Systems Engineering Requirements Analysis and Trade-off for Trusted Systems and Networks Tutorial

Notional Architecture Handout

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

Paul Popick
Johns Hopkins University Applied Physics Lab
Contents

• UAS Notional Architecture
• UAS Potential Supply Chains
• UAS Potential Development Lifecycles
• Generic Supply Chain & Malicious Insertion Threats/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 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

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

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

Find-Fix-Track Functional Architecture

**Execution mission tasking functions**
- Accept Mission Plan
- Allocate mission plan to sensors
- Initiate active sensor search plan (*Search*)
- Position sensor to identify contact with passive sensor(s)
- Accept tasking to either: 1) initiate tracking or 2) return to search plan (*Track*)
- Mission Control tasks return to mission plan execution – *next cycle in FFT kill chain execution*

**Find-Fix-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.
EO/IR & Housing – Functional

- Classification
- Sensor Processing
- Sensor Control
- Search Control
- Tracking Control
- Data Fusion
- EO/IR & Housing Including SW
- EO/IR Sensor Data Collection
EO/IR & Housing – Physical (Supply Chain 1)

- Processor
- Custom ASIC
- SW
- OS
- FW
- MEM
- Databases
- FPGA
- HDL
- Filter
- IR Sensor
- PrCB
- EO Sensor
EO/IR & Housing – Allocated (Supply Chain 1)
Potential Supply Chain 1

UAS

Prime AAA

Sub A - US

Tracking and Search

Sub ABC - US

Sensor Control HW

Sub ZZZ - US

Control, Tracking, & Search HDL

Sub DEF - US

Sensors

Development Tools

Tracking Algorithm Code

Various US and Foreign Suppliers

Custom Alpha/Beta tracker

Sub XXX Israel

Sub WXY - UK

Various Open Source Libraries

COTS Doppler correction

Sub WWW Israel

Unknown

IR Sensor

Sub XLK - France

EO Sensor

GOTS - AF

FPGA

Sub DEF - US

Sub HIJ - India

FPGA Test / Package

Sub QRS - China

FPGA Fab

Sub KLM India

Sub MNO - S. Korea

IR Sensor

Sub DEF - US

EO Sensor

GOTS - AF

FPGA

Sub DEF - US

Sub HIJ - India

FPGA Test / Package

Sub QRS - China

FPGA Fab

Sub KLM India

IR Sensor

Sub DEF - US

EO Sensor

GOTS - AF

FPGA

Sub DEF - US

Sub HIJ - India

FPGA Test / Package

Sub QRS - China

FPGA Fab

Sub KLM India
EO/IR & Housing – Physical (Supply Chain 2)

EO/IR & Housing Including SW

- Microcontroller
- Processor
- DSP
- SW
- MEM
- PrCB
- EO 1
- IR 1
- EO 2
- IR 2

Flow diagram showing the integration of EO/IR and housing elements, including SW and MEM components.
EO/IR & Housing – Allocated
(Supply Chain 2)

- Classification/Sensor Processing
  - Microcontroller
  - SW
  - MEM

- Sensor Control, Search Control, & Tracking Control
  - SW
  - MEM
  - Processor

- EO/IR Sensor Data Collection
  - EO 1
  - IR 1
  - EO 2
  - IR 2

- Data Fusion
  - DSP
  - SW
  - PrCB
Potential Supply Chain 2

UAS

Prime BBB

Tracking SW

Sub TUV-US

Tracking and Search

Sub B-US

Sensors

Sub BCD-US

Controller

Sub HIJ-UK

Development Tools

Custom Tracking Algorithm Software

Mathlib Open Source

Unknown

Various US Suppliers

Various US and Foreign Suppliers

GOTS EO Sensor

GOTS - AF

Custom EO Sensor

Sub TTT - Taiwan

Custom IR Sensor

Sub XLK - Germany

COTS IR Sensor

Sub HGF

Sub DEF - Aus

Various US and Foreign Suppliers

COTS Processor

Sub QSS-US

Open Source

Unknown

Sub QRS-US

Control SW

Sub QQQ-US

Development Tools

DoD Program Protection
March 2013 | Page-13

Distribution Statement A – Approved for public release by OSR on 3/15/13; SR# 13-S-1385 applies.
The Traditional (Waterfall) SW Development Lifecycle
Agile Development Lifecycle

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

Representative attacks illustrate where in the supply chain the infiltration occurs and what the malicious insertion accomplishes.

**Supply Chain**
- Program Office
- Contractor
- Distribution Process
- Distribution Network
- Processing/Packaging
- Primary Production

**Representative Supply Chain Attacks**
- 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 Insertion in the Software Development Life Cycle

Representative attacks illustrate what part of the 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
Generic Threats – Malicious System Exploitation Attacks

Representative Attacks and Vectors for Malicious Exploitation of Fielded Systems

- 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)

- Supply Chain
- Embedded Malware