



ICNS 2023

Cybersecurity and Infocentric ATM

Paul Hoyt Nelson , Senior Cybersecurity Advisor, ARMD



Digital Identity

- Current digital identity is used to identify and authorize individuals and some devices. PKI is used for some of this ($10^4 - 10^5$).
- Future highly automated operations will require digital identity for all system and system of system components.
- It's likely a federated approach to creation and management of certificates will be necessary ($10^6 - 10^?$).
- Interaction and operations of the current technologies does not scale so research is required to enable new models and capabilities:
 - Research and Develop certificate authority federation that actually works for many to many organizational relationships.
 - Research and Develop management models that significantly reduce resource requirements.
 - Research and Develop new methodologies for managing revocation/



Cybersecurity and Safety

- Cybersecurity spans a vast set of areas ranging from IT security to Avionics and Control systems.
- Approaches and Resources have been insufficient to address incidents just in the IT security realm. It's unlikely we'll have enough to cover all of the integrated IT and OT domain.
- The intersection between cybersecurity threats and vulnerabilities, and safety provides a very good methodology to focus on issues that impact safety of flight and safety of the flying public.
- NASA has started an effort under the IASMS (In-Time Aviation Safety Management System) to identify these issues from the safety and operations data. This is necessary research.
- AIA already has a mature approach with the Cyber Safety Commercial Aviation Team (Cyber Safety CAT) but that needs to be fully charted in a similar was to CAST.



Non-Human (Automation) Mediated Security Operations

- Concepts in the Info-Centric NAS require machine to machine operations and the speed of M2M.
- Current identification of security incidents is human, or machine driven. The future will require full automation.
- Current response to security incidents is largely human mediated (the speed of humans). The future will require fully machine mediated capabilities.
- This means incident response will have to be highly adaptive (ML/AI)
- Using an immune system model, we can break this down:
 - Innate Immune System: That part of the system that “knows” what the threat looks like and “knows” how to respond.
 - Adaptive Immune System: That part of the system that observes the attack and builds a response rapidly enough to make a difference. This is the research question.
- Doing this for the Infocentric NAS will require an integrated effort that begins now.