Overview of NIST Big Data Interoperability Framework Volume 4

Dr. Arnab Roy
Research Manager
Fujitsu Laboratories of America

NIST Campus
Gaithersburg, Maryland
June 1, 2017

Mark Underwood
AVP
Strategic Initiatives, Controls and Countermeasures
Presentation Overview

- Volume Presentation Outline
- Volume 1, Definitions (Nancy Grady, SAIC)
- Volume 2, BD Taxonomies (Nancy Grady, SAIC)
- Volume 3, Use Cases and General Requirements (Geoffrey Fox, Indiana University)
- Volume 6, Reference Architecture (David Boyd, InCadence Corp.)
- Volume 4, Security and Privacy (Arnab Roy, Fujitsu; Mark Underwood, AVP, Strategic Initiatives, Controls and Countermeasures)
- Volume 8, Reference Architecture Interface (Gregor von Laszewski, Indiana University)
- Reference Architecture Software Implementation Environment and Demonstration (Gregor von Laszewski, Indiana University)
- Volume 7, Standards Roadmap (Russell Reinsch, Center for Government Interoperability)
- Volume 9, Adoption and Modernization (Russell Reinsch, Center for Government Interoperability)
NBDIF Volume Overview

Vol. 1 BD Definitions
Defines common language

Vol. 2 BD Taxonomies
Hierarchy of NBDRA components

Vol. 3 Use Cases & Vol. 5 Arch Survey
Info gathered; requirements extracted

Vol. 6 NBDRA
Developed NBDRA

Vol. 4 S&P
Interwoven topics of S&P examined

Vol. 7 Standards Roadmap
Examine standards wrt NBDRA

Vol. 8 NBDRA Interfaces
Implementation of NBDRA

Vol. 9 Adoption & Modernization
Volume Presentation Outline

• For each volume
  – Scope of the volume
  – Brief recap of version 1
  – Highlights of version 2 accomplishments
  – Summary of version 2 areas needing contributions
  – Topics that could be considered for version 3
Volume 4

Document Scope

- Provide a context from which to begin Big Data-specific security and privacy discussions
- Analyze/prioritize a list of challenging security and privacy requirements that may delay or prevent adoption of Big Data deployment
- Develop the Security and Privacy Fabric integrated into the NBDRA
- Develop Big Data security and privacy taxonomies
- Explore mapping between the Big Data security and privacy taxonomies and the NBDRA
- Security and Privacy (SnP) considerations impact all components of the NBDRA
Volume 4

Version 1 Overview

- Provided an overview of SnP with respect to Big Data
- Collected security and privacy specific use cases
- Developed taxonomy of security and privacy topics
- Examined the interwoven nature of the SnP fabric with other NBDRA components
- Mapped collected SnP use cases to the NBDRA
Volume 4
Version 1 Reference Architecture

- End-Point Input Validation
- Real Time Security Monitoring
- Data Discovery and Classification
- Secure Data Aggregation

Privacy preserving data analytics and dissemination
Compliance with regulations such as HIPAA
Govt access to data and freedom of expression concerns

Big Data Application Provider

Data Centric Security such as identity/policy-based encryption
Policy management for access control
Computing on the encrypted data:
searching/filtering/deduplicate/fully homomorphic encryption
Granular audits
Granular access control

Big Data Framework Provider

- Securing Data Storage and Transaction logs
- Key Management
- Security Best Practices for non-relational data stores
- Security against DoS attacks
- Data Provenance
Volume 4

Version 2 Accomplishments

• Introduced a safety framework, suitable for use by unaffiliated citizens, big data software architects and IT managers
• Expanded the cryptology discussion
• Expanded discussions of various topics such as the intersection of BD system management and SnP guidelines
• Identified guidelines for integrating Big Data systems dedicated to SnP
• Provided for phase-specific BD systems guidance
• Explored relevance of model-based systems engineering to Big Data SnP
Volume 4

Version 2 Opportunities for Contribution

• Submit completed Use Case Template 2
• Contribute to development of Safety Levels chart
• Build/enhance frameworks for Big Data referencing existing ISO and other standards for big data life cycle, audit, configuration management and privacy preserving practices (Section 2)
• Enhance discussion of emerging technology effects on BD SnP (Section 2.4)
• Contribute risk management text (section 5.9)
• Expand discussion of SnP approaches in analytics
• Increase references to SnP focused standards
• Integrate security fabric concepts into Vol 8
Domain-Specific SnP Safety Engineering
Volume 4

Proposed Version 3 Topics

- Big Data SnP Applications for Blockchain
- Features of BD SnP Dependency Models
- Features of security-aware Big Data IDEs
- Traceability Frameworks for “Human Bit”
- Self-Managed, Self-Monitoring Big Data Risk Frameworks
- Impact of AI on Big Data SnP (As User / As Consumer)
- Big Data SnP Microservices and API-First Design Patterns
- DevOps and Container SnP
- Orchestration of SnP Processes
- Big Data Analytics for SnP: Best Practices, Use Cases
- System Communicator Checklists