CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS3

Maturity assessment of SDN/NFV technical specifications for secure TELECOM

G. RASCHE
EPRI
United States
grasche@epri.com

D. HOLSTEIN
OPUS Consulting Group
United States
holsteindk@ocg2u.com

T. GODFREY
EPRI
United States
tgodfrey@epri.com

Two relatively new technologies for telecommunication services have spawned a multitude of technical specifications. Cloud-based applications using software defined networking (SDN) and network function visualization (NFV) technology requires cybersecurity protection that involves people, processes, and technology. Most of the technical specifications do not address the combined topics in a holistic manner. They either focus attention on the SDN/DFV technologies or on cybersecurity protection.

One exception is a new IEEE project P1915.1. This standard will specify the security framework, models, analytics and requirements for SDN/NFV. However, P1915.1 is a work-in-progress and will not be ready until 2019. When gathering the data needed to develop P1915.1 it became clear that a template was needed to assess the maturity of the applicable technical specifications. Some specifications are technical reports, others are guides, recommended practices, trial use standards, and a few full standards. To facilitate a comprehensive maturity assessment, a macro-based EXCEL template was developed to summarize the information in a "maturity profile."

A typical maturity profile includes:

Type: standard, trial use standard, guide, report, etc.
Topic focus: people, technology, process, organizational responsibility, cybersecurity protection, physical security protection, access control, use control, data confidentiality, data integrity, data flow management, timely response to events, resource availability, segmentation zones, etc.
Description: title of the document
Status: published, approved – not started, working draft, draft for comment, draft for vote, FDIS, international specification, regional specification, etc.
Required by local law or regulation: YES, NO
Implementation maturity: unit bench test, hosted test (FAT), QA tests (live data feeds), commissioning (SAT), ISOC deployed, DMZ deployed, perimeter defense

deployed, IED embedded security deployed, smart meter infrastructure deployed, PP&O directives deployed, not deployed, unknown, etc.
Adoption level: prototype evaluation, less than 10 deployments, less than 100 deployments, wide scale deployment, not applicable, unknown, etc.
Ease of use: user friendly interfaces, well-formed specifications, configuration management issues, requires vendor-specific tools, interoperability issues, unknown, etc.
Notes: text description of issues, topics covered, etc.

The application security patterns consider:

- Secure communications – create a secure channel for client-to-server and server-to-server communications
- Secure message router – securely route and enforce policy on inbound and outbound messages without interruption of delivery
- Authentication enforcer – centralized authentication processes
- Authorization enforcer – specified policies for access control
- Credential tokenizer – encapsulate credential as a security token for reuse
- Assertion builder – define processing logic for identity, authorization and attribute statements
- User rule – identifies the role asserted by the entity initiating the transaction
- Purpose of use – identifies the purpose of the transaction

This paper describes the content of the maturity profile and how it was used to grade the maturity of the technical specification under consideration. Given these maturity profiles and using selected EPU telecom use cases, a decision process model was developed to define a framework to select the most applicable technical specifications. This paper describes the process to:

- Identify SDN maturity development as it relates to EPU deployment,
- Develop generic SDN migration strategies and options for EPU deployment, including risk mitigation roll-out schedule and cost abatement options, and EPU technical capabilities needed to integrate and manage SDN deployment,
- Identify SDN cybersecurity threat issues, and
- Develop generic SDN security mitigation strategies and options.