apriorit

CASE STUDY

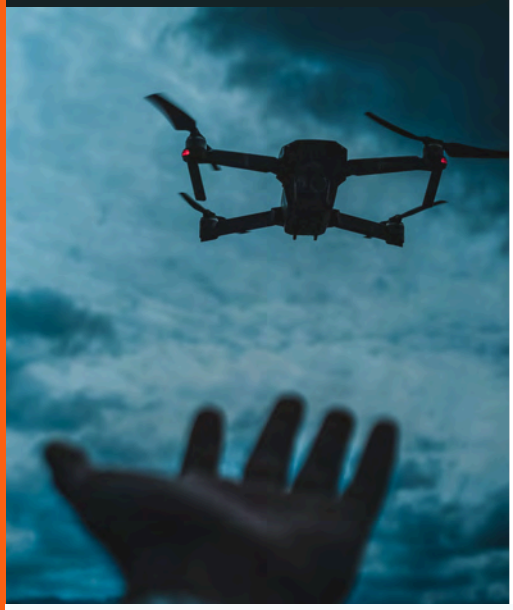
Ensuring compatibility with a closed mobile platform

REVERSE ENGINEERING

Background

In the energy sector, drones are a popular solution for infrastructure monitoring. In energy industry, drones help companies speed up and automate data collection and analysis, which in turn allows them to detect and fix issues faster and more safely.

A drone manufacturer asked us to help them integrate their hardware with a proprietary software platform used by organizations in the energy sector. They were looking for a strong reverse engineering team that could understand how a closed corporate system works and design an efficient and secure integration. Apriorit's team was up to the challenge.



The client

Our client is a US-based drone manufacturing company that builds custom drones for industrial applications.

Their hardware is popular with energy companies that need to inspect large remote networks of power lines, pipelines, solar panels, and wind turbines. Our client builds drones that automate visual and thermal inspections of such infrastructure. These inspections can be hazardous for human employees and take a lot of time when done manually.

Integration with corporate software used by energy companies is a cornerstone of our client's business.

Client:
NDA-protected

Location:
USA

Industry:
Robotics for the energy industry

Request:
Research a proprietary protocol

Our services:

- Reverse engineering
- PoC implementation for a custom protocol

The challenge

Our client encountered difficulties in integrating their screen mirroring feature with a closed proprietary platform (used by their customers) that powers operators' tablets and control stations.

This feature streams footage from a drone's proprietary link to an operator's device almost in real time and is essential for energy company operators to visually inspect their infrastructure.

Since the developer of the proprietary target platform doesn't provide device firmware, source code, or documentation, our client needed a way to ensure reliable integration. To overcome this challenge, they sought a partner who could help them define the technical requirements.

The result

Apriorit's reverse engineering team successfully researched the video mirroring protocol of the target platform.

With an understanding of how it works from the inside, our developers reconstructed the key exchange and handshake sequence. This knowledge helped our client reliably integrate their drones for solar, wind, and traditional energy infrastructure monitoring with a proprietary data management platform.

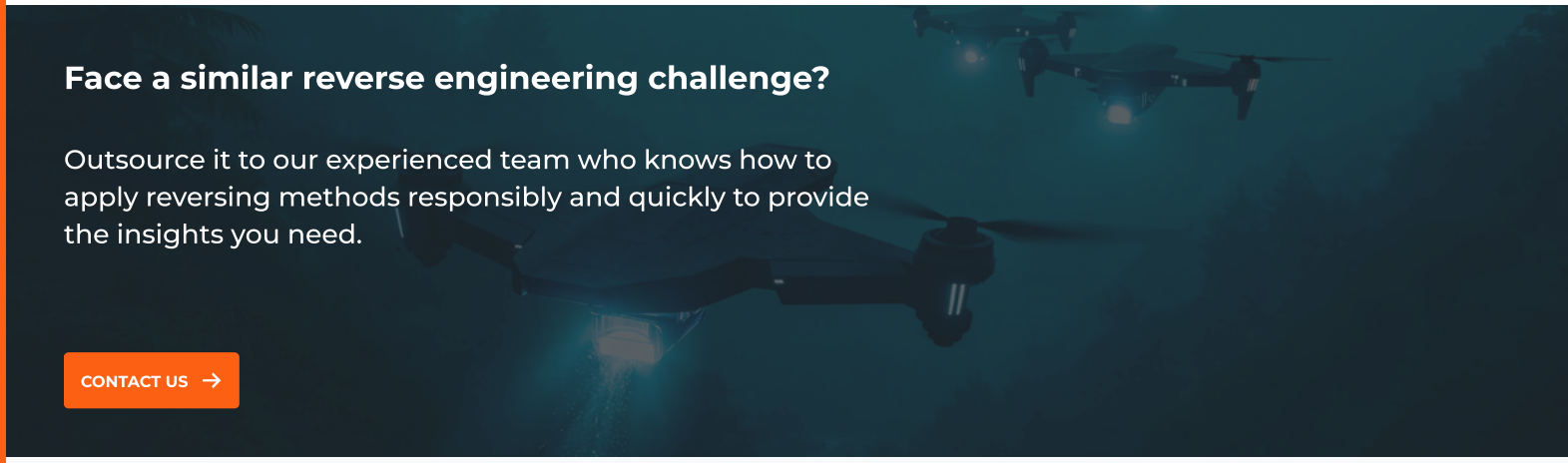
How we did it

The initial discussion with our client regarding this project provided us with a basic understanding of their expectations and requirements. To start the investigation, we gathered a project manager, reverse engineers, and developers with expertise in secure communication.

Our team assessed the client's requirements and the technical feasibility of the project, and we signed NDAs. Then, we started digging deeper into the proprietary software to understand how it works.

Note: *At Apriorit, we use our reverse engineering skills only for legitimate purposes: research, software compatibility, cybersecurity improvements, etc. We double-check all client requests with our legal team before proceeding.*

In this project, we didn't publish our findings or use them to copy proprietary solutions protected by copyright.



Face a similar reverse engineering challenge?

Outsource it to our experienced team who knows how to apply reversing methods responsibly and quickly to provide the insights you need.

CONTACT US →

Our approach to reversing device firmware

// Stage 1. Initial research of the target platform

At the beginning of the project, our reverse engineers had only publicly available information: the target device itself, firmware that was on the device, user documentation, etc. We had no clues about the internal working of the device or the way it communicates with other hardware.

After initial research of the target platform, we determined that our reverse engineers needed to analyze the handshake mechanism with key exchange used specifically for screen mirroring. Their findings would serve as a basis for the future development of custom functionality.

Stage 2. Reverse engineering the video mirroring protocol

As we started firmware reverse engineering, we realized that the handshake protocol used in the proprietary platform was complex and involved numerous undocumented functions.

To understand the undocumented code, we applied a combination of reverse engineering methods. For some parts, we used well-known methods like static and dynamic analysis, fuzzing, and protocol reconstruction. For more complex parts, we turned to nuanced approaches that our experts have created over years of reverse engineering software.

We discovered that the firmware used RTSP for screen mirroring, WebSockets for trusted authentication, and QUIC to improve the speed of stream transmission. This information was enough to understand how the protocol normally works and formulate a task for our engineers to build a prototype.

Stage 3. Prototyping the protocol

Our goal for this stage was to build a prototype for an improved version of the screen mirroring protocol that would connect our client's drones with energy operators' tablets. We needed to demonstrate to our client that this could be done securely and without infringing on protected intellectual property.

One of the techniques we employ to ensure the safety of reverse engineering results is clean-room design. This software development technique creates a division between the reverse engineering and development teams: developers only have access to the task and insights formulated by reverse engineers but not to the reversed proprietary code.

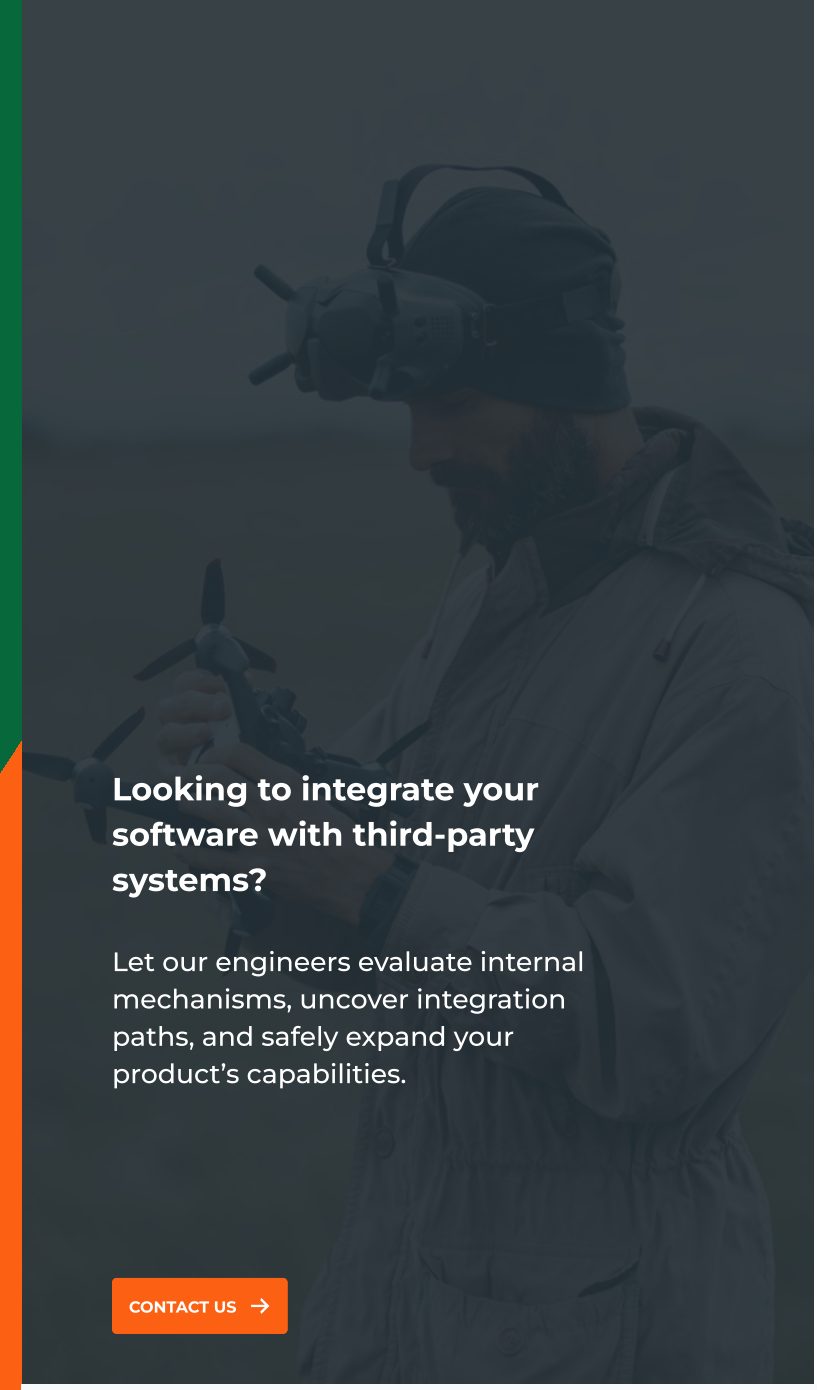
We built a simple proof of concept for a screen mirroring protocol that performed a full handshake process with the client's device.

Impact

Apriorit's research and prototype showed the client how they could extend their solution to a closed platform in an ethical, secure, and efficient way.

Using our prototype as the basis for their solution, the client designed a clear roadmap for developing device screen mirroring functionality and quickly implemented this feature. With extended support for other platforms, their drone software was better suited for customers in the energy sector. This improvement was crucial for boosting sales and solidifying our client's position in the industry.

> Our internal development team hit a wall with this task. Apriorit provided strong engineers, and their communication was clear and consistent throughout the project. Their team works both smart and hard. Most importantly, they delivered exactly what we wanted and within the agreed deadlines.



Looking to integrate your software with third-party systems?

Let our engineers evaluate internal mechanisms, uncover integration paths, and safely expand your product's capabilities.

CONTACT US →