DATE: May 26, 2021
COMMITTEE: NIST
ISSUE: Guidelines For Software Integrity Chains and Provenance.
AUTHOR: Peter Pavlovich, CTO, Censinet, Inc. ppavlovich@censinet.com

May 12, 2021 marked the beginning of a new era of cybersecurity awareness and activism as the details of President Biden's Executive Order on Improving the Cybersecurity of the Federal Government were released to the public. Among other things, this Executive Order directs that the Secretary of Commerce, through NIST, take immediate steps to identify standards, tools, best practices, and other guidelines to enhance the security of the software supply chain.

Conducting standard security and risk assessments is a key aspect of assessing software integrity chains and provenance with the intent of improving the cybersecurity of software solutions. A real world challenge we face today is the broad disparity in how cybersecurity and risk data is viewed, calculated, measured, and shared by the private and public sectors. Effective supply chain organizations include a process for addressing the security and risk of service providers. The security controls utilized, risk evaluation data, and relevant corrective action plans are captured in unique formats for each organization. The fundamental tenets of the Executive Order underscore the need for a unifying representation data model, enabling organizations a cohesive and unified methodology for sharing cybersecurity and risk information to determine and mitigate the risk of suppliers, identify vulnerabilities, and coordinate, communicate and respond to incidents as they occur.

To enhance or improve anything requires that a set of meaningful, measurable metrics be agreed upon, baselined, and then tracked over time to measure improvement. In the case at hand, such metrics will not likely be simplistic nor easily measured but will be a summarized result of synthesizing assessment data measuring vendors, products, and services against a predefined set of security and risk controls deemed to be relevant for the specific subject and its use within a given organization. To achieve our goal of protecting against cyber threats, vendors must improve the security of their contributions to the software supply chain. Industry transparency of their contributions is imperative.

By providing decision-makers with consistent risk measurement metrics that accurately represent the relative security of offerings in the marketplace, we create immediate transparency of inherent risk that will drive real market incentives for vendors to improve their security posture. The opportunity is to avoid risk by making well-informed decisions.

Data Model

Our ultimate goal is to enable the development of algorithms that, given relatively simple inputs, can predict the risk of security incidents. It will be necessary to experiment with various options for each of these inputs to achieve the desired outcome. This is a 'big data' problem that will require more extensive data sets than would typically be available within a single organization. The ability to easily share and aggregate such data will rely on having a uniform means of representing all the subjects, inputs, outputs, and workflows involved in the entire assessment process.

To move forward, we need a common data representation encompassing these metrics, the relevant controls, the data required to assess compliance with those controls, and appropriate workflows associated with the entire assessment process, along with any pertinent security incident data.

Data Sharing

Our next objective would be to design a standard means by which this data can be securely exchanged or pooled to provide larger and more representative data sets which can be used as input to candidate algorithms and processes.

Call to Action

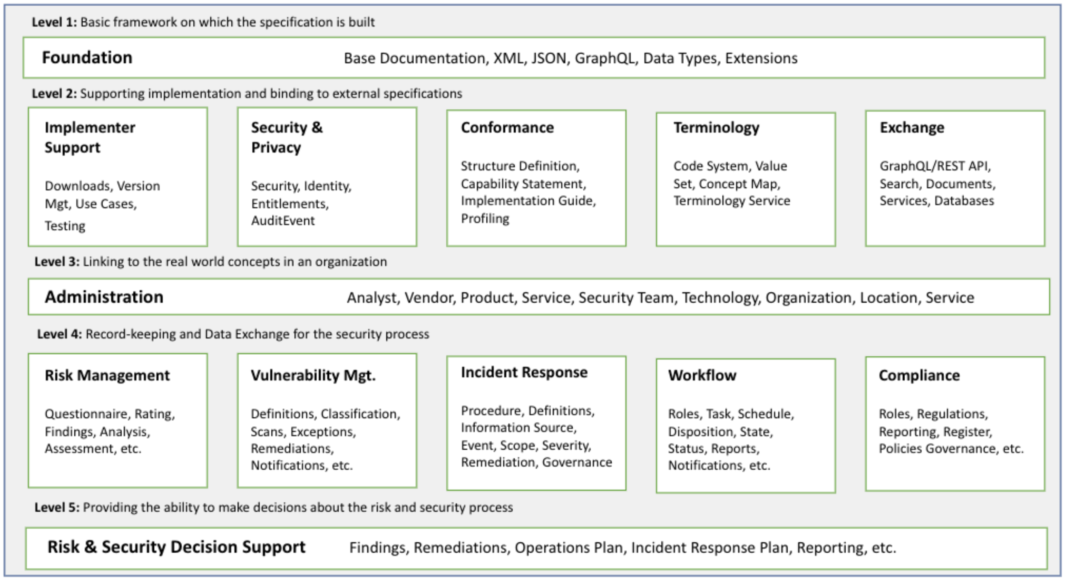
The cited EO provides the impetus to form a working group whose mission would be to create these standards, the availability of which would yield long-term benefits like those realized through the emergence of the SMART on FHIR standard. Specifically, they would facilitate sharing raw assessment data and results across organizations regardless of the specific tools or processes used to perform or manage those assessments. The ability for organizations to share computed assessment ratings via a uniform data schema would also enable NIST to compare various assessment methodologies and/or specific tools' abilities to accurately measure security when viewed as predictors of incident occurrences across the broader marketplace. Additionally, it would foster innovation by encouraging competition between software vendors by removing any proprietary barriers that discourage organizations from easily trying and, when deemed advantageous, adopting newer, more effective, or accurate solutions.

FHIR provides a layered, extensible specification framework that we can easily leverage to provide the foundation for a similar specification covering supply chain security assessment and management. By way of an example, collecting assessment data is often accomplished via a questionnaire resulting in a set of questionnaire responses. FHIR already has a completely adequate representation of these resources in its foundational layer (Layer 1) embodied in the Questionnaire and QuestionnaireResponse resources.

Similarly, we could look to SMART to provide a proven model for how users can securely interact with compliant sources of this data. Since FHIR was initially designed to address the needs of the healthcare domain, we acknowledge that some of the resource types necessary to completely describe the problem space under consideration would require net-new structures. But, clearly, many of the foundational elements needed for the definition and secure use of a successful standard already exist within the Smart on FHIR standard and are appropriate for reuse in this new context.

In summary, this process supports predictive analytics for security teams across the industry to reduce risk based on data. Establishing a working group with a mission to define the standard for the representation and exchange of data relevant to the assessment and management of security concerns and other risks will be instrumental in our efforts to enhance security in the software supply chain and that we should look to SMART on FHIR to provide a proven foundation on which to base that effort.

Cybersecurity on FHIR Standard Proposal



Level 1: Basic framework on which the specification is built

Foundation Base Documentation, XML, JSON, GraphQL, Data Types, Extensions

Level 2: Supporting implementation and binding to external specifications

Implementer Support Downloads, Version Mgt, Use Cases, Testing

Security & Privacy Security, Identity, Entitlements, AuditEvent

Conformance Structure Definition, Capability Statement, Implementation Guide, Profiling

Terminology Code System, Value Set, Concept Map, Terminology Service

Exchange GraphQL/REST API, Search, Documents, Services, Databases

Level 3: Linking to the real world concepts in an organization

Administration Analyst, Vendor, Product, Service, Security Team, Technology, Organization, Location, Service

Level 4: Record-keeping and Data Exchange for the security process

Risk Management Questionnaire, Rating, Findings, Analysis, Assessment, etc.

Vulnerability Mgt. Definitions, Classification, Scans, Exceptions, Remediations, Notifications, etc.

Incident Response Procedure, Definitions, Information Source, Event, Scope, Severity, Remediation, Governance

Workflow Roles, Task, Schedule, Disposition, State, Status, Reports, Notifications, etc.

Compliance Roles, Regulations, Reporting, Register, Policies Governance, etc.

Level 5: Providing the ability to make decisions about the risk and security process

Risk & Security Decision Support Findings, Remediations, Operations Plan, Incident Response Plan, Reporting, etc.