Cross Domain Capabilities

presented to:

CDSE Workshop
Who is Tresys?

- **Cyber security engineering company**
  - Founded in 1999, ~50 employees
  - 50% products, 50% services
  - Headquarters in Columbia, MD

- **Deep expertise in OS security, Cross Domain Solutions**
  - Security-Enhanced Linux (SELinux), SE for Android
  - Cross domain technology
  - Content filtering
  - Certification & accreditation
Customers

GOVERNMENT

COMMERCIAL

[Logos of various government and commercial entities]
Products

Cross Domain Solutions

- **XD Bridge™**
  Certified dual-guard cross domain appliance
- **XD Guardian™**
  Exportable dual-guard cross domain appliance
- **XD Sidecar™**
  Deep content inspection and filtering application

Portable Media Inspection

- **XD Air™**
  Media inspection and transfer appliance
XD Bridge

Low-Latency Dual-Guard, Quad-Diode Cross Domain Appliance
Overview

Dual-Guard, Quad-Diode 1U Appliance

- Independently configurable high- and low-side guards
- Integrated 1Gb send-only/receive-only optical diodes (one pair per guard)
- Low latency, high throughput
- Uni-directional or bi-directional
- File transfer or streaming
- On UCDSMO Baseline, TS/SCI ↔ unclassified
- TSABI certified, SABI pending
Environmental Specs

- Designed for data center, mobile or transportable environments
  - 1U server: 16 5/8” x 26” x 1 3/4”
  - 18 lbs.
  - 170W peak, 70W typical
- Number of Domains: 2
- OS: Red Hat Enterprise Linux w/ SELinux
- Throughput: 700MB/sec, <10ms Latency
Flexible Packaging

Rugged Avionics Interface Computer
- High End Performance – Intel Core i5 – Haswell
- Range of IO options with XMCs, mPCIe, removable SSDs
- 8.5” x 5.5” x 3.9” and <6 lbs.

Compact Avionics Interface Computer
- Low Power, Small Form Factor - Intel Atom processors
- Avionics IO expansion capabilities, mPCIe, removable SSD
- 5.5” x 5.0” x 1.5” and <2 lbs.

Nano Avionics Interface Computer
- Portable Maintenance Aids, Very Small Form Factor - ARM based
- Computing, Ethernet to 1553 bridging, 1553/429 Converter
- 3.5” x 2.5” x 1.5” and <1 lbs.
Filters

XML Imagery
MS Office, PDF
IP Data Streams

• ISR Sensor Data Streams
• Video
• Unclassified Data Feeds (NWS, FAA)
• Monitoring / Reporting Information
• Equipment Software Updates

Off-Board Mission Planning Systems
• Fusion Workstations
• Coalition Info Sharing
• Maintenance/Logistics Systems

Low-Side Security Domain

High-Side Security Domain
Roadmap

Raise the Bar
- Next Generation Filter architecture (NGF)
- Deep Content Inspection
- Data Format Description Language (DFDL)

Low-Latency Filtering
- Packet-filtering engine
- Messaging protocols
  - XML-based pub/sub
  - JSON, SOAP/REST
  - Link16
- Full motion video
  - KLV filtering
  - Transcoding
Content Aware Dynamic Routing Engine

**Incoming Packets**
- Frame Header
- IP Header
- UDP Header
- UDP Data
  - aircraft id
  - timestamp
  - speed
  - altitude
  - hdg
  - latitude
  - longitude

**CADRE**
- Inspect
- Modify
- Forward
- Drop

**CADRE Filtering Example**

<table>
<thead>
<tr>
<th>Inspect Payload and/or Headers</th>
<th>Modify Contents (optional)</th>
<th>Drop or Forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft ID on exclusion list</td>
<td>n/a</td>
<td>Drop</td>
</tr>
<tr>
<td>Timestamp within range</td>
<td>Redact aircraft id</td>
<td>Forward</td>
</tr>
<tr>
<td>Lat/Lon within region</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Format Description Language (DFDL)

Enables XML-based Filtering for non-XML Data

Non-XML Data

- aircraft id
- timestamp
- speed
- altitude
- hdg
- latitude
- longitude

XML Data

```
<track>
  <id>UA98</id>
  <speed>300</speed>
  <alt>34000</alt>
  <location>
    <lat>39.2037</lat>
    <lon>-76.8610</lon>
  </location>
</track>
```

DFDL Parser

DFDL schema

XML-based content inspection and filtering
Full Motion Video

Demux / Decode
- Video Data & Metadata
- Caption Data
- Audio Data
- KLV Data

Inspect / Sanitize
- Check header fields & flags
- Video frame data checks, frame rate
- Remove or filter caption text
- Pass or remove stream(s)
- Verify key in standard dictionary
- Compare length of value field
- Verify checksum
- Remove sensitive keys / values & frames

Encode / Mux
- Sanitized Video Data & Metadata
- Sanitized Captions
- Sanitized Audio
- Sanitized KLV Data

MPEG Transport Stream

Input

Output
Advantages

- Very strong edge of network protection
- Fast – low latency, high throughput
- Hardware enforced uni- or bi-directional transfers
- Flexible filtering – customer/integrator can add/maintain filters including Deep Content Inspection
- Flexible packaging: 1U server to tactical
- SABI/TSABI certifications
Exportable Dual-Guard, Quad-Diode Cross Domain Appliance
Overview

- Exportable CDS capability
- UCDSMO evaluation in process
  - SDR complete 2/27/2016
  - Functionality Body of Evidence available
  - Same level of testing as the US SABI process
- XD Bridge sponsor has approved the product creation
- Will require a TAA and approval by the State Department
  - XD Guardian is currently export restricted under the International Traffic in Arms Regulations (ITAR), but is expected to transition to Commerce Department purview, Export Administration Regulation (EAR), in mid-2016.
  - Under the ITAR restrictions, a Technical Assistance Agreement (TAA) is required for export of XD Guardian. When the EAR approval is granted, no TAA will be required.
Differences from XD Bridge

- Processing pipeline software reviewed for export by NSA
- "RuggedDrive" key fob
- Physical key controls write access to crypto key storage
- Tamper switches
- Redundant hot-swappable power supplies
- Separate management network port
Questions?

Ken Walker
kwalker@tresys.com
410-290-1411