Particle

Security Checklist for the Internet of Things

An essential guide to securing connected products

January 3rd, 2017

By the end of 2020, there will be 21B IoT devices worldwide,[**] creating a massive network of self-driving cars, connected energy grids, and smart appliances. As innovative companies build towards this connected future, they must constantly evaluate the risks that come with these large IoT networks.

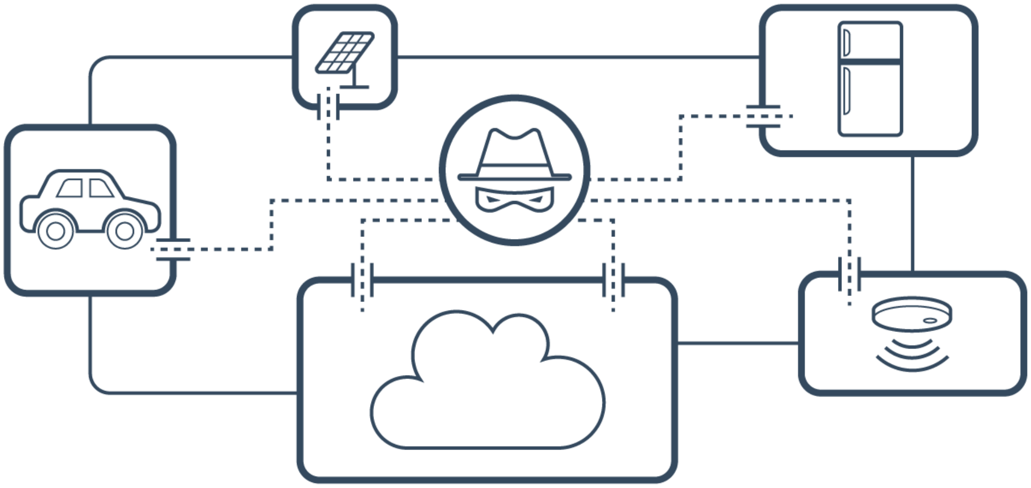
This paper will detail the unique risks of connected devices and best practices for IoT security. It is based on the advice of experienced professionals and leaders in this emerging field. It includes:

- An Exploration of Security Risk (3)
- A Security Checklist for IoT Products (5)
- The Particle Approach to Security (7)
    - Device Protocol Security
    - Hardware and Device Security
    - Cloud Security
    - Physical Security
    - Company Policies

Selecting an IoT platform can mitigate risk if the platform has implemented appropriate, full-stack security practices. These practices extend from the device hardware to the cloud.

[**] http://www.gartner.com/newsroom/id/3165317

An Exploration of IoT Security Risk



In October 2016, a botnet of IoT security cameras, set-top boxes, routers and similar devices attacked Dyn, a prominent domain and service provider. Dyn underwent a massive internet outage that cost millions of dollars in productivity losses alone. In the wake of the Dyn hack, many decision-makers realized that they needed to consider not just functionality, but security and reliability as key features of the IoT platforms they were buying and building.

The Dyn hack, while the most visible, is not the only example of critical IoT security failures in recent years. Vulnerabilities in some solar panels allow hackers to spy on and control power access to homes. Security holes in certain toys exposed images of children and their parents to malicious third parties. In industry and consumer fields alike, security has already been compromised and data lost.

To protect devices, customers, and businesses, decision-makers must be vigilant about the unique risks of an IoT system. These risks include:

Customer Data Exposure

Many IoT devices measure and transmit sensitive data. Fitness trackers, heart rate monitors, sleep trackers, and security systems all transmit data that could be used maliciously.

Corporate Data Exposure

When connected directly to a company's data center, IoT devices open security holes fundamentally outside the expertise of most in-house IT staff. These systems may cause catastrophic vulnerability and data loss.

Physical Damage

Many IoT products contain actuators which can physically harm customers if they are improperly triggered. Heating elements found in connected ovens and coffee makers can potentially cause a fire. Connected cars can be shut off mid-drive, or have their brakes disabled by a third party.

High-Risk Downtime

Some IoT services can pose fatal threats in the case of service failure. Connected medical devices must still function correctly when offline. An automated pet feeder could endanger the life of a pet if the service supporting it has unplanned downtime.

Broader Liability

As detailed above, IoT hacks can create liability for physical harm that goes beyond data loss or identity theft. Hacks to these products can have existential life and property liability, which has been shifted to the companies producing connected devices.

Reputation and Brand Damage

Brand-focused corporations can suffer massive losses in the wake of a security attack. With numerous outlets online and off, consumers have increased voice and impact. Companies must guard against any large scale news event that damages reputation.

A Security Checklist for IoT Products

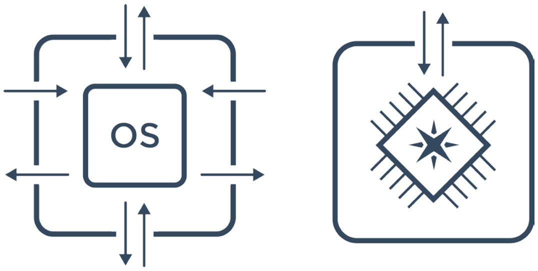
Developers and decision-makers can combat the unique risks of IoT by preventing potential attacks and taking actions to ensure the continued safety of their connected systems. This checklist covers areas to review in creating a **minimal attack surface area**, as well as **features and actions** key to maintaining a secure system in a rapidly evolving field.

Minimal Attack Surface Area

Reducing potential attack vectors is crucial to building a secure system. The following components of an IoT system must be reviewed for possible vulnerabilities:

Operating Systems

Each open port and available protocol is a potential point of attack. Code on microcontroller units (MCUs) runs "bare metal" with no supporting operating system; each type of communication required by a product is intentionally added by the product developer. In contrast, many SOCs and Linux systems have multiple open ports by default, adding a vast array of attack vectors product developers may not even be aware of.



Systems built on SOCs leave more potential points of attack than those built on MCUs.

Applications

Applications running on devices may contain security holes. It is important to audit and sanitize these programs to ensure a safe experience. The more programs running on a device, the larger the task of auditing those programs for security.

Dependencies

Outside code dependencies such as libraries must be kept up to date and validated to comply with modern encryption and communication protocols. As with application security, a larger number of dependencies requires more work to maintain.

Communication

All communications between the device and the cloud should be encrypted to ensure confidentiality, integrity, and authenticity. This is critical to preventing man-in-the-middle or replay attacks against IoT infrastructure.

Cloud

Securing a cloud or cloud servers requires minimizing the network, application, and dependency risk for each server.

User Access and Security

Granular access controls prevent users from controlling applications or devices that aren't theirs. Two-factor authentication and strong password requirements prevent compromise through lax user security.

Features and Actions

All systems require maintenance to stay ahead of evolving security risks. The following features and actions help prevent future vulnerabilities.

Penetration Testing

Businesses can stay ahead of modern hacking techniques by repeatedly testing their systems with security researchers and fixing potential vulnerabilities as they develop.

Firmware Application Code Reviews

Security experts can sanitize application flaws during firmware development, preventing fatal application flaws at a customer level.

Security Update Mechanisms

Security protocols change and improve over time. Allowing for rapid firmware deployment to all devices at once improves security.

A comprehensive IoT platform with encrypted connectivity is critical to success. In an extremely risky landscape, it is important to pick an experienced partner to help navigate security risks. The best partners openly assess the evolving security risks unique to hardware, and provide insightful recommendations based on experience. Whether you choose Particle or a different IoT partner, we hope you will follow these essential recommendations in building a safe and secure connected product.

The Particle Approach to Security

At Particle, security is a constant consideration in every decision we make. We take the security of our cloud, our customers, and their devices and data very seriously. Every device is protected with the same powerful encryption and best practices, from your first prototype to a high-profile product release. Although no system can ever be perfectly secure, Particle is committed to be an industry leader in security and happy to be transparent about our practices.

Particle's platform is designed to be used at every stage of the product lifecycle, from prototyping to production. Our state-of-the-art platform provides a secure, scalable infrastructure for IoT products, as well as easy-to-use tools for managing your devices and the software that they run. Particle is the most widely used Internet of Things platform, with a community of more than 100,000 companies, developers, and engineers deploying products in over 170 countries.

The platform includes important features such as:

- A fully managed hosted cloud infrastructure with guaranteed service levels (SLAs)
- Encryption and security applied to all communications to and from your devices
- Secure and encrypted communications across cloud integrations
- Easy-to-use management tools that give you full visibility into your "fleet" of devices
- SIM cards and data plans for cellular-connected devices
- Low-cost hardware pre-provisioned to the platform
- Portability to mitigate technology lock-in risk

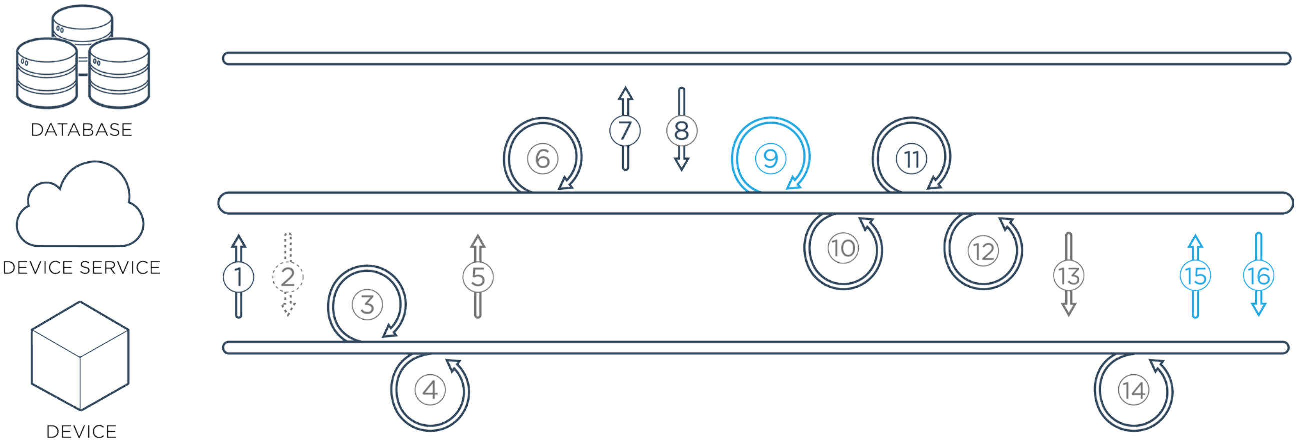
While some customers deploy products using the self-service tools, Particle also provides an array of professional services to help customers develop and deploy products.

- Software development and custom integrations
- Support for preferred hardware architectures
- Embedded software development
- Design reviews
- Project management and consulting services
- Premium enterprise Support options

Device Protocol Security

Communications between the Particle Cloud and each Particle device are encrypted by default. Every device ships with a unique device-specific RSA or Elliptic Curve key-pair, and has a pinned Cloud public key. The device public key is typically pinned in the cloud during manufacturing, but can be updated later by an authorized user. Strong unique keys and bidirectional pinning help prevent man-in-the-middle attacks against devices and data.

Particle's TCP service uses an RSA handshake to establish a session key for a fast rotating AES-128-CBC session. Each message is encrypted and is checked via a message id for replay attacks or out-of-order messages. Any anomaly in the session causes it to immediately end. Although all Particle devices include hardware random number generators, the RSA/AES cloud handshake includes a cryptographically random nonce, to ensure there is sufficient randomness on these low-power devices.



┈ Plaintext
▭ RSA keypair encrypted
▭ AES encrypted

1. Open TCP connection
2. 40 byte random nonce
3. Retrieve Server Public RSA key
4. Encrypt using key 40 byte nonce + 12 byte Device ID + optional 162 byte Device Public Key = 256 bytes
5. 256 byte ciphertext
6. Decrypt ciphertext using Server Private RSA Key
7. Device ID
8. Device Public RSA Key
9. Generate 40 bytes = 16 byte key + 16 byte IV + 8 byte salt
10. Encrypt 40 bytes using Device Public Key = 128 byte session key
11. Create HMAC from 40 bytes using SHA1
12. Sign HMAC with Server Private Key = 256 byte signature
13. 128 byte session key + 256 signature
14. Decrypt and Verify with Device Private Key & Server Public Key
15. "Hello" message with product_id and fw_version counter = 4 MSB of IV encrypted with AES Session Key
16. "Hello" message with counter = random encrypted with AES

The encrypted handshake in the Particle TCP service.

Particle's UDP service uses DTLS, a version of TLS designed for low-bandwidth and lossy UDP packets. TLS is the new standard for secure browser traffic worldwide. Particle leverages the open source mbed TLS library supported by ARM and used by other security conscious companies such as OpenVPN, nginx, and Linksys. 256 bit ECC keys are used for the DTLS service, roughly equivalent to a 3072-bit RSA key.

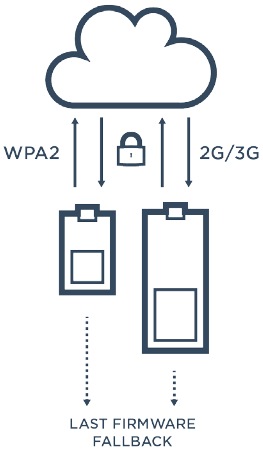
We believe that strong crypto should be based on established best practices and algorithms, and that the use of these standards should be transparent. If a secure communications system can't withstand public scrutiny, then it's not sufficiently secure. This is why we've open sourced our encryption protocols and techniques. All the device communication source code is available here:

https://github.com/spark/firmware/tree/develop/communication/src

Hardware and Device Security

Maintaining a secure, authenticated connection to the Particle Cloud gives you confidence to deploy firmware and issue commands to your devices. Secure by default, Particle devices don't leave any incoming ports open for port scanners or active side attacks. Radio connections are encrypted by industry standard WPA2, or standard 3G / 2G radio protocols. A secure device protocol adds future proofing and end-to-end encryption to the cloud on top of existing secure radio protocols.

The device is also protected against failures during the Over The Air (OTA) firmware update process. Each firmware module includes a verifiable hash and metadata to ensure the code is appropriate for that platform and product. If a corrupted firmware is sent to a device, or a mismatched firmware for that product, the device will safely fall back to the last known good firmware stored locally in flash. Product Creators can also pin a known version of firmware for their products, which the cloud will enforce, to help ensure your customers are getting the best experience. The firmware is also split into modules, so the speed of the update is as fast and as low risk as possible, minimizing any interruptions during an upgrade.



In the case of a failed or corrupted OTA firmware upload, the device will fall back on locally stored good firmware.

Additionally regardless of whether the device connects via Wi-Fi, Cellular, or other radio protocols, the network authentication credentials are never transmitted to the cloud, and are only stored locally or on a SIM card.

Cloud Security

Particle exercises best practices and cutting-edge cloud operations to minimize attack surface area in both the service layer and data. The Particle Cloud uses best-in-class hosting with ISO 27001, 27017, and 27018 physical security and risk management, and Particle monitors and tests its infrastructure regularly for potential vulnerabilities.

Particle reduces its attack surface area through a variety of techniques. API-based attacks are filtered out with a scalable traffic load balancer. The API utilizes a 2048-bit TLS certificate and is accessible only via HTTPS. It also supports the OAuth 2.0 standard for secure login for integrations, with strongly salted and hashed passwords likely to resist brute force attacks and compromise. Furthermore, Particle intentionally limits the scope of user-data stored in the cloud. As a matter of policy, the Particle Cloud does not store any personally identifiable information or data that could be used to compromise products or customers.

FIREWALL PROTECTION
SCALEABLE CLOUD
MINIMAL ATTACK SURFACE AREA
PENETRATION TESTING

Essential elements of Particle's cloud security.

Server availability zones are housed in a secure, firewalled private network, and each box is also strictly firewalled both within this network and from the internet in general. Particle uses a sophisticated dev-ops system of automated deployments, containers, and service checks to automatically ensure servers are up-to-date, and running only the expected applications. Servers are protected with a variety of automatic intrusion detection software to discourage automated attacks. Additionally, Particle engineers routinely destroy and re-provision boxes to reduce the risk or scope of any undetected issues or lingering old versions of libraries or other software. Human access to these boxes is severely limited to a trusted server operations team, and that access is granted only via a single bastion host, which is strictly monitored.

Particle services are designed from the ground-up to scale horizontally. This means that the Particle Platform can scale infinitely to uniform machines in the face of an attack or large customer demands. Businesses, developers, and customers depend on Particle to be available and responsive, and performance is a crucial aspect of security. A fully instrumented and scalable Particle Cloud is also available for private deployments when data and availability isolation are key to your IoT strategy.

Particle regularly hires professional penetration testing consultants to proactively prepare for any emerging threat models. We also engage in an open dialogue with a large, security-conscious community of developers and researchers. This active conversation helps us stay ahead of potential customer concerns and improves the Particle Platform for all of our customers.

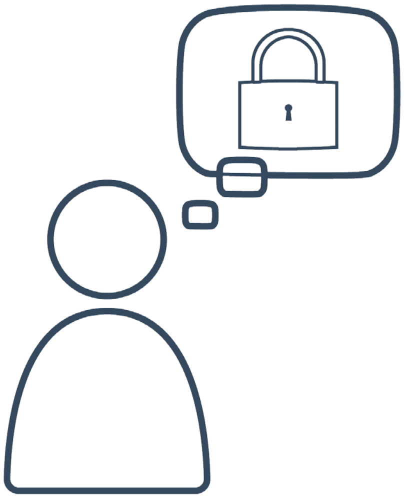
Physical Security

Particle ensures the physical security of our servers by using best-in-class hosting via established and trusted hosting companies. AWS is used when possible. Information on AWS's best security practices can be found here:

https://aws.amazon.com/security

Trusted cloud hosting vendors protect against physical threats such as fire, natural disasters, power or connectivity outages, hardware failures and more. Furthermore, the Particle Cloud utilizes multiple geographically disparate availability zones to protect against catastrophic data center failure.

Company Policies



At Particle we recognize that security doesn't stop at our APIs or services or devices. Our colleagues and our actions as a company are part of our security model. By being open and transparent, and by encouraging a positive conversation with our community and our product creators, we create the best opportunity to learn and adapt to new threats.

New employees at Particle are required to use two-factor authentication for any service that supports it, and their workstations must use full-disk-encryption. New employees go through social engineering training, and every Particle employee must use a password management application to generate strong, random passwords for every account they access. When we need to share secrets internally, they are strongly encrypted using a trusted, employee specific public RSA key, and that message is destroyed afterwards.

We celebrate our security culture by playing security games and staying current with trends and best practices. This creates a positive atmosphere and increases adoption of simple practices such as locking your workstation, or not connecting an unknown / found device to a trusted network.

We encourage our community to practice ethical disclosure. This means they know they'll be rewarded and celebrated if they bring us new security risks first, instead of ignoring them, or keeping them secret or selling them to another company. Every Particle employee knows to escalate anything resembling a security bug or issue to the engineering team, and that team knows to evaluate and address that concern as soon as possible.