Deployment of cyber defensive measures: issues of responsibility

Salve!

I am Arianit Dobroshi

LL.M. Air and Space Law

Sr. Int'l Cooperation Officer,

Kosovo CAA

Member of Kosovo National Cyber Security Council

Vulnerabilities by priority

Integrity

Information has not been tampered with in transit and therefore remains as foreseen by the sender/source.

Availability

Information is available within agreed, reasonable timelines without undue delays.

Confidentiality

Information can be accessed or used only by the authorized or intended recipients.

A changing cybersecurity world for aviation

- Increasing vectors of attack
  - Commoditized equipment
  - More systems, more interfacing, more vendors
- Criminalization of cybersecurity threats is not an effective deterrence
  - Attribution problems
  - Crossborder
  - Asymmetry

Aviation cyber security 1/2

- A modern airplane has ~500 computers, plenty of software inside
  - “The cost to change one line of code on a piece of avionics equipment is $1 million, and it takes a year to implement” (Source: Aviation Today)
  - Current threat likelihood low but expected to increase
- Allegations that software is increasingly and ultimately to blame for crashes

Aviation cyber security 2/2

- Long lead certification time
- Open nature of some infrastructure
  - ex. ADS-B, TCAS, ACARS
- Rare events, high impact
- Three cybersecurity theatres
  - Airports (on the ground)
  - ANS provision (in the air)
  - Aircraft (in the air)

An approach

- A more specific approach
  - Not all cyber threats should be treated equally
  - Breaches will happen, resilience should be the aim
  - Service disruptions should be dealt by general means
  - Safety of life will take improved measures
- Raise certification standards
- Legalize and encourage cybersecurity auditing and testing, including by third parties

From bug reports to safety directives 1/2

- Each software bug is a potential safety bulletin.
- What is a bug in computer software can be a hidden defect in product liability in aviation
  - Ex. 2 recent CPU bugs dating to 1995 (Meltdown and Spectre).
- Product liability increases incentive to patch known security problems.
- Ethical hacking, exposing flaws and insecurities are active acts of building resilience. States should stop from criminalising cyber security testing.

From bug reports to safety directives 2/2

- Should regulatory compliance lead to state of the art defence? What is state of the art in aviation?
- Need for certification agencies to move faster with software patches.
- If updates, or fixes for vulnerabilities aren't provided within a reasonable timeframe after their discovery, manufacturers should be held liable. States should revise and extend product liability rules to that end.
- Continuity of support for products in widespread use through a best-by date.

Liability 1/2

- Increasing liability provides an increased incentive to patch known security problems.
- A cybersecurity breach:
  - Could be due to a design defect (OEM programming)
  - Negligence (lax configuration by airline) and/or
  - Criminal act (attack).

Liability 2/2

- In software what is state of the art today might not be so in 10 years.
- Problem of certification of patches/updates.
- In software there is only design defect since strictly speaking production will always be the same.
- State of art defence in EU Law refers to the point in time that a product was put into circulation as the moment at which state of the art is measured
  - But software is easily upgradable, is meant to be so and often is.

The way forward 1/2

- Focus on a narrower definition but execute deep/layered cyber defence.
- Welcome and encourage more testing by 3rd parties with disclosure.
- Learn and build on experience from other industries.
- Strengthen supply chain cyber security.
- Raise certification standards
  - Request graceful degradation and resilience.
- Build parallel data input and cross-check.
- Enable liability for not responding to known vulnerabilities.

The way forward 2/2

- Establish policies and allocate resources when needed to ensure that critical aviation systems are:
  - Secure by design;
  - Resilient;
  - Methods for data transfer and at rest are secure, ensuring integrity and confidentiality of data.
- Systems monitoring, and incident detection and reporting; and
- Forensic analysis of cyber incidents is carried out.

(ICAO Resolution A39-19)

Thank you!

Any questions?

You can find me at:

 /in/arianit

 arianit@gmail.com