Minimum Standards for Tackling IoT Security - Read, Write, Participate - Medium

Mozilla

Despite growing concerns about the safety and security of the Internet of Things, companies are still cranking out connected devices with insecurities, from baby monitors to drones. All too often, companies aren't required to maintain the security of their devices. Cloudpets, the connected toy was pulled from retailer shelves this fall, but there's no guarantee that it won't be replaced by yet another insecure toy marketed to kids around the world. The status quo isn't working.

So what should be done? Mozilla, Consumers International and the Internet Society believe there needs to be a simpler, more proactive approach. As a baseline, industry should start talking about what some of the initial 'red lines' are in this space, and should phase out practices that lead to the most egregious security failings in connected devices.

That is why today we are proposing five minimum required guidelines that companies making connected devices should reasonably be expected to satisfy.

Minimum Security Standards

1. **Encrypted communications**
   The product must use encryption for all of its network communications functions and capabilities. This ensures that all communications are not eavesdropped or modified in transit.
2. **Security updates**
   The product must support automatic updates for a reasonable period after sale, and be enabled by default. This ensures that when a vulnerability is known, the vendor can make security updates available for consumers, which are verified (using some form of cryptography) and then installed seamlessly. Updates must not make the product unavailable for an extended period.
3. **Strong passwords**
   If the product uses passwords for remote authentication, it must require that strong passwords are used, including having password strength requirements. Any non unique default passwords must also be reset as part of the device's initial setup. This helps protect the device from vulnerability to guessable password attacks, which could result in device compromise.
4. **Vulnerability management**
   The vendor must have a system in place to manage vulnerabilities in the product. This must also include a point of contact for reporting vulnerabilities or an equivalent bug bounty program. This ensures that vendors are actively managing vulnerabilities throughout the product's lifecycle.
5. **Privacy Practices**
   The product must have a privacy policy that is easily accessible, written in language that is easily understood and appropriate for the person using the device or service. Users should at minimum be notified about substantive changes to the policy. If data is being collected, transmitted or shared for marketing purposes, that should be clear to users and, as in line with GDPR, there should be a way to opt-out of such practices. Users should also have a way to delete their data and account. Also in line with the EU's General Data Protection

Regulation (GDPR), this should include a policy setting standard retention periods wherever possible.

We will also use these guidelines to directly engage with retailers and device makers. We hope that retailers can directly integrate these into their products, so that consumers are no longer put at risk.

Appendix:

This section is designed to answer some questions we encountered when designing these guidelines. As well as links to further information and resources about how to take further action on these issues should you wish to.

1. **On unsecured Wi-Fi connections:**
   When we asked many manufacturers about these standards, a common response around encryption was that it depends on the security provided by customer's local wifi. In an ideal world, we believe that most products should only connect to secure networks, but in terms of minimum standards, we believe that as long as communication is encrypted , that would meet the minimum requirement.
2. **On Strong Passwords:**
   Some connected devices use strong Bluetooth pairing and authentication that does not involve passwords. This is consistent with the intent of the guideline and for the purpose of the buyers guide is considered to satisfy the guideline. The guideline is also not intended to require that all devices have a password. It is intended for devices that use passwords for *remote* authentication, rather than devices that are in hand.
3. **Security updates:**
   Automatic updates are critical to creating a secure product ecosystem. Nonetheless, we have heard concerns that automatic updates can also be used in ways that are adversarial towards users. This guideline is not intended in any way to encourage or condone the use of update mechanisms to push software that would weaken the privacy properties of products or modify security or privacy settings in ways that are inconsistent with users' choices and expectations.

The following resources provide more detail and support on implementing and going beyond the above principles.

IoT Trust Framework
The Internet Society's Internet of Things (IoT) Trust Framework includes a set of 40 strategic principles necessary to address IoT security, privacy and lifecycle issues. It was developed through a process involving more than 100 stakeholders. It can be used by manufacturers to incorporate "trust by design" into their offerings, by retailers and other distribution channels as a filter to assess proper levels of security and privacy and by policymakers as principles for informed advocacy and economic policy regarding IoT.

Securing Trust in the Internet of Things
Consumers International, working with ICRT, BEUC and ANEC have produced Securing Trust in the Internet of Principles and Recommendations, which sets out the main challenges and opportunities for consumers, along with a set of principles from which specific recommendations in terms of policy, standards, testing and business practice will be developed.

Retailers of children's IoT products checklist
Developed by Consumer International, this retailer checklist lists the key privacy and security considerations that retailers of children's connected products need to be aware of when selling such toys. Through the checklist, retailers are able to vet potential suppliers against a set of simple criteria to ensure that the products they stock meet a basic standard of safety for the end user. It is not intended as a replacement for mandatory or voluntary standards that are in development but is a useful tool while these are in development.

The checklist has been informed by technical experts in both system security, penetration testing and by Consumers International's members work in digital

standards, cybersecurity and product safety, principles for the internet of things and national governmental codes of practice.