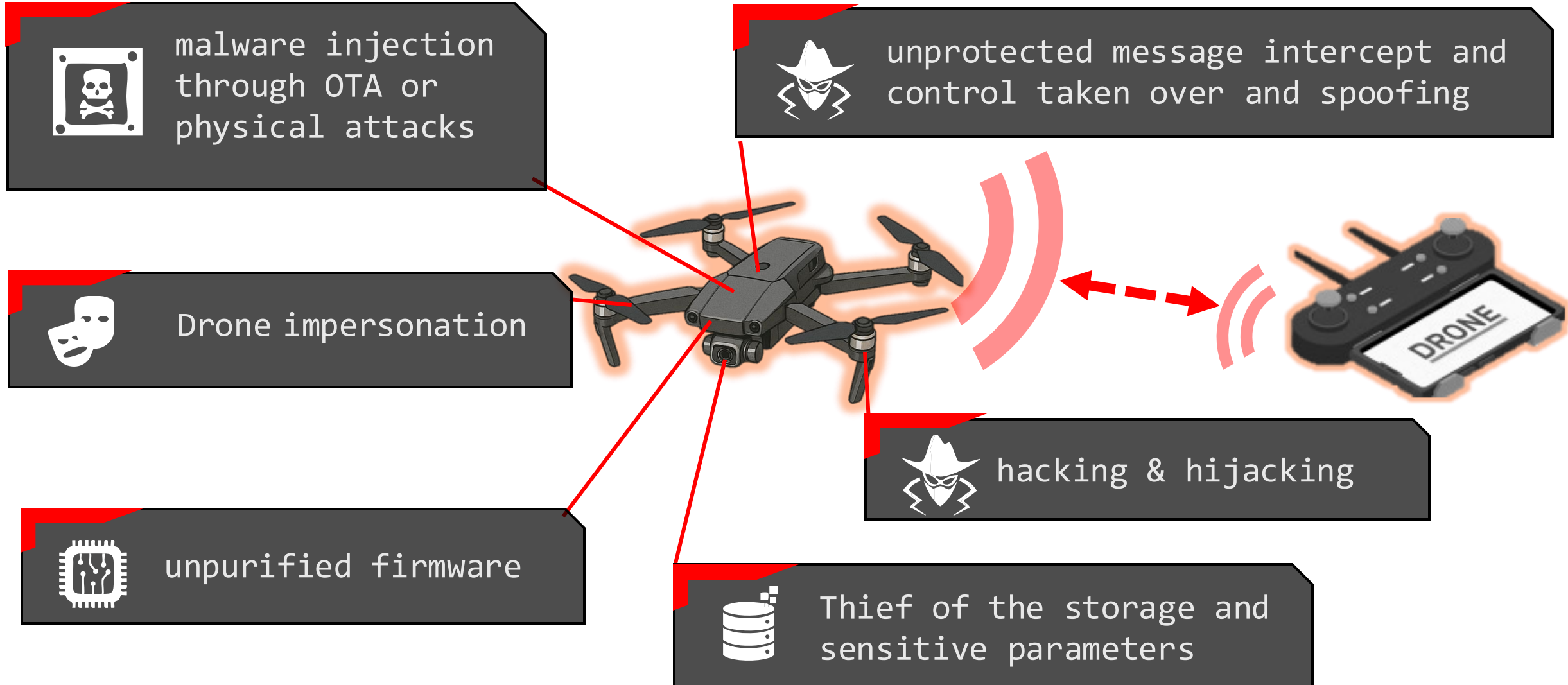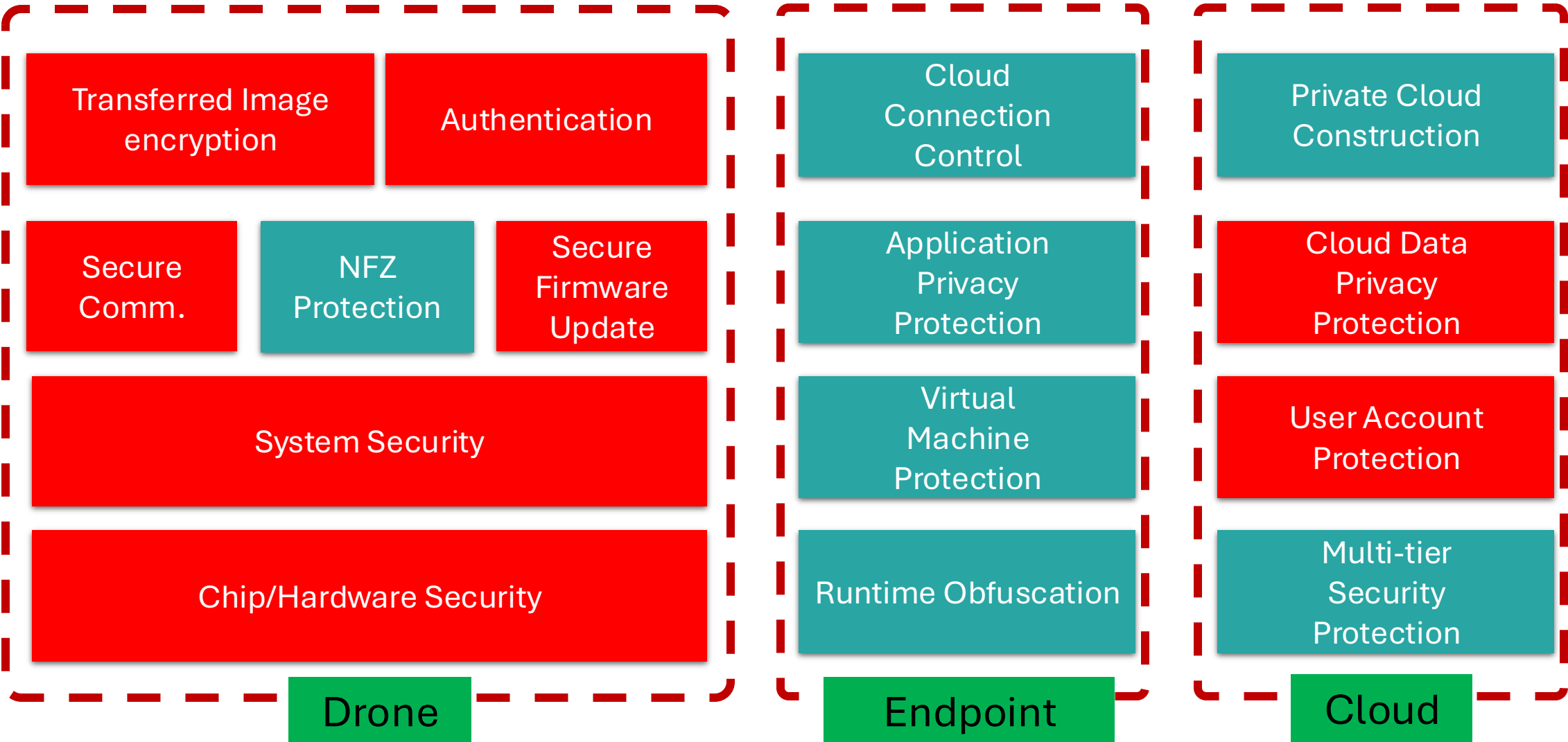# WiSECURE Drone Security Solution Brief

May 2025

Security Risks in the Drone

malware injection through OTA or physical attacks

unprotected message intercept and control taken over and spoofing

Drone impersonation

hacking & hijacking

unpurified firmware

Thief of the storage and sensitive parameters

Required Solution in "Drone Security Guide"

Drone

- Transferred Image encryption
- Authentication
- Secure Comm.
- NFZ Protection
- Secure Firmware Update
- System Security
- Chip/Hardware Security

Endpoint

- Cloud Connection Control
- Application Privacy Protection
- Virtual Machine Protection
- Runtime Obfuscation

Cloud

- Private Cloud Construction
- Cloud Data Privacy Protection
- User Account Protection
- Multi-tier Security Protection

『 Drone security guide v.5.0. 』 https://www.secure-drone.org/news/2024/0603-drone_security_guide_r5/

WiSECUREtech

Drone Protections: Chip/Hardware Security

Lightweight, hardware-based Root-of-Trust (RoT) as a Hardware Security Module

	Wisecure VeloCrypt™ MicroSD HSM	**WAP-USPO-FB196** XXXX XXXXX-XXX	**kvSoftKey**
Adoption	microSD Slot on PCBA	PCBA Layout	SoC CPU
Integration efforts	F/W modification (in weeks)	F/W re-design (in months)	F/W modification (in weeks)
Features highlighted	• Secure boot and HSM • Authenticated access • Protected storage	• PQC-ready • Versatile interfaces available • HSM with the high-performance AES	• Firmware library • Bundled with the CPU (32/64-bit architecture required) • Simple HSM
Product Brief	[Product Brief]	[Product Brief]	[Product Brief]

wisecuretech

WiSECURE Inc. was founded in 2024, aiming to design standardized hardware security modules in various form factors, including PCIe cards, microSD cards, USB tokens, etc. WiSECURE specializes in cryptographic implementation and key management, which are fundamental in storage encryption, authentication, emerging digital assets, industrial control, IoT, WFH (Working from home), digital rights managements (DRM) and other innovative services and applications.