Obsolescence Management Challenges

Layered Assurance Workshop

W. Mark Vanfleet

National Security Agency

Global Network Analyst
INFOSEC Analyst
Mathematician

Aug 4, 2009

With Thanks to…

- **Jess Irwin**
  - **Northrop Grumman Corporation**
  - Information Architect
- **Gordon Uchenick**
  - **Objective Interface Systems, Inc.**
  - Senior Mentor / Principal Engineer

Most Urgent Challenges

- The two most urgent mission critical system challenges
- **BEING ON SCHEDULE!**
- **BEING WITHIN BUDGET!**
- While simultaneously…
  - ✓ Architecting systems that affordably **survive obsolescence** and **maintain assurance** against attack.
  - ✓ Building an **infrastructure** for next generation weapons, communications, security and safety critical systems, and "Systems of Systems."

Total Cost of Ownership

- Implementation, Certification & Accreditation
- Deployment
- Operations and Maintenance
- **Technology Refresh**
- **Countering smarter and stronger attackers**
- **Obsolescence**

Obsolescence Cost Factors

- Parts, peripherals, sensors, memory, processors, etc., no longer available
- Standards deprecated or no longer supported
- “Lord High System Guy” unavailable
  - Lord High System Guy: Last surviving member of the original implementation team
- Dysfunctional design documentation
  - Accepted at PDR and CDR, but insufficient to
    - Rebuild the system
    - Modify the system to meet changing requirements
    - Extend the system for interoperability
  - Not updated to “as built”
  - Not purchased or put into escrow
- “Standard Platform” with undocumented modifications
- Attackers get smarter and stronger over time

Obsolescence Management

- Isolate architectural components that evolve at different rates
  - Abstraction Layers isolate S/W (evolves slowly) from H/W (Moore's Law)
- Open interfaces that conform to business objectives
  - Open interfaces around elements, support insertion of 3rd party components
- Use canonical modularity of the system
  - Most mature domains already have well defined H/W and S/W boundaries, need to be opened
- Architect for Separation, Composability, Reuse (multiple instantiation), and Technical Refresh
  - Open Architecture (OA) and Information Assurance (IA) both manage obsolescence
- "Standard Platforms" should be unmodified
  - Hands Off the internals – allows non-disruptive H/W and peripheral upgrades
- Separate Infrastructure from Mission Capabilities
  - Separation enables Composability and Compositionality

- **(Separation || Composition)** ***is the only game in town for managing obsolescence***

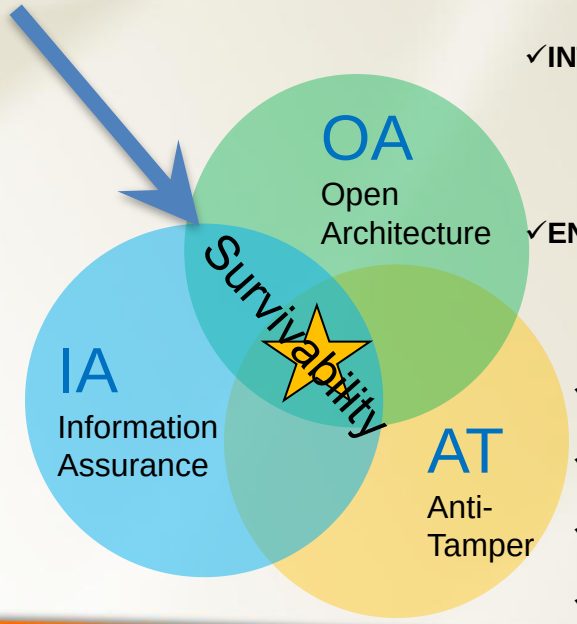
Enterprise Management

- Manage Dialog
  - ISO 15386 Dublin Core
- Manage Content
  - ISO 11179 Metadata Registry
- Manage Exchange
  - ISO 19757 Regular-grammar-based validation - RELAX NG
- Manage Consistancy
  - ISO 20943 Procedures for achieving metadata registry (MDR) content consistency
- Manage Geospatial / Temporal Context
  - ISO 19100 - ISO 19141 Geographic Information Standards
- Manage Business
  - ISO 15000 Electronic business eXtensible Markup Language
- Manage Criteria
  - ISO 15408 Evaluation criteria for IT security
- Manage Assurance
  - ISO 15026 Systems and Software Assurance
- Manage Security
  - ISO 27001 Security techniques — Information security management systems
  - ISO 17799 Code of practice for information security management

OA-IA-AT Principles

- ✓Resistance (observe)
- ✓Recognition (orient)
- ✓Recovery (decide, reactive)
- ✓Adaption (act, proactive)

- ✓CONFIDENTIALITY
- ✓INTEGRITY
- ✓AUTHENTICATION
- ✓AUTHORIZATION
- ✓NON-REPUDIATION
- ✓AVAILABILITY

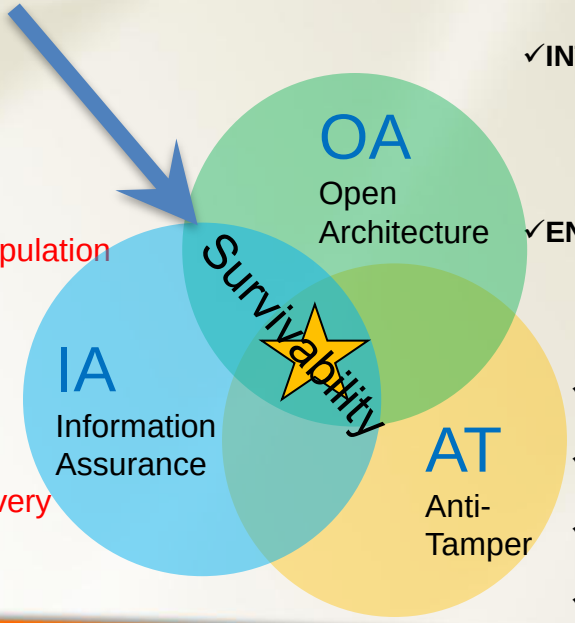


- ✓DESIGNATE KEY INFORMATION EXCHANGES
- ✓MODULARITY & VISIBILITY
- ✓RE-USEABLE COMPONENTS
- ✓INTEROPERABILITY & SECURITY (CJCSI 6212.01E)
- ✓ENABLING ENVIRONMENTS
- ✓DETERRENCE
- ✓PREVENTION
- ✓DETECTION
- ✓RESPONSE

The Details, For Later Discussion

- ✓**Resistance (observe)**
  - Defense in Depth
- ✓**Recognition (orient)**
  - Monitoring
- ✓**Recovery (decide, reactive)**
  - Update API's and protection
- ✓**Adaption (act, proactive)**
  - update policy and definitions
  - reconfiguring network, restrict access

- ✓**CONFIDENTIALITY**
  - Critical Data **PROTECTED**
- ✓**INTEGRITY**
  - Free of Unauthorized Manipulation
- ✓**AUTHENTICATION**
  - Identity Confirmed
- ✓**AUTHORIZATION**
  - Privilege Confirmed
- ✓**NON-REPUDIATION**
  - Proof of Data Origin & Delivery
- ✓**AVAILABILITY**
  - Critical functions **READY**



- ✓**DESIGNATE KEY INFORMATION EXCHANGES**
  - Standardize similar areas at Enterprise level based on community of interest
  - Blue force tracking, strike, mission planning , weather
- ✓**MODULARITY & VISIABILITY**
  - Enable affordable, safe and secure tech. refreshes
  - Enable low cost rapid technology insertion
- ✓**RE-USEABLE COMPONENTS**
  - Commercial based standards (POSIX, Open GL)
  - Published standards (IEEE 1394, 802.11)
  - Established proprietary standards (USB, Blue Ray)
- ✓**INTEROPERABILITY & SECURITY (CJCSI 6212.01E)**
  - Information Enterprise Architecture
  - Use of same policy to trust each other
  - PL5 MLS Need to know vs. Legacy End Node
  - Support for Distributed degree of trust systems
- ✓**ENABLING ENVIRONMENTS**
  - Infrastructure and Enterprise API's Separable
  - Decouple data producers and consumers
  - Register data grams within metadata registry

- ✓**DETERRENCE**
  - Undesirable Consequences
- ✓**PREVENTION**
  - Minimize Attack Surface
- ✓**DETECTION**
  - Visual, Alarm, Loss of Function
- ✓**RESPONSE**
  - Destruction, Disabling, Zeroization