Aviation Cyber Security
Touchdown to Takeoff

Jon C. Haass
Professor Cyber Intelligence and Security
We landed safely ... all secure!

How is aviation like (and unlike) other sectors
Important differences to be considered
Airport (and Aircraft) vulnerabilities and threats
Best practices ... emerging standards
The future outlook – The Airport of Things (AoT)
Could be any company ... Or a government
NSA’s view of the world

Every network can be (is) breached

Anything on a computer can be stolen.

General Keith Alexander (retired)
Former NSA, Cyber Command
now CEO IronNet
Are Aircraft Manufacturers OK?

Hackers carry out $55m cyber heist from Boeing aerospace parts manufacturer

By James Billington
January 27, 2016 20:25 GMT

Airbus boarded by 12 nation-state, crimeware 'breaches' every year

State-sponsored hackers will do 'everything' to get in, says CISO

13 Apr 2016 at 03:30, Darren Pauli

ACSC 2016 Airbus chief security officer Stephane Lenco says the company is hit by successful state-sponsored and ransomware attacks a dozen times each year.

The attacks aren't full breaches, instead representing penetration beyond simple scanning trigger a response from the aviation giant's security and computer emergency response team.
Aircraft Industry – BIG $ Targets

Revenue data 2014
Vulnerabilities and Threats

Aircraft complex, so are the aviation systems

Size and complexity
Vendor / Airline makeup
Degree of automation
Level of sophistication
Governance models
Physical security
Cybersecurity is not an "information technology" issue, it is an organizational risk management issue.

Another area to consider for safety and the economics of transportation today.
“Cybersecurity threats know no boundaries. That’s why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC. Through our engagement with other government agencies as well as with the industry and educating the investing public, we can all work together to reduce the risk of cyber attacks.”

— SEC Chair Mary Jo White
Connected Aircraft

- Wired and wireless connections
- Ground crew comms
- Flight plan updates
- Glass cockpit
- EFB

Background Image: © SITA
Electronic Flight Bags – EFB

- Could they become a vector for APT?

- Multiple Classes of Device
  - COTS – Almost all are based on standard tablets/OS
IBM study shows app insecurity

Fastest growing internet applications
Mobile apps

40% did not have adequate security
33% had not performed basic security testing

How does this impact Aircraft?

BYOD increases attack surface
Aircraft Builders ...
like other large companies

Malicious email borne attacks
Entry into critical networks
Development and Key employees

June 23, 2015 – FBI alerts ISACs of Business e-mail Compromise attacks that are increasingly successful, well crafted and malicious fronts for APT (Advanced Persistent Threats)
Once inside – escalation

to / from the internet

Phish

Port 443

Internal resources / servers

In flight systems?

BYOD
Aircraft as System Integrator

Complex system of multi-vendor suppliers linked via physical and network connections.

Security shortcomings in one area impact all

Post delivery add-ons

Primary ownership responsibility?
The Internet of Things

Devices accessible via internet

For efficiency
For management
For control or measurement
For updating, alerting

Aircraft Supply Chain large and complex
Connectivity of Industrial Control Systems
Example: Industrial Controls

- Fueling systems
- Controls on board aircraft
- Load and balancing sensors
- Many manufacturing devices
- Baggage management systems
- Will aircraft management systems be next?

External 3rd party vendors
Default security settings
Future outlook

Bright ideas needed!
NIST Cyber “Best Practice”

Service Providers can support
Embry–Riddle Cyber Research

Security of EFB / PED for crew and passenger
Embry-Riddle Cyber Research

Security of EFB / PED for crew and passenger

Aircraft Coms
Embry–Riddle Cyber Research

Security of EFB / PED for crew and passenger

Aircraft Coms

UAS – “drones”
Embry-Riddle Cyber Research

Security of EFB / PED for crew and passenger

Aircraft Coms

UAS – “drones”

Airport of Things
What is unseen can hurt!

Future trends becoming clearer
Questions and comments

Jon C. Haass
Professor Cyber Intelligence and Security
Embry–Riddle Aeronautical University
Jon.Haass@erau.edu
Airports – critical infrastructure

Acknowledgements:

ACRP Report 140*
Guidebook on
Best Practices for Airport Cybersecurity
Funded by National Academies
PI – Randy Murphy, Grafton Technologies

*trb.org/Publications/Blurbs/172854.aspx