DDS is a Data-Centric Communications Middleware

- **Distributed** Data Communications – no brokers required
- System Components are **Decoupled**
- **Robust** infrastructure for critical systems
- **Scalable** from edge to cloud, from bare metal to servers
• DomainParticipant
  • Associated with a Domain
  • Communicates with other DomainParticipants in the same Domain
  • Contains Data Writers, Data Readers, Topics

• Data Writers and Data Readers are “matched” during Discovery

• DataWriter publishes data on a Topic
• DataReader subscribes to a Topic
• Each Topic has a defined Data Type
• Automatic
  • No configuration of IP address, port numbers, servers, or brokers
  • Peers may be on the same machine or across a network
  • Simply indicate your intent to publish or subscribe, and start writing/reading

• Dynamic
  • Peers may come and go, or move at any time
  • Publishers and Subscribers may be created an deleted
  • Networks may be disconnected and reconnected
DDS Configurability: QoS

QoS Policy
- DURABILITY
- HISTORY
- LIFESPAN
- WRITER DATA LIFECYCLE
- READER DATA LIFECYCLE
- ENTITY FACTORY
- RESOURCE LIMITS
- RELIABILITY
- TIME BASED FILTER
- DEADLINE
- CONTENT FILTERS

QoS Policy
- USER DATA
- TOPIC DATA
- GROUP DATA
- PARTITION
- PRESENTATION
- DESTINATION ORDER
- OWNERSHIP
- OWNERSHIP STRENGTH
- LIVELINESS
- LATENCY BUDGET
- TRANSPORT PRIORITY
Cyber Threats
Real World Examples
Example Threat Analysis

SWARMS

Smart and Networking Underwater
Robots in Cooperation Meshes
SWARMS Case Study

Corrosion Prevention

Pollution Monitoring

Plume Tracking

Seabed mapping
Berm Building
• Threat Analysis
  
  • Take over of unmanned and autonomous vehicles
    • Oil / gas lines
    • Military / civilian vessels
  
  • Unauthenticated drone infiltrating swarm
  
  • Release of Confidential Information
    • Information on drone mission, capability
    • Nature of items found on sea floor (weapons, e.g.)
    • Environmental data
Example Threat Analysis

Duke Energy Emerging Technology Office

OpenFMB Cyber Security Overview
OpenFMB Case Study

Key Observations:
1. Single-Purpose Functions
2. Proprietary & Silo'ed systems
3. Latent, Error-prone Data
4. OT/IT/Telecom Disconnected
5. No Field Interoperability!

Key Observations:
1. Multi-Purpose Functions
2. Modular & Scalable HW&SW
3. End-to-End Situational Awareness
4. OT/IT/Telecom Convergence
5. True Field Interoperability!
• Loss of power, small areas to wide scale
  • Loss of life
  • Safety and Security Issues
  • Failure of critical infrastructure operation

• Masquerade / Takeover control applications
  • Control the Switch / Breaker / Recloser / Voltage Regulator / PCC
  • Spoof Status
  • Change Setpoints, Disable Protection
  • Drive Distributed Denial-of-Service attack (DDoS)
Cyber Security Elements
• I&A: Identification & Authentication
  • Who is this participant on the network?
  • Do I trust this participant is who he claims?
  • Is this participant authorized to be part of these communications?
Access Control

• Access Control
  • Is checked after Identification & Authentication
  • Does this participant have permission to join the network?
  • Does this participant have read and/or write access on the network?
• Integrity
  • Has the data been tampered with?

• Confidentiality
  • Hide the data, keep it secret.
DDS Security
The Basics
• Secure communications solution fully integrated into the DDS architecture
  • Standardized API and wire protocol for Portability and Interoperability

• Covers all aspects of secure communications, including:
  • Authentication
  • Integrity
  • Confidentiality
  • Access Control

• Plug-in model
  • Standardized
  • User defined
Why DDS Security

• DDS Security is still DDS
  • Decoupled, Flexible, Scalable architecture
  • Eases development of distributed systems across disparate computing platforms
  • Powerful configurability

• Scalable high-performance Security
  • Topic-by-Topic configuration (not transport-level configuration)
Who Uses DDS Security

• Military:
  • Avionics
  • Naval
  • Unmanned Vehicles
  • Ground Stations

• Commercial:
  • IIoT Systems
  • Avionics
  • Automotive
  • Consumer Electronics
  • Energy Solutions / Smart Grid
  • Medical Devices
DDS Security: Plug-in Architecture

- Standardized API
  - Interface between modules and DDS Security protocols
  - Modules may be Standard or Custom
  - Includes all aspects of secure communications

- Standardized modules
  - Interoperable
  - Use common crypto algorithms
• Standardized Plugin Modules
  • PKI + GCM + GMAC
  • AES 256
  • ECDH Key Derivation

• Interoperable
• Apply security policies
  • Integrity / Encryption / Access Controls
• With fine grained controls
  • Individual Topics
  • Application Data, Discovery Data, Liveliness Data
DDS Security Components

- **Identity**
  - Secure Publisher
  - Secure Subscriber

- **Permissions**
  - Domain Governance

- **Certificate Authority (CA)**
  - Identity
  - Permissions

(Each component is marked as "CERTIFIED" with a stamp icon.)
DDS Security
Live Demonstration
• **Covers all Aspects** of secure communications
  - Authentication
  - Access Control
  - Integrity
  - Confidentiality

• **Full Configuration Flexibility** on a Topic-by-Topic basis

• **State-of-the-art** Security Technologies
  - PKI Crypto
  - GCM/GMAC, AES
  - Forward Secrecy

• Maintains key benefits of DDS:
  - **Distributed** Data Communications – no brokers required
  - System Components are **Decoupled**
  - **Robust** infrastructure for critical systems
  - **Scalable** from edge to cloud, from bare metal to servers
Thank you!

Nina Tucker
ntucker@twinoakscomputing.com
http://www.twinoakscomputing.com