IETF INCH Working Group Meeting
5th August 2004, San Diego CA US

Extending the Charter: Addressing Vulnerability and Exploit Information

Ian Bryant
Head, Capability Development Group
& Co-Chair, TF-CSIRT VEDEF WG

Yurie Ito
Liaison Manager

Vulnerability & Exploit DEF

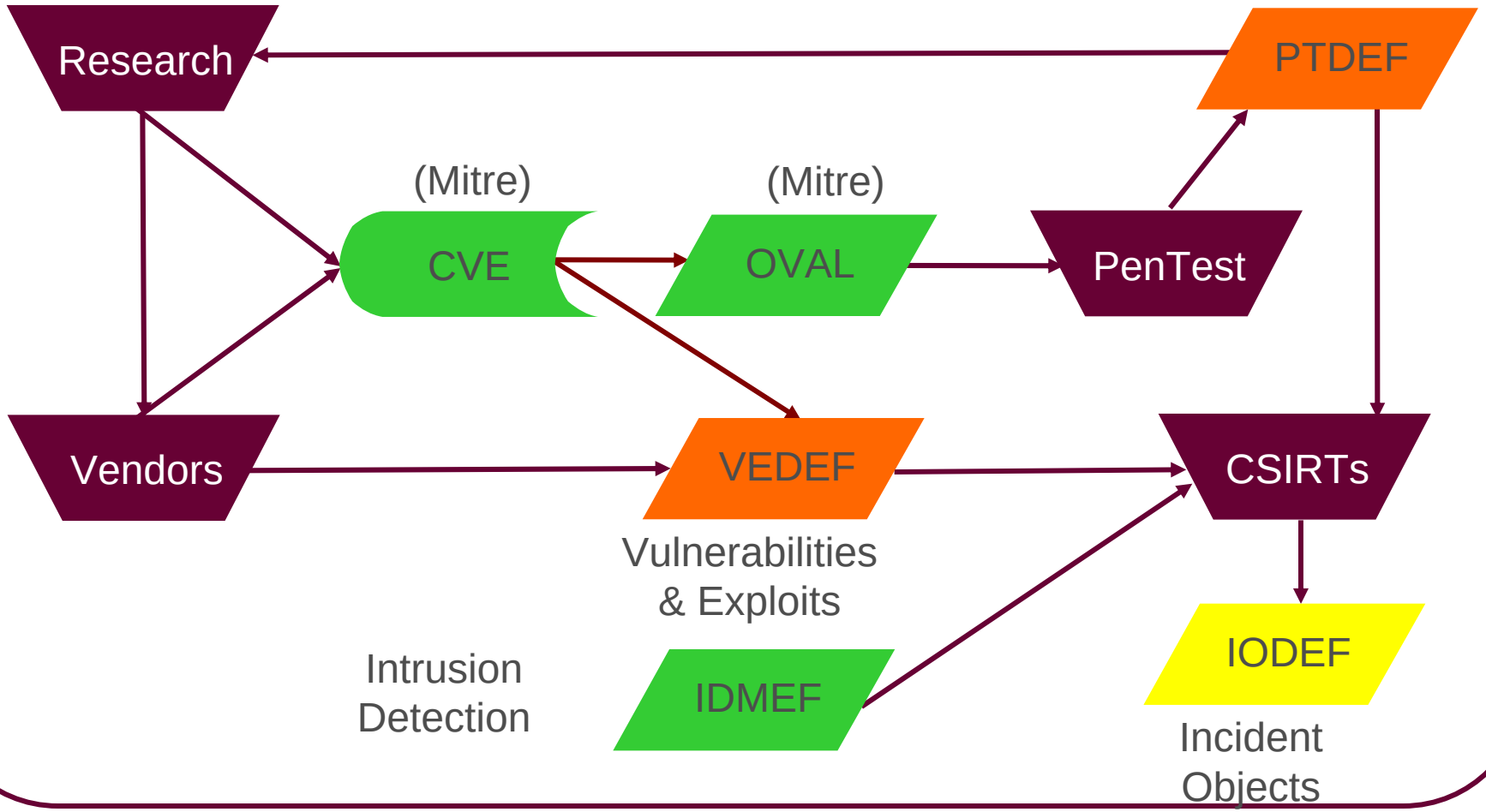
- Background
- Standardisation Requirement
- Current Activity
- Working with IETF INCH
- Questions ?

Background

Description & Exchange Formats (DEFs)

- Area of Information Security most ripe for standardisation is information sharing formats, ideally based on XML
- Current thinking suggests that 4 Description & Exchange Formats (DEFs) are required:
  - **IDDEF : Intrusion Detection DEF**
    - Covered by IETF IDWG (IDMEF)
  - **IODEF: Incident Object DEF**
    - Being actively progressed by IETF INCH
  - **PTDEF: Penetration Testing DEF**
    - Initial work being done by Military
    - OVAL
  - **VEDEF: Vulnerability and Exploit DEF**
    - Multiple initiatives
    - Needs concerted development

Information Flow Relationships



Standardisation Requirement

Vulnerability and Exploit DEF

- The *de facto* standard for storage of Vulnerability information is Mitre's Common Vulnerabilities and Exposures (CVE)
- Mitre's OVAL (Open Vulnerability Assessment Language) format aimed (approximately) at PTDEF
- A Vulnerability and Exploit DEF (VEDEF) for CSIRT community is therefore needed
- There are (at least) 6 existing initiatives :
  - Varying degrees of activity in their development
  - Being proposed by differing regions / communities
  - No real efforts towards their deconfliction

VEDEF - Existing Initiatives

EISPP	Common Format for Vulnerability Advisories	Under active development
RUS-CERT	Common Announcement Interchange Format (CAIF)	Under active development
OpenSec	Advisory and Notification Markup Language (ANML)	Last updated during January 2003
OASIS	Application Vulnerability Description Language (AVDL)	Initial issue published June 2004
	Classification Scheme for Web Security Vulnerabilities	No obvious progress since 1st meeting June 2003
JPCERT/CC	VulDEF element of Vendor Status Notes (JVN)	Under active development

Basic Information Requirement

- Description of the platform(s) affected
- Description of the nature of the problem
- Description of the likely impact if the Vulnerability and/or Exploit were, accidentally or maliciously, triggered
- Available means of remediation
- Disclosure restrictions

Proposed Deliverable Set

Document series consolidating Best Practice for Vulnerability and/or Exploit description

- Functional requirements for collaboration between Vendors, CSIRTs, and end users
- Specification of the extensible, data language to describes the data format(s) to satisfy requirements
- Guidelines for implementing the WG data format, with a set of sample Vulnerability and/or Exploit reports and their associate representation
- Extension to support Resource Description Framework (RDF) Site Summary (RSS) feeds

Current Activity

TF-CSIRT VEDEF WG

- European Task Force (TF) on Computer Security Incident Response Teams (CSIRT), who initiated IODEF
- Co-chaired between NISCC and Cisco
  - Select underlying Vulnerability Format(s) to be developed
  - Evolve with :
    - IODEF / RFC3067 nomenclature etc.
    - CMSI to formalise the System Information
    - Cisco update tool
    - RSS extension
- Collaboration with JPCERT/CC
  - Joint sponsor of this amendment

TF-CSIRT Pilots

- EISPP
  - Initial work funded by EU FP5
  - Version 2.0 of the XML Common Format for Vulnerability Advisories now published
  - In active use with 7 European CSIRTs
- NISCC
  - Filtered Warning and Alerting Software (FWAS)
  - Being trialled with WARP communities

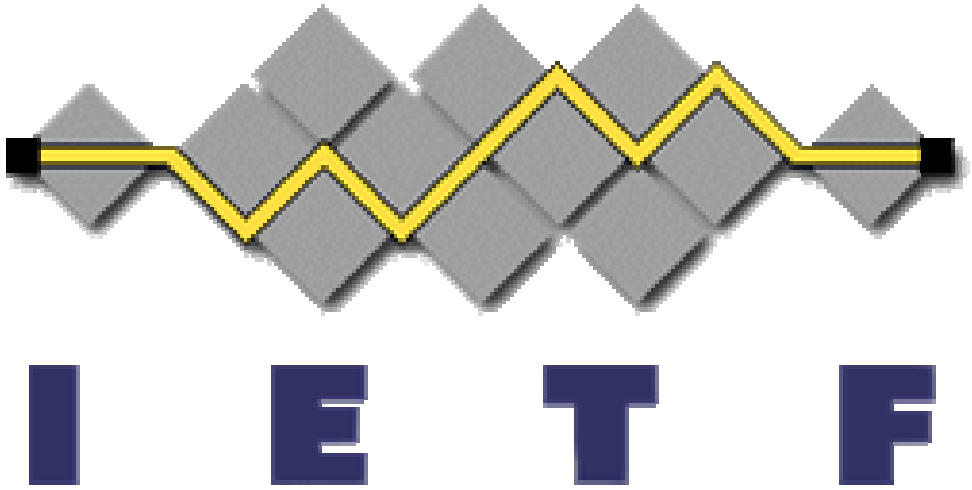
Cisco Proposed Extension

- Extended Usage of Security Advisories
- Distribute Advisories, or only parts of them, as XML files
- Embed XML tags which would carry additional information regarding the vulnerability and solution
- Additional software on the customer side to parse this information and, optionally, verify devices and download appropriate fixed code
- Not proposed to automatically perform and upgrades or configuration changes on a device

JPCERT/CC Pilots

- JVN / VulDEF
  - JPCERT/CC and Japanese domestic vendors
  - Currently using Version 1.0
  - Currently implemented on Portal site
- JVN RSS extension being used to provide information to general public
- Collaborative initiative with CERT/CC and NISCC for Vulnerability Management

Working with INCH



Current Charter Summary

Background

Computer security incidents occur across administrative domains often spanning different organizations and national borders. Therefore, the free exchange of incident information and statistics among involved parties and the responsible Computer Security Incident Response Teams (CSIRTs) is crucial for both reactionary analysis of current intruder activity and proactive identification of trends that can lead to incident prevention.

Scope

The purpose of the Incident Handling (INCH) working group is to define a data format for exchanging security incident information used by a CSIRT.

High Level Charter Revisions

Background

Computer security **challenges and** incidents occur across administrative domains often spanning different organizations and national borders. Therefore, the free exchange of incident **and vulnerability** information and statistics among involved parties and the responsible Computer Security Incident Response Teams (CSIRTs) is crucial for both reactionary analysis of current intruder activity and ~~*proactive identification of trends that can lead to*~~ incident prevention.

Scope

The purpose of the Incident Handling (INCH) working group is to define ~~*a*~~ data format**s** for exchanging **vulnerability and** security incident information used by a CSIRT.

Summary of Deliverables

- Requirements Specification
  - Informational
- Data Model
  - Standard
- Implementation Guidelines
  - Informational
  - Derived from inter-CSIRT, JVN, EISPP and Cisco pilots
- RSS Extension
  - Informational
  - Derived from JPCERT/CC prototypes

Summary - VEDEF WG Project Plan

Milestone	Activity
Sep-04	Initial Draft of the Requirements Specification by TF-CSIRT / JPCERT
Oct-04	Initial Internet-Draft (I-D) of the Requirements Specification
Nov-04	Submit Requirements Specification I-D to IESG as Informational
Jan-05	Initial Draft of the Data Model by TF-CSIRT / JPCERT
Feb-05	Initial I-D of the Data Model
Mar-05	Submit Data Model I-D to IESG as Standard
May-05	Initial Draft Implementation Guidelines document by TF-CSIRT / JPCERT
Jun-05	Initial I-D of the implementation guidelines
Jul-05	Submit implementation guidelines I-D to IESG as Informational
Sep-05	Initial Draft of the RSS Extension Specification by TF-CSIRT / JPCERT
Oct-05	Initial Internet-Draft (I-D) of the RSS Extension Specification
Nov-05	Submit RSS Extension Specification I-D to IESG as Informational

Questions?

Contact Details

Ian Bryant
Head of Capability Development
NISCC
PO Box 832, London
SW1P 1BG, England

Telephone:
+44-20-7821-1330 x 4565

Internet
ianb@niscc.gov.uk
http://www.niscc.gov.uk

Yurie Ito
Liaison Manager
JPCERT/CC
Tokyo
Japan

Telephone:
+81 (3) 3518-4600

Internet
yito@jpcert.or.jp
http://www.jpcert.or.jp