Industry Consortium for Advancement of Security on the Internet

The Common Vulnerability Reporting Framework (CVRF)

Presented by Jim Duncan, Juniper SIRT

FIRST Conference 2010, Miami FL USA

2010 June 15

Agenda

- **What is CVRF?**
- **Why CVRF?**
- **Who built CVRF and how?**
- **What's the value of CVRF?**
- **What's the timeline?**
- **Which member companies will adopt CVRF?**
- **Q&A**

What is CVRF?

- **CVRF = the Common Vulnerability Reporting Framework**
- **XML-based language**
- **Provides a standard format for the dissemination of security-related information**
- **48 Discrete Elements**
- **XML → machine readable → easier production and consumption**

CVRF Roles

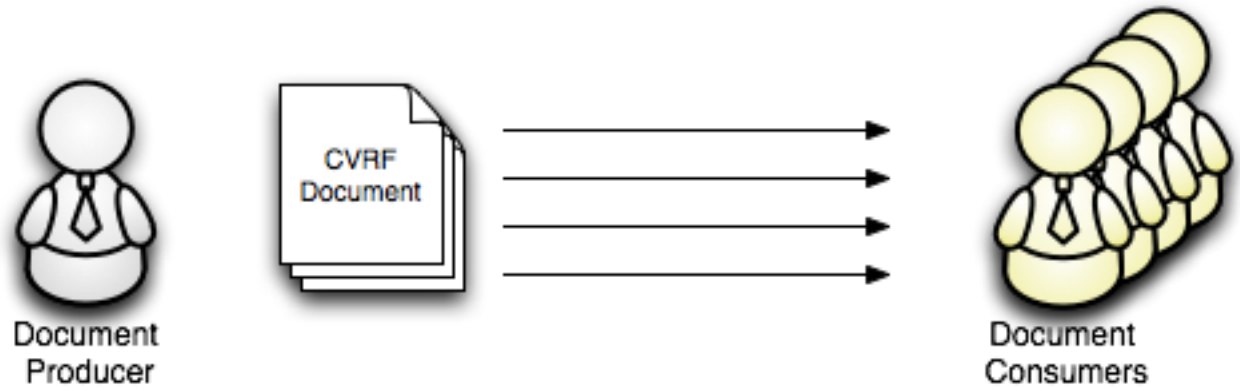
Document Producer

Vendors
Coordinators
Researchers

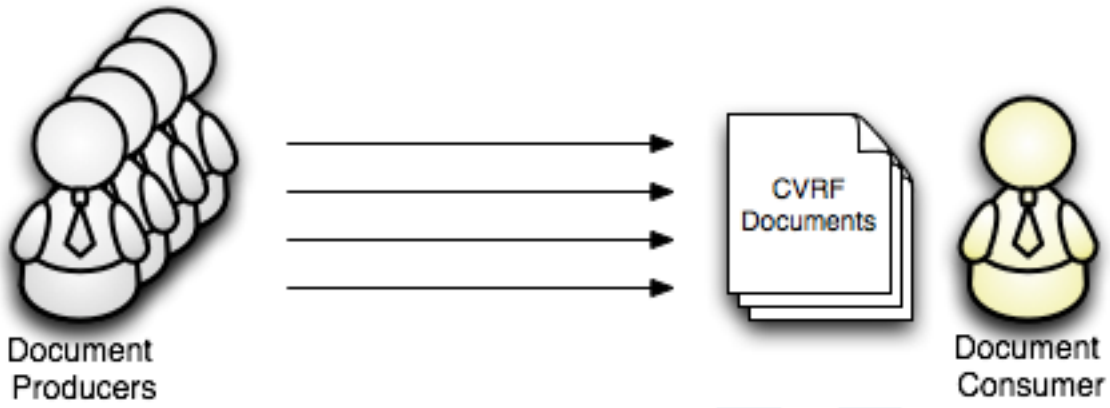
Document Consumer

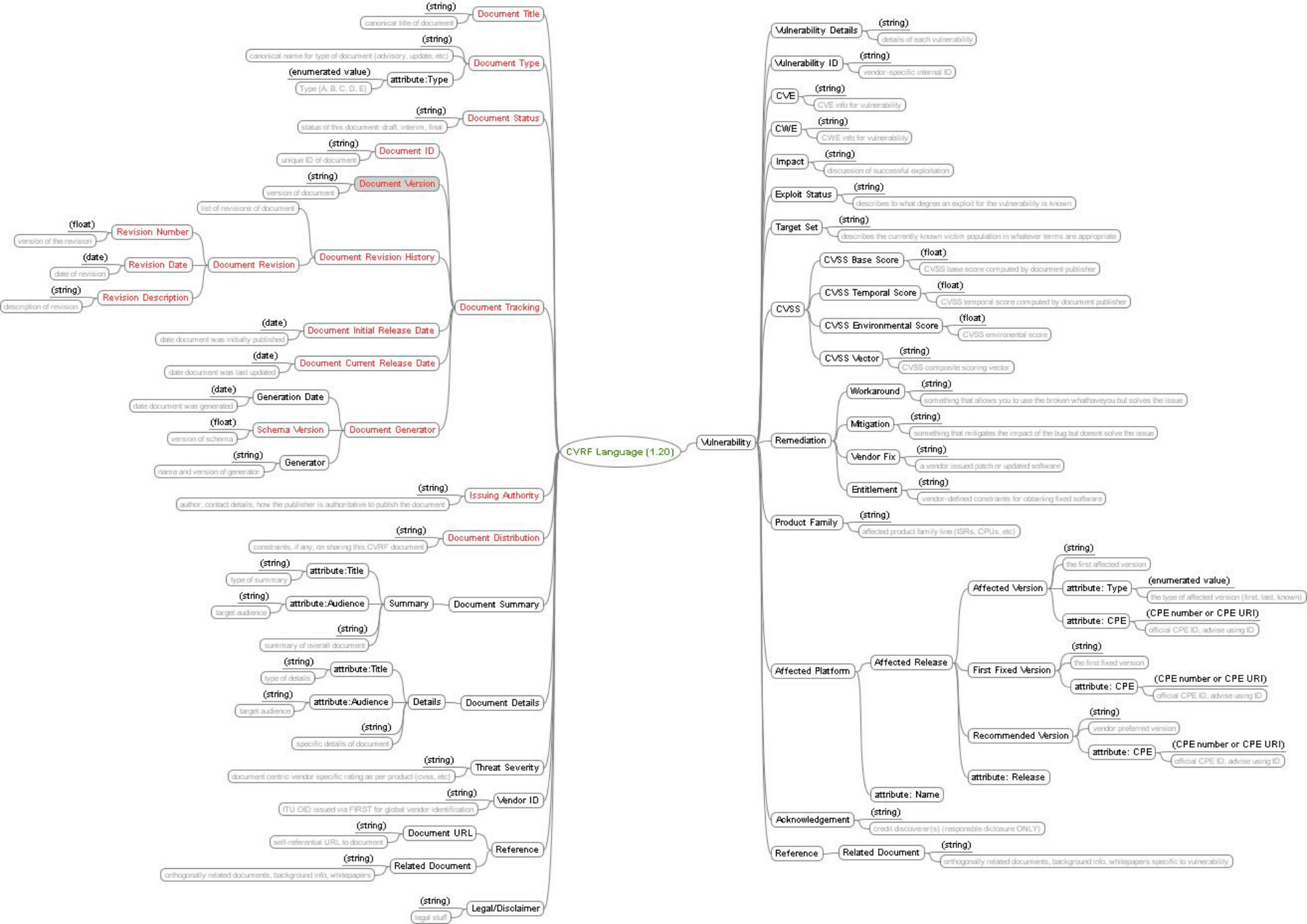
Security Practitioners
Administrators
etc

CVRF Roles: Document Producer



CVRF Roles: Document Consumer




CVRF Language (1.20)
Document Tracking
Document Title
(string)
canonical title of document
Document Type
(string)
canonical name for type of document (advisory, update, etc)
attribute:Type
(enumerated value)
Type (A, B, C, D, E)
Document Status
(string)
status of this document: draft, interim, final
Document ID
(string)
unique ID of document
Document Version
(string)
version of document
Document Revision History
list of revisions of document
Document Revision
Revision Number
(float)
version of this revision
Revision Date
(date)
date of revision
Revision Description
(string)
description of revision
Document Initial Release Date
(date)
date document was initially published
Document Current Release Date
(date)
date document was last updated
Document Generator
Generation Date
(date)
date document was generated
Schema Version
(float)
version of schema
Generator
(string)
name and version of generator
Issuing Authority
(string)
author, contact details, how the publisher is authoritative to publish the document
Document Distribution
(string)
constraints, if any, on sharing this CVRF document
Document Summary
Summary
attribute:Title
(string)
type of summary
attribute:Audience
(string)
target audience
(string)
summary of overall document
Document Details
Details
attribute:Title
(string)
type of details
attribute:Audience
(string)
target audience
(string)
specific details of document
Threat Severity
(string)
document centric vendor specific rating as per product (cvss, etc)
Vendor ID
(string)
ITU OID issued via FIRST for global vendor identification
Reference
Document URL
(string)
self-referential URL to document
Related Document
(string)
orthogonally related documents, background info, whitepapers
Legal/Disclaimer
(string)
legal stuff
Vulnerability
Vulnerability Details
(string)
details of each vulnerability
Vulnerability ID
(string)
vendor-specific internal ID
CVE
(string)
CVE info for vulnerability
CWE
(string)
CWE info for vulnerability
Impact
(string)
discussion of successful exploitation
Exploit Status
(string)
describes to what degree an exploit for the vulnerability is known
Target Set
(string)
describes the currently known victim population in whatever terms are appropriate
CVSS
CVSS Base Score
(float)
CVSS base score computed by document publisher
CVSS Temporal Score
(float)
CVSS temporal score computed by document publisher
CVSS Environmental Score
(float)
CVSS environental score
CVSS Vector
(string)
CVSS composite scoring vector
Remediation
Workaround
(string)
something that allows you to use the broken whatchaveyou but solves the issue
Mitigation
(string)
something that mitigates the impact of the bug but doesnt solve the issue
Vendor Fix
(string)
a vendor issued patch or updated software
Entitlement
(string)
vendor-defined constraints for obtaining fixed software
Product Family
(string)
affected product family line (ISRs, CPUs, etc)
Affected Platform
Affected Release
Affected Version
(string)
the first affected version
attribute: Type
(enumerated value)
the type of affected version (first, last, known)
attribute: CPE
(CPE number or CPE URI)
official CPE ID, advise using ID
First Fixed Version
(string)
the first fixed version
attribute: CPE
(CPE number or CPE URI)
official CPE ID, advise using ID
Recommended Version
(string)
vendor preferred version
attribute: CPE
(CPE number or CPE URI)
official CPE ID, advise using ID
attribute: Release
attribute: Name
Acknowledgement
(string)
credit discoverer(s) (responsible diclosure ONLY)
Reference
Related Document
(string)
orthogonally related documents, background info, whitepapers specific to vulnerability

Why CVRF?

- **No existing standard in this unique vulnerability reporting space**
- **Others are ad hoc, producer-specific**

Document Producer Reports at a Glance

Cisco	
Summary	Text blob
Affected Products	Container
Vulnerable Products	List of text blobs
Products Confirmed Not Vulnerable	Bulleted list
Details	Text blob
Vulnerability Scoring Details	Text blob
Impact	Text blob
Software Versions and Fixes	Table
Workarounds	Text blob
Obtaining Fixed Software	Text blob
Exploitation and Public Announcements	Text blob
Status of this Notice	Text blob
Distribution	Text blob
Revision History	Table
Cisco Security Procedures	Text blob

Microsoft	
General Information	Container
Executive Summary	Text blob
Affected and Non-Affected Software	Container
Affected Software	Table
Non-Affected Software	Table
FAQ	Text blob
Vulnerability Information	Container
Severity Ratings and Vulnerability Identifiers	Table
0 or more vulnerabilities sorted by CVE	Container
Vulnerability Description	Text blob
Update Information	Container
Detection and Deployment Tools Guidance	Text blob
Security Update Deployment	Text blob
Other Information	Container
Acknowledgements	Text blob
Microsoft Active Protections Program	Text blob
Support	Text blob
Disclaimer	Text blob
Revisions	Bulleted list

Document Producer Reports at a Glance, cont'd

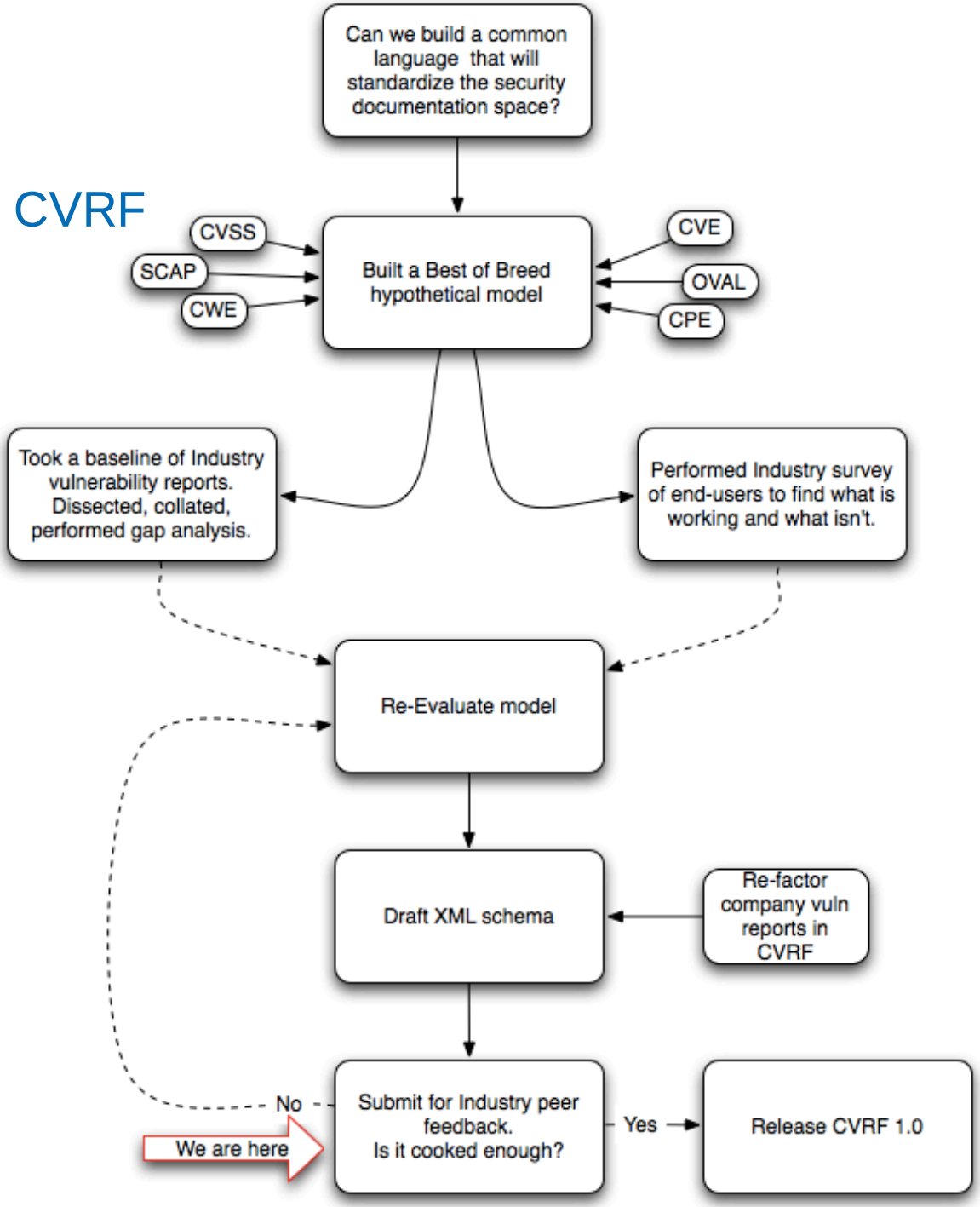
CERT	
Target	Bulleted list
Access Vector	Bulleted list
Impact	Bulleted list
Remediation	Bulleted list
Details	Text blog
Impact	Text blog
Severity	Text blog
Vulnerability Coordination Information	Text blog
Vendor Information	Bulleted list
Remediation	Text blog
References	Bulleted list
Contact Information	Text blog
Revision History	Bulleted list

Secunia	
Secunia Advisory	String
Release Date	Date
Last Update	Date
Popularity	Integer
Comments	Text blob
Criticality Level	Enum
Impact	Enum
Where	Enum
Authentication Level	Text blob
Report Reliability	Text blob
Solution Status	Text blob
Systems Affected	Text blob
Approve Distribution	Text blob
Automated Scanning	Text blob
Operating System	Bulleted list
Secunia CVSS Score	Text blob
CVE References	Bulleted list
Description	Text blob
Solution	Text blob
Provided and/or Discovered by	Text blob
Changelog	Text blob
Original Advisory	Text blob
Other References	Text blob
Alternate/Detailed Remediation	Text blob
Deep links	Text blob

Who's involved?

- **Internet Consortium for Advancement of Security on the Internet (ICASI)**
- **Formed in 2008 to address international, multi-product security challenges**
- **Non-profit, vendor agnostic**
- **ICASI members include Cisco, IBM, Intel, Juniper, Microsoft, and Nokia**
- **Non-ICASI member contributors include Oracle and Red Hat**

How was CVRF built?



What is the Value of CVRF?

- **CVRF is a response by industry to customer demand**
- **Customers are looking for a simple automated way to absorb security-related information**
- **Vendors are looking for an easily produced capacity to enable machine readable generation of security documentation using current methodology**
- **CVRF is delivering the capacity to enable the assimilation of disparate security-related data-sets via a standard format**

Timeline

- 2008
  - Issue proposed as a goal for ICASI
  - CVRF work group formed
- 2009
  - Investigation and gap analysis
  - Gathered reports from vendors and CERTs
  - Comparison with surveys
  - Draft problem statement and use cases
  - Design common Framework
- 2010
  - Define standard
  - Develop dictionary, schema and sample style sheets
  - Test internal to working group
  - Conduct Peer review
  - Incorporate peer review comments
- Late 2011
  - Implementation

Company Adoption

Company	Plans	Role	Timeline
Cisco	evaluating	producer	2011
IBM	limited support	producer/consumer	2011/12
Intel	limited support	producer/consumer	2011
Juniper	limited support	producer/consumer	2011/12
Microsoft	support	producer	2011
Nokia	evaluating	producer	2011
Oracle	evaluating	producer/consumer	2011/12
Red Hat	support	producer	2010

The “ask”:

- **Well qualified organizations for Peer review**
- **Would your organization use an industry proposed framework to accomplish the purpose outlined here?**
- **Please email cvrf@icasi.org to request participation**
- **Other comments or questions?**