Cybersecurity Threat Assessment of Small Unmanned Aerial System (UAS) Aircraft Configurations

Dr. Corey A. Ippolito
Intelligent Systems Division
NASA Ames Research Center
Moffett Field, CA 94035

Australian Ministry of Law Enforcement:

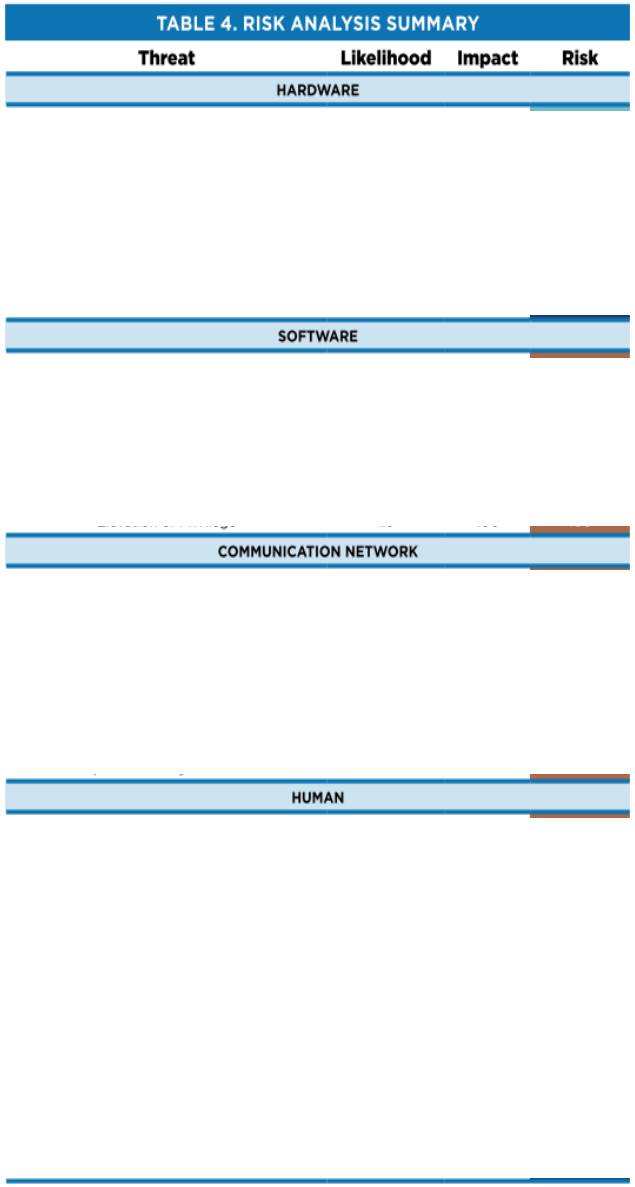
- *What are your biggest cybersecurity concerns for emerging technology and autonomous systems?*
- *What interesting insight have you gained from your trip to Silicon Valley?*

UAS Cybersecurity Challenges

- Rapidly evolving systems and market
- Evolution towards cyber-physical systems within system-of-systems
- Continual emergence of new threats, vulnerabilities, and attack vectors.
- Lack of formal methods and standardization for cybersecurity
- Approaches
  - Best practices, using a combination of techniques
  - Analysis
  - Experience
  - Enumeration
  - Intuition
  - Constant vigilance
  - Build cybersecurity into the methods, procedures, and oversight roles throughout an organization
  - Compliance requirements and accountability

DoD Comprehensive Threat Model for Smart-Device Controlled UAS (Mansfield 2015)

- High-level top-down analysis of smart-device controlled UAS
- Threat model analyzed three categories
  1. Hardware
  2. Software
     - Operating System
     - Software Applications
  3. Communication Networks
  4. People and Processes
- Approach for each category
  - Describe attack motivation
  - List threats
  - Describe attack methods/vectors
  - Suggest mitigations
- Limitations and Gaps
  - High-level, general, non-specific
  - Relies on top-down enumeration
  - Does not address malicious manufacturers/ providers or malicious GCS software developers



(Mansfield 2015) Mansfield, Katrina, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani. DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model. Defense Acquisition Research Journal (ARJ), April 2015, Vol. 22, No. 2: 240-273.

DoD Comprehensive Threat Model for Smart-Device Controlled UAS (Mansfield 2015)

- High-level top-down analysis of smart-device controlled UAS
- Threat model analyzed three categories
  1. Hardware
  2. Software
     - Operating System
     - Software Applications
  3. Communication Networks
  4. People (Mansfield 2015)
- Approach for each category
  - Describe attack motivation
  - List threats
  - Describe attack methods/vectors
  - Suggest mitigations
- Limitations and Gaps
  - High-level, general, non-specific
  - Relies on top-down enumeration
  - Does not address malicious manufacturers/ providers or malicious GCS software developers

TABLE 4. RISK ANALYSIS SUMMARY

Threat	Likelihood	Impact	Risk
HARDWARE			
Battery Exhaustion	0.5	100	50
Flooding	1.0	50	50
Surveillance	1.0	100	100
USB	0.1	10	1
Storage Snooping	0.5	50	25
Storage Jamming	0.5	10	5
Storage Erasure/Alteration	0.1	50	5
SOFTWARE			
Malware	1.0	100	100
Phishing	0.5	50	25
Data Leakage	1.0	50	50
Spyware	1.0	100	100
Data Tampering	1.0	50	50
Elevation of Privilege	1.0	100	100
COMMUNICATION NETWORK			
Eavesdropping	1.0	100	100
Spoofing	0.5	100	50
Denial of Service	1.0	100	100
Jamming	1.0	10	10
Weak/Compromised Cryptography	0.5	50	25
Unencrypted Communication	0.1	50	5
Impaired Quality of Service	0.5	100	100
HUMAN			
Breaking Policy	1.0	100	100
Inadequate Policy	1.0	100	100
Unencrypted Communication	0.5	50	25
Carelessness with Cryptographic Keys	1.0	50	50
Harmful Data Leakage	0.5	50	25
Compromise of Personnel	0.5	100	50
Poor Risk Decisions	0.5	100	50
Poor Management/Maintenance	1.0	100	100
Overloading the Operator	0.5	10	5
Prevention of Accountability from Being Stored	0.1	10	1
Destruction of Accountability Data	0.1	10	1
Modification of Accountability Data	0.1	10	1

(Mansfield 2015) Mansfield, Katrina, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani. DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model. Defense Acquisition Research Journal (ARJ), April 2015, Vol. 22, No. 2: 240-273.

sUAS Cybersecurity Threat Model Analysis (Javaid, 2002)

- Define the system
- Develop network and architecture models for analyis
- Enumerate and categorize threats (top-down and bottom-up)
- Perform risk assessment of each threat
- Take action based on severity of risks
  - Track, Mitigate, Redesign
- Continually reevaluate the threat model

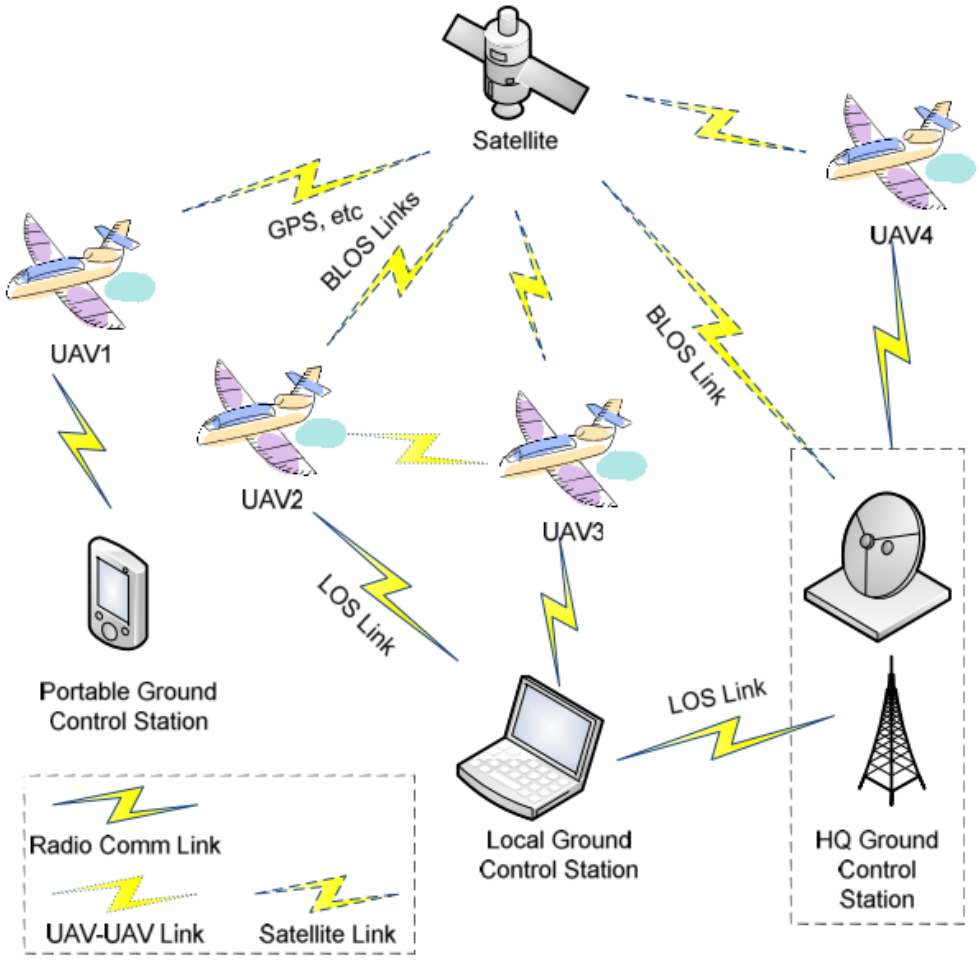


Figure 1. Typical UAV Communication Scenario

(Javaid, 2012) Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 585–590. https://doi.org/10.1109/THS.2012.6459914

sUAS Cybersecurity Threat Model Analysis (Javaid, 2002)

- Define the system
- Develop network and architecture models for analyis
- Enumerate and categorize threats (top-down and bottom-up)
- Perform risk assessment of each threat
- Take action based on severity of risks
  - Track, Mitigate, Redesign
- Continually reevaluate the threat model

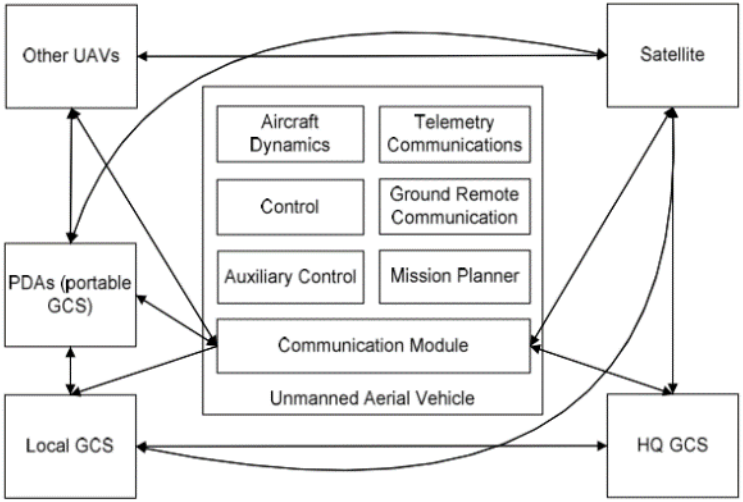


Figure 3. UAV Communication Model

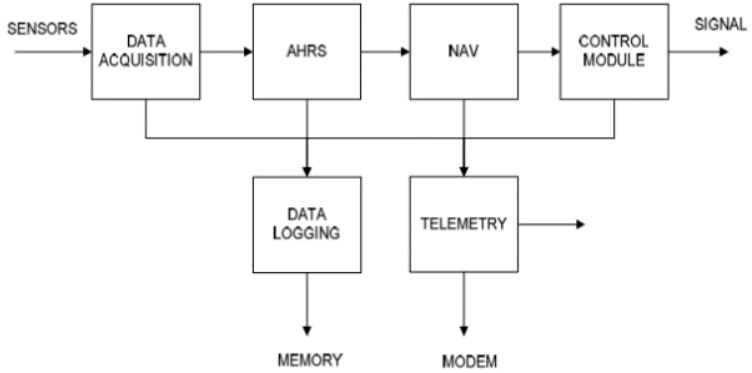


Figure 2. Simple UAV block diagram

(Javaid, 2012) Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 585–590. https://doi.org/10.1109/THS.2012.6459914

sUAS Cybersecurity Threat Model Analysis (Javaid, 2002)

- Define the system
- Develop network and architecture models for analyis
- Enumerate and categorize threats (top-down and bottom-up)
- Perform risk assessment of each threat
- Take action based on severity of risks
  - Track, Mitigate, Redesign
- Continually reevaluate the threat model

TABLE I. RISK EVALUATION GRID

		Rationale		
Criteria	**Cases**	**Difficulty**	**Motivation**	**Ranks**
Likelihood	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
		User	***System***	
Impact	Low	Annoyance	Very Limited Outages	1
	Medium	Loss of Service (LoS)	Limited Outages	2
	High	Long time LoS	Long time Outages	3
Risk	Minor	No need for countermeasures		1,2
	Major	Threat need to be handled		3,4
	Critical	High priority		6,9

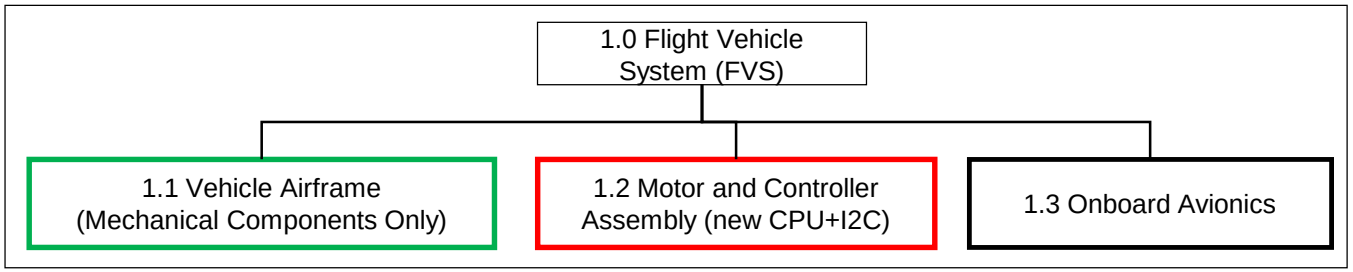
TABLE II. ANALYSIS SUMMARY

Threat	**Algorithm(s)**	**Likelihood**	**Impact**	**Risk**
Jamming		3	1	3
Scrambling/Distortion		2	1	2
Eavesdropping		3	2	6
Cross Layer Attacks		2	1	2
Multi-Protocol Attack		2	1	2
Social Engineering		2	2	4
Spoofing	Device List	3	3	9
	X.509 device Auth.	2	3	6
Command and Control Message Modification	No MAC	3	3	9
	SHA-1 MAC	2	3	6
	AES MAC	1	3	3
Data Traffic Modification	Without AES	3	1	3
	With AES	1	1	1
DoS on UAV/GCS	EAP/SHA-1/AES/MAC	3	3	9
Signal Integrity		3	2	6
Malicious Code, Subroutine Exploit		1	3	3
Virus, Malware, Trojans and Keyloggers		3	2	6

(Javaid, 2012) Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 585–590. https://doi.org/10.1109/THS.2012.6459914

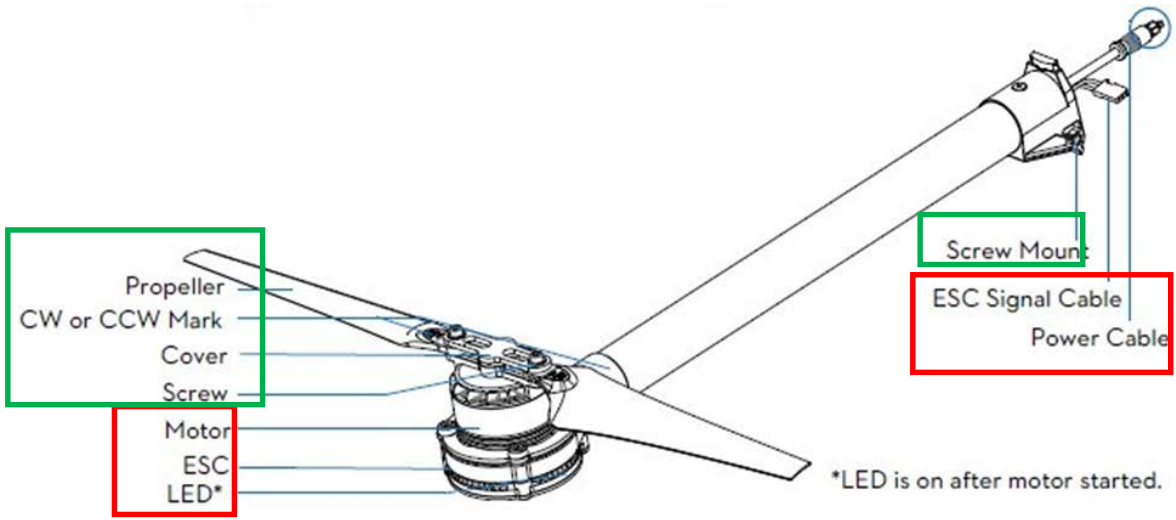
Updating Threat Model Analysis

- Cybersecurity models must be constantly updated and reviewed
  - Particularly for changes/revisions or when new cybersecurity concerns are identified

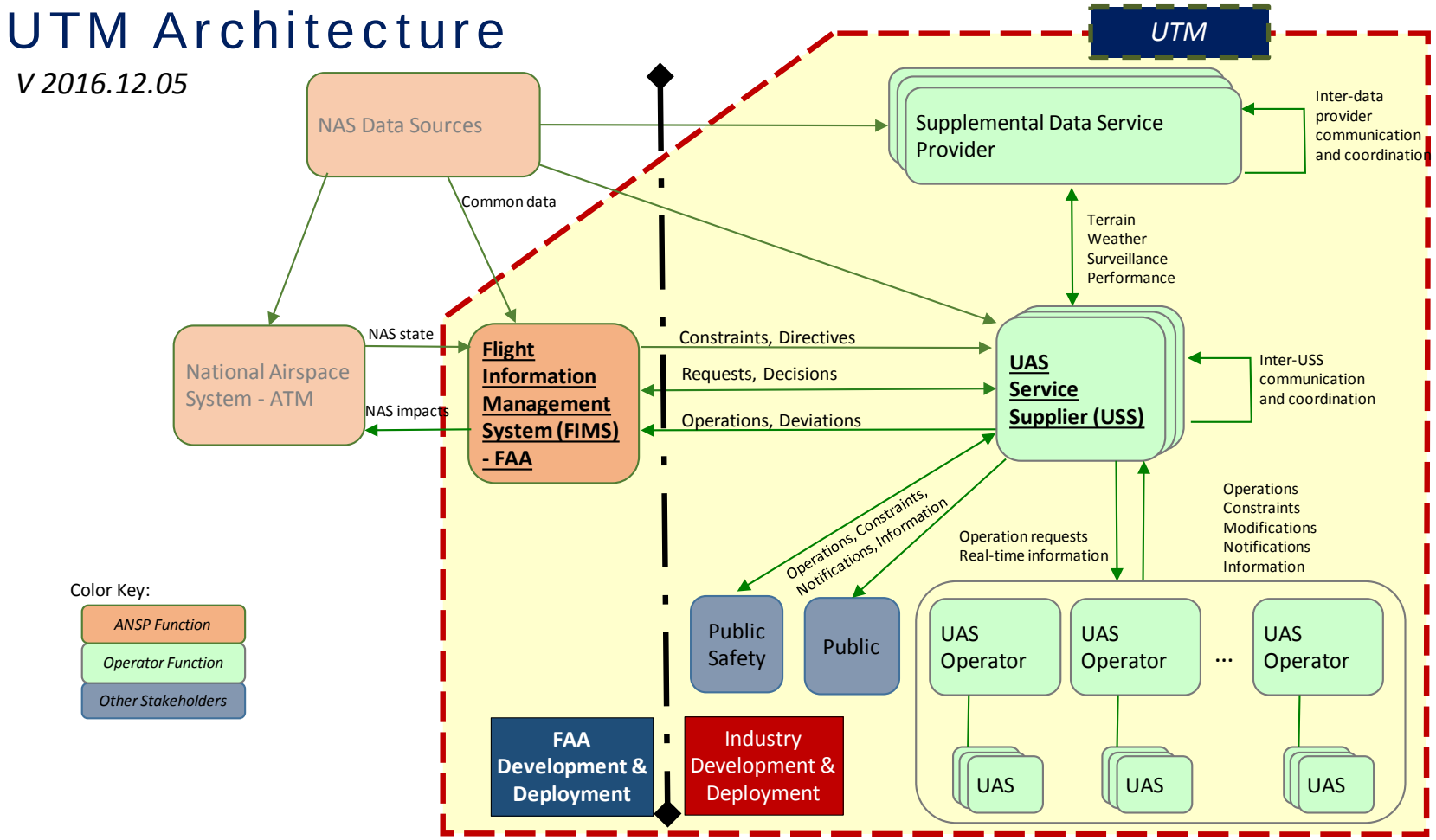


No New Cybersecurity Concern

New Cybersecurity Concern



Systems are getting more complex…



See https://utm.arc.nasa.gov/ for more details.

- *How will we secure the future of unmanned aviation?*