Online Trust Alliance
an Internet Society initiative

Top Vulnerabilities in Consumer-Grade IoT Products

The advent of connected things in our day-to-day lives brings the promise of convenience, efficiency and insight, but also creates a platform for shared risk. Juniper Research projects that more than 38 billion Internet of Things (IoT) devices will be connected by 2020. Ranging from fitness trackers to smart thermostats, locks and appliances, IoT represents a massive market and will ultimately redefine how people interact with the world around them.

Consumer confidence is critical for IoT to thrive and grow, yet many of today's products and services are rushed to market at the lowest possible cost, with little consideration for basic security and privacy protections. These vulnerabilities, if left unaddressed, introduce various levels of risk to both consumers and the Internet itself. Here are some examples:

- **Surveillance.** Insecure devices with cameras and microphones can be accessed to monitor conversations or activity in a home.
- **Data compromise.** Insecure IoT devices can be used as an entry point to access unencrypted data (e.g., passwords or other personal information) on the network, or data residing on laptops, tablets and other devices on the same network.
- **Physical access or harm.** Since many smart homes now have smart locks or garage door openers, vulnerabilities can allow physical access. Likewise, insecure connected thermostats, appliances and sprinkler systems can be accessed by unauthorized parties, and be used to cause physical harm – e.g., via overheating, lack of heating or overwatering.
- **Attacking other Internet services.** As demonstrated in the 2016 Mirai botnet attacks, insecure devices can be used to target other services anywhere on the Internet, whether a specific site or the Internet infrastructure itself.

To properly assess risk, the threats profiled here should be put in the context of an overall threat model – some attacks can be executed at scale from anywhere on the Internet, while other attacks are confined to a single device within close physical proximity. Ideally, IoT devices should be designed with sufficient security and privacy controls to minimize these risks. This will simultaneously protect and empower consumers, while minimizing the ability of these devices to attack services on the Internet or the Internet itself.

The Online Trust Alliance (OTA), now an initiative of the Internet Society, developed a recommended set of core actions – the IoT Trust Framework – which contains principles that address common security and privacy vulnerabilities. These top vulnerabilities include:

- **Default/hardcoded passwords.** Many devices ship with easily discoverable default or hardcoded passwords, which can be used to remotely access and commandeer IoT devices.

- **Inability to update software/firmware.** To reduce cost and maximize battery life, many IoT devices have minimal processing power and memory and therefore cannot be updated. As a result, discovered security vulnerabilities may not be able to be patched.
- **Software/firmware vulnerabilities.** Many IoT devices utilize off-the-shelf third-party code that has not been thoroughly tested from a security standpoint, and/or are not tested as a system before release. This leaves devices exposed to known attacks.
- **Authentication vulnerabilities.** Nearly all IoT devices utilize some kind of wireless connection (e.g., WiFi, Bluetooth, etc.), yet many allow unauthenticated connections making them easy to access and therefore compromise. Similarly, software or firmware updates should only be possible via an authenticated source (e.g., signed code over a secure connection), but this is often not the case. Finally, many devices are also accessible via Telnet or other protocols that bypass typical login procedures, leaving the device exposed.
- **Lack of data encryption.** Due to resource constraints, many IoT devices do not support encryption of data in transit or at rest. This leaves the data exposed so that attackers can view or modify passwords, settings and other personal information.
- **Security status of apps and backend services.** While the focus is often placed on IoT devices and sensors, it is just as important to secure the applications that control the devices and the backend services that support them. A broad range of vulnerabilities can exist within these categories, ranging from lack of encryption to improperly configured security protocols to code that is not thoroughly tested.
- **Ability to delete data on device/services.** Though at first glance this may not seem like a vulnerability, many IoT devices and services do not allow data to be deleted if devices are lost, stolen or transferred to another user, potentially leaving highly sensitive data exposed.
- **Use of collected data.** Again, though on the surface this may not be an obvious vulnerability, many IoT vendors do not clearly disclose what data they are collecting, how it will be used and whether it will be shared. Understanding the vendors' stewardship of data is an important element of consumer empowerment, allowing them to have better choice and control over collection and use of their data.

The Online Trust Alliance is an initiative within the Internet Society (ISOC), a global non-profit dedicated to ensuring the open development, evolution and use of the Internet. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, ethical privacy practices and data stewardship. https://otalliance.org/iot

R0402

