NTIA Supply Chain Transparency

Framing Working Group
2019-04-11

Éamonn Ó Muirí
https://flic.kr/p/46dsiz
https://creativecommons.org/licenses/by/2.0/legalcode

Stable Topics 1

Required elements, without which there is no SBOM

- Core component identity, sufficient uniqueness
  - Minimum viable identification (MVI)
  - Recommended constructs
    - namespace:name
    - supplier:component:version:hash
- Relationships between components
  - Minimum: “includes”, “alias”?

Optional elements, meta-information needed for most use cases/applications

- Nearly anything you want
  - Yes, really, see “Open Topics 3”

Stable Topics 2

Problem statement [ref]

Terms, partially stable [ref]

- Supplier
- Component
- SBOM
  - overall collection of data and processes
- Inventory
  - core identification, subset of SBOM

When in to produce SBOM, type of SBOM

- Time of build, packagingas, delivery, “as-built”
  - Yes, these are technically different
  - Binary/object, not source
  - Change means new component and new SBOM

Stable Topics 3

Semi-stable?

Depth, one-/multi-hop

- Not either-or, but both
- Supplier creates SBOM for their components
  - Defines components and sufficiently unique names
  - Records dependencies
- Supplier ideally obtains SBOMs for included components from their upstream suppliers
  - One hop upstream required
  - Additional hops optional, but fragile
  - Supplier has first-hand knowledge of what they include and relationship with upstream supplier
  - When not possible, supplier obtains or creates component identifiers
- Supplier delivers collected SBOMs to customer
  - One hop downstream

Open Topics 1

How are SBOMs shared, exchanged? What does transparency look like?

- Multiple techniques, different types of software and systems
  - Files included with distribution
  - URL, unique ID lookup
  - Atom/ROLIE (RFC 8322), SParts?

SBOM history

- Supplier or consumer can maintain records
- Not relying on any central repository, but not preventing archival

Open Topics 2

Opaqueness, transition

- What happens when SBOM is not available?
- Record differences between components
  - Knowledge that there are no further upstream components/dependencies
  - Lack of such knowledge (opaqueness), component may be a terminal/root node or not

Awareness, adoption, how-to, tools

Open Topics 3

Common use cases/applications include

- Intellectual property management
  - License, entitlement, copyright, attribution, other
  - Clear terms for “license” and “entitlement”
- High assurance
  - Provenance, pedigree, forumulation, integrity
- Vulnerability management
  - Requires a catalog of vulnerabilities, like CVE
  - Requires mapping between vulnerabilities and components
  - Means to convey exposure/exploitability of vulnerabilities
- What else should we call out?

Open Topics 4

Awareness, adoption, how-to, tool support

- Easy start guide for “crawl” stage
- Examples
  - Health care proof of concept
  - SWID, SPDX
  - Existing tools?

Services, not-on-premises components and systems

- Provider/operator wants SBOM like any other user?
- Service user man not care, SBOM may change rapidly (daily/hourly)
- Not prevented, but not primary focus?

Spreadsheet

	A	B	C	D	E	F
1	**Supplier**	**Component**	**Version**	**Hash**	**Includes**	
2	OpenSSL	OpenSSL	0.9.8a	0x113a8...	N/A	
3	Apache	httpd	1.3.26	0x33af2...	OpenSSL 0.9.8a	
4	MDM1	FooPump	4.0	0x44a83...	Apache httpd 1.3.26	

namespace: name

org.openssl:”OpenSSL 0.9.8a”

org.apache:”httpd 1.3.26”

com.mdm1:”FooPump 4.0 0x44a83…”

SWID

<SoftwareIdentity name="openssl"
tagId="openssl/openssl@0.9.8a" version="0.9.8a"/>

<SoftwareIdentity name="apache_httpd"
tagId="apache/httpd@1.3.26" version="1.3.26"/>
<Link href="swid:openssl/openssl@0.9.8a"
rel="requires"/>

<SoftwareIdentity name="apache_httpd"
tagId="apache/httpd@1.3.26" version="1.3.26"/>
<Link href="swid:openssl/openssl@0.9.8a"
rel="requires"/>

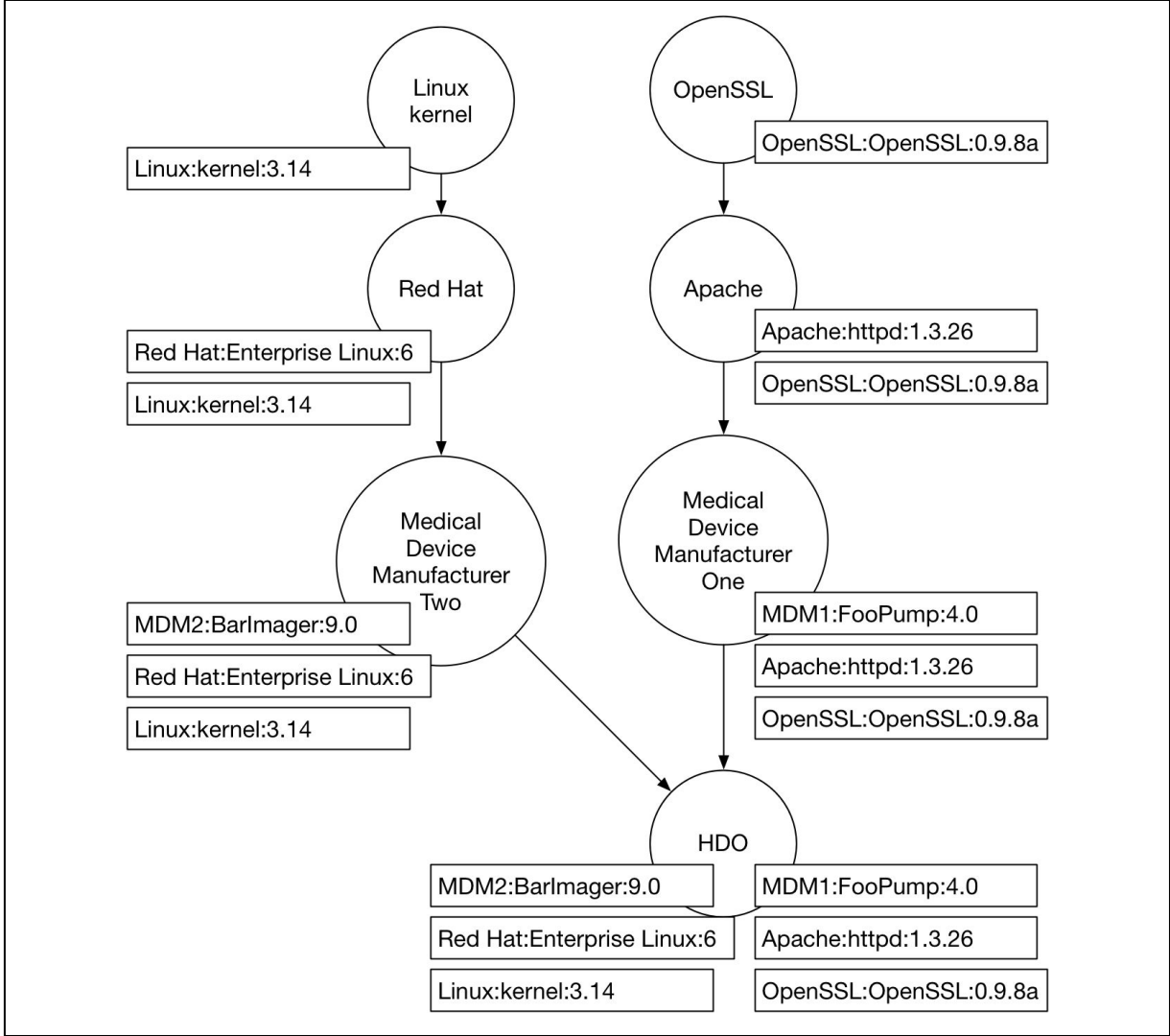
SPDX

PackageName: openssl
SPDXID: openssl/openssl@0.9.8a
PackageVersion: 0.9.8a

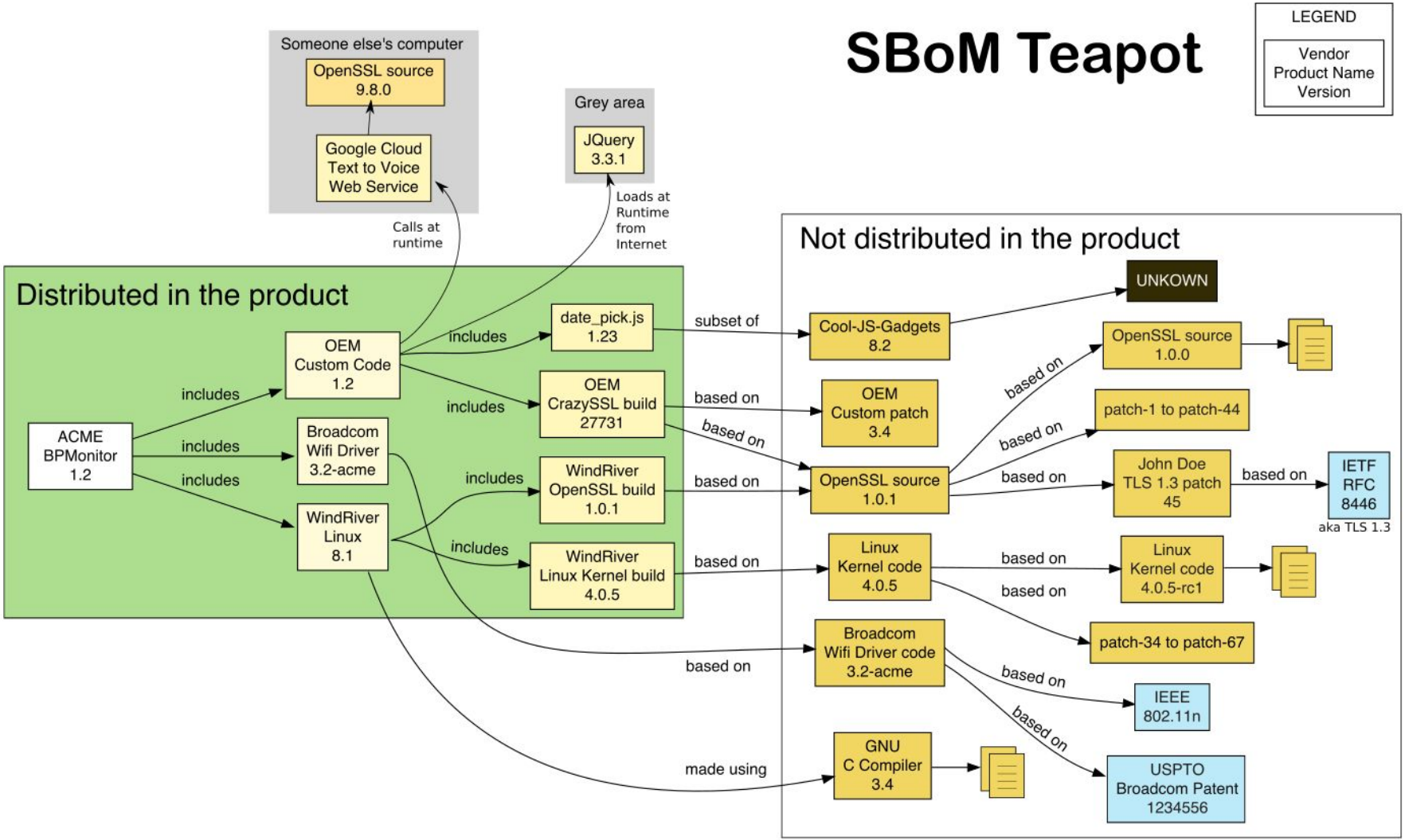
PackageName: apache_httpd
SPDXID: apache/httpd@1.3.26
PackageVersion: 1.3.26
Relationship: openssl/openssl@0.9.8a
PREREQUISITE_OF apache/httpd@1.3.26

PackageName: ”MDM1 FooPump”
SPDXID: mdm1/foopump@4.0
PackageVersion: 4.0
Relationship: apache/httpd@1.3.26
PREREQUISITE_OF mdm1/foopump@4.0

Graph


Linux kernel
Linux:kernel:3.14
OpenSSL
OpenSSL:OpenSSL:0.9.8a
Red Hat
Red Hat:Enterprise Linux:6
Linux:kernel:3.14
Apache
Apache:httpd:1.3.26
OpenSSL:OpenSSL:0.9.8a
Medical Device Manufacturer Two
MDM2:BarImager:9.0
Red Hat:Enterprise Linux:6
Linux:kernel:3.14
Medical Device Manufacturer One
MDM1:FooPump:4.0
Apache:httpd:1.3.26
OpenSSL:OpenSSL:0.9.8a
HDO
MDM2:BarImager:9.0
Red Hat:Enterprise Linux:6
Linux:kernel:3.14
MDM1:FooPump:4.0
Apache:httpd:1.3.26
OpenSSL:OpenSSL:0.9.8a

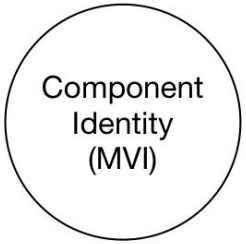
SBoM Teapot


LEGEND
Vendor
Product Name
Version
Someone else's computer
OpenSSL source
9.8.0
Google Cloud
Text to Voice
Web Service
Grey area
JQuery
3.3.1
Calls at
runtime
Loads at
Runtime
from
Internet
Distributed in the product
ACME
BPMonitor
1.2
OEM
Custom Code
1.2
Broadcom
Wifi Driver
3.2-acme
WindRiver
Linux
8.1
includes
includes
includes
includes
includes
includes
includes
date_pick.js
1.23
OEM
CrazySSL build
27731
WindRiver
OpenSSL build
1.0.1
WindRiver
Linux Kernel build
4.0.5
Not distributed in the product
subset of
based on
based on
based on
based on
based on
based on
Cool-JS-Gadgets
8.2
OEM
Custom patch
3.4
OpenSSL source
1.0.1
Linux
Kernel code
4.0.5
Broadcom
Wifi Driver code
3.2-acme
GNU
C Compiler
3.4
made using
UNKOWN
OpenSSL source
1.0.0
patch-1 to patch-44
John Doe
TLS 1.3 patch
45
IETF
RFC
8446
aka TLS 1.3
Linux
Kernel code
4.0.5-rc1
patch-34 to patch-67
IEEE
802.11n
USPTO
Broadcom Patent
1234556

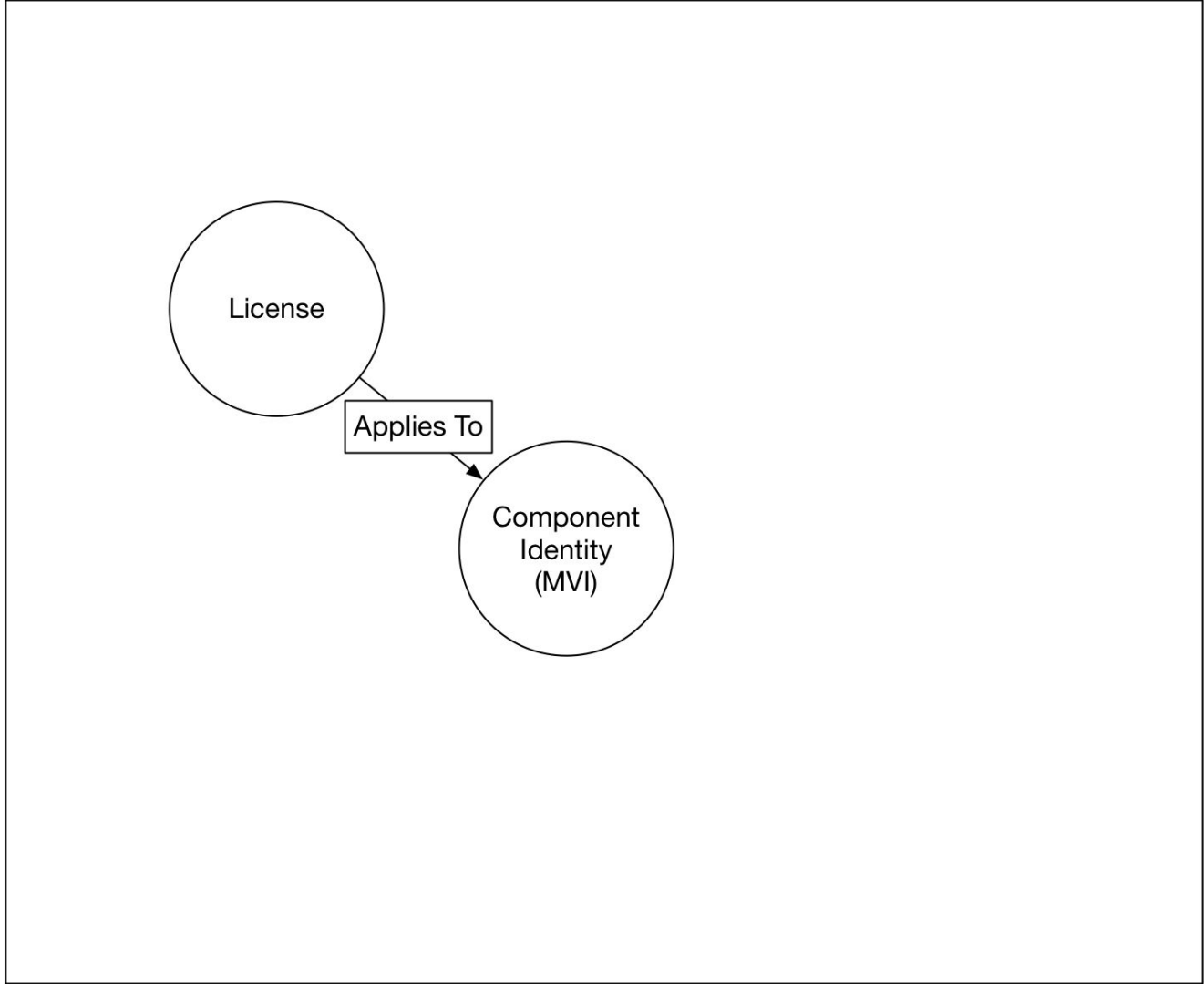
Sample of other data

	SWID	SPDX
Hash	hash-entry hash-alg-id hash-value	PackageVerificationCode PackageChecksum FileChecksum
License		LicenseConcluded PackageLicenseDeclared LicenseName
Entitlement	@entitlementKey	

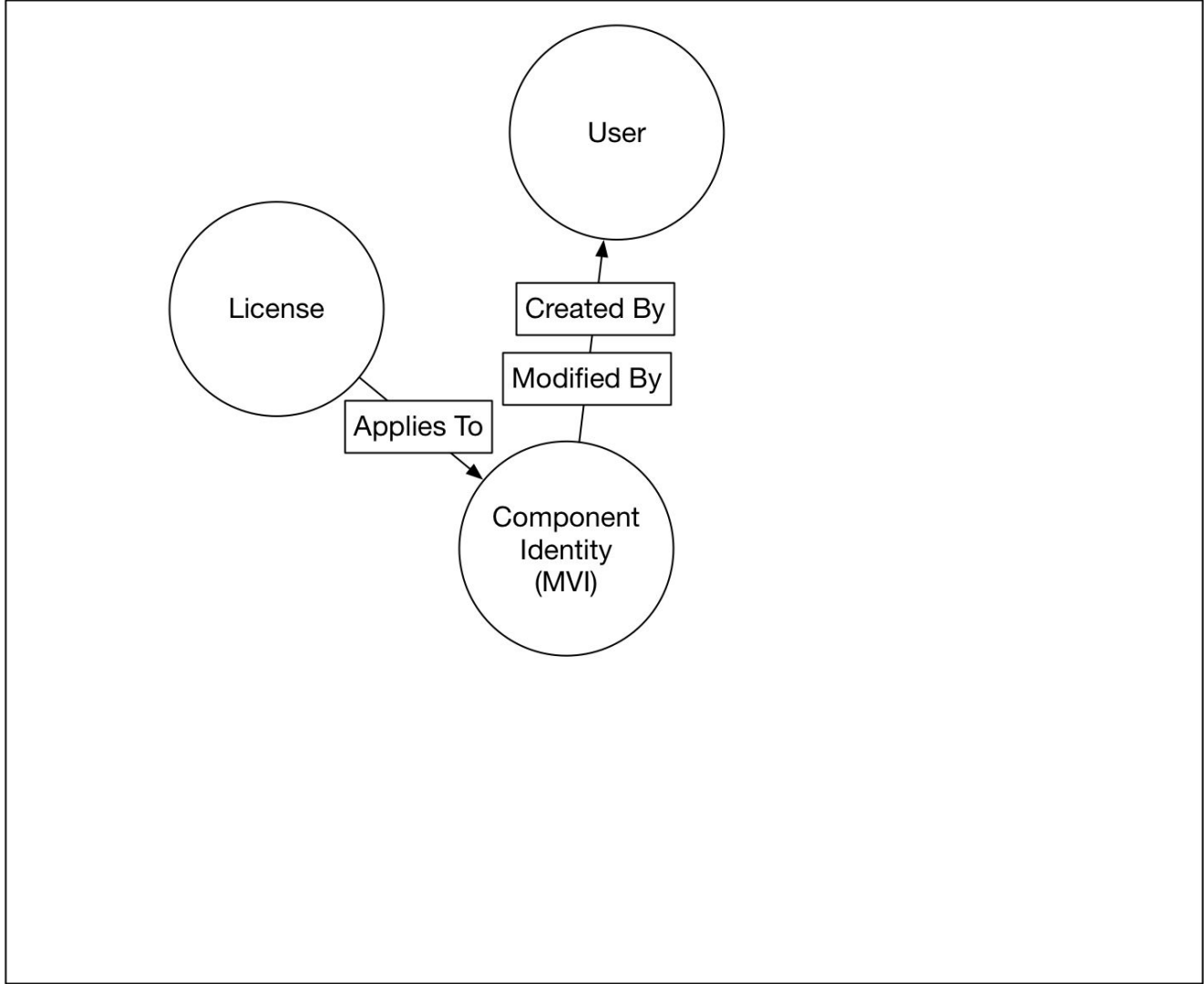
Required



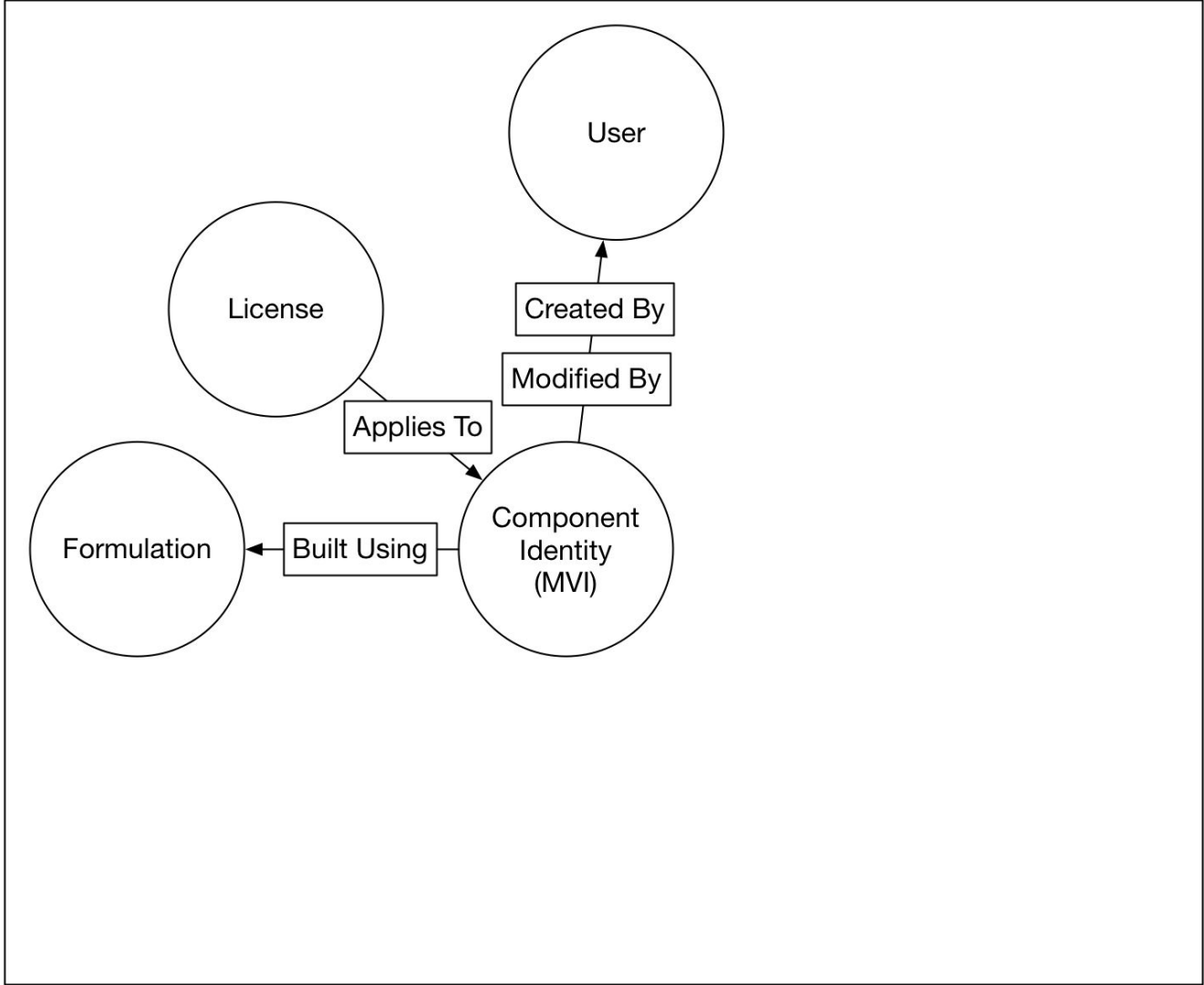
License



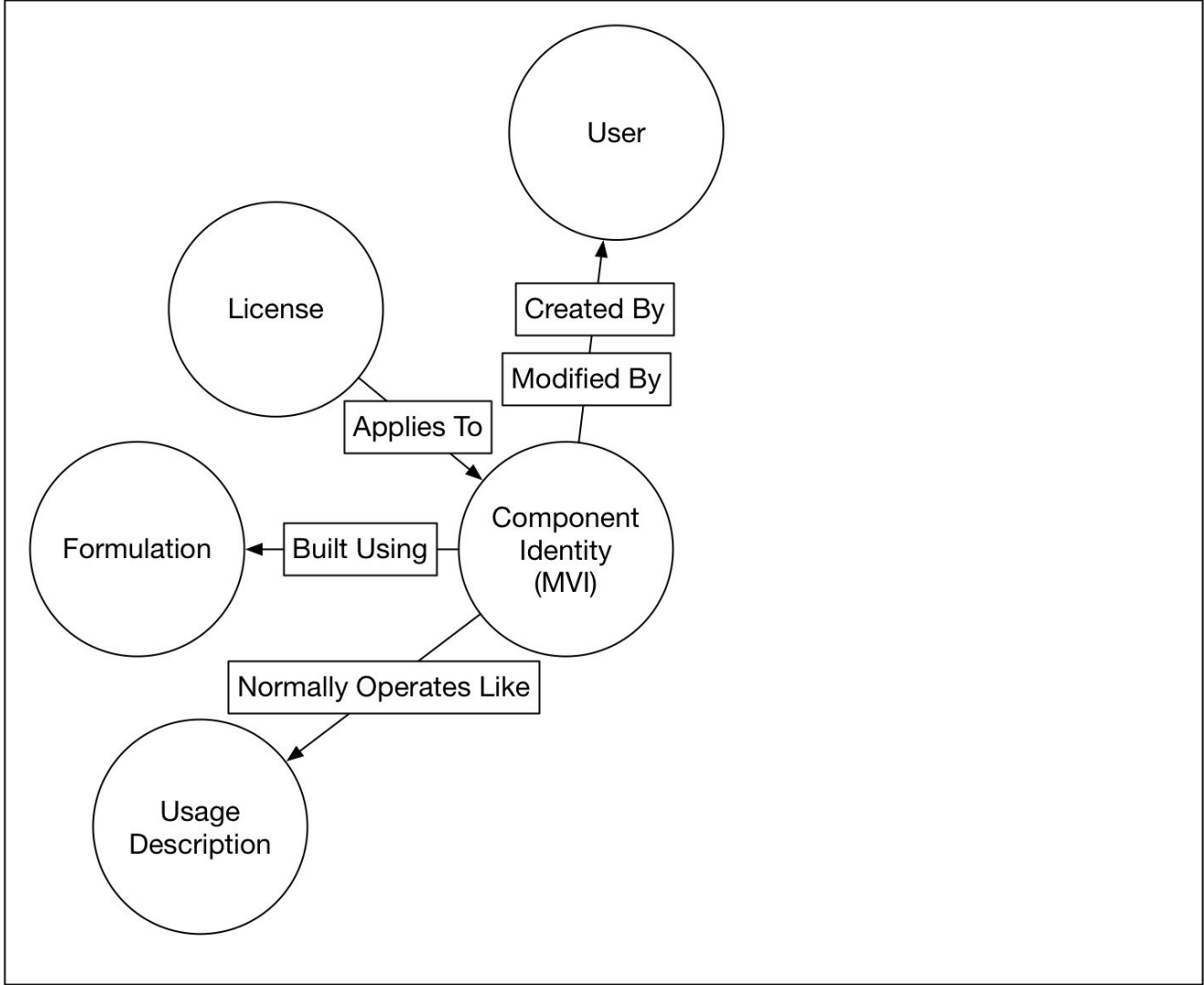
Provenance


User
License
Created By
Modified By
Applies To
Component
Identity
(MVI)

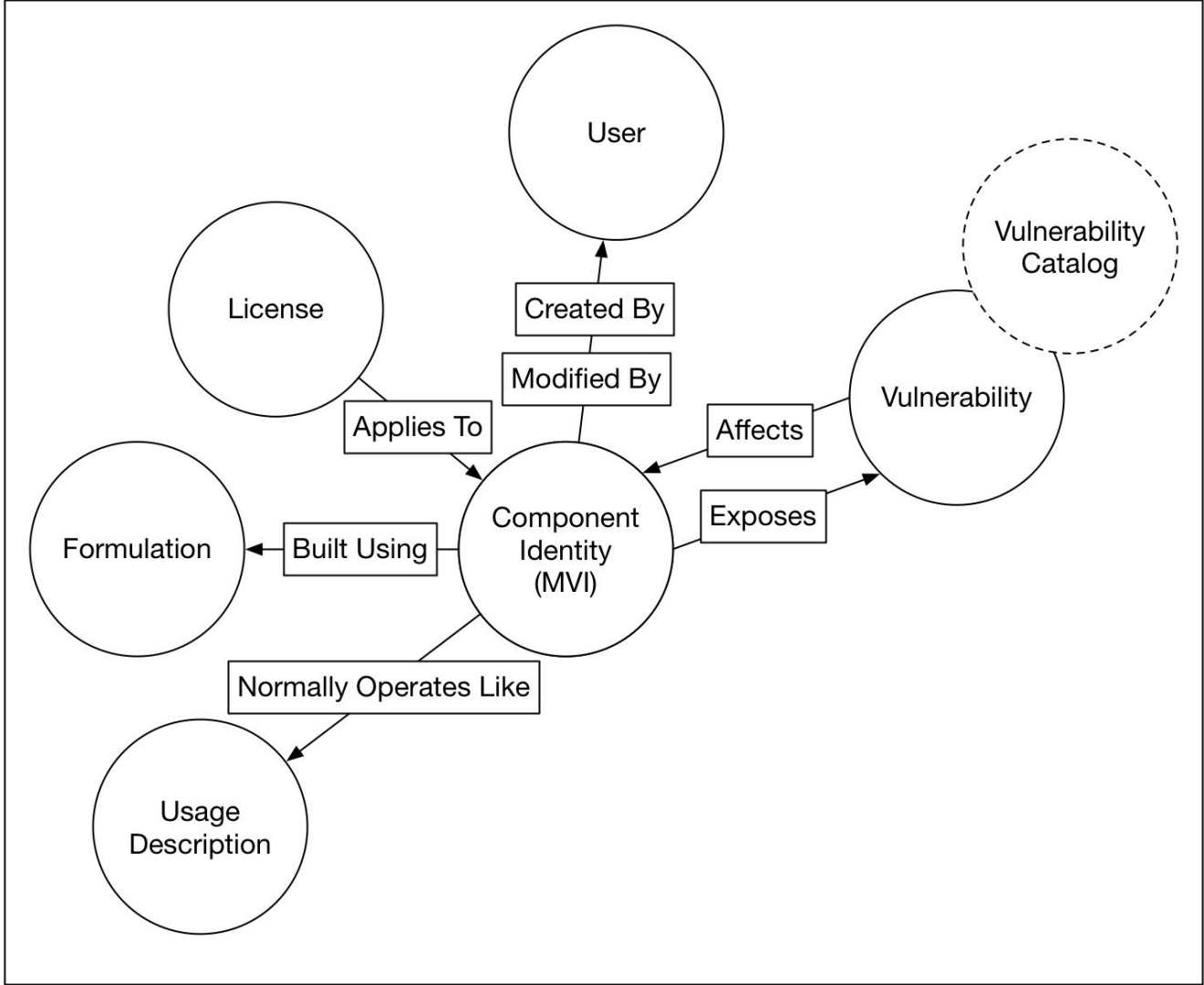
Formulation



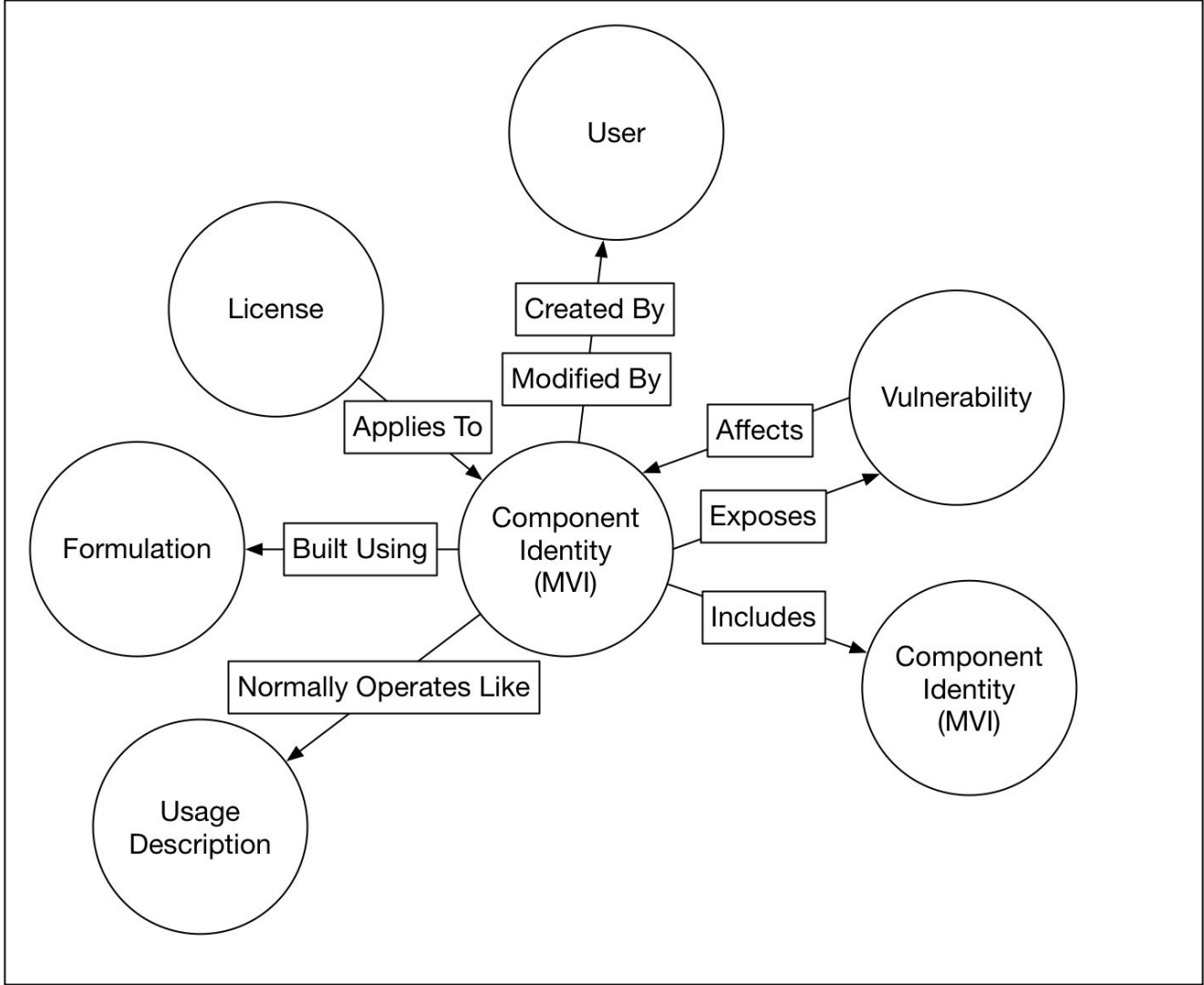
Expected Usage



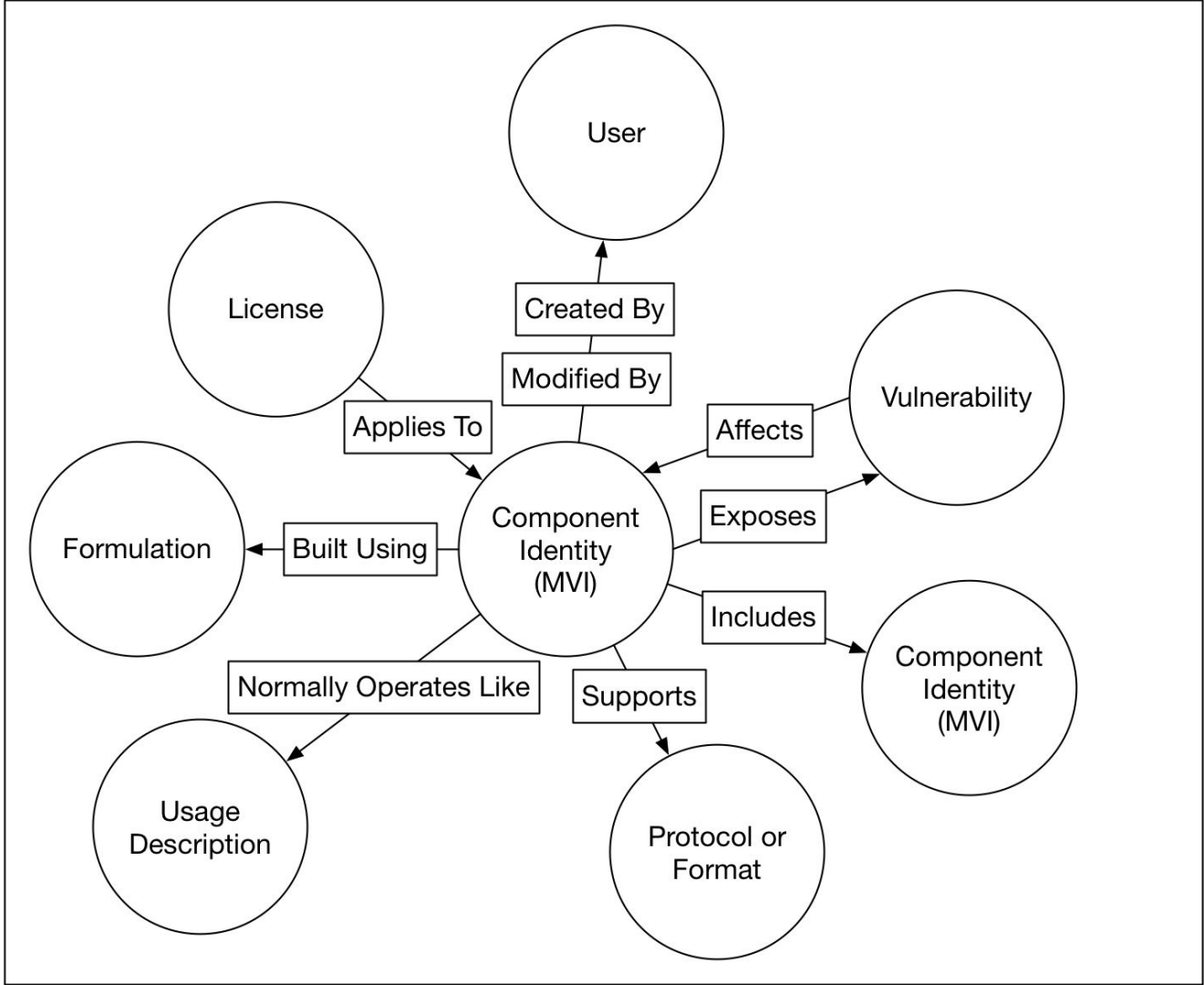
Vulnerability Management



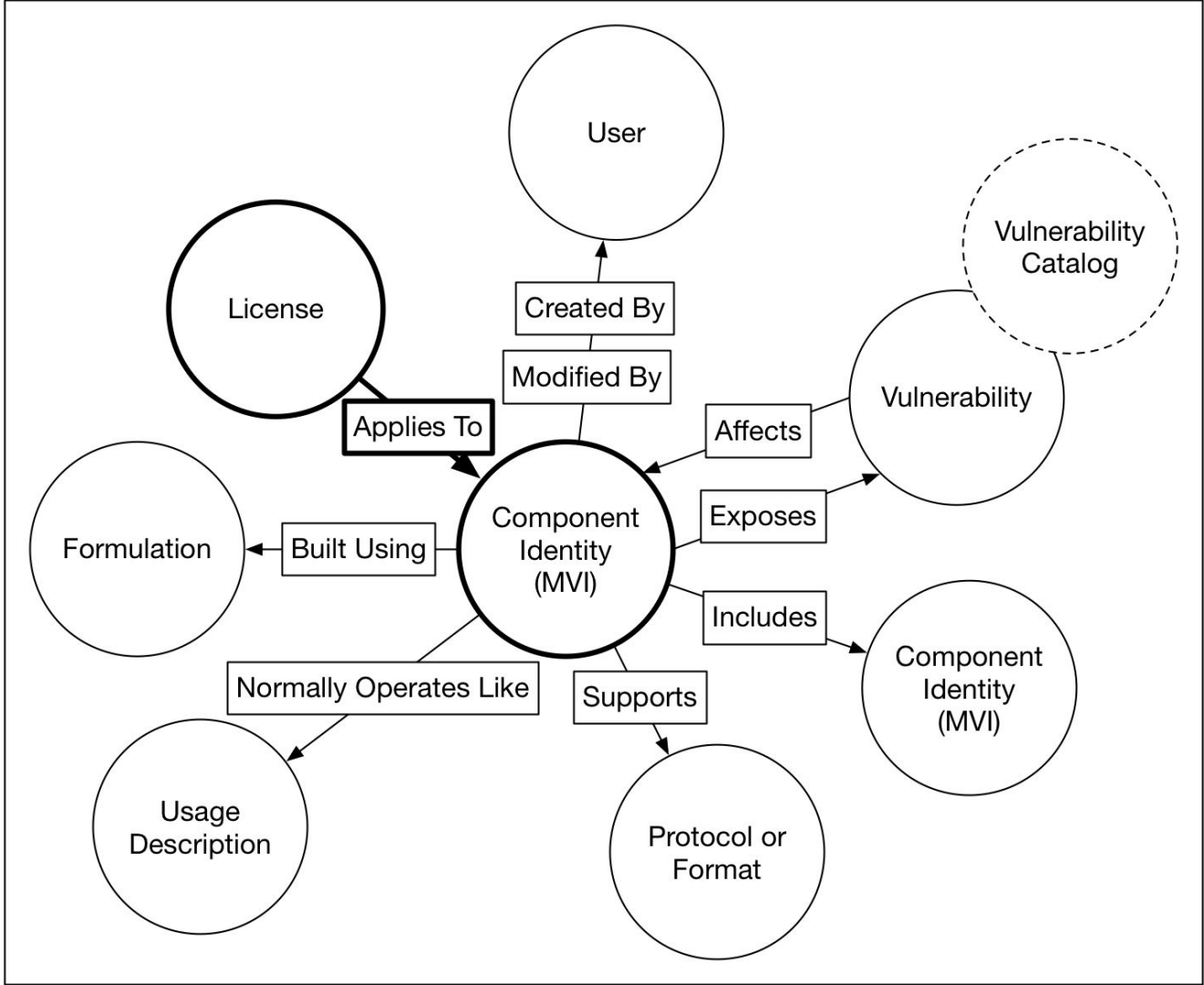
Inclusion


User
License
Created By
Modified By
Applies To
Affects
Vulnerability
Formulation
Built Using
Component Identity (MVI)
Exposes
Includes
Component Identity (MVI)
Normally Operates Like
Usage Description

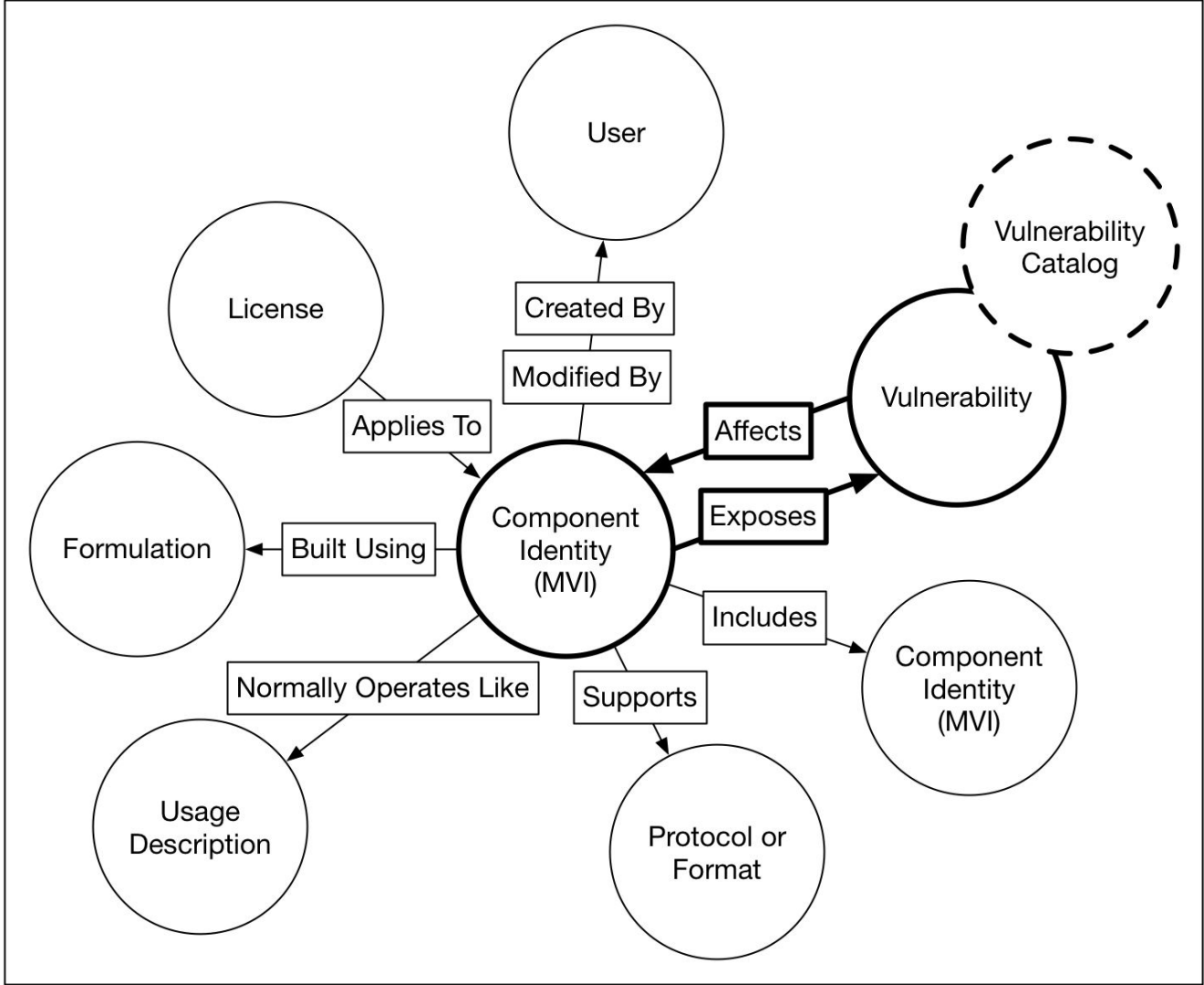
Feature Support



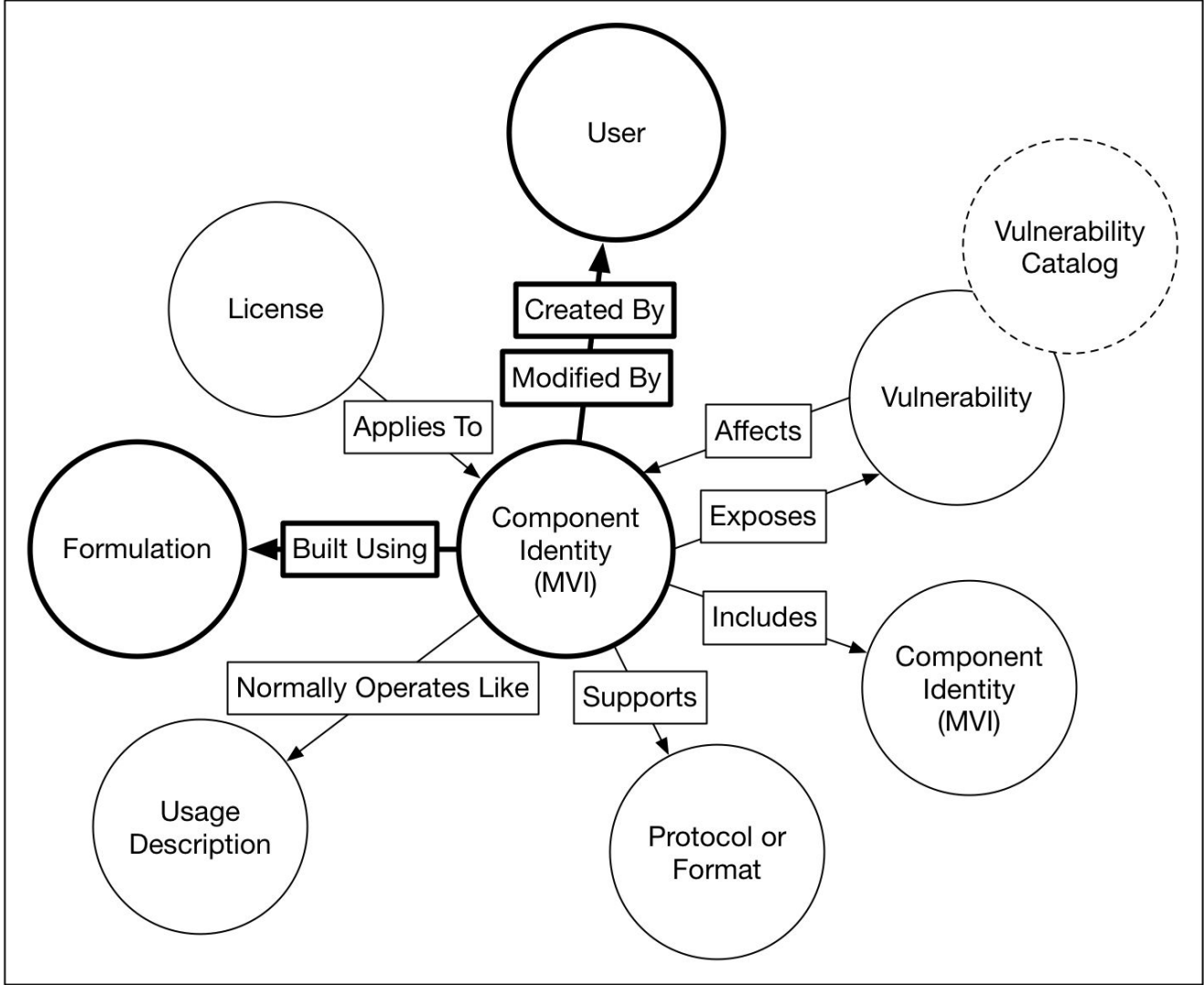
License


User
License
Created By
Modified By
Vulnerability Catalog
Vulnerability
Applies To
Affects
Formulation
Built Using
Component Identity (MVI)
Exposes
Includes
Component Identity (MVI)
Normally Operates Like
Supports
Usage Description
Protocol or Format

Vulnerability Management



High Assurance



Framing WG Logistics

Co-chairs

- Michelle Jump <michelle.jump@novaleah.com>
- Art Manion <amanion@cert.org>

Current meeting schedule

- Weekly Fridays at 2 PM EST

Mailing list

- https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing

Google Drive

- https://drive.google.com/drive/folders/1vOvpGE1gWuKwfnmvLApHJYI0Nl62cUxH