out or the creation of lock out periods of varying durations (such as 15 min lock out after three failed attempts, 1 hour lock out after 10 failed attempts, etc.). Consider blocking the ranges of country IP addresses which are not consistent with where the user resides or typically might travel to.

    - Computer Weekly – Techniques for preventing a brute force attack http://www.computerweekly.com/answer/Techniques-for-preventing-a-brute-force-login-attack
    - Preventing Brute Force Attacks on ADFS 3.0 https://social.msdn.microsoft.com/Forums/en-US/c8945feb-922f-4727-b2b4-c0705c314063/preventing-brute-force-attacks-on-adfs-30?forum=Geneva
    - Why Use CAPTCHA http://stackoverflow.com/questions/33306438/php-login-why-use-captcha
    - OWASP Blocking Brute Force Attacks https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

13. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s). To secure against unintended or unauthorized password reset and use, developers should send user alerts for all password resets, particularly when sign-ons are detected from an unknown device or IP address. Such notices can help limit the impact of device compromise and unauthorized password resets. Any password change, recovery or reset should include secure authentication of the user. Although there are various authentication approaches, a multi-factor procedure such as a one-time-use token sent via a side-channel – for example, a randomly generated code with a limited time period issued via SMS – is recommended. This approach places multiple hurdles before attackers increasing defense-in-depth.

    - How to Prevent Fraud Using Out of Band Authentication http://www.outofbandverification.com/category/one-time-password/page/2/
    - OWASP Forgot Password Cheat Sheet https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet

14. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted. Applies to all credentials stored to help prevent unauthorized access and brute force incidents. Encrypting of passwords is a required control as passwords are often reused and in clear text when in transit with many Bluetooth and wireless networks. User data including passwords and bio-metrics can be easily captured from scanning devices stealthily operating in public places such as the sidelines of a sporting event, a public street or at a mall. Cryptographic techniques themselves vary and have evolved over time including approaches to salting (adding randomized information into the encryption function). It is critical to be aware of limitations to simple encryption approaches and be sure to employ up to date best practices.

    - OTA cyber incident and data protection resources: https://otalliance.org/Incident
    - A commentary on limits to simple hashing https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous
    - NIST Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf
    - NSA Suite B Cryptography is a set of cryptographic algorithms published by the National Security Agency. It serves as an interoperable cryptographic base for both unclassified information and most classified information: https://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography

PRIVACY, DISCLOSURE & TRANSPARENCY

15. Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download, or enrollment. In addition to prominent placement on product packaging, on their website, it is recommended companies utilize QR Codes, user friendly short URLs and other similar methods maximizing disclosure at point-of-purchase. A key principle of responsible privacy practices is to provide users clear and concise disclosure notices *prior to product use or product download*, including the ability to control the collection, use and sharing of their data. Unlike websites or mobile apps where a user can choose to not return to the

site or uninstall the app, installation and use of physical IoT products introduces unique challenges. The lack of full disclosure of these topics can drive product returns and consumer remorse.

To help address these issues, privacy and data use disclosures must be readily available for review prior to purchase independent of the device used to access them. For IoT, disclosure solutions may include providing a short notice on product packaging, point-of-sale materials as well as a link to an online privacy policy. The working group acknowledges the need to have flexibility in how and when notices are provided. For example, notices may be provided on first use or when activating a new feature or within the "read me first" packet affixed to the outside of the product box. Other recommended practices include utilizing QR Codes, brief, understandable URLs (instead of lengthy alpha-numeric URLs) and other similar methods.

Best practices can be summarized as follows:

a) Create a layered, concise summary linking to an expanded or long form privacy policy, which may have expanded legal language (as required).
b) Include key sections outlining
    - Data attributes collected
    - The identity of data sharing parties and how they may or may not be limited on the use and further sharing of such data.
c) Publish easily discoverable and comprehensible privacy policies. Write your policy for the lay consumer versus a plaintiff's attorney.
d) Share details of your data retention policies including clear disclosure if such data is retained after the online interaction is terminated.
e) Use navigational aids such as icons or links to help consumers find and understand the policy elements more easily. Provide a clear statement including details if, what and for what purposes personal data is being shared with third parties. See OTA short form, linking to the full policy – http://otalliance.org/privacy-policy.
f) Write policies for your site's target audience and demographics. Consider providing multi-lingual versions representing the diversity of your site's visitors. For an example, see our Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
g) Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the statement "To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process."

Resources:

- Example privacy policy design from TRUSTe: http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/
- Example privacy policy design from PrivacyCheq: http://privacynq.com/OTA
- OTA's short form privacy policy (with links to full policy) as another example: http://otalliance.org/privacy-policy

16. Disclose the duration and end-of-life security and patch support, (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase. *(It is recognized IoT devices cannot be indefinitely secure and patchable.*

Consider communicating the risks of using a device beyond its usability date, and impact and risk to others if warnings are ignored or the device is not retired). The ongoing security of the IoT solution after product purchase is vitally important. It needs to be understood separately from product warranties and should be provided at no-charge for the expected life of the product. Consumer disclosures need to specify any limitations, including the time frame during which software and firmware will be supported considering the expected lifespan of the product, service or system. For example, a product warranty on a connected refrigerator could be one to three years, but the product life could easily be ten years. In summary, companies have the responsibility to continue security support beyond basic warranty periods, throughout the product's realistic life span.

17. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes. For example, a fitness tracker could potentially disclose that it tracks physical location, personal vitals (heart rate, pulse, blood pressure), as well as profile data. A home thermostat could disclose that it collects the time of temperature changes and the proximity of the user (which could reveal when the home is unoccupied).

    Consistent with FIPPs, limiting data collection to the minimum needed for functionality is a best practice not only for consumer protection but to protect Companies by minimizing what data can be impacted in an attack. Further, disclosures about the purposes of data collection are consistent with international guidelines (see ENISA report on Security and Resilience in Smart Home Environments). Notably, there are sources currently advising that clearly explaining these practices in the privacy policy are not enough, but additional "enhanced" notices should be provided whenever data is collected in an unusual way or fashion that would not be readily apparent to the consumer. Requiring "opt in" consents (historically the default in the EU) is not currently mandated in the United States, but increasingly is being touted as a best practice in transparency so that an organization can demonstrate the consumer understands and agrees to data collection and sharing practices. Challenges associated with these additional enhanced consents in devices without a user interface may be included within an associated platform but could cause adverse operational impact if functionality is dependent on receiving consent. Such disclosures and opt-in requests provide the opportunity to outline the consumer value or benefit of such collection and sharing.

    - FTC Guidance https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
    - European Union Agency for Network and Information Security (ENISA) good practices https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices
    - See also EU-U.S. Privacy Shield http://europa.eu/rapid/press-release_IP-16-216_en.htm and EU General Data Protection Regulation (GDPR) http://www.eugdpr.org/

18. Disclose what features will fail to function if connectivity or backend services become disabled or stopped including but not limited to the potential impact to physical security. *(Consider building in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality, based on the device usage, balancing out potential life/safety issues).* Disclosures must clearly identify which, if any, core functions and/or product features will cease function if connectivity should fail. For example, it should still be possible to open a connected garage door or brew coffee in a connected coffee maker, even if the "smart" capabilities are disabled due to an outage in Internet connectivity.

19. Disclose the data retention policy and duration of personally identifiable information stored. Specify what data is retained and for what duration. Data retention regulations vary by industry and geography, and continue to evolve. Aside from regulatory compliance, other factors in a establishing a comprehensive data retention policy include defining what records will be collected, their business purpose, the level of sensitivity (to the company and/or to the consumer) and the risk exposure of keeping such data. Data retention policies should reflect the specific data utilized for the product or service in question. Identifying the specific purpose(s) for collected data can be a key indicator for how long data should be retained. For example, key contact data should be retained for product warranty and recall purposes, other data on usage patterns or personal data attributes should be destroyed upon request of the user or when the device/service is no longer used.

    - NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
    - EU Data Protection Directive http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm
    - Office of the Privacy Commissioner (Canada) best practices: https://www.priv.gc.ca/information/pub/gd_rd_201406_e.asp

20. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services. Such notices or indicators are required to prevent unauthorized devices connecting or acquiring device data and/or prevent devices from inadvertently joining unauthorized networks. Devices should have unique immutable attestable device IDs to help prevent device ID spoofing.

    - Guide to Bluetooth Security http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

21. Publicly disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker). Because the lifespan of some connected devices may last many years or even decades, provisions for transferring ownership must be considered. The ownership of longer-life connected home devices such as keyless entry systems, gates, home automation and garage doors will transfer upon home sale. Companies should clearly explain procedures for such transfers including but not limited to how to reset passwords, how to purge or remove personally identifying elements from historical data, how to update user contact information so new owners can be contacted in future communications (updates, recalls, etc.). For fitness devices, users may want to download as well as purge, reset or make anonymous their personal fitness data upon selling or discontinuing use of the device and such provisions should be anticipated. For additional information regarding both smart homes and smart devices, see related consumer recommendations for buyers and sellers: https://otalliance.org/iotconsumer.

22. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that third party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access. Privacy policies and service provider contracts should require third parties to maintain the confidentiality of the information and prohibit them from using that information for any other purpose (for example, their own marketing or product development). Depending on the sensitivity of the data being shared, additional controls – such as independent validation of the third party's information security and breach response plans – should be undertaken and documented. Many standard services agreements include audit rights which may be used to demonstrate vendor due diligence, however, actual failure to exercise these audit rights with a service provider – particularly in the case of a long term contract or subsequent to an actual data breach or data loss by way of the third party - may be referenced to support liability and unreasonable security practices. In designing a vendor management program, consideration should be given to non-traditional sources of vendor intelligence but which might reveal important information on the likelihood of a vendor to be victim to cyberattack, for example, prior litigation or regulatory investigation, consumer complaints, and logging, record retention, system uptime or patching performance statistics. In addition, third party service providers should be bound to notify companies on any unauthorized use, data loss or breach incident.

    - Language from US Dept of Education Privacy Technical Assistance Center: http://ptac.ed.gov/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20(2014-05-06)%20%5BFinal%5D.pdf
    - State of California http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/COPP_bus_reportinfo_sharing1.pdf
    - Federal Trade Commission Privacy & Security Update https://www.ftc.gov/reports/privacy-data-security-update-2015
    - TRUSTe Model Privacy Policy Disclosures http://www.truste.org/docs/Model_Privacy_Policy_Disclosures.doc

    See relevant Appendix A examples: #14

23. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default." Ideally, all setup parameters can be customized, restored to a prior setting or reset to an initial setting. The ability to reset or restore to factory defaults is particularly important when ownership or use of the device may be transferred to another user. It is suggest online document provide an explanation of the benefits and tradeoffs when enabling or disabling privacy enhancing features.

24. Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained. Consumer data transfers have been a key issue with bankruptcy filings and ownership transfers. Parties should follow Federal Trade Commission guidance both in designing their privacy policies and during due diligence of a proposed transaction. As with other data collection, transfer or use practices, consideration of the consumer's expectation on the use of their data should be the guiding factor. For example, to avoid interruption of the services for which a consumer has paid, an additional consent should not be required provided the acquiring company does not propose additions or modifications to the data use. When additional or different data practices are proposed by the acquiring party – such as additional data element collection, transmission, sharing or use – the changes must be disclosed in a transparent way with consumers opting in to these revisions. Failing to adhere to this practice has resulted in liability.

    - FTC summary guide to lessons learned from recent cases: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
    - A discussion of data transfer and sale in the Radio Shack bankruptcy noting a contrast to the FTC action against Toymart online retailer: http://www.infolawgroup.com/2015/06/articles/privacy-law/radioshack-bankruptcy-case-highlights-value-of-consumer-data/

25. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance. Unlike a mobile app which presents use and privacy practices to consumers prior to implementation, the data collection, use and privacy practices associated with a physical IoT device may not be fully understood until the device is purchased and set up. Conversely the opting out of such data collection may adversely impact the core product feature and functionality of the device. In such cases, the consumer should have the ability to return the device at no-charge (with exception of possibly shipping charges) and vendors should accept such returns. Prior to return, users should have the ability to restore the device to factory settings to help prevent the risk of any user data remaining on the device.

    - Econsltancy – Handing online returns https://econsultancy.com/blog/9906-handling-online-returns-14-best-practice-tips

26. Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end-user. The purpose is to protect the manufacturer from actions by consumers who may feel they were not given a reasonable right to reject a use policy being enacted by the manufacturer.

27. Comply with applicable regulations including but not limited to the Children's Online Privacy Protection Act (COPPA) and international privacy, security and data transfer regulatory requirements. Companies, products and services must be in compliance with any law or regulation of the jurisdiction that governs their collection and handling of personal and sensitive information. Failure to comply may constitute non-compliance with this framework.

    - COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
    - EU-US Privacy Shield Framework www.commerce.gov/privacyshield
    - EU General Data Protection Regulation (GDPR) www.eugdpr.org

28. Publicly post the history of material privacy notice changes for a minimum of two years. Best practices include date stamping, redlines, and summary of the impacts of the changes. Such disclosure aids consumer understanding of material changes to data collection, use and sharing. It is recommended pages be data stamped on the upper right of the first page, and links to red-lined changes on previous versions.

    - Google's privacy policy archives is an excellent example, dating back over 15 years: https://www.google.com/intl/en/policies/privacy/archive/

29. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing, loss, or sale of device. The user or authorized person on behalf of the user (e.g., a proxy) must be able to delete or make anonymous personal or sensitive data being stored after the user no longer uses a connected product.

    - 3 Simple Ways to Delete Your Data for Good http://www.usatoday.com/story/tech/columnist/komando/2013/07/05/delete-your-data-hard-drive/2480151

30. Provide the ability to reset a device and application to factory settings, providing the ability for erasure and zeroization in the event of transfer, loss or sale. Many common delete functions only delete the directory link to data and do not delete the actual data on media. Zeroization is the practice of erasing the underlying data contents by altering its contents to binary zeroes. This helps prevent disclosure of sensitive data if the equipment is captured (found or stolen), or reused (sold).

    - "Zeroization" https://en.wikipedia.org/wiki/Zeroisation

NOTIFICATIONS & RELATED BEST PRACTICES

31. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. Domains should implement SPF, DKIM and DMARC, for all security and privacy related communications and notices as well as for parked domains and those that never send email. Consumer communications are increasingly being spoofed (forging the "from" line, "user friendly" address or phone number) with the goal of prompting recipients to open a message and accept a malicious download. Since 2004 the email community has been advancing email authentication protocols to counter these exploits.

The industry has standardized on SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail), which, when combined, allow senders or domain holders to specify who is authorized to send email on their behalf. Senders are recommended to employ both their top level domain name (typically the domain which resolves to their web address) and all delegated sub-domains. Building on email authentication protocols, DMARC (Domain-based Message Authentication, Reporting & Conformance) adds a policy assertion providing receivers direction on handling of messages which fail or are detected to be spoofed through SPF and/or DKIM authentication checks. With precision exploits increasingly targeting businesses (e.g., Business Email Compromise), all companies should implement inbound authentication checks of all mail to protect employee and corporate systems.

To best utilize these technologies:

a) Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
b) Implement DMARC for all appropriate domains, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
c) Implement inbound email authentication and DMARC checks to help protect employees and from malicious email and related spear phishing exploits.

- Email Authentication Overview & Resources https://otalliance.org/eauth
- Domain-based Message Authentication, Reporting & Conformance Overview & Resources https://otalliance.org/dmarc
- SPF & DMARC Record Validator https://otalliance.org/resources/spf-dmarc-record-validator
- OTA 2016 Data Protection & Breach Readiness Guide (page 7) https://otalliance.org/Breach

32. For email communications within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, helping ISPs and receiving networks to reject email which fail email authentication verification checks. DMARC (Domain-based Message Authentication, Reporting & Conformance), is a technical specification created to reduce the potential for email-based abuse by solving several operational, deployment, and reporting limitations related to SPF and DKIM email authentication protocols.

    DMARC standardizes how email receivers, including ISPs and corporate networks, handle email results (both pass and fail) using SPF and DKIM. Moving from an initial monitor only policy (p=none) to a reject or quarantine policy is a simple process of revising a text record published in the domain's DNS. Prior to making such a policy assertion, domain holders should monitor the DMARC reports from receiving networks to help assure all outbound mail streams including delegated sub-domains are properly authenticated. Organizations should monitor their mail streams and DMARC reports for at least 90 days before moving to a reject (or quarantine) policy.

    Depending on the number of third parties used to send mail on an organization's behalf, this period may be longer or shorter. Third party mail systems may include customer shipping confirmation, email service providers, investor reporting, surveys, event registration systems and others. Organizations need to review all such systems and establish processes to monitor their respective infrastructure changes to assure their messages are not blocked or flagged as malicious.

- The Internet Engineering Task Force published IETF RFC 7489, “Domain-based Message Authentication, Reporting, and Conformance (DMARC)” on the Independent Submission stream on March 18th, 2015. https://tools.ietf.org/html/rfc7489
- OTA’s Domain-based Message Authentication, Reporting & Conformance Overview & Resources https://otalliance.org/dmarc
- Global Cyber Alliance – DMARC Resources https://dmarc.globalcyberalliance.org/

33. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message. Email is essentially a plaintext communication sent from email clients to receiving email servers or from one server to another. This design simplicity leaves the content of a message in transit open to eavesdropping from an unprotected hotspot (such as airport or coffee shop) to your ISP and internet backbone providers that carry your messages throughout the world.

    Transport Layer Security (TLS) helps solve this issue by encrypting messages while "in transit" from one secure email server to another. TLS helps prevent eavesdropping on email as it is carried between email servers that have enabled TLS email protections. Just as TLS can be used to secure web communications (HTTPS), it can secure email transport. In both applications, TLS has similar strengths and weaknesses. To maximize the content security and privacy, TLS is required between all the servers that handle the message including hops between internal and external servers.

    Key features of TLS includes:

    a) Encrypted messages: TLS uses Public Key Infrastructure (PKI) to encrypt messages from mail server to mail server, making it more difficult for hackers to intercept and read messages.
    b) Authentication: TLS supports the use of digital certificates to authenticate the receiving servers. Authentication of sending servers is optional. This process verifies that the receivers (or senders) are who they say they are, which helps to prevent spoofing.
    c) Opportunistic TLS is accomplished when used by both sending and receiving parties to negotiate a secured SSL/TLS session and encrypt the message. Today leading ISPs and mailbox providers including Comcast, Google, Microsoft and Yahoo are now supporting TLS.

    - STARTTLS for email https://en.wikipedia.org/wiki/STARTTLS
    - Google http://www.google.com/support/enterprise/static/postini/docs/admin/en/admin_ee_cu/ib_tls_overview.html
    - TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email
    - MAAWG https://www.m3aawg.org/blog/new-pervasive-monitoring-sig-urges-you-to-turn-on-opportunistic-tls-now
    - RFC 5246 The Transport Layer Security (TLS) Protocol https://www.m3aawg.org/blog/new-pervasive-monitoring-sig-urges-you-to-turn-on-opportunistic-tls-now

34. Implement measures to help prevent or make evident any physical tampering of devices. Such measures help to protect the device from being opened or modified for malicious purposes after installation or from being returned to a retailer compromised.

35. Consider how to accommodate accessibility requirements for users who may be vision, hearing and or mobility impaired to maximize access for users of all physical capabilities.

36. Develop communications processes to maximize user awareness of any potential security or privacy issues, end-of life notifications and possible product recalls, including in app notifications. Communications should be written maximizing comprehension for the general user's reading level. Consider multi-lingual communications recognizing that English may be the "second language" for users (see related principles regarding security and message integrity).

36. Enact a breach and cyber response and consumer notification plan to be reevaluated, tested and updated at least annually and / or after significant internal system, technical and / or operational changes. Breach readiness is critical for any organization and all organizations will experience some sort of cyber incident. A well-designed and tested response plan is essential for timely notification to regulators, law enforcement and consumers. An acceptable plan should have mechanisms to help detect, mitigate (isolate), respond and remediate the impact of cyber incidents such as ransomware or DDoS risk or data loss incident.

    Working with leading response organizations, the Federal Bureau of Investigation and the Secret Service OTA publishes an annual Cyber Incident Response Guide. Content is designed to help aid a broad range of stakeholders from business and technical decision makers and privacy and security professionals, to web and app developers. The goal is to help readers better understand the issues and solutions which can enhance their protection practices and enable them to develop readiness plans to reduce risk, rapidly respond to incidents and minimize business interruption.

    Even the most cyber-savvy organizations have found themselves exposed and ill prepared to manage the effects of a ransomware attack or data breach. The best defense is implementing a broad set of operational and technical best practices that helps protect your company and your customers' personal data throughout its life cycle. The second step is to be prepared with a plan that allows you to immediately respond. Handling an incident is a shared responsibility of every functional group within your organization. A key to success is transitioning from merely a compliance perspective to one of responsible stewardship. This perspective recognizes the long term impact to your market brand and reputation, the importance of overall consumer trust and the implications this has for vendors and business partners.

    - OTA Cyber Incident & Breach Readiness https://otalliance.org/Incident

ADDITIONAL CONSIDERATIONS

Beyond the IoT Trust Framework principles and criteria, the ITWG recognizes additional issues and suggests developers consider the following as they apply to products and services:

- Focus on User Experience and putting users' interests first for any advertising-supported device or service. Business models based on advertising revenue can provide positive low or no cost opportunities for consumers. Even so, companies must consider the risks and responsibilities third party advertising bring to any connected device or service. In addition to security issues of malvertising attacks or socially engineered data threats, marketing efforts within the connected ecosystem give rise to potential user annoyance and backlash. Further, issues of clear identification of advertising versus content may be particularly confusing for consumers within a connected device context. For example, receiving ad messages on a connected fitness device may appear to the user as endorsements unless steps are taken to clearly indicate advertising messages. More Info https://otalliance.org/resources/advertising-integrity-fraud

RECOMMENDED RESOURCES

Several organizations have begun publishing analyses, case studies and guidance related to various elements of IoT safety. Below are additional documents useful for understanding the connected landscape. For updates please visit https://otalliance.org/resources/iot-industry-resources#RELATED