
27th ANNUAL
FIRST CONFERENCE
BERLIN
14-19 JUNE 2015
UNIFIED SECURITY:
IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN
14-19 JUNE 2015

VRDX-SIG:
Global Vulnerability Identification

Art MANION (CERT/CC)

Takayuki UCHIYAMA (JPCERT/CC)

Masato TERADA (IPA)

Outline

- Background
- Problems
- Goals
- Charter
- Activity
- Observations
- Options

About

- VRDX: **V**ulnerability **R**eporting and **D**ata e**X**change
  https://www.first.org/global/sigs/vrdx
- Glossary
  - VDB – Vulnerability database

Background

- 2011
  - *IVDA: International Vulnerability Database Alliance* (Zheng et al.)
    Second Worldwide Cybersecurity Summit
  - Future of Global Vulnerability Reporting
    7th Annual IT Security Automation Conference
- 2012
  - Global Vulnerability Reporting & Identification
    8th Annual IT Security Automation Conference
  - Future of Global Vulnerability Reporting Summit
    Kyoto 2012 FIRST Technical Colloquium
- 2013
  - VRDX-SIG

Problems
Identification

- What is a vulnerability?
  - Abstract concept
  - Different expert definitions
  - Bias
    - Selection, publication, measurement
    - Researcher, vendor, VDB
- What is being identified?
  - Bug, defect
  - Vulnerability report, case
  - Vulnerability (verified)
  - Collection of vulnerabilities
  - Document, advisory

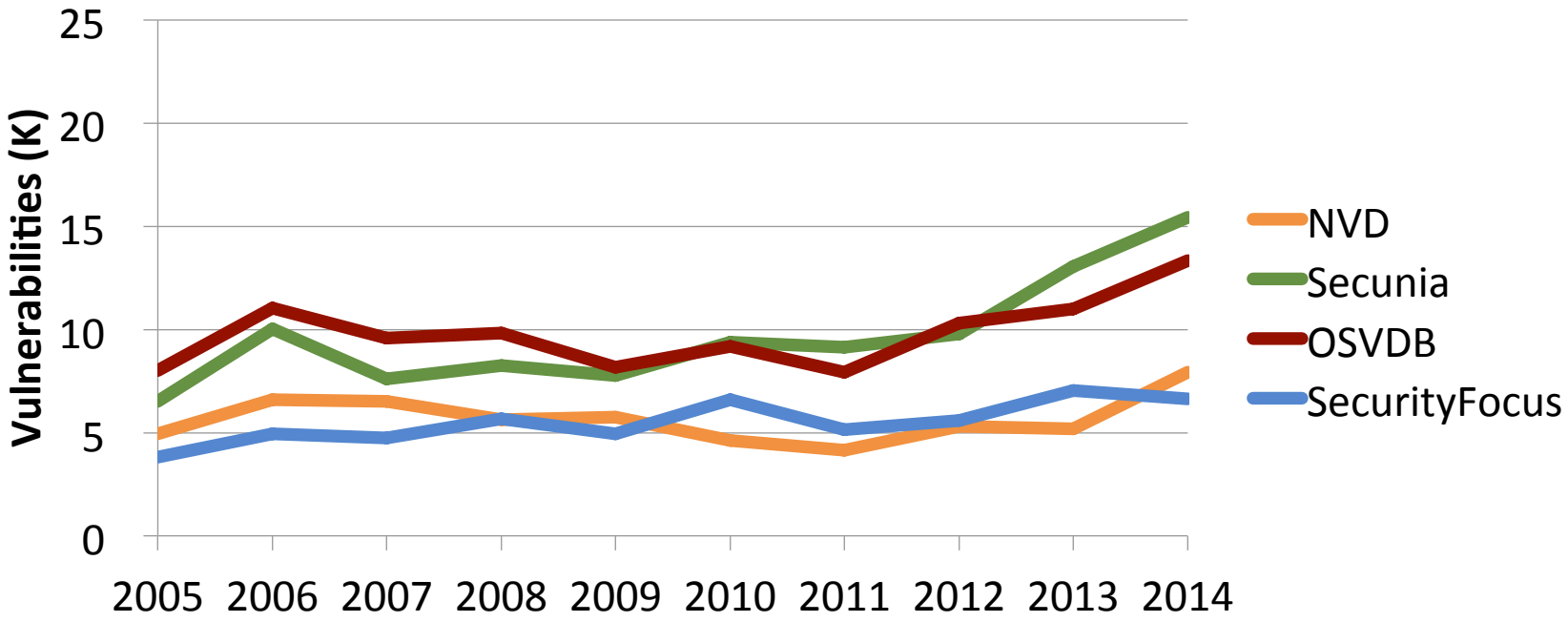
http://danacooperfineart.blogspot.com/

Problems
Identification

- Different IDs for different things
- Example: CUPS vulnerabilities published 2015-06-08
  - CERT/CC: VU#810572
    - CUPS print service is vulnerable to privilege escalation and cross-site scripting
  - CUPS: STR #4609
    - cups: privilege escalation via cross-site scripting and bad print job submission used to replace cupsd.conf on server (plus weird ld.so interaction)
  - FreeBSD: r389006
    - svn commit: r389009, Security update to 2.0.3
  - CVE: CVE-2015-1158, CVE-2015-1159
    - CVE entries not populated as of 2015-06-18
  - OSVDB: Search broken ☹
- Duplicates, de-confliction
- For much, much more detail, see: *Buying Into the Bias: Why Vulnerability Statistics Suck* (Martin and Christey)

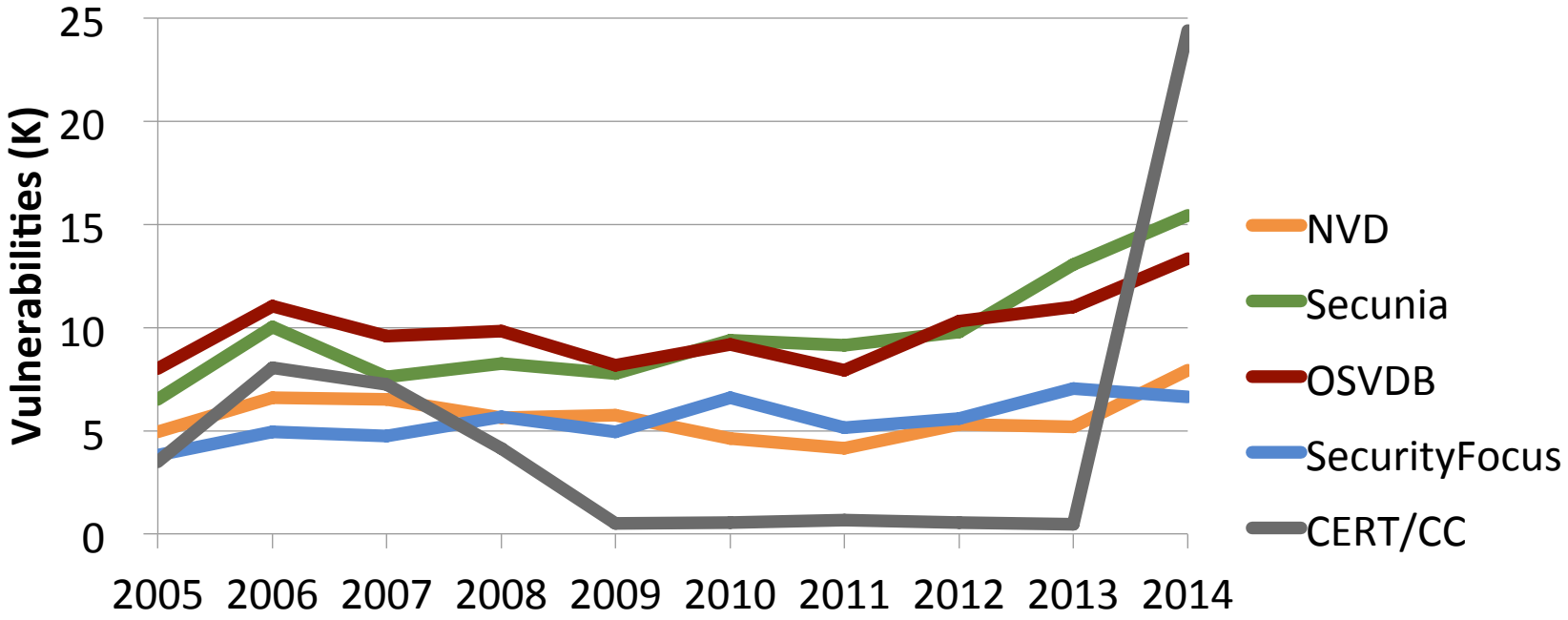
Problems
Counting

- How many vulnerabilities are there?
  - Public disclosures in a year?



Problems
Counting

- CERT/CC automated Android SSL testing
  - Tested ~1M apps, found ~23K vulnerabilities



Problems
Coverage

- Coverage is selection bias
  - CVE sources and products
  - Mobile apps not listed
- "…significant disadvantages in coverage and regional differences." [IVDA]
- No VDB, with the possible exception of OSVDB, even claims comprehensive coverage
- Overlap, close relationships between VDBs

Problems
Duplication of Effort

- Do you have an internal VDB?
  - Paid subscription to vulnerability data feed?
    - What are their sources?
  - Effort? Lines of code?
- What if there existed a public VDB (or integrated system of VDBs) with sufficient coverage, consistency, reliability, and usability?

Problems
Vulnerability Management

- Why should you care?
- Turn off CVE (and OSVDB) for 30 days
  - Expand the vulnerability naming trend?
    - In English?
- Vulnerability identification is infrastructure
  - Needed a name for what is being reported, fixed, exploited, detected
  - Vulnerability management depends on identification
  - Better identification supports better management

Goals

- Assess current state, scope, problems
  - Confirm understanding of problems
- Make findings available
  - If any use to others
  - Document work
- Suggest solution/way forward/options
- Scope is constrained to vulnerability identification
  - Not disclosure
  - Not severity
  - Not supply chain, although component identification has similar issues
    - CPE, SWID, etc.

Charter

- …research and recommend ways to identify and exchange vulnerability information across disparate vulnerability databases.
  - Review existing vulnerability identification schemes and exchange formats
  - Produce a report documenting identified issues in existing schemes
  - Develop best practices and requirements for a vulnerability identification and exchange scheme

Activity

- Review existing vulnerability identification schemes and exchange formats
  - Survey
- Produce a report documenting identified issues in existing schemes
  - VDB Catalog
  - This presentation
- Develop best practices and requirements for a vulnerability identification and exchange scheme
  - Options for consideration (this presentation)

Activity
VDB Survey

- Sent written survey to nine public VDBs
  - Five responses
  - SIG members filled in using publicly available information
- SIG members researched public and vendor VDBs
- Additional data from CERT/CC vulnerability disclosure policy survey
- Distinction between
  - Public VDBs
  - Vendor VDBs
- Survey results summarized in VDB Catalog

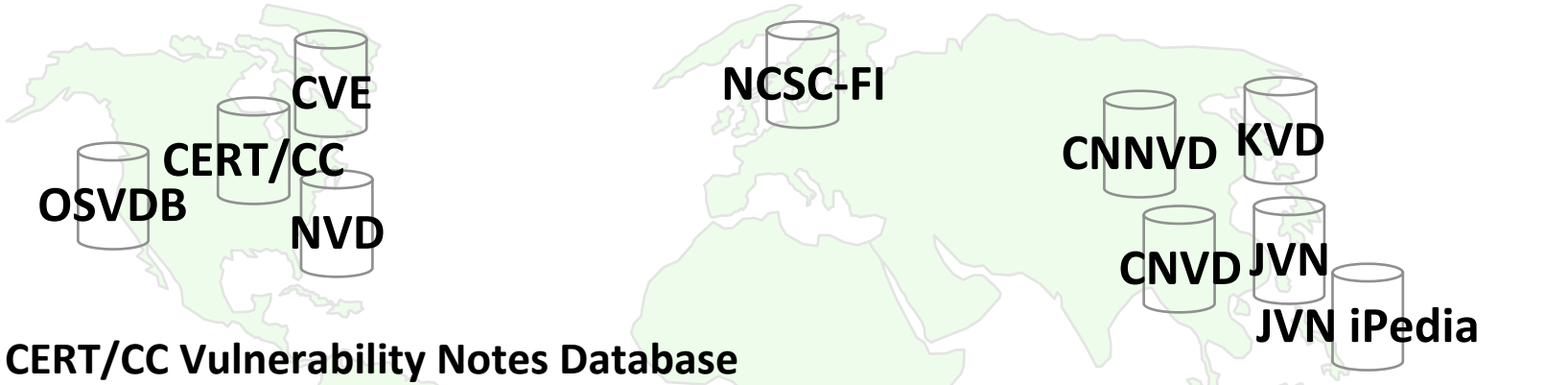
Activity
VDB Catalog

- Data collected, so make it available
- Public
  - Publicly, freely available
  - Somewhat inclusive coverage, not specific to one vendor's products
  - http://jvnrss.ise.chuo-u.ac.jp/vrdx/vdb_public.html
- Vendor
  - Public, freely available
  - Vendor-specific
  - Perhaps more of an advisory list than database
  - Only surveyed vendors included
    - Many vendors make maintenance impractical
  - http://jvnrss.ise.chuo-u.ac.jp/vrdx/vdb_vendor.html

Public VDB Catalog
Contents

Item	Description
Overview	Name, Maintainer, URL and description
ID scheme	Number of ID schemes, ID format and Vulnerability Definition
CWE	Use of CWE IDs and Use all CWE IDs or subset
CVSS	Base, Temporal and Environmental Metrics
CPE	Use of CPE
Data Feed	Use of CVRF, RSS/Atom and other XSD
VDB contents	Contents, available languages and etc.

Public VDB Catalog
Map



CERT/CC Vulnerability Notes Database
CNNVD (China National Vulnerability Database of Information Security)
CNVD (China National Vulnerability Database)
CVE (Common Vulnerabilities and Exposures)
JVN (Japan Vulnerability Notes)
JVN iPedia
NCSC-FI Vulnerability Database
NVD (National Vulnerability Database)
OSVDB (Open Sourced Vulnerability Database)

Public VDB Catalog
IDs

VBD Name	Description
CERT/CC	VU#{NNNNNN…} (6+ digits)
CNNVD	CNNVD-{YYYY}{MM}-{NNN} (3 fixed digits)
CNVD	CNVD-{YYYY}-{NNNNN} (5 fixed digits)
CVE	CVE-{YYYY}-{NNNN...} (Variable length digits)
JVN	JVN#{NNNNNNNN} (8 fixed digits) JVNVU#{NNNNNNNN} (8 fixed digits)
JVN iPedia	JVNDB-{YYYY}-{NNNNNN} (6 fixed digits)
NCSC-FI	FICORA #{NNNNNN} (6 fixed digits)
NVD	CVE-{YYYY}-{NNNN...} (Variable length digits)
OSVDB	{NNN...} (variable length digits)

Public VDB Catalog
ID Examples

VBD Name	Description
CERT/CC	VU#123456 (6+ digits)
CNNVD	CNNVD-201501-001 (3 fixed digits)
CNVD	CNVD-2015-00001 (5 fixed digits)
CVE	CVE-2015-1234567 (Variable length digits)
JVN	JVN#12345678 (8 fixed digits) JVNVU#12345678 (8 fixed digits)
JVN iPedia	JVNDB-2015-123456 (6 fixed digits)
NCSC-FI	FICORA #123456 (6 fixed digits)
NVD	CVE-2015-1234567 (Variable length digits)
OSVDB	1234567 (variable length digits)

Public VDB Catalog
Features

VBD Name	CWE	CVSS v2	CPE
CERT/CC	-	Base, Temporal, Environmental	-
CNNVD	-	-	-
CNVD	-	Base	-
CVE	-	-	-
JVN	-	Base	-
JVN iPedia	CWE-635	Base	CPE 2.2
NCSC-FI	-	-	-
NVD	CWE-635	Base	CPE 2.2/2.3
OSVDB	-	Base	-

Public VDB Catalog
Feeds

VBD Name	CVRF	RSS/Atom	Other
CERT/CC	-	Atom	-
CNNVD	-	-	-
CNVD	-	-	-
CVE	CVRF v1.1	-	cve_1.0.xsd
JVN	-	RSS 1.0	-
JVN iPedia	CVRF v1.1	RSS 1.0	vuldef_3.1.xsd
NCSC-FI	-	-	-
NVD	-	RSS 1.0	nvd-cve-feed_2.0.xsd
OSVDB	-	-	-

Vendor VDB Catalog
Contents

Item	Description
Overview	Advisory and Blog URLs
IDs	Use of Advisory ID, Use of Coordination ID
CWE	Use of CWE IDs and Use all CWE IDs or subset
CVSS	Base, Temporal and Environmental Metrics
CPE	Use of CPE
Data Feed	Use of CVRF, RSS/Atom and other XSD
Vulnerability Handling	Vulnerability Handling related URL

Vendor VDB Catalog
IDs

Vendor	Description
Adobe	APSA{YY}-{NN}, APSB{YY}-{NN} (2 fixed digits)
Cisco	cisco-sa-{YYYY}{MM}{DD}-{product name}
Hitachi	HS{YY}-{NNN} (3 fixed digits), HCVU{NNNNNNNNN} (9 fixed digits), AX-VU{YYYY}-{NN} (2 fixed digits) and more.
Huawei	Huawei-SA-{YYYY}{MM}{DD}-{RR}-{product name}
Microsoft	MS{YY}-{NNN} (3 fixed digits)
Oracle	CPU Month Year
Red Hat	RHSA-{YYYY}:{NNNN} (4 fixed digits)
Siemens	SSA-{NNNNNN} (6 fixed digits)

Vendor VDB Catalog
Contents

Vendor	Description
Adobe	CVE
Cisco	CVE
Hitachi	CVE, JVN, JVN iPedia
Huawei	CVE, HWPSIRT-{YYYY}-{NNNN} (4 fixed digits)
Microsoft	CVE
Oracle	CVE
Red Hat	CVE
Siemens	CVE

Vendor VDB Catalog
Features

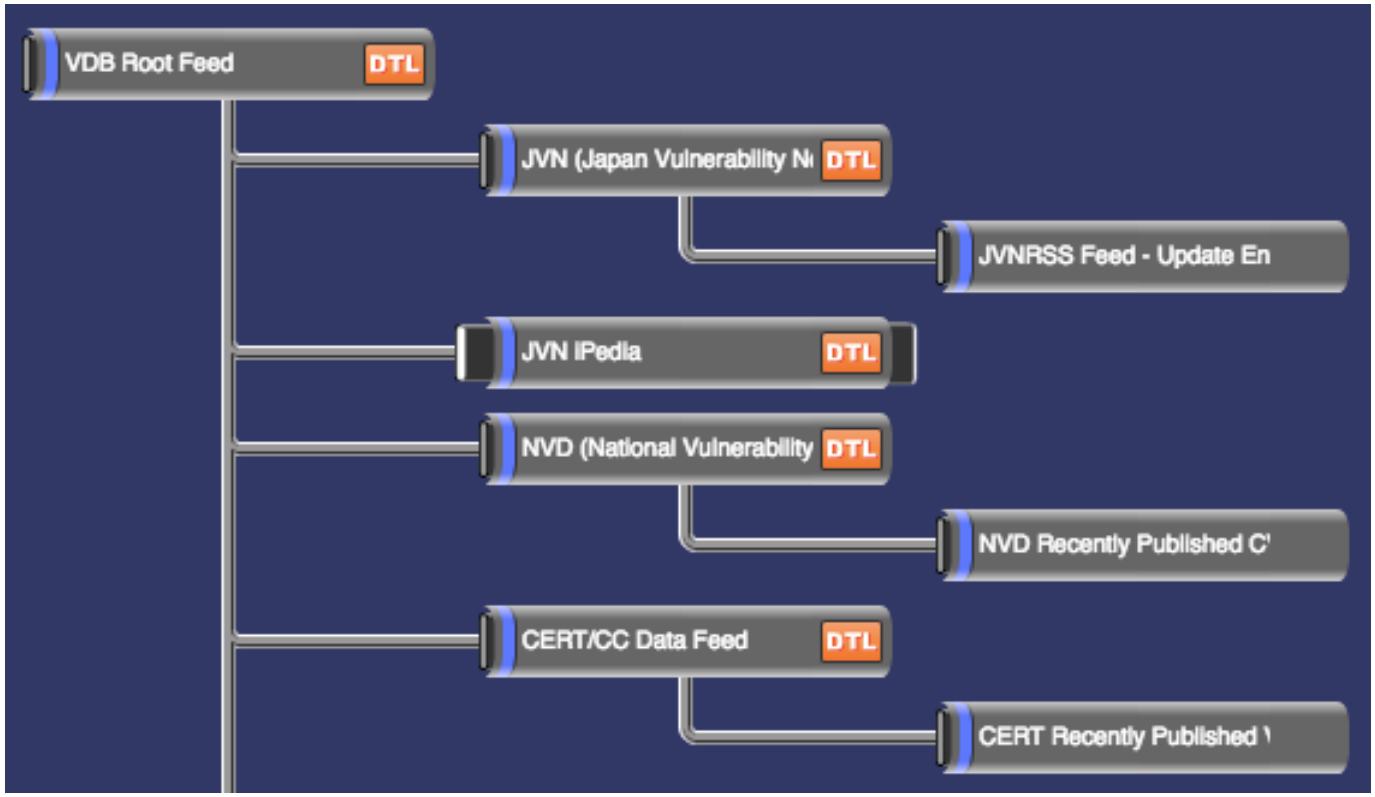
Vendor	CWE	CVSS v2	CPE
Adobe	-	-	-
Cisco	YES	Base	-
Hitachi	-	Base	-
Huawei	-	Base, Temporal	-
Microsoft	-	-	-
Oracle	-	Base	-
Red Hat	YES	Base	CPE 2.2
Siemens	-	Base, Temporal	-

Vendor VDB Catalog
Feeds

Vendor	CVRF	RSS/Atom	Other
Adobe	-	-	-
Cisco	CVRF v1.1	RSS 1.0/2.0	OVAL
Hitachi	-	RSS 1.0	-
Huawei		RSS 2.0	-
Microsoft	-	-	-
Oracle	CVRF v1.1	Atom	-
Red Hat	CVRF v1.1	-	OVAL
Siemens	-	RSS 1.0	-

Bonus
VDB Feed Tree

- http://jvnrss.ise.chuo-u.ac.jp/vrdx/vdb_public.html



Observations
VDB Survey

- Identification (abstraction)
  - Not many published definitions of “vulnerability”
  - Different levels (bug, report, case, vulnerability, advisory)
- ID systems
  - Many, generally one (or more) per VDB
- Coverage
  - Gaps and overlap
- Use of CVE
  - All surveyed public and vendor VDBs used CVE
  - CERT/CC Disclosure Policy study
    - 26/47 VDBs, including many vendors, use CVE

Observations
Requirements

- Any solution or improvement will have technical and organizational aspects
  - Technical
    - Specification, protocol, API
    - Standards, definitions, terminology
  - Organizational
    - Membership, governance, decision making
    - Governance
      - Oligarchy
      - Feudalism
      - Dictatorship
      - Confederacy
      - Anarchy

Observations
Addressing Problems

- Hard problems are hard
- Identification, agreeing on the definition of "vulnerability"
  - Agreement not likely
  - Not entirely necessary?
- ID systems
  - Agreement not likely, although technically possible
  - Not entirely necessary?
- Coverage
  - Not likely to be able to force greater coverage
  - Better coverage and de-confliction can be supported

Options
VRDX-SIG (2015)

- Do nothing
- Single VDB
- Franchise
- Federation
- ID interoperability specification

Options
VRDX-SIG (2015)

VDB	Pro	Contra
Do nothing	Easy, inexpensive	Current problems remain
Single VDB	Consistency	Agreement, adoption, scale, coverage, performance, reliability
Franchise	Coverage	Organizational complexity, participants must agree
Federation	Coverage	Organizational complexity, participants must agree
ID Interoperability specification	Agreement not needed, supports coverage, consumer retains choice	Adoption, coverage

Options
CERIAS Report (1999)

- Organizational models [CERIAS]
  - Open
    - "Assume that this database is completely open. Anyone can add to it, and anyone can access it."
  - Centralized
    - “Even if the CVDB had 10,000 records (considered unlikely)…“
  - Federated
    - ‘We assume that all entities involved have a common definition for "security vulnerability" and "security vulnerability data.”’
  - Fragmented/status quo
    - Reasons for current state (in 1999)

Options
ID Interoperability Specification

- Describe relationship between two vulnerability reports (IDs)
  - "join table" for IDs
- Supports reasoning
  - If $ID_1 > ID_2$ and $ID_2 == ID_3$ then $ID_1 > ID_3$

Relationships	
Same as	**==**
Superset of, parent of	**>**
Subset of, child of	**<**
Different than, disjoint	**!=**
Related to, similar to	**~**

Options
ID Interoperability Specification

- Assertions
  - VDB asserts relationship between IDs
  - Consumer can choose to trust VDB's assertion
    - Could accept assertion if certain or multiple VDBs agree
    - Could trust VDB making assertion about its own ID

VDB	Date	ID 1	Relationship	ID 2
CERT/CC	2015-06-17	VU#123456	==	CVE-2015-5432
OSVDB	2015-06-15	OSVDB 2346	<	CVE-2015-5432

  - Can be signed
  - Can include expiration date

References

- [IVDA] *IVDA: International Vulnerability Database Alliance* (Zheng et al.)
  http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5978787
- [STATS] *Buying Into the Bias: Why Vulnerability Statistics Suck* (Martin and Christey)
  https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-Slides.pdf
  http://attrition.org/security/conferences/2013-07-BlackHat-Vuln_Stats-draft_22-Published.pptx
- [CERIAS] *Final Report of the 2nd Workshop on Research with Security Vulnerability Databases* (Meunier and Spafford)
  https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/99-06.pdf