PEN TEST PARTNERS

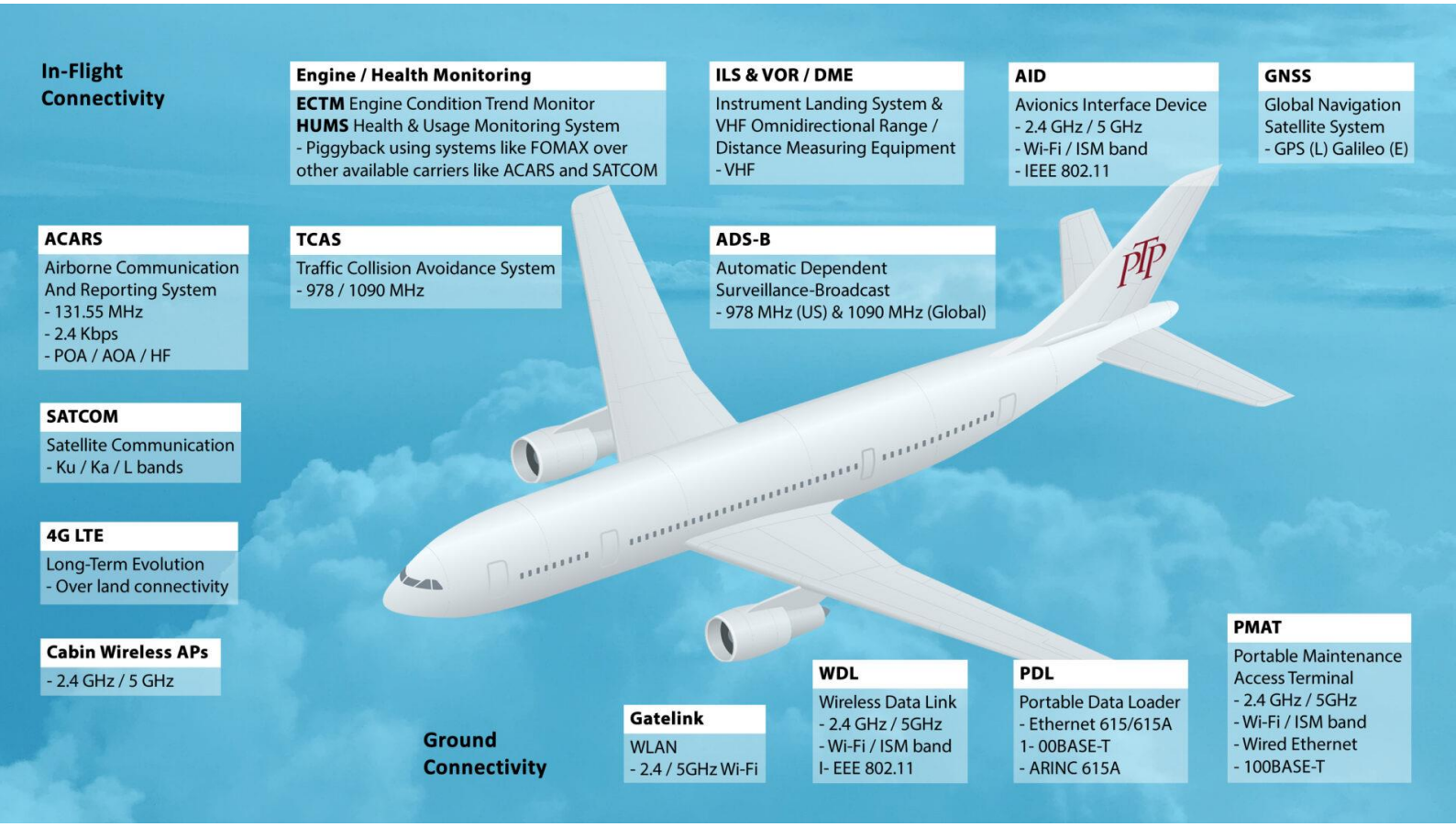
Contact us today:
info@pentestpartners.com
+44 (0)20 3095 0500

Aviation Cyber Security

UK Civil Aviation Authority ASSURE

Securing Airplanes & Airports

For a long time, the primary security model for airplanes has been physical. Airside security controls are there to prevent access by unauthorised personnel. However, as connectivity with e-enabled aircraft has increased, for reasons of efficiency, safety and passenger convenience, the physical security model has been eroded. Whilst press stories of 'airplane hacking' are often misleading, particularly owing to strong domain segregation, multiple redundant systems and human pilots in the loop, security of avionics and airborne networks is still essential.



When on the ground an aircraft's communications with the airport and their company are prodigious, using Wi-Fi and other RF protocols to exchange data, but also simple crew laptops/tablets and phones in the briefing room.

The biggest single challenge is the sheer volume of different entities that need access: passengers, crews, airline staff, security personnel, Police, Customs and other government agencies, freight, meal service and many more.

Dedicated Aviation Security Services

Electronic Flight Bags and Applications

EFBs are now categorised as "portable" or "installed" and can run different "classes" of applications. Regardless of the type of device it must be robustly secured against tampering and interception, whilst at the same time being available for the pilots to use quickly in an emergency. Applications need to validate the integrity of data and updates, particularly for performance and weight & balance calculations. We have loads of experience and can help both OEMs and operators to harden EFBs in line with AMC 20-25.

Aircraft Passenger Domain testing

Testing of interfaces and equipment accessible or exposed to passengers is important to ensure the reliability of service, continuity of revenue, and proper segregation between other aircraft domains.

Aircraft Information Services Domain testing

Systems in the AISD are not safety critical but are often have connected with the control domain. The AISD can be considered akin to a DMZ on a "traditional" network, however whilst it is common for there to be a network-level security boundary it is often left to individual units to implement their own protections. It is therefore important to review any exposed interfaces that could potentially allow a pivot between domains, particularly where units bridge across them, such as SATCOM and wireless quick access recorders which can have GSM/4G connectivity for ground use.

IFE security review

Seat-back inflight entertainment are the most exposed units to a potential malicious actor and whilst should be relatively standalone, or incorporate one-way connectivity to other systems, hardening of these devices must be performed to limit breakout, denial of service, and lateral movement. Reviews can typically incorporate a "kiosk" mode assessment, exposed ports (typically USB), and assessment of data lines available to seat boxes.

Satellite terminal security review

Review of hardware for exposed physical and management interfaces (e.g. serial, ARINC 429, telnet or web), hardcoded passwords, and firmware update mechanisms.
Network configuration review to ensure appropriate segregation between any implemented VLANs (e.g. passenger and information domains), any exposed WAN-side interfaces, and of any ancillary control systems.

Aircraft domain segregation review

Typically an initial paper-based review of systems, interconnections, and cable routes, followed by assessment of high-risk LRUs. This would examine

PEN TEST PARTNERS

deployed functionality and firmware, exposed interfaces, and any buses / protocols /virtual links exposed to other systems in other domains to verify message integrity and correct source/sink configuration, plus any network routing and firewalling configuration.

Gatelink wireless security review (aircraft and / or airside review)

Verify correct and secure storage of Wi-Fi credentials in onboard units, plus update mechanisms. Determination of protection from typical wireless attacks include deauth and “evil twin”, verification of levels of authentication and encryption (e.g. 802.1x certificate verification or strong WPA-PSKs). Review of airport AP deployments including correct segregation of traffic from airport corporate / hotel-side networks.

Avionics network protocol review

Attempt to circumvent bus protections (sink to source etc) and resilience of units of replay of commands / injection of error messages.

Dataloading / maintenance crew equipment security review

End to end process review, with build reviews against engineering field laptops, deployment procedure gap analysis, and PKI for verification of navigational databases / LSAPs etc.

Avionics hardware reverse engineering

Reverse engineering of deployed technology stacks from part numbers, enumeration of chip-connection interfaces such as JTAG, SWD, UART etc. , attempts at firmware extraction/modification via debug interfaces or chip removal, verification of firmware update mechanisms/signing, integration with other systems/components.

Aviation RF security review

Resilience of protocols to spoofing and injection, and reverse engineering of proprietary encryption mechanisms layered on top (e.g. ACARS)

How we can help you

Creating a security strategy will improve your posture. We have engineers and pilots on our team, so we understand airports, aircraft, and all things hardware.

Working hand-in-hand with airport cyber security teams we can help identify vulnerabilities and process gaps to improve your resilience to the myriad of threats that you face.

By emulating bad actors we can perform tactical security audits of your aircraft, hardware, and land-side operations to identify the 'easy wins' for security in the short term. Reviews of systems and software before deployment to an airline fleet can save significant time and money down the line.

Related Aviation Security Services

- Scenario Based Penetration Testing
- Red Teaming
- Infrastructure Vulnerability Assessment
- Wireless Assessments (802.11, ZigBee, BLE, & custom RF)
- Embedded Hardware Testing
- SCADA/ICS Security Testing
- End User Device Testing including kiosks
- Social Engineering
- Phishing Attack Testing
- CCTV Control Reviews
- Building Access Security Audits
- Facilities Management System Reviews
- Corporate Resistance to Targeted Attack
- Code Reviews
- General Security Awareness Workshops
- Information Security Incident Management
- Risk Assessments

CREST PEN TEST ASSURE STAR CSIR VA

CBEST CHECK IT Health Check Service TIGERSCHEME CYBER ESSENTIALS bsi. ISO/IEC 27001 Information Security Management PCI Security Standards Council QUALIFIED SECURITY ASSESSOR