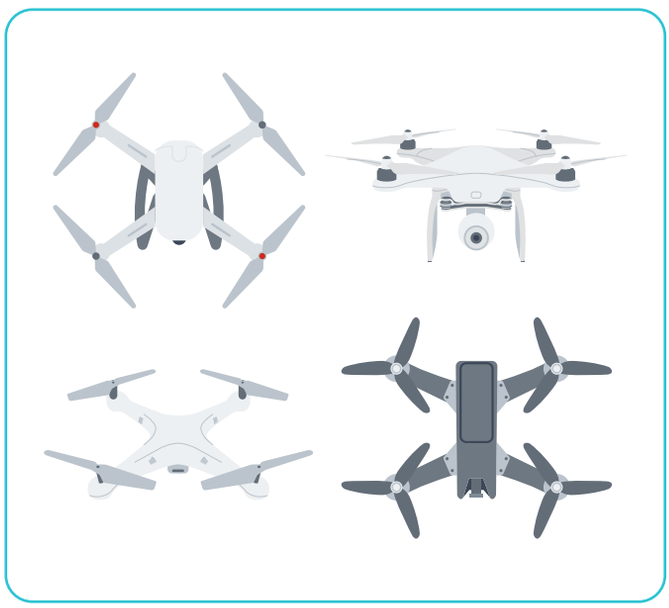
CyberDanube:
Drone Cybersecurity Testing

In-Depth Technical Security Assessments of a Drone

Unmanned Aerial Vehicles (UAVs), commonly known as drones, play a growing role in both civilian and military sectors. Civilian uses include agriculture monitoring, infrastructure inspection, aerial photography, and delivery services. In the military domain, drones are deployed for reconnaissance, targeted strikes (including kamikaze-style attacks), surveillance, and perimeter patrols.

However, these capabilities come with significant security risks. If a drone is hijacked—whether by a malicious actor or even the original vendor maintaining covert access—it can compromise sensitive operations, leak data, or be turned against its operator. Such vulnerabilities highlight the critical need for robust security controls in both hardware and software layers of UAV systems.



Preparation

The preparation phase of a drone penetration test begins with defining the scope during a kick-off meeting. For drones equipped with smart, cloud-connected flight control systems, this scope must include not only the drone itself but also its ground-based counterpart—commonly referred to as the drone platform or drone dock. These docks are typically connected to the internet via Wi-Fi or Ethernet and serve as critical communication hubs. As such, including them in the assessment is essential.

Cloud-enabled drones can be operated remotely through various devices via cloud platforms. In contrast, more cost-effective drones without cloud integration connect directly to a handheld remote controller, often paired with an internet-connected mobile phone. In these cases, the phone and the associated drone app become the central communication interface.

A thorough technical drone penetration test covers all relevant components: the drone, its dock (if present), and the remote controller. The assessment evaluates hardware, firmware, and software—including any associated cloud platforms. However, testing self-developed or proprietary cloud platforms may be limited unless the vendor's API access is available, which is often a constraint in real-world engagements.

Technical Assessment

- Hardware Inspection and Memory Extraction
- Mobile App Testing
- Firmware Emulation and In-Depth Analysis
- Fuzz Testing of Various Network Services (Drone Platform / Dock)
- Reverse Engineering of Update Procedure and Proprietary Protocols

When conducting a technical assessment of drones, we evaluate the entire ecosystem - not just the drone itself. This includes the base station, such as the remote controller or docking platform. Our experience has shown that critical smart components (both in hardware and software) are often embedded in the remote control or platform rather than the drone.

The drone typically functions as a connected sensor or actuator, transmitting measurement data and video stream. As such, our focus during civilian drone testing is primarily on wireless communication interfaces. In military-grade drones, particularly those with self-destruct capabilities, fiber-optic connections are also used for performance and security reasons.

The most valuable target during testing is often the base station. If it can be hijacked or emulated, full control of the drone is possible. To assess this, we extract and analyze memory from the platform or dock, or in the case of lower-cost drones, we reverse-engineer the associated mobile application to uncover security flaws and potential entry points.

With the help of CyberDanube's digital twin framework MEDUSA we have the major advantage of identifying vulnerabilities in the platform/dock and fuzz test services of this part effectively on scale. We also leverage the advanced tooling provided by MEDUSA to do accelerated reverse engineering of the platform/dock.

Typical Challenges

- **Extracting Memory** – Disassembling the drone and the platform/dock without destroying memory chip.
- **Reverese Engineering the Mobile App** – Such apps are often obfuscated and use anti-debugging techniques.
- **Limited Scope** — The cloud is often out-of-scope as the vendor usually do not give permission for testing.

Technical drone assessments come with several recurring challenges. Memory extraction is a especially challenging — disassembling drones or platforms without damaging the memory chip requires precision and experience. If we are successful when sniffing firmware updates during network transit, we often face encrypted or proprietary formats. Reverse engineering the mobile apps is also difficult, as they're typically obfuscated and protected with anti-debugging techniques. Scope limitations are also a usual issue. Cloud components, essential for many drones' operations, are often off-limits due to vendor restrictions.

Typical Findings

- Backup/Backdoor Connections
- Vulnerabilities in Firmware Update Process
- Outdated and Vulnerable Software Components

A typical finding during an assessment of UAVs is a so-called backup channel to the vendor. It is intended to fix the operating system of the drone or its platform/dock with this kind of additional channel but this could also be abused by the vendor. Therefore, we classify such findings as Backdoor connections in case of an occurrence. Other problematic issues which we are often facing during drone testing are vulnerable firmware update processes. It leads to a so-called jailbreak of the drone, which means that a 3rd party firmware can be uploaded to the drone or its base station. A general problem which we frequently see are outdated and vulnerable software components in devices. This does not exclusively applies to drones and the ecosystem but poses a problem in many embedded devices.

Such findings often let us write a full exploit-chain to take over control over the drone.

Experts Contact

Thomas Weber
Industrial Security Expert

Sebastian Dietz
Industrial Security Expert

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Pentest of an OT Infrastrucutre or an IoT/IIoT/Embedded Device (e.g. a Drone),

get in touch with us: office@cyberdanube.com

This Whitepaper has been inspired by real word projects.