SECURING UNMANNED AUTONOMOUS SYSTEMS FROM CYBER THREATS

PAPER BY: BHARAT B MADAN, MANOJ BANIK, DOINA BEIN

SLIDES BY: CONNOR BURNETT

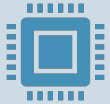
MOTIVATION

- In 2011, an RQ-170 Sentinel drone was successfully hacked by Iranian military
- Causes?
  - Malfunctioning or jamming of command and control (C2) links leading to crash landing
  - Hijacking the vehicle by taking over its C2 links
  - Spoofing of global position system (GPS) transmitters

THREE SECURITY ATTRIBUTES

Confidentiality

Ability of a system to assure it can prevent access to data by unauthorized entity



Integrity

Ability of a system to assure it can prevent unauthorized alterations of data by any entity

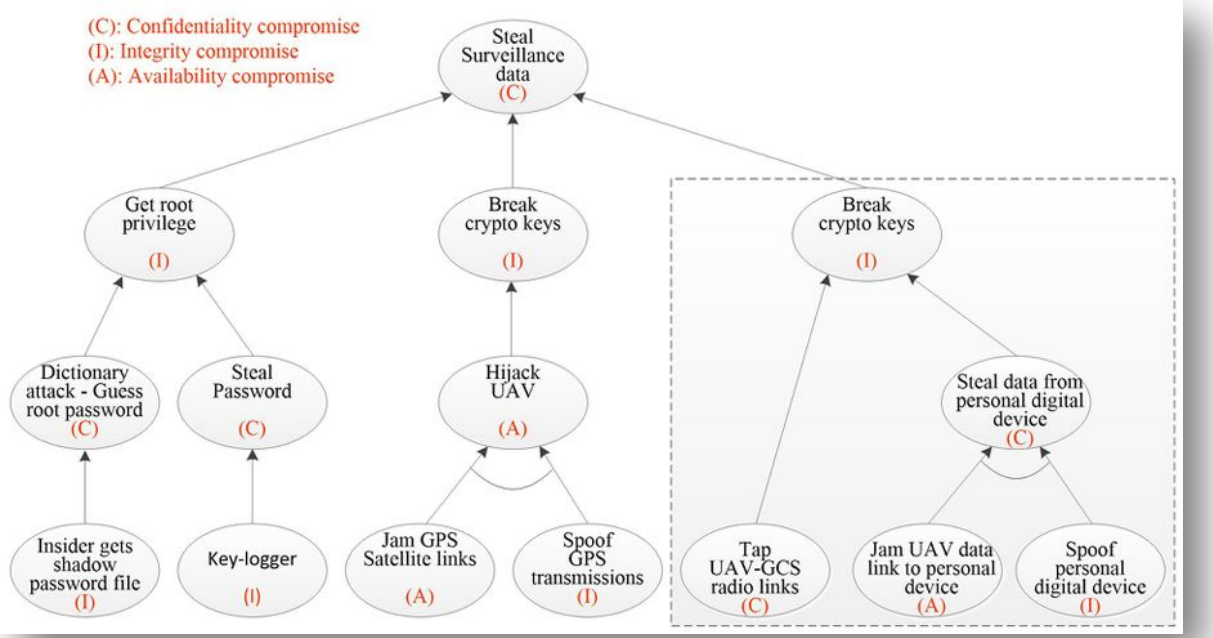
Availability

Ability of a system to assure that data and system resources are made available within specified time to all authorized entities

FORMALIZING ATTACK STRATEGIES: ATTACK TREES

Security mechanisms must be designed so an attacker cannot reach the root node from its "child"

Finding a solution can be reduced to *n* simpler problems



DEFENDING AGAINST CONFIDENTIALITY THREATS

Common attacks

- Internal personnel attack: internal employee gets higher privileged access to a computer
- Capture data over the network: packet sniffing from wireless communication

Must enforce access control policies based on **Bell-Lapadula (BLP) privacy model**

- L = {Top Secret, Secret, Confidential, Un-classified}
- No read up, No write down
- Does not handle integrity (data can be changed by unauthorized members)

Use the most up-to-date encryption techniques

- Wired Equivalent Privacy (WEP) or Wireless Protected Access (WPA) with RC4 encryption use 64-bit keys that can easily be broken
  - WPA2 and AES use 128- or 256-bit keys

DEFENDING AGAINST INTEGRITY THREATS

Common attacks

- Man-in-the-Middle (MITM): data sent by sender is modified by attacker before it arrives at receiver
- Origin Authentication: attacker assumes the identity of the sender and sends fake data that appears real

Biba's Model

- Simple integrity axiom: "No read down" – prevents higher levels from reading lower classification, preventing bad information from moving up the classification levels.
- Integrity axiom: "No write up" – prevents lower classifications from modifying higher classification data.
- Biba's model is used when system integrity is more important than system confidentiality (Bell-Lapadula)

Digital Signature (DS)

- Generate a unique hash *h(m)* to an arbitrary size data block or message *m*
- Store data, file, or communication message is now stored as a tuple: *<m, h(m)>*
- Receiver can verify authenticity of message by using sender's public key

DEFENDING AGAINST AVAILABILITY ATTACKS

Common attacks

- Jamming communication links: sending high-energy random noise to increase interference
- Malware injection: stack buffer overflow can overwrite return address with random bytes

Spread-Spectrum digital communication

- Signal within a certain frequency is deliberately spread to produce a signal with a larger frequency
- Reduces the ability for a specific frequency band to be targeted

StackGuard and NX bit

- Mitigate stack smashing and buffer overflows
- "No Execute" bit in Intel X86 processors ensures bytes place on the stack cannot be interpreted as executable code

CVSS CYBER RISK (COMMON VULNERABILITY SCORING SYSTEM)

- Base score assigns a risk score to vulnerability based on exploitability and impact
  - **Exploitability**
    - Access Vector (AV)
      - Local = 0.395, Adjacent Network = 0.646, Public Network = 1.0
    - Access Complexity (AC)
      - High = 0.35, Medium = 0.61, Low = 0.71
    - Authentication (Au)
      - Multiple = 0.45, Single = 0.55, None = 0.705
  - **Impact**
    - Scores confidentiality, integrity, and availability
      - None = 0, Partial = 0.275, Complete = 0.66

$$Exploitability = 20 \times AV \times AC \times Au$$

$$Impact = 10.41 \times [1 - (1 - Impact_C)(1 - Impact_I)(1 - Impact_A)]$$

$$Base\ Score = f(Impact) \times [(0.6 \times Impact) + (0.3 \times Exploitability) - 1.5)]$$

EXAMPLE CVSS TABLE

Threat	AV	AC	Au	$Impact_C$	$Impact_I$	$Impact_A$	B-Secore
C2 radio link jamming	Adj Net	Low	None	None	None	Comp.	5.4020
Data link snooping	LocNet	High	Mult	Comp.	None	None	3.6691
MITM Command Link	PubNet	High	Mult	None	Part.	Part.	3.2021
MITM Data Link (local)	LocNet	High	Mult	None	Comp.	None	3.6691
MITM Data Link (Pub)	PubNet	High	Mult	None	Comp.	None	4.5656
Malware infection	PubNet	High	Mult	Part.	Part.	Part.	4.2639
KeyLogger	LocNet	High	Mult	Comp.	Part.	Part.	4.8538
WiFi DisAssociate (DoS)	LocNet	Low	None	None	None	Comp.	4.9413
WiFi DisAssociate (KeyTheft)	LocNet	High	Single	Comp.	Part.	Part	5.1842

AV: Access Vector; AC: Access Complexity; Au: Authentication; C2: command and control; MITM: Man-in-the-Middle; DoS: Denial of Service.

CVSS v3.0 Ratings

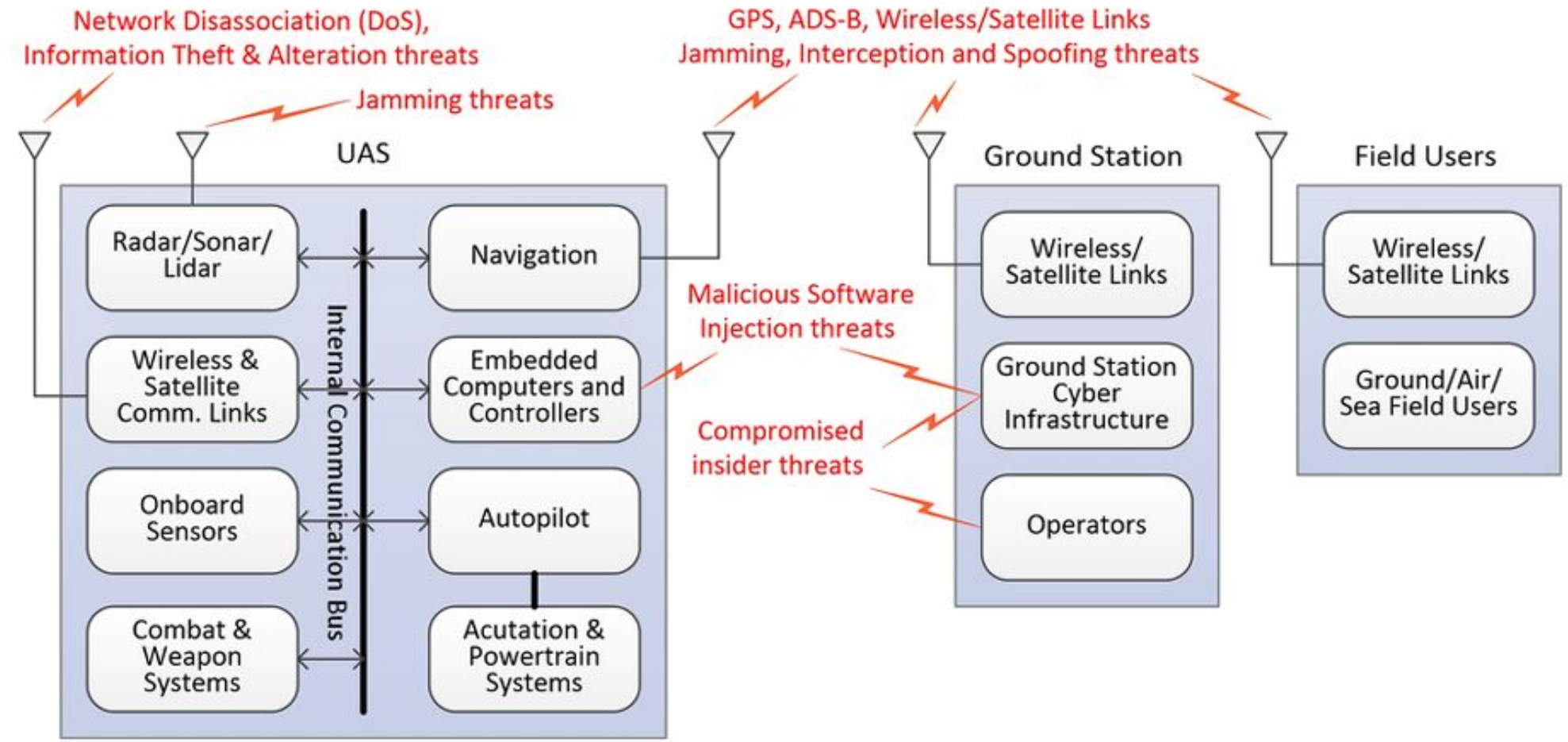
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

WOULD I ACCEPT THIS PAPER?

- No.
  - The paper lacked any novel ideas and offered security solutions that are already industry standards (WPA2, DS, StackGuard)
  - Very repetitive and not well organized

DISCUSSION

- What security measures would you implement in a modern military drone to prevent critical systems from being attacked?


Network Disassociation (DoS),
Information Theft & Alteration threats
Jamming threats
GPS, ADS-B, Wireless/Satellite Links
Jamming, Interception and Spoofing threats
UAS
Ground Station
Field Users
Radar/Sonar/
Lidar
Navigation
Wireless &
Satellite
Comm. Links
Embedded
Computers and
Controllers
Onboard
Sensors
Autopilot
Combat &
Weapon
Systems
Acutation &
Powertrain
Systems
Internal Communication Bus
Malicious Software
Injection threats
Compromised
insider threats
Wireless/
Satellite Links
Ground Station
Cyber
Infrastructure
Operators
Wireless/
Satellite Links
Ground/Air/
Sea Field Users