The International Aviation Trust Framework (IATF)

Rob Segers,
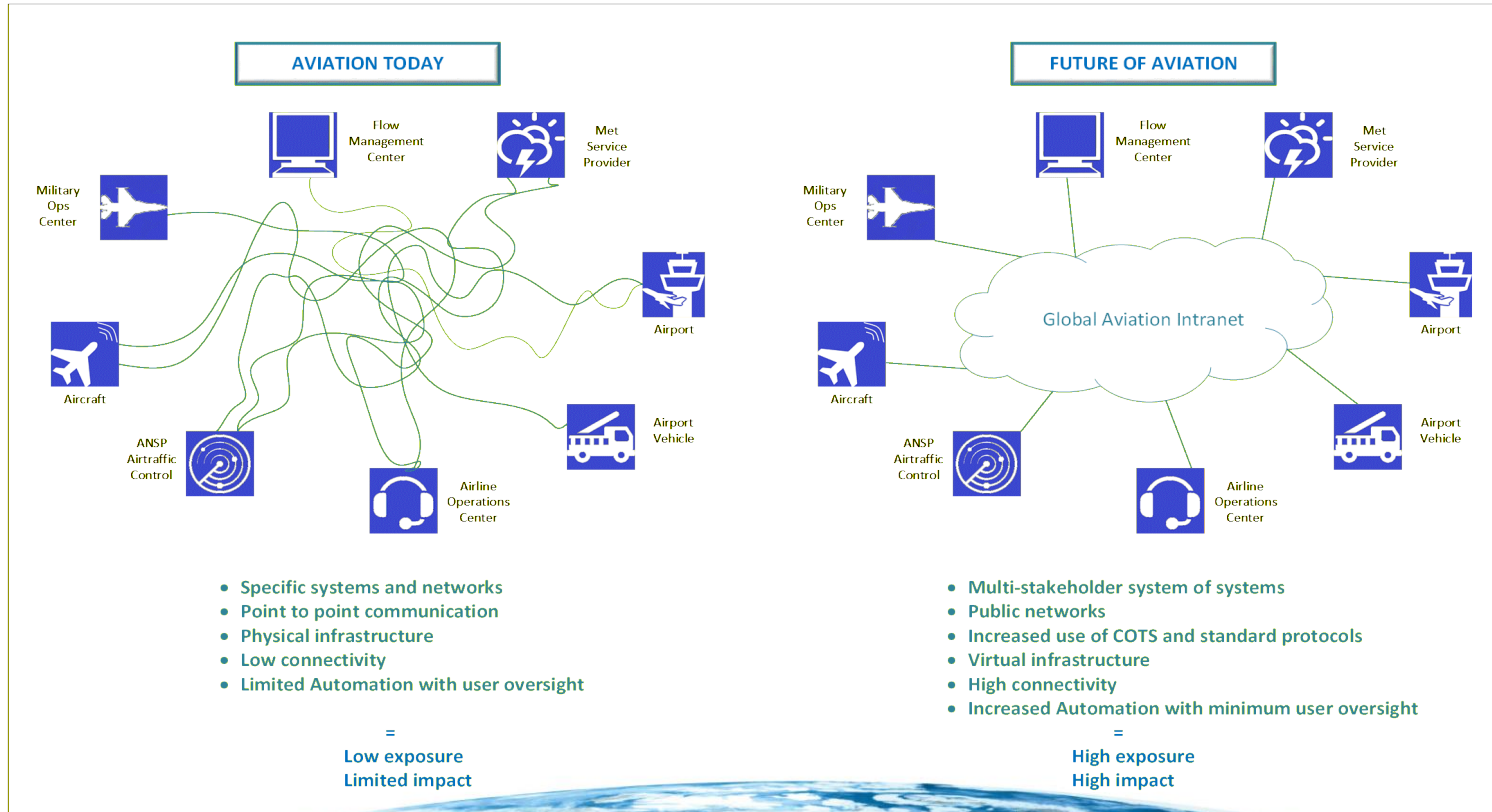
NextGen ISS Architect

Drivers for change in Aviation

- The Telecommunication industry is eliminating dedicated telecommunication services which are used between the FAA and many organizations and countries

- The cost of fit for purpose networks and the use of protected spectrum limits the ability to grow the network connectivity, bandwidth and worldwide ATM automation integration required to grow aviation capacity and the integration of Unmanned Areal systems

- The use of ubiquitous network peering across commercial networks including unprotected spectrum will require end to end information integrity between information producer and consumer to assure network trust and safety

Fit for purpose network evolution to IATF

AVIATION TODAY

Flow Management Center
Met Service Provider
Military Ops Center
Airport
Aircraft
Airport Vehicle
ANSP Airtraffic Control
Airline Operations Center

- Specific systems and networks
- Point to point communication
- Physical infrastructure
- Low connectivity
- Limited Automation with user oversight

=
Low exposure
Limited impact

FUTURE OF AVIATION

Global Aviation Intranet

Flow Management Center
Met Service Provider
Military Ops Center
Airport
Aircraft
Airport Vehicle
ANSP Airtraffic Control
Airline Operations Center

- Multi-stakeholder system of systems
- Public networks
- Increased use of COTS and standard protocols
- Virtual infrastructure
- High connectivity
- Increased Automation with minimum user oversight

=
High exposure
High impact

Man in the Middle (MITM) Attacks: an IATF Trust Threat

- Man-in-the-middle (MITM) attacks occur when the attacker manages to position themselves between the legitimate parties to a conversation

- The attacker spoofs the opposite legitimate party so that all parties believe they are actually talking to the expected party

- A MITM attack allows the attacker to eavesdrop on the conversation between the parties, or to actively intervene in the conversation to achieve some illegitimate end


Original connection

New connection

Man in the middle, Phisher, or annonymous proxy
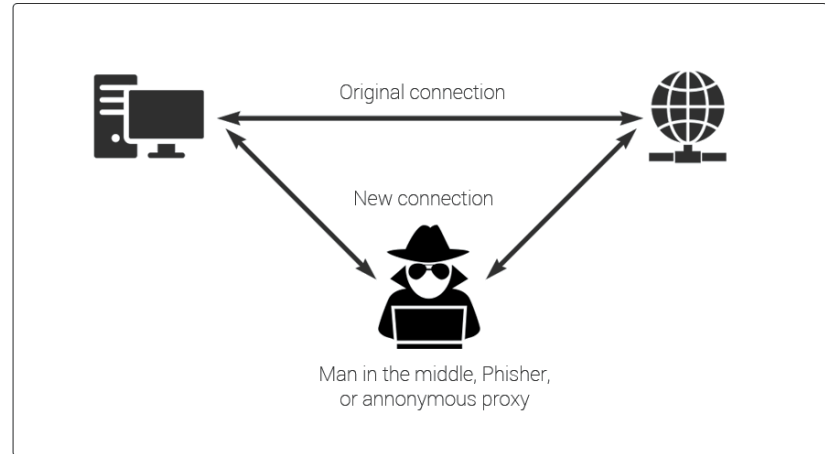
- A MITM attack can also occur by modifying information at rest (e.g. stored on a cloud server)

Attribution of the origin of information

- IATF participant Identities must be trustable:
  - Common IATF Master Trust Framework agreement
  - Common Identity Policies audited through IATF
- Information flow between IATF participants must be attributable to the IATF identity source of the information by digitally signing the information
- IATF compliant networks called Global Resilient Aviation Information Networks (GRAIN)s must be trustable:
  - Trusted Network addressing
  - Trusted Domain Naming Services
  - Trusted Network Operations through IATF audited Information Security Management Systems (ISO 27000/NIST)

ATM – UTM integration using IATF
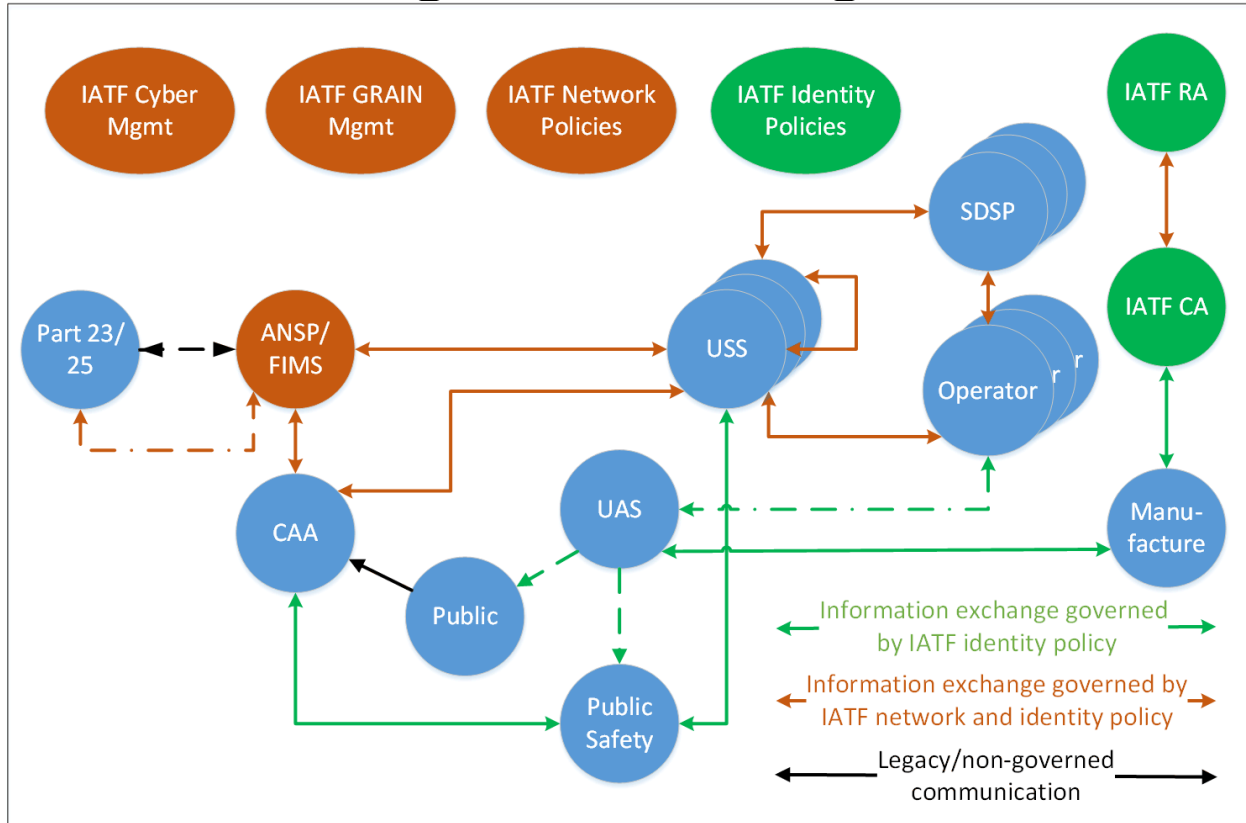
Questions

Rob Segers,
NextGen ISS Architect