Use case extension
- Nobuo Aoki

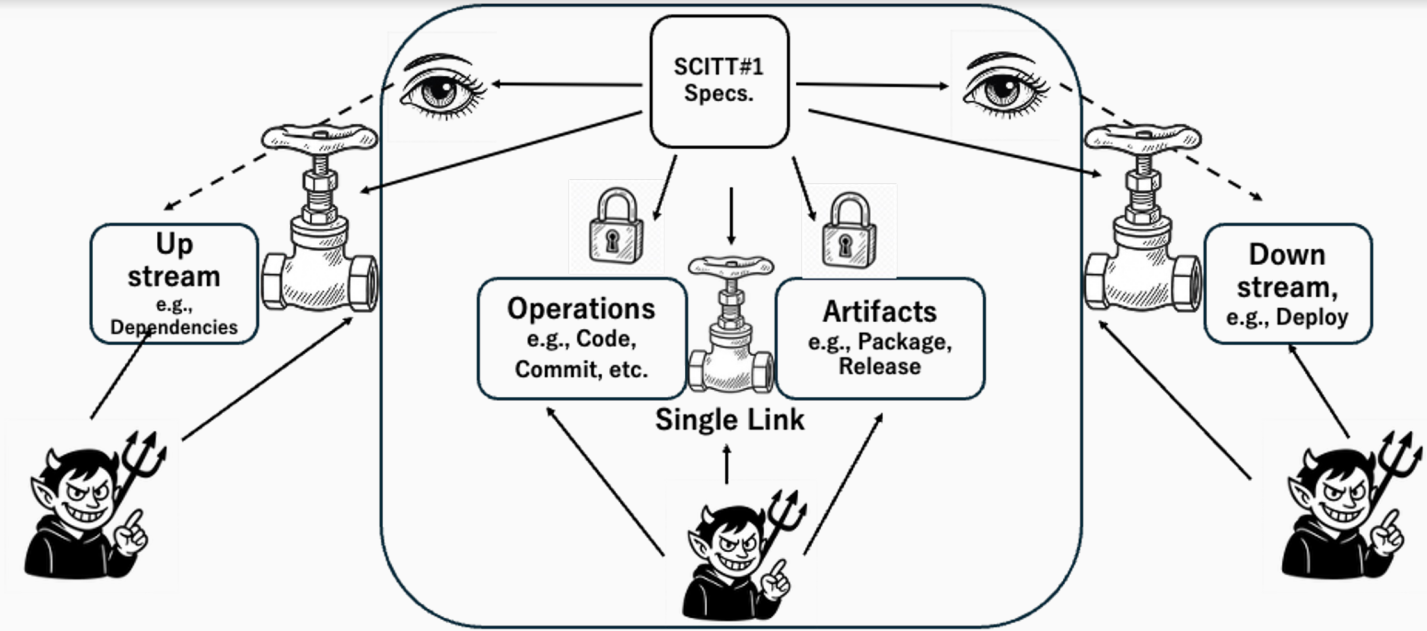
Quick Recup: Use Case Extension I-D

- Extension Request for maximize the appeal of SCITT WG
  - **SCITT** WG is no **S**oftware supply **C**hain **I**ntegrity, **T**ransparency, and **T**rust, but **S**upply **C**hain **I**ntegrity, **T**ransparency, and **T**rust
  - Add Hardware and Computer Architecture Layer
- Main reason author wanted WG support in the draft
  - Revision of chapter#2 for Post SCITT Spec.
  - Consensus is most important

Problem Statement: Level 1/3

- How to comprehensively provide Supply Chain Security information for a Computing Host resource (Software & Hardware)?

SCITT Chapter#1 Specs. Advantages



✅ Delivery of supply chain information throughout the E2E supply chain

Related Specs. to Supply Chain Security

- IETF RFC 9472
  - A YANG Data Model for Reporting Software Bills of ...
  - Successful mapping of SBOM and vulnerabilities
- x-BOM (i.e., Statement for SCITT)
  - SBOM, HBOM, E-BOM, M-BOM, etc.
- Others
  - OpenSSF some project, OCP S.A.F.E. Program, etc.

What are the Challenges in the SCITT Chapter#1 and Other Specs.

- Key-aspects of Supply Chain Security in Cybersecurity
  - Outstanding commander
  - Shield wall

Example case:

HW	e.g., HBOM
SW (e.g., System SW)	e.g., SBOM
SW (e.g., Virtualization Infra.)	e.g., SBOM
SW (App. SW Package)	e.g., SBOM
SW (App. SW Configuration)	e.g., something statement

Even if statements format is perfect, there is ambiguity in the relationships between the statements and some parts remain unclear

Picture Citation from https://en.wikipedia.org/wiki/Shield_wall

Problem Statement: 2/3

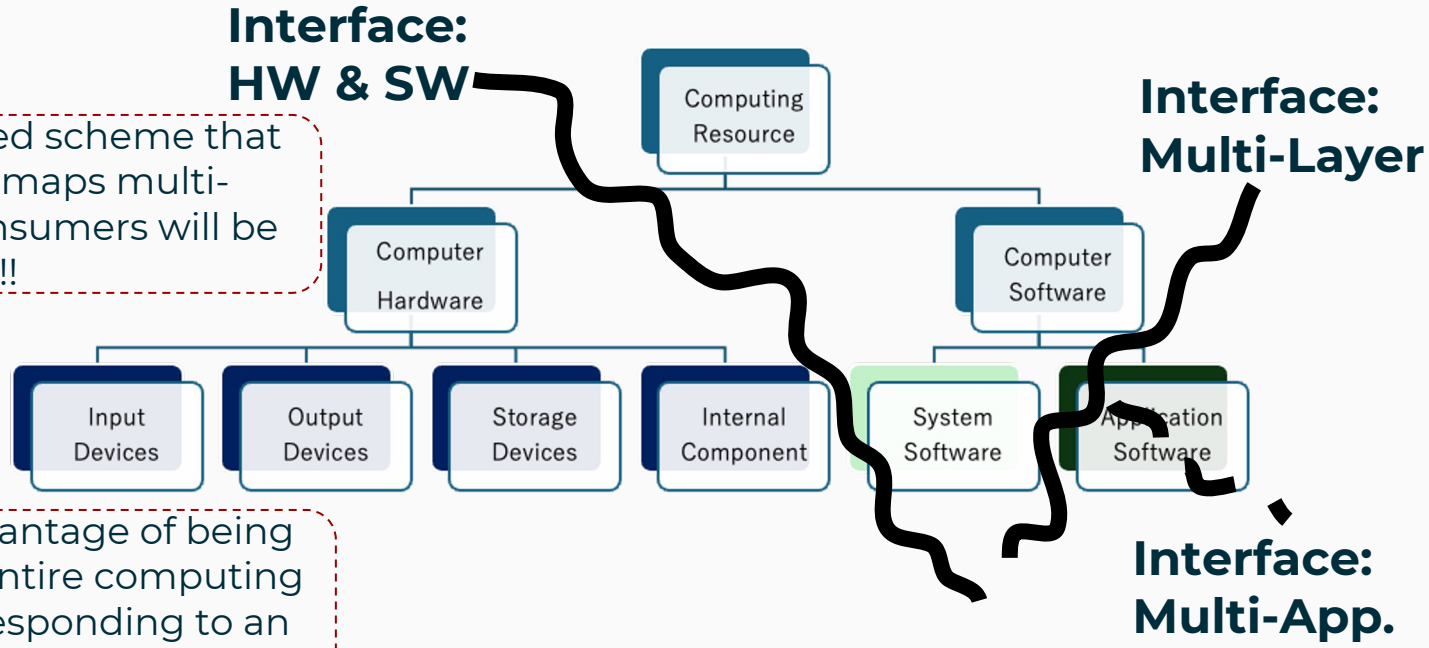
- How to comprehensively provide Supply Chain Security information for a computing resource (Software & Hardware)?

- To express the entire computing resource, isn’t it necessary to combine types of statements?

Boundary of Responsibility for Stakeholders in Computing Resource

If there is an extended scheme that comprehensively maps multi-statements, end-consumers will be happy!!

There is also the advantage of being able to present the entire computing component when responding to an incident easily!!



Problem Statement: 3/3

- How to comprehensively provide Supply Chain Security information for a computing resource (Software & Hardware)?

- To express the entire computing resource, isn't it necessary to combine types of statements?

- Is it possible to map multi-statement supply chain security information?
  - E.g., Extended YANG/MUD-Based Schema to serve as adhesive for interface

Next Steps:

- Placeholder