Payatu

IoT Ecosystem Assessment of a Smart Security Device

Payatu Casestudy

Problem

Our client is a Pioneer in manufacturing smart video doorbells and wanted to test the security of their device's complete ecosystem. The device is a video-enabled doorbell that allows the owner to interact with the visitor through a mobile app from anywhere, which is connected to Wi-Fi.

This device captures video, audio, and images during an interaction. The data generated during these interactions is saved on the cloud. So, the device's ecosystem to be tested contained hardware (the device itself), the cloud that holds data, and the mobile app.

The client reached out to the Payatu team with the following:

Security Concerns

- **Data security**

The device pushes massive data on the cloud. Audiovisuals and images of visitors make the data sensitive and confidential. So, the client wanted to assess the data security for any leakages. Any compromise with sensitive data could cost a severe dent in the client's reputation.

- **IP theft**

For a device in the home automation segment, its firmware is quite susceptible to cloning. A malicious intruder could sneak away with this IP due to any loophole in the ecosystem's security.

Solution

The Payatu team performed a comprehensive security assessment of the whole ecosystem.

1. We performed a detailed analysis of the mobile app. Thus, we could successfully extract the hardcoded keys responsible for encrypting the data between the mobile app and the cloud server.
2. We could access the device using the debug interface. This helped us successfully gain root privileges by performing the command injection on the device's serial console. Eventually, we were able to extract the firmware and compromise the cloud infrastructure due to information leakage in the firmware.

Based on these security breaches, Payatu suggested an apt risk mitigation strategy to the client.

Benefits

Both, IP theft and data leakage, are nightmares for home automation device manufacturers and dealers. Data security could dent the company's reputation among the users.IP theft could have caused a severe financial loss due to cloned and cheap products.

With our comprehensive security assessment of the whole ecosystem of the product, the client managed to mitigate security concerns and avoid a substantial financial loss.

About Payatu

Payatu is a Research Focused, CERT-In impaneled Cybersecurity Consulting company specializing in security assessments of IoT product ecosystem, Web application, Cloud, & Network with a proven track record of securing applications and infrastructure for customers across 20+ countries.

Our deep technical security training and state-of-the-art research methodologies and tools ensure the security of our client's assets.

At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.

Payatu Security Consulting Pvt. Ltd.

www.payatu.com
info@payatu.com
+91 20 41207726