IoT Security: A Perspective

Bret Jordan, CISSP
Chief Security Strategist, Afero
Chair, UN ITU-T SG17 Working Party 2

Overview

With the explosion of consumer electronics and connected devices, enterprise networks are no longer the sole target of intrusion sets and threat actor campaigns. Most consumer electronic devices on the market today are generally insecure, do not follow secure development strategies, and are not patchable in the field because doing so is hard, takes significant time, and ultimately costs a lot of money. This makes these devices easy to compromise remotely, causing security and data privacy issues for organizations and consumers. In addition, once compromised, these devices can serve as a launch point for attacks on higher-value targets (e.g., the Dragonfly cyberattack). Organizations and consumers need products and solutions that are secure by design and only use secure building blocks. This is the strategy Afero has adopted through its unique IoT Platform as a Service.

The Afero Way

Information security and data privacy are critical elements in a modern holistic cybersecurity and risk management strategy. This means organizations need to more fully understand their attack surface, posture, and risk profile to combat the ever-increasing activity and targeted campaigns from intrusion sets and threat actors. Afero has taken the following steps to ensure good security practices and to enable consumers to be confident in using Afero connected products:

Standalone Instance

Afero provides a standalone instance of its cloud platform for each customer, ensuring a complete separation of customer data and logs.

Data Privacy

All traffic between Afero-enabled products and the Afero cloud uses mutually authenticated end-to-end encryption based on an elliptic curve Diffie-Hellman key exchange with AES-GCM session keys. This is in addition to any radio- or transport-level security/encryption, such as TLS, WiFi, etc.

Born Secure

All Afero modules are securely provisioned, programmed, and encrypted at the factory by Afero technology. This enables a complete and secure supply chain for product manufacturers and ensures that modules cannot be modified or changed after they are created. In addition, the Afero factory programming process locks and disables on-chip debugging hardware to protect the firmware and modules from direct hardware attacks. In conjunction with these safeguards, key generation and key management are designed

so private keys are generated on the device and never leave the device. Further, a compromise of any individual device does not compromise any other Afero devices.

No Device Services

Unlike most IoT devices on the market, Afero-enabled products do not run services or daemons exposing open ports. This means end users and threat actors cannot talk to the devices directly, as the devices can only talk with the Afero cloud, and only via mutually authenticated end-to-end encrypted channels. This greatly reduces the traditional IoT attack surface.

Device Updates

All Afero-enabled products are over-the-air updatable, and patches are routinely and securely pushed to products after review and acceptance by the corresponding customer.

Security Compliance

Afero is developing and implementing policies, processes, and procedures to ensure SOC2 and ISO27001 compliance. Other certifications, such as NIST CSF, EN 303 645, and CMMC 2.0, are also under review.

Secure Code

Source code for all Afero products is tightly controlled and routinely audited. All libraries used by Afero solutions are routinely monitored for vulnerabilities and patched accordingly.

Third Party Testing

The Afero technology is routinely tested by third-party pentesters, red-team experts, former government agency professionals, and third-party testing labs to ensure that the devices are secure. If any issues are found, they are promptly resolved. Given the high degree of security that Afero implements in its products, ioXt uses Afero products as the baseline when evaluating new companies that wish to test and certify other IoT products on behalf of ioXt. In addition to ioXt certifications, Afero is actively pursuing other certifications for its products.

Cloud

Afero runs its cloud on the Google Cloud Platform (GCP) thus ensuring high availability, low latency due to Google's layer 3 peering strategy, and a robust security solution.

Data

All data in the Afero platform is encrypted both at rest and in transit. Personally identifiable information (PII) and other sensitive data are further encrypted using AES256 with partner-specific keys.

Customer Networks

There is no direct connectivity between our customers' corporate networks/clouds and the Afero platform. As such, there is no risk of lateral movement in either direction in the event of a compromise on either side.

Disaster Recovery

The Afero infrastructure runs on GCP and has full redundancy and a verified and tested disaster recovery plan. Afero also stores redundant, immutable, and separately encrypted snapshots of the Afero cloud with different cloud providers to ensure recoverability in the event of any disruption.

Closing Thoughts

Afero has a mission to deliver world-class user experiences for devices that are secure by design, with no way for the device to be made insecure. This is made possible by the core team at Afero, which has decades of experience working on secure systems and solutions for companies such as Google, Apple, Nest, Symantec, Danger, Microsoft, Amazon, Twitter, Netflix, Roku, Eero, and other leading platform companies. This core Silicon Valley experience has enabled us to innovate (over 130 issued US patents so far) and implement secure technologies in our solutions that other companies would deem too hard, too complicated, too time-consuming, or ultimately too costly.

4410 El Camino Real Suite 200, Los Altos CA 94022