Aug 15th, 9:30 AM - 10:45 AM

Aviation Cybersecurity: An Overview

Gary C. Kessler
Embry-Riddle Aeronautical University, gck@garykessler.net

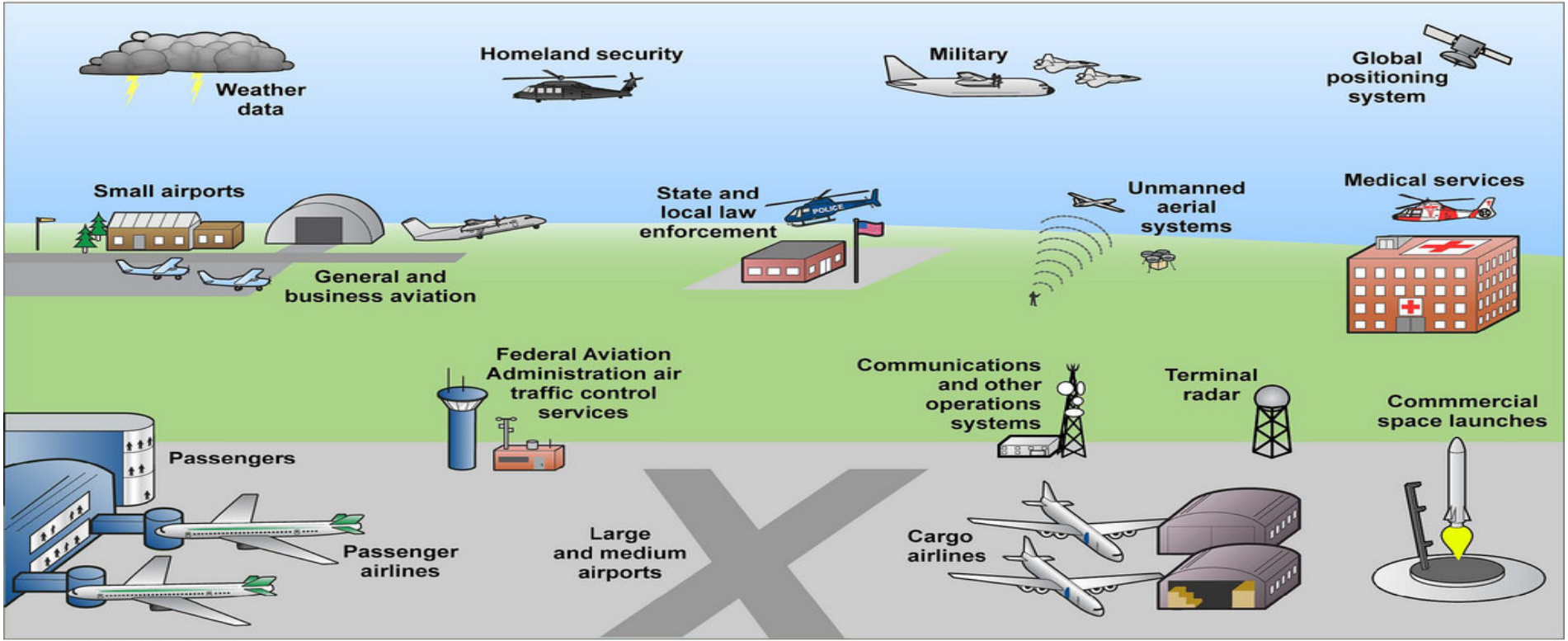
J. Philip Craiger
Embry-Riddle Aeronautical University, craigerj@erau.edu

Aviation Cybersecurity

J. Philip Craiger, Ph.D. CISSP, CCFP, CEH
&
Gary C. Kessler, Ph.D., CCE, CISSP
Security Studies & International Affairs Dept.
Embry-Riddle Aeronautical University

Presentation for the 31st National Training Aircraft Symposium, Embry-Riddle Aeronautical University, Daytona Beach, FL, August 15, 2018.

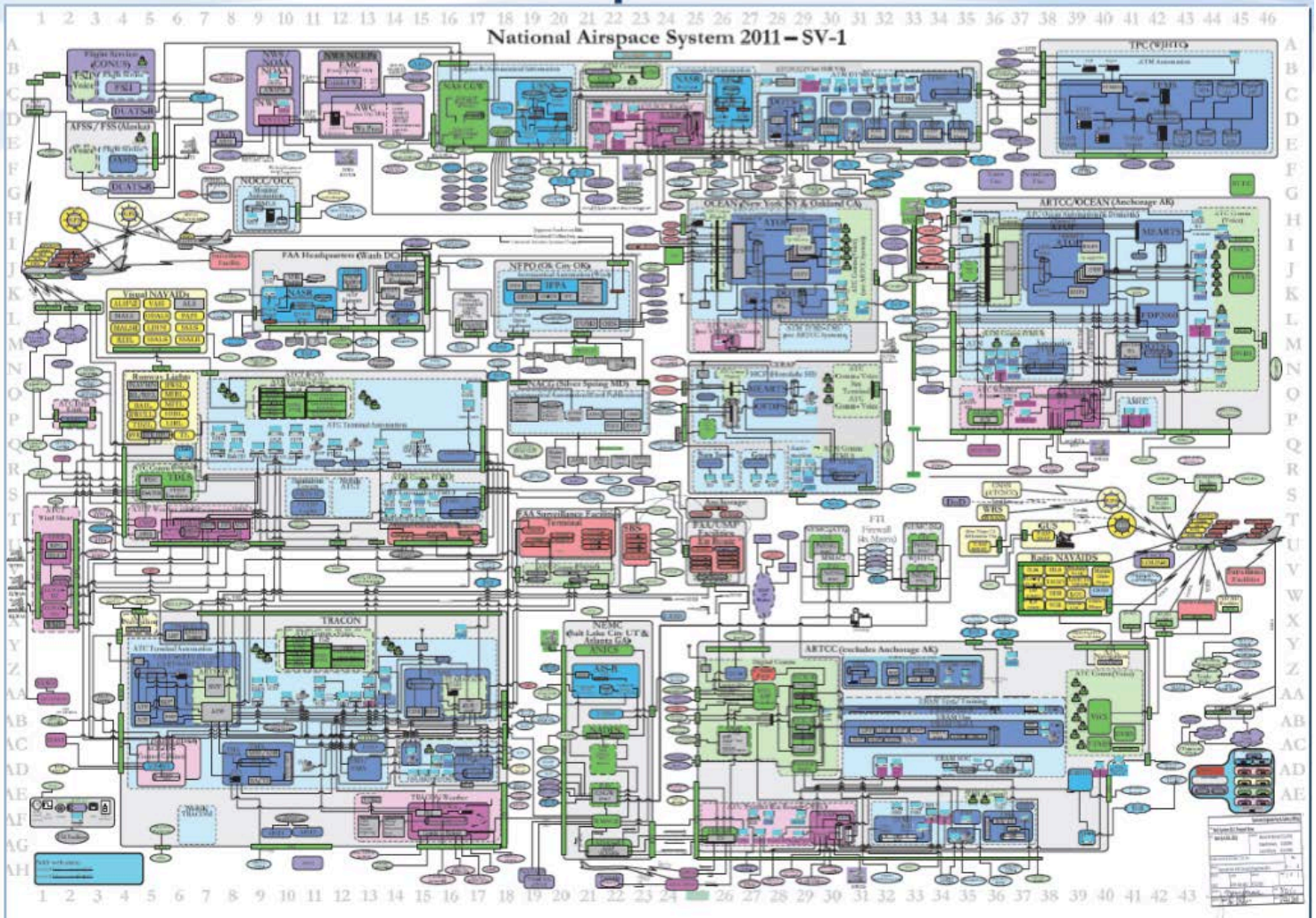
Users of the NAS



Source: GAO. | GAO-17-131

Attack Vectors

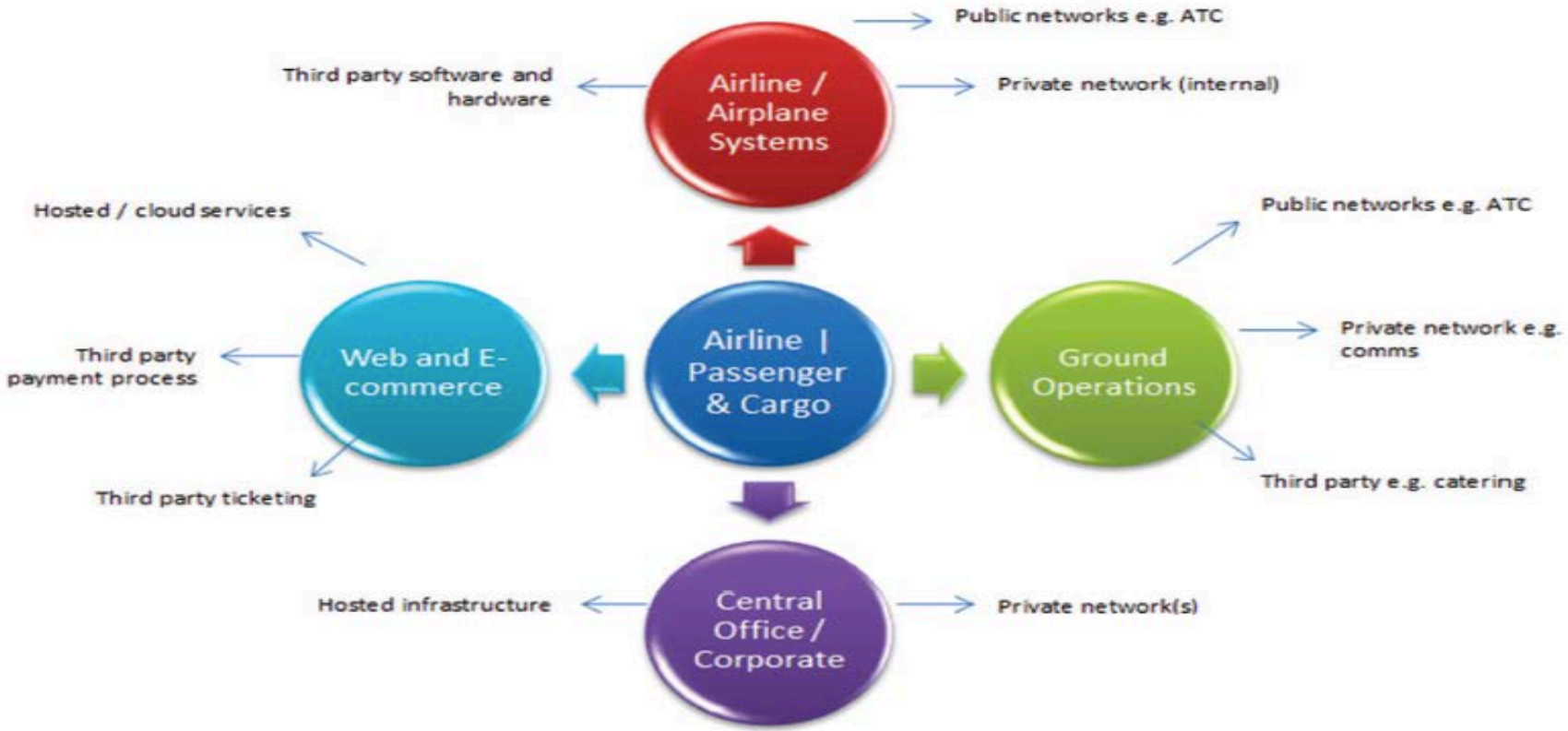
The Simplified NAS



Threat Actors and Motivations

- Cybercriminals
  - Costs to global economy $450B+ annually
- Cyberactivists/Hacktivists
  - Motivated by philosophy, politics, and non-monetary goals
- Cyberspies
  - Financial, industrial, political, and diplomatic espionage
- Cyberterrorists
  - Political, religious, ideological, or social violence
- Cyberwarriors
  - Attack by a nation-state in order to advance strategic goals

...And You Only Have Limited Control



Aviation Cyberattacks

Compromise at "Major Airport"

- McAfee Labs reported that hackers were selling remote access to a "major airport" for $10 on the Dark Web (07/2018)
  - Underground forums contain IP addresses for remote desktop protocol (RDP) access to hundreds of compromised systems
  - At least one "major" international airport is amongst the compromised networks

Air Traffic Control

- Dozens of aircraft **vanish** from ATC in Austria, Czech Republic, Germany, and Slovakia, twice over a 6-day period (6/2014)
  - Ostensibly due to nearby military e-warfare exercise...

- Cyberattack launched by Russian APT group APT28 (aka Pawn Storm) jammed Sweden's air traffic control capabilities, grounding hundreds of flights over a 5-day period (11/2015)
  - Outage initially said to be due to solar flares

Aircraft Vulnerability (2)

- DHS reports Boeing 757 vulnerable to hacking (11/2017)
  - DHS team performed a remote, non-cooperative penetration (09/2016)
    - No one touched anything on the plane. No insider threat. Used equipment that would pass through security.
    - Were able to establish a presence on the aircraft network
  - Boeing claims to have witnessed the test and states "that there was no hack of the airplane's flight control systems."

Aircraft Vulnerability (3)

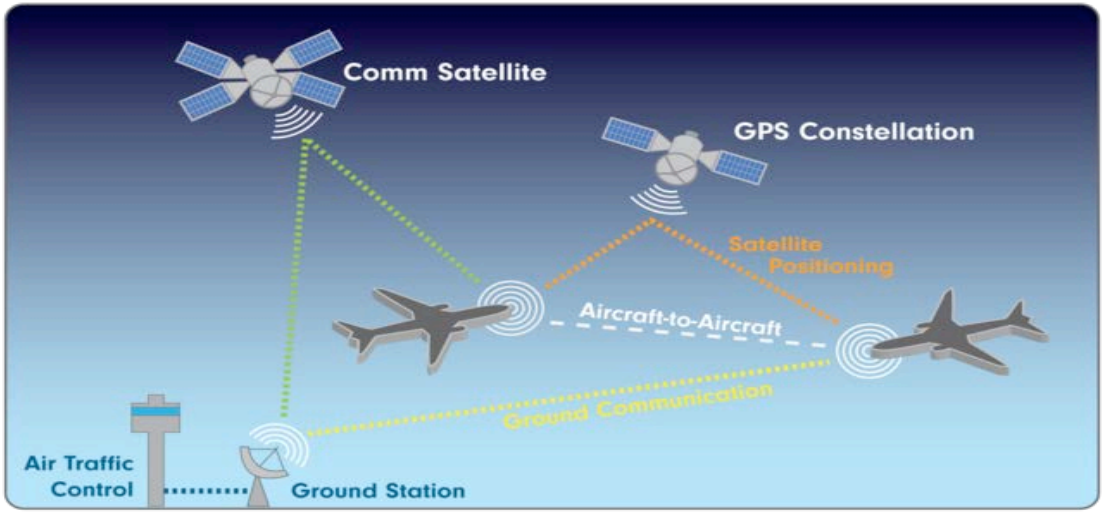
- Pacific Northwest National Laboratory (PNNL), a Dept. of Energy research lab, concluded that the hack of an airplane is only a "matter of time" (01/2018)
- **Estimated cost of $1M to change a line of avionics code and years to implement the change**
  - Patching avionics code is code prohibitive
  - 90% of commercial aircraft are "legacy" systems – i.e., designed in 1970s and '80s -- not built with security in mind

Aircraft Communications Addressing and Reporting System (ACARS)

- Flight plan information sent to planes can be "forged"
  - Some experts claim that this is not a safety issue but merely one of confusion because pilots will catch an error
  - Some of these problems exacerbated because different planes have different display formats (although they all use the same datalink protocol)
- Hacks into ACARS are suspected in grounding of 10 LOT airplanes at Warsaw Chopin Airport (6/2015) and all United planes in U.S. (5/2015)

ADS-B

- Automatic Dependent Surveillance - Broadcast
  - Aircraft obtain position information from GPS
  - Aircraft simultaneously broadcast position and other data to aircraft and any ground station equipped to receive
  - Ground stations transmit aircraft position information to ATC



Threats to ADS-B System

Threat	Type	Likelihood	Severity	Effect
GPS: Denial-of-Service	Intentional	Low	2	Availability
GPS: Bad Data/Receiver Malfunction	Hazard	Medium	2	Integrity
ADS-B: Turned Off	Intentional	Low	1	Availability
ADS-B: Data Input Error/Malfunction	Hazard	Medium	3	Integrity
Prop. Path: Jamming Data Link	Intentional	Medium	3	Availability
Prop. Path: Delayed Retransmission	Intentional	Low	4	Availability
Prop. Path: ADS-B Spoofing	Intentional	Medium	2	Integrity
Prop. Path: Excessive Bit-Error Rate	Hazard	High	2	Availability
Ground Station: Intentional Damage	Intentional	Low	2	Availability
Ground Station: Data Manipulation	Intentional	Low	2	Integrity
Ground Station: Training latency	Hazard (human error)	Medium	3	Availability/ Integrity

L. Purton, H. Abbass, & S. Alam. 2010. Australasian Transport Research Forum 2010 Proceedings 29 September – 1 October 2010, Canberra, Australia

Vulnerabilities of Comms Systems

- ACARS and ADS-B can be breached wirelessly
- Both lack security features and encryption
- Open source sites such as *flightaware.com* and *flightradar24.com* display ADS-B and ACARS data
  - After acquiring this data, a hacker can easily determine what Flight Management System (FMS) is being used by the aircraft
  - A hacker might then exploit the FMS to potentially lead to a complete remote takeover of the aircraft

GPS Jamming

- Several incidents of GPS jamming occurred at Liberty International Airport (EWR) while tests were ongoing for new ground-based augmentation system (GBAS) (08/2012)
  - 1st Boeing 787 made GBAS Landing System capable landing in 10/2012
- GPS jammer found to belong to a truck driver who didn't want his company to be able to track his location at certain times on certain days
  - A truck on the NJ Turnpike ran with a GPS jammer between 03/2009-04/2011 before being caught

GPS Issues (1)

- Between 2013 and mid-2016, ~80 reports of GPS signal interference or malfunction were reported to NASA
  - Reports from small to large aircraft, general and commercial flights, and countries from France and the U.S. to Egypt and Turkey
  - Majority of incidents were total signal loss or misreporting location

GPS Issues (2)

- Multiple (unconfirmed) incidents reported in eastern Mediterranean Sea (03/2018)
  - Five ships and one airplane reported extended GPS periods of GPS interference/disruption
  - Resulted in inaccurate or no GPS position reported

And Some New Concerns...

Here comes the big one …


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
Payment will be raised on
5/15/2017 20:34:43
Time Left
02:23:53:13
Your files will be lost on
5/19/2017 20:34:43
Time Left
06:23:53:13
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt

Ransomware

- Malware encrypts the files on your computer
  - Might also encrypt all network shares
- Ransom paid via anonymous cryptocurrency
  - Small ransom for individuals,
  - larger ransom for organizations
  - Help desk often available to assist!!
- Most Popular Cybercrime Tool, 2017

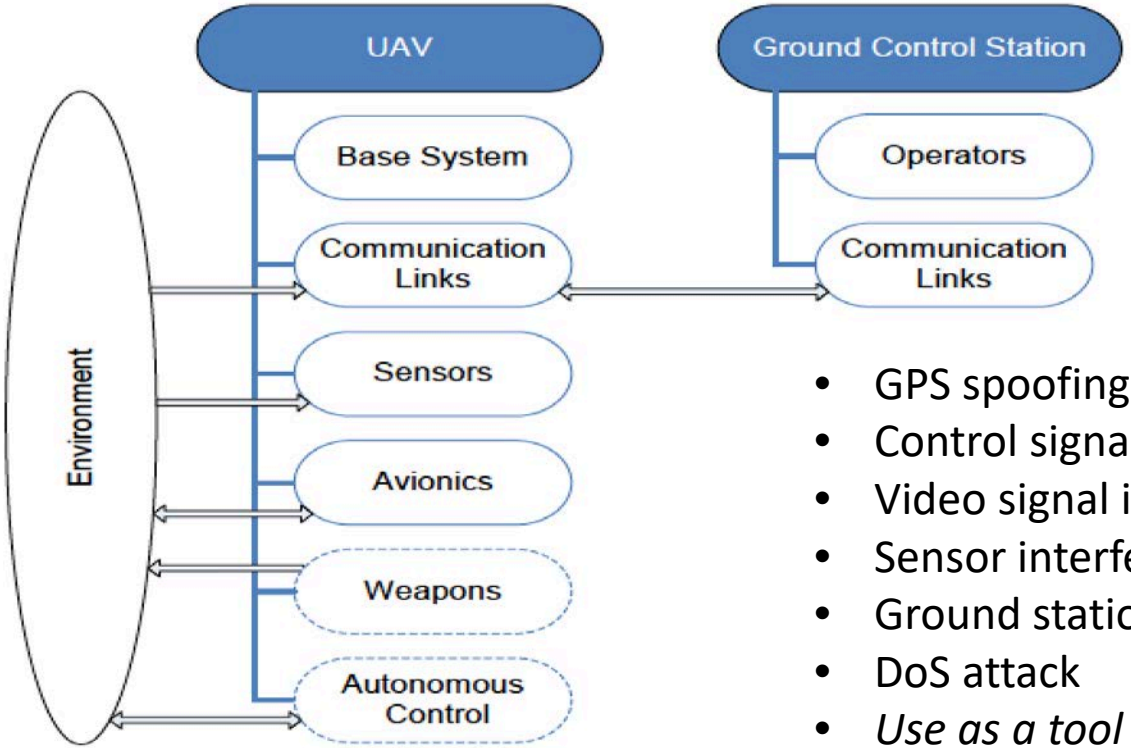
WannaCry/Petya

- *WannaCry* detected on 12 May 2017
  - By 13 May, had infected 10s of thousands of computers in 99 countries throughout the Americas, Asia, and Europe
  - By 14 May, had impacted more than 200,000 computers in 150 countries
  - Petya followed on 26 June
  - Worldwide cost could top $4B
- Airlines and the aviation industry were not specific targets but were susceptible (e.g., Windows XP)
  - Boryspil International Airport (KBP), Kiev and Boeing were among aviation victim sites worldwide

Supply Chain Vulnerabilities

- A 2018 survey concluded that supply chain vulnerabilities are rampant
  - If an attacker cannot break into their primary target's network, they will look at other attack vectors
  - Aircraft manufacturers and airlines are obvious targets and they are popular targets for hackers
    - The global, highly interconnected supply chains within aviation have been aggressively digitizing operations and security has been a secondary focus

UAV Components



- GPS spoofing
- Control signal interception/spoofing
- Video signal interception
- Sensor interference
- Ground station malware
- DoS attack
- *Use as a tool of terrorism*

From Hartmann & Steup (2013), The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment

The Danger of Drones

- This was a purposeful yet illegal and foolish episode...

[2:20]

Terrorism

- Venezuela arrests six over drone explosions during Maduro speech (8/5/18)

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 17, 2017

Alert Number
I-101717a-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

COMMON INTERNET OF THINGS DEVICES MAY EXPOSE CONSUMERS TO CYBER EXPLOITATION

In conjunction with National Cyber Security Awareness Month, the FBI is re-iterating the growing concern of cyber criminals targeting unsecure Internet of Things (IoT) devices. The number of IoT devices in use is expected to increase from 5 billion in 2016 to an estimated 20 to 50 billion by 2020. Once an IoT device is compromised, cyber criminals can facilitate attacks on other systems or networks, send spam e-mails, steal personal information, interfere with physical safety, and leverage compromised devices for participation in distributed denial of service (DDoS) attacks.

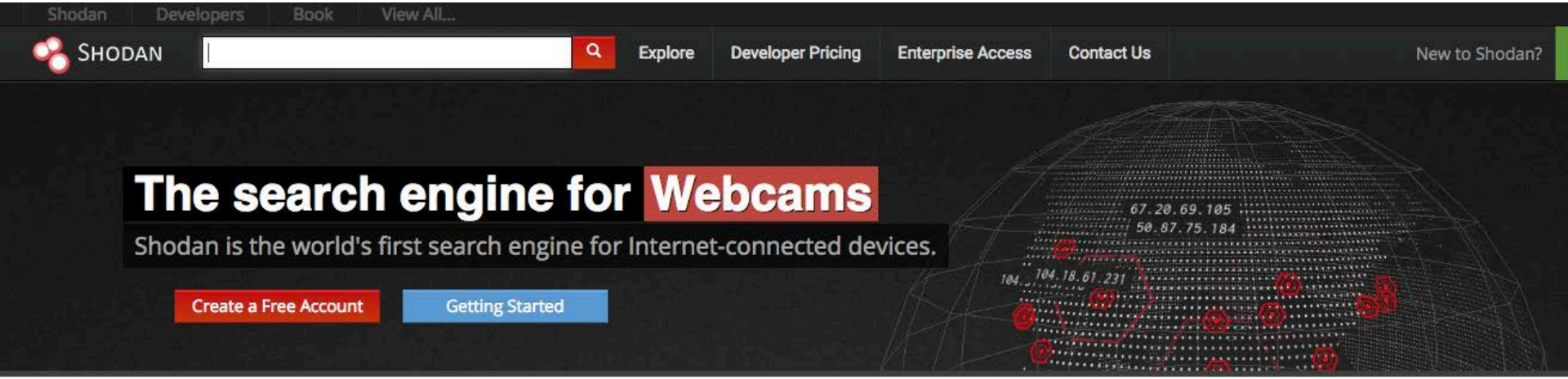
IoT refers to a network of physical devices, vehicles, buildings, and other items (often called "smart devices") embedded with electronics, software, sensors, actuators, and network connectivity enabling these objects to collect and exchange data. Below are examples of IoT devices:

- Home automation devices (e.g., devices which control lighting, heating and cooling, electricity, sprinklers, locks);
- Security systems (e.g., alarm systems, surveillance cameras);
- Medical devices (e.g., wireless heart monitors, insulin dispensers);
- Wearables (e.g., fitness trackers, clothing, watches);
- Smart appliances (e.g., refrigerators, vacuums, stoves);
- Office equipment (e.g., wireless printers, computer mouse, outlets, interactive whiteboards);
- Entertainment devices (e.g., DVRs, TVs, gaming systems, music players, toys); and
- Hubs (devices that control other IoT devices through a single app).

IoT

- The Internet of Things (IoT) -- aka The Internet of Everything (IoE) -- is incredibly difficult to secure
  - Low-cost, consumer grade products frequently have minimal user interface, default passwords, and fixed passwords
  - Target of several large DDoS attacks (e.g., Dyn, 10/2016)
  - Not built with security in mind
- Internet growth...
  - 1992: Tens of thousands of devices
  - 2017: 10B devices
  - 2020: 30B+ devices
  - 2025: 75B+ devices

Hacked IOT DB



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

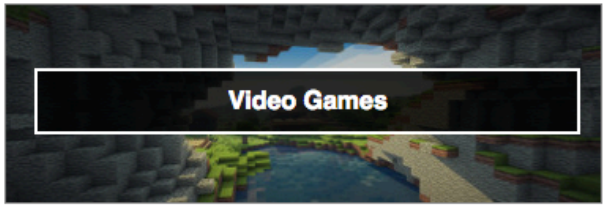
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Featured Categories



Top Voted

10,108

Webcam
best ip cam search I have found yet.

webcam surveillance cams 2010-03-15

3,991

Cams
admin admin

cam webcam 2012-02-06

2,223

Netcam
Netcam

netcam 2012-01-13

1,522

default password
Finds results with "default password" in the ba...

router default password 2010-01-14

Recently Shared

1

Unsecured Linksys Webcams
Unsecured Linksys web cams. Sorry the other one...

webcam cam 2018-07-30

1

Unsecured Linksys Webcams
Linksys cams with no passwords.

webcam cam unsecure 2018-07-30

4

mobile hacking
9284366392

2018-07-28

1

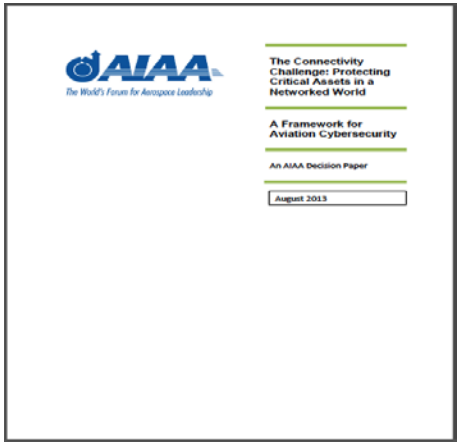
ecshop

2018-07-28

What Now?

AIAA Framework

- *A Framework for Cybersecurity* (AIAA, 2013)
  1. Establish common cyber standards for aviation systems
  2. Establish a cybersecurity culture
  3. Understand the threat
  4. Understand the risk
  5. Communicate the threats and assure situational awareness
  6. Provide incident response
  7. Strengthen the defensive system
  8. Define design principles
  9. Define operational principles
  10. Conduct necessary research and development
  11. Ensure that government and industry work together



http://www.aiaa.org/AviationCybersecurity/

Summary

- The aviation network is complex
- The systems are highly intertwingled
- There are a vast number of attack vectors
- You can't control all parts of the network
- You need response, contingency, and business continuity plans
- Cybersecurity problems are real
  - Corollary: The threat landscape is constantly changing
- Cyberthreats can be mitigated, not solved

Conclusion

- If left unchecked, cyberattacks are an existential threat to the industry
  - As more automation is introduced into systems, they become more prone to attacks -- *the exploits are there just waiting for the enabling vulnerabilities to catch up*
- "We have to move the discussion on cybersecurity from the expert level to the corporate level" (Peter Andres, Lufthansa)
- "Anyone who thinks that technology can solve their problem does not understand technology or their problem." (A paraphrase by GCK)

EMBRY-RIDDLE
Aeronautical University
DAYTONA BEACH, FLORIDA

Questions?