Principles
Requirements
Framework
Features
Tests

Which generic security and privacy principles to ensure a Trusted IoT environment?

The consumer view

Who is Test-Aankoop / Test-Achats?

- Belgium largest consumer association – approx. 350,000 members
  - Testing products and services
  - Consumer defense actions (policy, judicial)
- Associated with independent consumer organizations in Spain (OCU), Italy (Altroconsumo), Portugal (DECO) and Brazil (Proteste!)
- Participates in ICRT (International Consumer Research & Testing), pursuing joint technical lab testing of products
- Member of BEUC (Bureau européen des Unions de Consommateurs), advocating consumer-friendly regulation and policy at EU level
- Cooperates with ANEC (the "European consumer voice in standardization")
- Member of Consumers International (world federation of consumer groups)

Why are consumers concerned?

https://youtu.be/lAOj0H5c6Yc

https://youtu.be/OkYVSag-uik

(Today)

You choose: from a product design perspective, is this

(a) Incompetent?

(b) Irresponsible?

(c) Unethical?

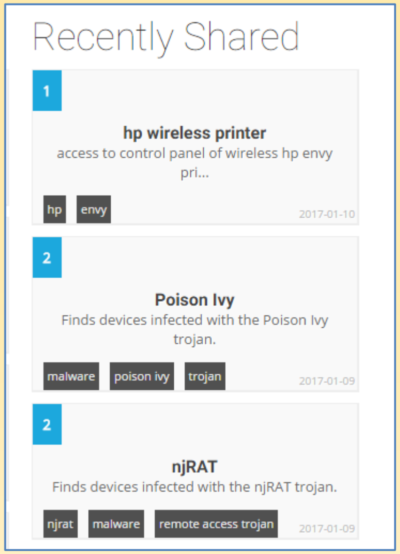
(d) Negligent?

(e) Illegal?

(f) OK???

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.



Recently Shared

1

hp wireless printer

access to control panel of wireless hp envy pri...

hp envy 2017-01-10

2

Poison Ivy

Finds devices infected with the Poison Ivy trojan.

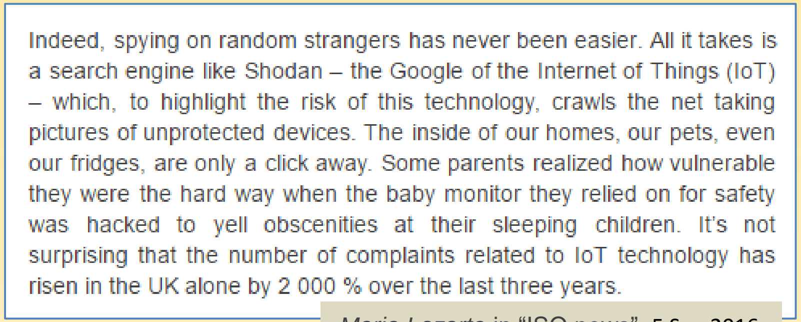
malware poison ivy trojan 2017-01-09

2

njRAT

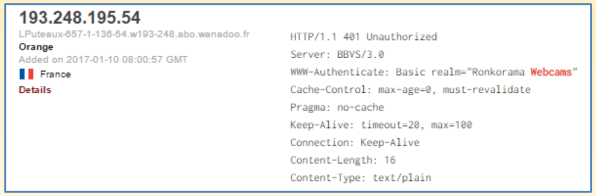
Finds devices infected with the njRAT trojan.

njrat malware remote access trojan 2017-01-09



Indeed, spying on random strangers has never been easier. All it takes is a search engine like Shodan – the Google of the Internet of Things (IoT) – which, to highlight the risk of this technology, crawls the net taking pictures of unprotected devices. The inside of our homes, our pets, even our fridges, are only a click away. Some parents realized how vulnerable they were the hard way when the baby monitor they relied on for safety was hacked to yell obscenities at their sleeping children. It's not surprising that the number of complaints related to IoT technology has risen in the UK alone by 2 000 % over the last three years.

Maria Lazarte in "ISO news", 5 Sep 2016



193.248.195.54

LPuteaux-657-1-136-54.w193-248.abo.wanadoo.fr

Orange

Added on 2017-01-10 08:00:57 GMT

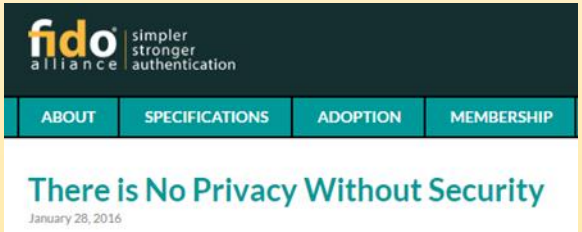
France

Details

```
HTTP/1.1 401 Unauthorized
Server: BBVS/3.0
WWW-Authenticate: Basic realm="Ronkorama Webcams"
Cache-Control: max-age=0, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=20, max=100
Connection: Keep-Alive
Content-Length: 16
Content-Type: text/plain
```

Privacy and security

Distinct but complementary topics;
Multiple facets to look at…



There is No Privacy Without Security

January 28, 2016

Privacy

- Data protection law (GDPR) and e-privacy dir/reg
- “My data is mine”, throughout the **data lifecycle**
  - Consent & control on collection, processing, sharing and retention of personal data ⇨ **transparency** and consumer **empowerment (pre-and post purchase)**
  - **Effective** disclosure (also of changes to policy)
  - Erasure, portability of personal data; end-of-life support
- Privacy by design **and by default**
- Complex business ecosystem ⇨single-point of **accountability**

Security

- ISO/IEC 27000 (27001-2013)
  - Confidentiality, integrity (completeness, accuracy), availability (incl continuity)
- Cybercrime
  - Known **cyberthreats**: Hacking, DDOS, Ransomware, ID theft…
  - In IoT may extend to **corporal and property threats**
- Security across **the whole technology environment**
  - Device, apps, communications and back-end systems
- Security safeguards across the **software lifecycle, for**
  - Data both in transit and in storage
  - User access and recovery mechanisms
- Security **patching as a minimum** legal (post-) warranty obligation
- Disclosures must be **timely, actionable** and a **“managed process”**

Legal

- Disclosures / policies
- Warranties and Liabilities
  - Injuries / damages
  - Security breaches
  - Privacy infringements
- Consumer redress

Technical/Practical

- Standards
  - Safety
  - Interoperability
  - Sustainability
- Testing protocols
- Certification: “Trusted IoT label”

IoT = physical <u>product</u> + digital <u>services</u>

⇨ focus on full lifecycle

- [1] Purchase and Set-up
  - Secure account creation ; device pairing ; disclosures
- [2] Use
  - Data collection, transfer and storage; software updates ; pw recovery ; notifications
- [3] Decommissioning / end-of-life
  - User account and data
- [4] Terms & Conditions
  - Discoverability, readability (length, style), content, updates

Software updates, upgrades, patches for connected devices: a whole new ballgame for many manufacturers…

⚠
- Immediate risk of continued use of unpatched devices
- Expectation: Security patches as a minimum

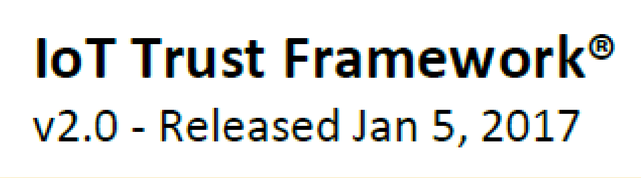
⚠
- Longer term risk: Early / planned obsolescence
- Expectation: accept - reject options for feature upgrades

"The average life expectancy for a properly maintained refrigerator is between 14 and 17 years" (SFGate Homeguides)

17 years ago, in 2000, Windows98 was still the mainstream OS for PC's ; Apple did not introduce the first iPhone until 2007…

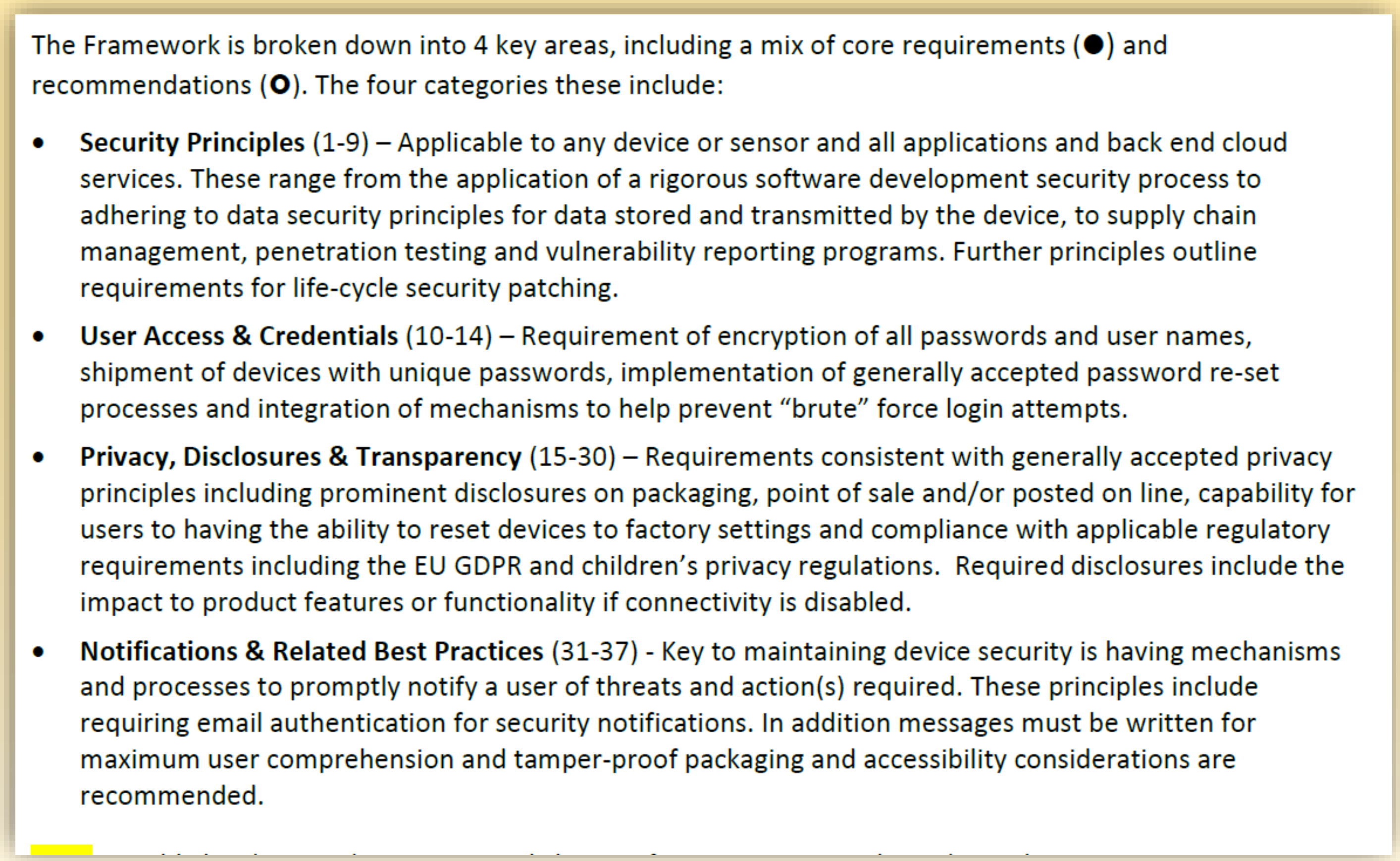
A valuable starting point:

Online Trust Alliance



IoT Trust Framework®

v2.0 - Released Jan 5, 2017



The Framework is broken down into 4 key areas, including a mix of core requirements (●) and recommendations (**O**). The four categories these include:

- **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. These principles include requiring email authentication for security notifications. In addition messages must be written for maximum user comprehension and tamper-proof packaging and accessibility considerations are recommended.

Guy Van Peel
Digital Consumption Expert
CC Products & Services

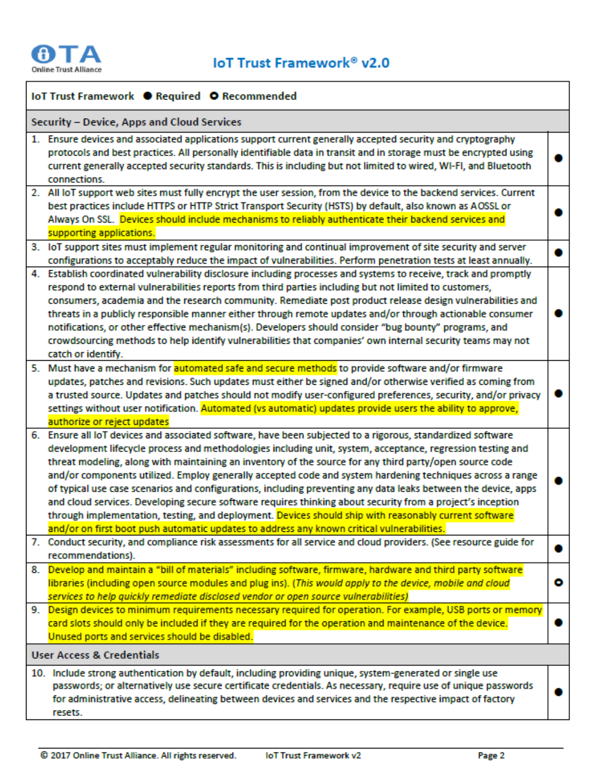
T: +32 (0) 2892 3767
Hollandstraat 13 Rue de Hollande
Bruxelles 1060 Brussel
gvanpeel@test-aankoop.be
www.test-aankoop.be

THANK YOU

Security and privacy –
Reference frameworks and consumer organization testing checklists

ANNEX

37 requirements and recommendations of the OTA framework

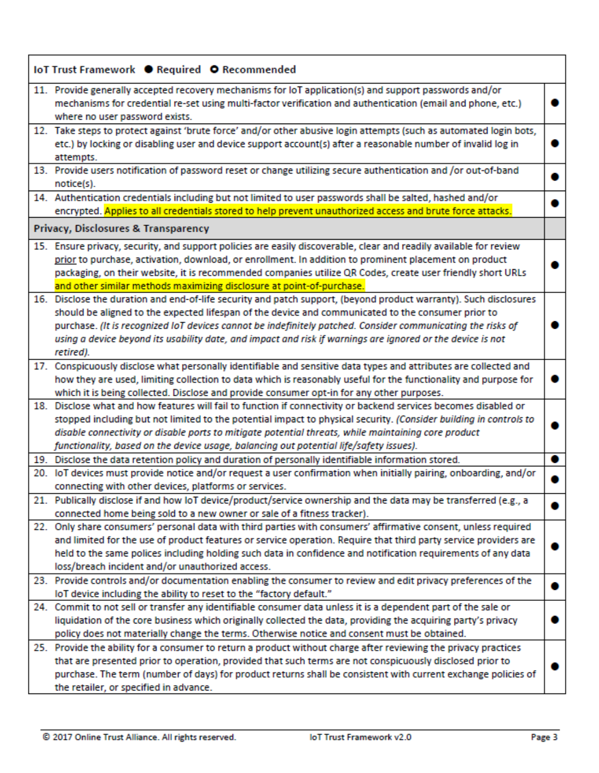


OTA Online Trust Alliance

IoT Trust Framework® v2.0

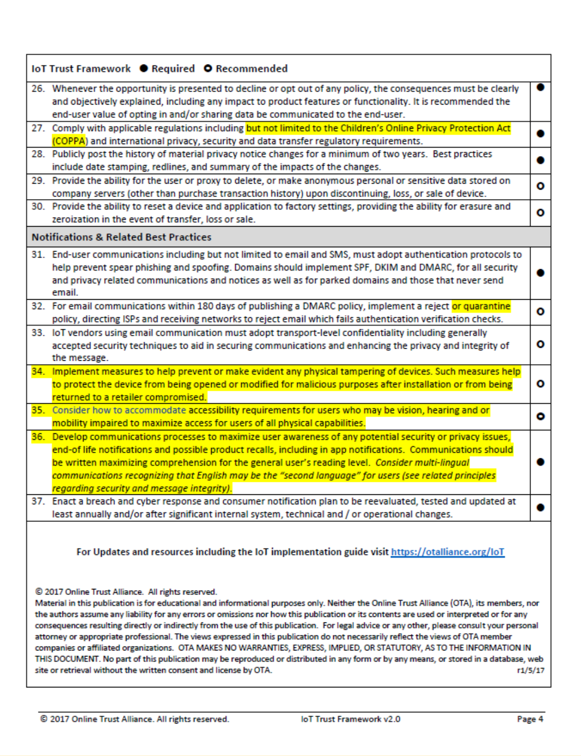
IoT Trust Framework ● Required ○ Recommended	
Security – Device, Apps and Cloud Services	
1. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, and Bluetooth connections.	●
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.	●
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.	●
4. Establish coordinated vulnerability disclosure including 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). Developers should consider "bug bounty" programs, and crowdsourcing methods to help identify vulnerabilities that companies' own internal security teams may not catch or identify.	●
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 automatic) updates provide users the ability to approve, authorize or reject updates	●
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.	●
7. Conduct security, and compliance risk assessments for all service and cloud providers. (See resource guide for recommendations).	●
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)*	○
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.	●

© 2017 Online Trust Alliance. All rights reserved. IoT Trust Framework v2 Page 2



IoT Trust Framework ● Required ○ Recommended	
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.	●
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.	●
13. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●
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 attacks.	●
Privacy, Disclosures & 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, create user friendly short URLs and other similar methods maximizing disclosure at point-of-purchase.	●
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 patched. Consider communicating the risks of using a device beyond its usability date, and impact and risk if warnings are ignored or the device is not retired).*	●
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.	●
18. Disclose what and how features will fail to function if connectivity or backend services becomes 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).*	●
19. Disclose the data retention policy and duration of personally identifiable information stored.	●
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.	●
21. Publically 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).	●
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.	●
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."	●
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.	●
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.	●

© 2017 Online Trust Alliance. All rights reserved. IoT Trust Framework v2.0 Page 3



IoT Trust Framework ● Required ○ Recommended	
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.	●
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.	●
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.	●
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.	○
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.	○
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.	●
32. For email communications within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, directing ISPs and receiving networks to reject email which fails authentication verification checks.	○
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.	○
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).*	●
37. 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.	●

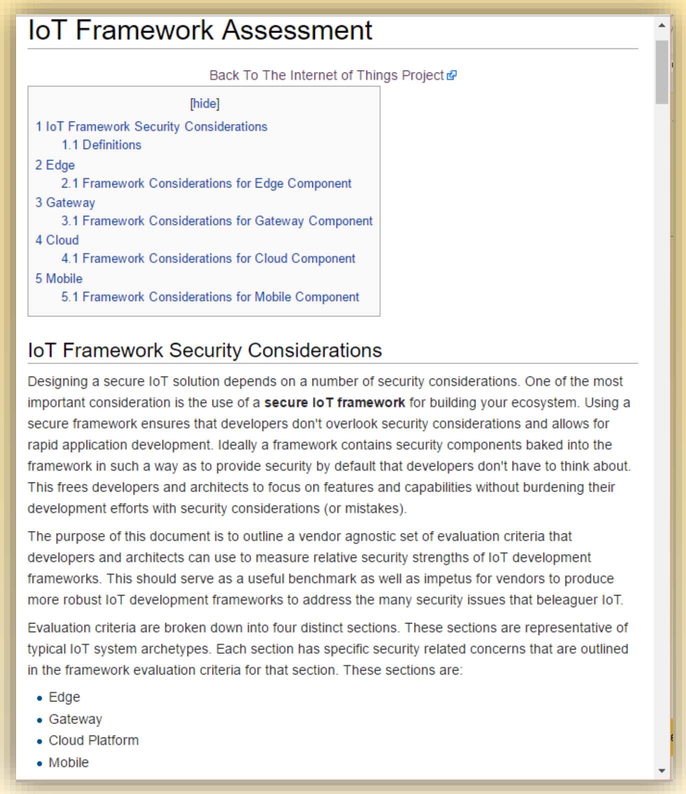
For Updates and resources including the IoT implementation guide visit https://otalliance.org/IoT

© 2017 Online Trust Alliance. All rights reserved.
Material in this publication is for educational and informational purposes only. Neither the Online Trust Alliance (OTA), its members, nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent and license by OTA. r1/5/17

© 2017 Online Trust Alliance. All rights reserved. IoT Trust Framework v2.0 Page 4

http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT%20Trust%20Framework.pdf

OWASP
Open Web Application
Security Project



IoT Framework Assessment

Back To The Internet of Things Project

[hide]
1 IoT Framework Security Considerations
1.1 Definitions
2 Edge
2.1 Framework Considerations for Edge Component
3 Gateway
3.1 Framework Considerations for Gateway Component
4 Cloud
4.1 Framework Considerations for Cloud Component
5 Mobile
5.1 Framework Considerations for Mobile Component

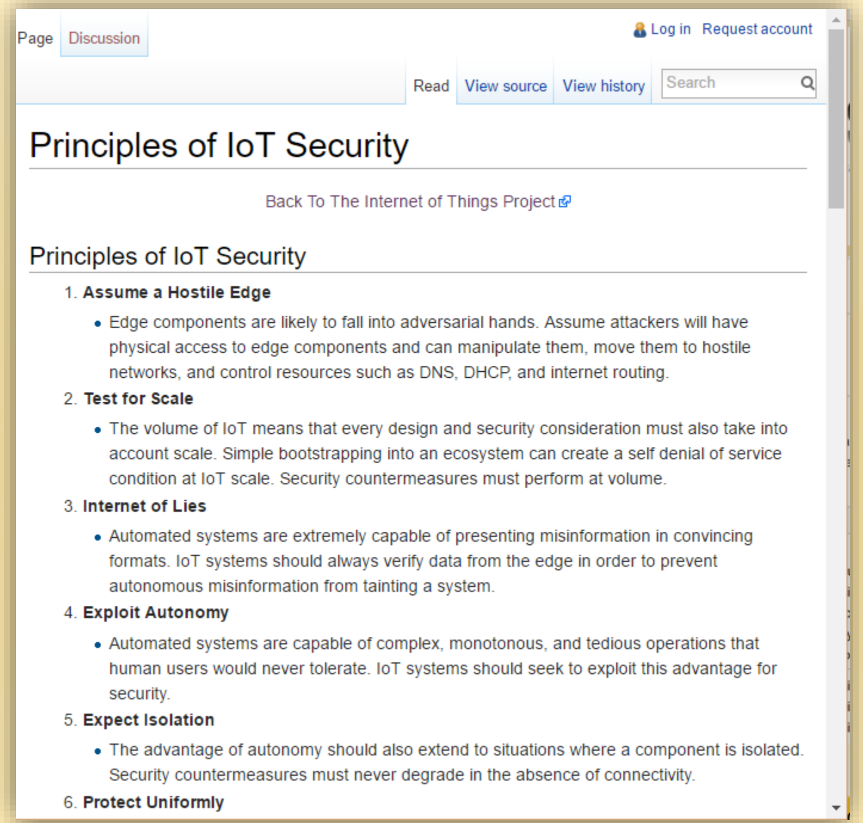
IoT Framework Security Considerations

Designing a secure IoT solution depends on a number of security considerations. One of the most important consideration is the use of a **secure IoT framework** for building your ecosystem. Using a secure framework ensures that developers don't overlook security considerations and allows for rapid application development. Ideally a framework contains security components baked into the framework in such a way as to provide security by default that developers don't have to think about. This frees developers and architects to focus on features and capabilities without burdening their development efforts with security considerations (or mistakes).

The purpose of this document is to outline a vendor agnostic set of evaluation criteria that developers and architects can use to measure relative security strengths of IoT development frameworks. This should serve as a useful benchmark as well as impetus for vendors to produce more robust IoT development frameworks to address the many security issues that beleaguer IoT.

Evaluation criteria are broken down into four distinct sections. These sections are representative of typical IoT system archetypes. Each section has specific security related concerns that are outlined in the framework evaluation criteria for that section. These sections are:

- Edge
- Gateway
- Cloud Platform
- Mobile

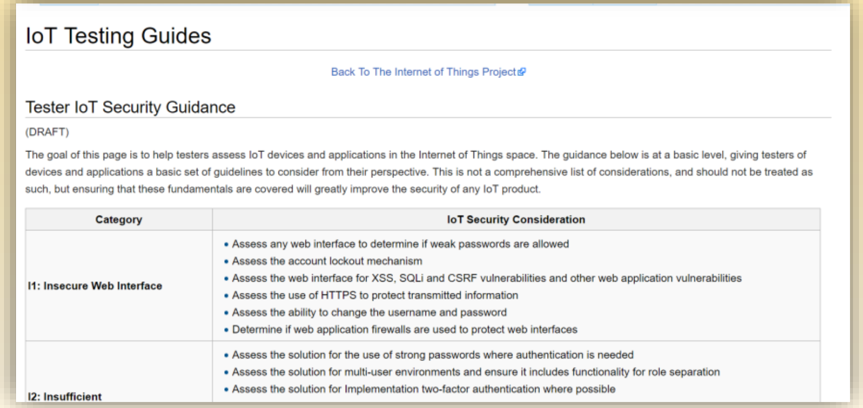


Principles of IoT Security

Back To The Internet of Things Project

Principles of IoT Security

1. **Assume a Hostile Edge**
   - Edge components are likely to fall into adversarial hands. Assume attackers will have physical access to edge components and can manipulate them, move them to hostile networks, and control resources such as DNS, DHCP, and internet routing.
2. **Test for Scale**
   - The volume of IoT means that every design and security consideration must also take into account scale. Simple bootstrapping into an ecosystem can create a self denial of service condition at IoT scale. Security countermeasures must perform at volume.
3. **Internet of Lies**
   - Automated systems are extremely capable of presenting misinformation in convincing formats. IoT systems should always verify data from the edge in order to prevent autonomous misinformation from tainting a system.
4. **Exploit Autonomy**
   - Automated systems are capable of complex, monotonous, and tedious operations that human users would never tolerate. IoT systems should seek to exploit this advantage for security.
5. **Expect Isolation**
   - The advantage of autonomy should also extend to situations where a component is isolated. Security countermeasures must never degrade in the absence of connectivity.
6. **Protect Uniformly**



IoT Testing Guides

Back To The Internet of Things Project

Tester IoT Security Guidance

(DRAFT)

The goal of this page is to help testers assess IoT devices and applications in the Internet of Things space. The guidance below is at a basic level, giving testers of devices and applications a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly improve the security of any IoT product.

Category	IoT Security Consideration
I1: Insecure Web Interface	• Assess any web interface to determine if weak passwords are allowed • Assess the account lockout mechanism • Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities • Assess the use of HTTPS to protect transmitted information • Assess the ability to change the username and password • Determine if web application firewalls are used to protect web interfaces
I2: Insufficient	• Assess the solution for the use of strong passwords where authentication is needed • Assess the solution for multi-user environments and ensure it includes functionality for role separation • Assess the solution for Implementation two-factor authentication where possible

Privacy – Security Product Testing Checklist (US-CR)

Onboarding	Are initialization/registration properly encrypted?
	Do default settings prioritize privacy?
User control/permissions	What access permissions are requested?
	Are more permissions requested than needed?
	Can the user deny specific permissions? (e.g. location)
	Can the user select which user interfaces are enabled – e.g. web, mobile app, tablet app, desktop app?
License/T&Cs/EULA	What is the user forced to agree to?
	Is the document in legalese, plain language (or even the usual language for the territory)?
	Are the main permissions highlighted and clearly mentioned in a transparent way?
	Will the app provider provide reasonable or advance notice if the terms are changed?
Information transferred	What information is sent by the device? (e.g. User ID, password, location, MAC address, machine ID, network, Wi-Fi…)
	What information is actually needed to have the device fully utilized?
	If the device tracks data of the user's activity, what info is collected and how often?
Transfer method(s)	What channels are used? (e.g. BT, RFID, internet, mobile network)
	Directly, or via a hub? (e.g. PC, Smartphone/tablet, Apple TV)
Encryption	Are logins/passwords encrypted?
	Is all personal data stored in an encrypted fashion?
	Is the data at rest encrypted?
	Are software/firmware updates sent encrypted and/or signed?
	What type and strength of encryption is used ?
	Is it end-to-end or just transport encryption?
	Is there a secure method to recover/resert password/login info?
Destination of data	Is data sent finally to an App? (on user's phone, tablet or PC)
	Is all collected data under the control of the user?
	Is the data stored by the manufacturer on a server?
	Is there a web interface to access user's data?
	How is the data used? Is the data shared with/sold to 3rd parties?
	Can the user select extent of data sharing?
	Is user data left on the device after the app is deleted?
	Can the user delete their account within the app?
	Is user data left on the mfr's server after the account is deleted?
	Can the user upgrade to a higher privacy level, at cost?
Interoperability	Is the communication proprietary, or is it possible to mix products from different manufacturers?
	Is the product limited to one 'ecosystem' (iOS, OSX, Android, Windows, …)

In the Privacy of Your Own Home

That smart TV, your connected thermostat, even your washing machine—they're all tracking your daily habits. Why you need to know who's watching.

LAST SPRING, AS 41,000 RUNNERS made their way through the streets of Dublin in the city's Women's Mini Marathon, an unassuming redheaded man by the name of Candid Wueest stood on the sidelines with a scanner. He had built it in a couple of hours with $75 worth of parts, and he was using it to surreptitiously pick up data from activity trackers worn on runners' wrists. During the race, Wueest managed to collect personal info from 563 racers, including their names, addresses, and passwords, as well as the unique IDs of the devices they were carrying.

Fortunately, Wueest is not a data criminal. He's one of the good guys–a security researcher at Symantec, the company behind Norton antivirus software. His experiment was done to expose some of the risks associated with the growing constellation of "smart" devices known collectively as the Internet of Things.

Many of those devices are versions of familiar, even friendly, consumer products: thermostats, refrigerators, light switches, televisions, and door locks.

What Rights Should Consumers Expect?

Consumer Reports thinks that manufacturers of Internet-connected devices should tell consumers in easy-to-understand language about the types of information being collected by those devices and how that information could potentially be shared, sold, and used. Device manufacturers should also give consumers options to control the collection and use of their data. We also support the work of the Federal Trade Commission, whose recent report on the topic states that the agency "… will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the Internet of Things to promote appropriate security and privacy protections." The FTC also urges more self-regulatory efforts by industry, as well as better data security and broad-based privacy legislation.

24 JUNE 2015

PHOTOGRAPHS BY DAVID BRANDON GEETING

Electronics / Computers & Internet / Printers / Lab Report: Connected Printers Have A Security Glitch

Lab Report: Connected Printers Have a Security Glitch

An old printer that you sold or gave away could still be printing your e-mailed documents

By Dean Gallea and Daniel Katz (Intern)
Last updated: September 29, 2015

Connected toys
Privacy : Analysis of terms (NoCC)

- Accessibility
- Readability
- Notice about changes
- Defining personal data
- Data minimization
- Permissions
- Purpose limitation – Sharing data with third parties
- Purpose limitation - Advertising toward children
- Purpose limitation - Further use of voice data
- Data retention
- Deleting an account
- Supporting the service
- Termination from the service

- Device vulnerabilities
- Bluetooth – phone communication (pairing, range)
- Internet communication

#Toyfail

An analysis of consumer and privacy issues in three internet-connected toys

Desember, 2016

FORBRUKERRÅDET