System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial

Notional Architecture Handout

Melinda Reed
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

15th Annual NDIA Systems Engineering Conference
San Diego, CA | October 22, 2012
Contents

- UAV Notional Architecture
- UAV Potential Supply Chains
- UAV Potential Development Lifecycles
- Generic Supply Chain & Malicious Threat Vectors
UAS Functional Architecture

**Air Vehicle (AV) Functions**
- Execute taxi, takeoff and landings
- Conduct In-Flight Operations:
  - Execute tasking
  - Communicate
  - Navigate
  - Maintain stable, maneuverable flight conditions
- Provide AV with stable power supply & environmental services
- Perform pre-flight preparations
- Conduct post-flight AV systems health & status checks
- Conduct sustain flight ops

**Mission Control Functions**
- Conduct Mission Planning
- Communicate
- Execute Mission
- Conduct ISR data analysis & distribution

**Mission Payload Functions**
- Execute Mission Tasking:
  - Active sensor(s) operations
  - Passive sensor(s) operations
- Perform sensor data collection & storage
- Accomplish onboard sensor data processing
- Execute sensor data off-board distribution
- Perform pre-mission preparations
- Conduct post-mission sensor system health & status check
- Conduct sustain mission payload ops

**Ground Support Functions**
- Provide sustain maintenance support
- Conduct pre & post flight diagnostics
- Accomplish pre & post flight mission support
Find-Fix-Track Scenario

Find, Fix, and Track Functional Order:
1. Accept Mission Plan
2. Allocate mission plans to sensors
3. Initiate active sensor search plan (Search)
4. Collect and process sensor returns
5. Determine if contact is possible target or not (Detect)
6. Locate contact and establish location, course and speed (Locate)
7. Position sensor to identify contact with passive sensor(s)
8. Gain passive sensor(s) data and analyze for contact classification (Classify)
9. Pass sensor data and analysis results to mission control for confirmation (Communicate)
10. Accept tasking to either: 1) initiate tracking or 2) return to search plan (Track)
11. Mission Control tasks return to mission plan execution

Note: Search, Detect, Locate, Classify, Communicate and Track are mission thread functions.
UAS High Level System Design

Air Vehicle
- Airframe/Flight Controls
- Propulsion/Fuel
- Landing/Arresting Gear
- Electrical/Hydraulics/Environmental
- Communications/Navigation/IFF Including SW

Flight Computer Including SW

Radar & Antenna Including SW
- ESM & Antenna Including SW
- Mission Computer Including SW

EO/IR & Housing Including SW

Mission Vehicle Payload

Ground Support System
- Pre & Post Flight Diagnostics
- Maint Support Including SW
- Pre & Post Mission Activities

Flight and GIG Communications
- Mission Execution Including SW
- Mission Planning Including SW
- ISR Data Analysis & Distribution

Mission Control System

GIG
Air Vehicle Mission Payload Diagram

To Air Vehicle

Air Vehicle Mission Payload

Diagram
EO/IR & Housing - Functional

EO/IR Sensor Data Collection

Classification

Sensor Processing

Search Control

Tracking Control

Sensor Control

Data Fusion

Sensor Data Filtering

EO/IR & Housing Including SW
Potential Supply Chain 1

Prime AAA

UAS

- Tracking and Search
  - Sub A - US
    - Sensor
      - Sub ABC - US
      - Controller
        - Sub DEF - US
  - Tracking SW
    - Sub ZZZ - US
      - Tracking Algorithm Code
        - SUB WXY - UK
        - Mathlib Open Source
          - Unknown
  - Development Tools
    - Various US and Foreign Suppliers
      - Custom Alpha/Beta tracker
        - Sub XXX Israel
      - COTS Doppler correction
        - Sub WWW Israel

- Sensors
  - Sub DEF - US
    - IR Sensor
      - Sub XLK - France
    - EO Sensor
      - GOTS - AF

- FPGA
  - Sub DEF - US
    - FPGA Design
      - Sub KLM India
      - FPGA Fab
        - Sub QRS - China
      - FPGA Test / Package
        - Sub MNO - S. Korea

Various US and Foreign Suppliers

Unknown

IR Sensor

EO Sensor

FPGA

GOTS - AF
EO/IR & Housing - Allocated (supply chain 2)
Potential Supply Chain 2

Prime BBB

UAS

Tracking and Search

Tracking Function

Sub TUV -US

Developm ent Tools

Various US Suppliers

FPGA

SUB SSS - UK

Various Open Source Libraries

Custom Tracking Algorithm Software

Sub - TTT - Taiwan

GOTS EO Sensor

GOTS - AF

Unknown

Custom EO Sensor

Sub XLK - Germany

COTS IR Sensor

Sub - HGF

Sub DEF - Aus

Various US and Foreign Suppliers

Various US Suppliers

GOTS EO Sensor

Unknown

Unknown

COTS IR Sensor

Sub QRS - US

Development Tools

Open Source

Sub QQQ - US

Unknown

Sub BCD -US

Controller

Sub HIJ -UK

COTS Processor

Sub QRS - US

Development Tools

Open Source

Unknown
The Traditional (Waterfall) SW Development Lifecycle
Agile Development Lifecycle

http://www.agilegator.com/pmdevelopment.html
Generic Threats – Supply Chain Attacks

Coverage is for what part of the chain is infiltrated and what the malicious insertion accomplishes

**Supply Chain**

**Attack Vectors**

- Clandestine changes to mission data
- Infiltration of sites to insert back doors and malicious logic into some micro electronics (FPGAs and other devices)
- Infiltration of company receiving department to add / substitute components with backdoors to allow remote penetration during operations, denial of service, etc.
- Infiltration of transportation companies to intercept DoD component shipments (developmental or COTS) and substitute components that have malicious code inserted
- Insertion of malicious software in the open source used for math libraries
- Infiltration allowing malicious software implantation through 3rd party bundling
- Establishment of shell company to insert counterfeit parts
- Infiltration to manipulate the hardware or software baselines
- Infiltration of company software development to insert software which exfiltrates data
- Infiltration to compromise the design/fabrication of hardware

Can have multiple levels: OEMs → subassembly suppliers → assembly suppliers → integrators
Generic Threats – Malicious System Exploitation Attacks

Attack Vectors for Malicious exploitation of fielded systems

Exploitation of system design vulnerabilities

Denial of Service (embedded malware)
Kill Switch Activation (embedded malware)
Mission Critical Function Alteration (embedded malware)
Exfiltration (by adversary)
Network Threat Activity (host discovery)
Compromised Server Attacks (on clients)
Malicious Activity (disruption, destruction)
Auditing Circumvention (evading detection)
Web Based Threats (disclosing sensitive info)
Zero Day Vectors (vulnerabilities without fixes)
Improper File/Folder Access (misconfiguration)

Configuration, Operational Practices
Supply Chain (penetration, corruption)
Malware (downloaded, embedded)
External Mission Load Compromise
DNS Based Threats (cache poisoning)
Applications (built-in malware)
E-mail Based Threats (attachments)
Data Leakage (via social media)
Password Misuse (sharing)
Generic Threats – Software Development Life Cycle Malicious Insertion

Coverage is for what part of SDLC is targeted and how malicious insertion is accomplished

**Attack Vectors for Malicious Code Insertion**

- Hidden in software’s design (or even requirements)
- Appended to legitimate software code
- Added to linked library functions
- Added to installation programs, plug-ins, device drivers, or other support programs
- Integrated into development tools (e.g., compiler generates malicious code)
- Inserted via tools during system test