Introduction to Data Centric Security (DCS)

Architecture Approach to Policy-driven Data-centric Information Sharing and Safeguarding

June 2019
Overview

• The target of the Data Centric Security (DCS) at CWIX
  • NATO has the same requirements as an collaborating group of partner agencies

• Overview of Modeling ISS Policy

• The Elements of the Proposed DCS solution for CWIX

• Questions
The Information Sharing and Safeguarding Challenge?

“At the heart of information sharing and safeguarding there lies a paradox”

Information is valuable only if it can be shared with, and used by authorized decision makers

And by increasing the amount information shared, the risk of compromise also increases

• This paradox exists in every domain where sensitive (Private, Confidential, Legally-Significant or classified) information is gathered, processed, used and shared

• While sharing and safeguarding priorities and concerns appear to be mutually exclusive; in reality they are mutually reinforcing concepts:
  o Mechanisms that strengthen protection for sensitive information elements help to build **TRUST** within and between communities
  o Increased **TRUST** increases the willingness to share

• Achieving an effective balance between Sharing and Safeguarding:
  o Requires flexible, agile and adaptive mechanisms and controls during design, implementation, testing, deployment, operations and auditing
  o Represents a data/information management versus technology deficit
  o Cannot be delivered by a single organization, agency or technology
Data Usage: Data Collection, processing and Analysis

- Data is collected from all available sources, and:
- Data is tagged, labeled and catalogued to facilitate discovery, processing, sharing and safeguarding.
- Data is curated and transformed to reflect institutional standards that enables and facilitates analytics
- Data is staged for analytics, business intelligence, and machine learning ...
- Analytics is performed in order to inform situational awareness (hindsight and insight), intelligence (foresight), and planning

The ability to gather all-source data and create quality information for decision makers is the primary role of IM/IT.
Information Sharing and Safeguarding (ISS)

Why Share Data/Information

• Inform Decisions
  • Shared Situational Awareness (Hindsight, Insight);
  • Shared Intelligence (Foresight)

• Enable Collaboration Planning / Collective Action

• Improve Operational Posture – higher quality information:
  • (Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable, Understandable, Reliable, ..., Trusted)

• Resource Multiplier
  • enable and automated response
  • Better allocation available resources

Information is only valuable or useful if it can be shared

• Data must be packaged (aggregated, transformed, marked, redacted and formatted) to balance user need and institutional security policy, assuring:
  • The quality of the information (Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, ..., Trusted)
  • The protection of sensitive (private, confidential, legally-significant and classified) data

• Data and information elements must be tagged and labeled, to and facilitate discovery, processing, sharing and safeguarding

Responsible Information Sharing

Maximize the availability of quality information to authorized users, in accordance with legislation, regulation and policy, while protecting sensitive (private, confidential, legally-significant and classified) data from unauthorized access, release, or manipulation"
Data Sharing and Safeguarding

• Assuring that all information sharing agreements are fulfilled is a complex task
• No good plan / architecture survives for ISS will survive first contact with the operational environment
  • The legislation, regulation, ISAs, MOUs, ..., and operating procedures directing information to be shared are not written in a manner that easily translates into interface design
  • Legislation, regulation, ISAs, MOUs, ..., and operating procedures must be applied to each dataset separately
  • Information sharing and security policies contradict each other
  • It is unlikely that the data/information needs of each internal or external recipient are well understood
  • Requirement for data/information are in a constant state of flux
• Tradition interface (API) design and maintenance approaches cannot keep pace

The ability to share information in a responsible and trusted manner is the cornerstone of a digital strategy

Responsible Sharing
Maximizing the sharing and availability of information of information, while simultaneously protecting sensitive (private, confidential, legally-significant and classified) information from unauthorized access, use, release, or manipulation.

Quality Information
Providing of Information that is Timely, Accurate, Current, Actionable, Complete, Concise, Accessible, Relevant, Consumable / Understandable, Reliable, Trusted, etc…
Modern Information Management on a slide

Our focus area

- Other Data Sets
- Sensor Data (IOT)
- Partner Data
- Records & Reports
- Transactional Data

Our Focus area

- Analytics
  - Descriptive, Diagnostic, Discovery, Predictive, and Prescriptive
- Business Intelligence
- Machine Learning
- Real-time Analytics

Data Lake

- Data Ingest
- Data Curation
- Text Mining
  - Data Mining
- Data Transformation
  - Data Aggregation, Data Integration, Data Staging, Data Mashup, MapReduce, and
- Tagging and Labeling
  - Data Cataloging, Data Validation, Data Wrangling, Data Cleansing, and Data Enrichment

Intelligence

Collaborative Planning

Situational Awareness

High Trust

Moderate Trust

Some Trust

Low Trust

Recipients
Keys to a Solutions Success

• Separate Business, IM and IT Concerns

• Augment and not replace user applications and infrastructure

• Increase flexibility, adaptability and agility during development and operations
  • Model driven architecture / Use of MBSE
  • Rule-based applications / Separate business rules from the code
  • Separate life-cycle for business rules and software
  • Run load of business rules
  • Runtime administration of rules (increased flexibility, adaptability and agility)

• Enhanced logging and auditing
  • Demonstrate responsible, Trusted and Auditable ISS
  • Enable real-time monitoring
  • Enable forensic Auditing

• Integration of open standards
Policy Life-cycle – Separating Concerns

- Networks and Platforms can be deployed independent of applications (e.g., Cloud, On-prem, Hybrid)
- Application are developed to enforce policies (rules and constraints) based on standardized policy models and rapidly deployed to deployed infrastructure
- Policies are defined by the business - based on user / business / operational needs - and deployed to the applications as data sets that are ingested at runtime.
- Libraries of policy models can be maintained and deployed as needed
The UAF is the evolution of the Unified Profile for DODAF and MODAF. The UAF is not another Framework; it is common ontology, UML Profile, and domain model for aligning Architecture Frameworks with Standard Modeling Languages.
Full Traceability ISA to Data Element
STANAG 5525 Example
Participation Models

- Identify the specific participation of a partner in the Information Sharing Agreements, CoIs, ...
- Reduces complexity of diagrams for stakeholders
- Models can be mined to produce spreadsheets and report to aid discussion with stakeholders
Redacting Data Elements

- Redact can be performed by:
  - Sub-setting the data during modeling
  - And Operation in the consuming TransactionalElement
Operations Add many Capabilities.

- Operations can be used to:
  - Transform Data
  - Redact Data
  - Tag and Label Data
  - And more
Separating Policies and Rules from Enabling Technology

Legend:
- IEPPS Defined Elements
- Community Defined Elements
- User Defined Elements

IEF Packaging and Processing Service (IEPPS)
Information Exchange Controller
Semantic Processing
User Data

User Application
User Selected Middleware
Message

Reusable Policy and Library Components
Parser Library
Transformation Library
Business Rules / Decision Logic
Component Configuration

Transforms that Align Data Elements between the Exchange and Storage schemas
Rules governing the tagging and labeling, and filtering (Redaction) of Information

Information Exchange Specifications
Information Exchange Spec
Information Exchange Req
electronic Information Sharing Agreements (eSA)

Policies that Define How Data is Packaged
(Aggregated, Transformed, Masked, Redacted and Permitted) And Processed
(Parsed, Transformed and Marshaled)
Operational Node

Common software for each node with operational needs being addressed by:

- Policies specific to their operations and data environment
- Libraries configured to their specific needs
- Conflation and rules tailored to their needs
Testing at CWIX is seeking to verify that the proposed Architecture drive approach can be used to:

- **Add DCS capability**
  - Tagging and labeling (4777)
  - Selective data redaction
  - Balance the data needs and security considerations for partners at different levels of trust

- **Mediate the flow of data two operational domains with differing:**
  - Information semantics
  - Messaging and network protocols
Evolutionary approach to ISS Capability
Back-up Slides
Information Exchange Framework (IEF)

• Standards Specifications
  • http://www.omg.org/spec/IEPPV/
  • http://www.omg.org/spec/IEF-RA/
  • IEPPS RFP was issued Dec 2017 and currently being developed