IETF INCH WG Interim Meeting
13th June 2004, Budapest HG

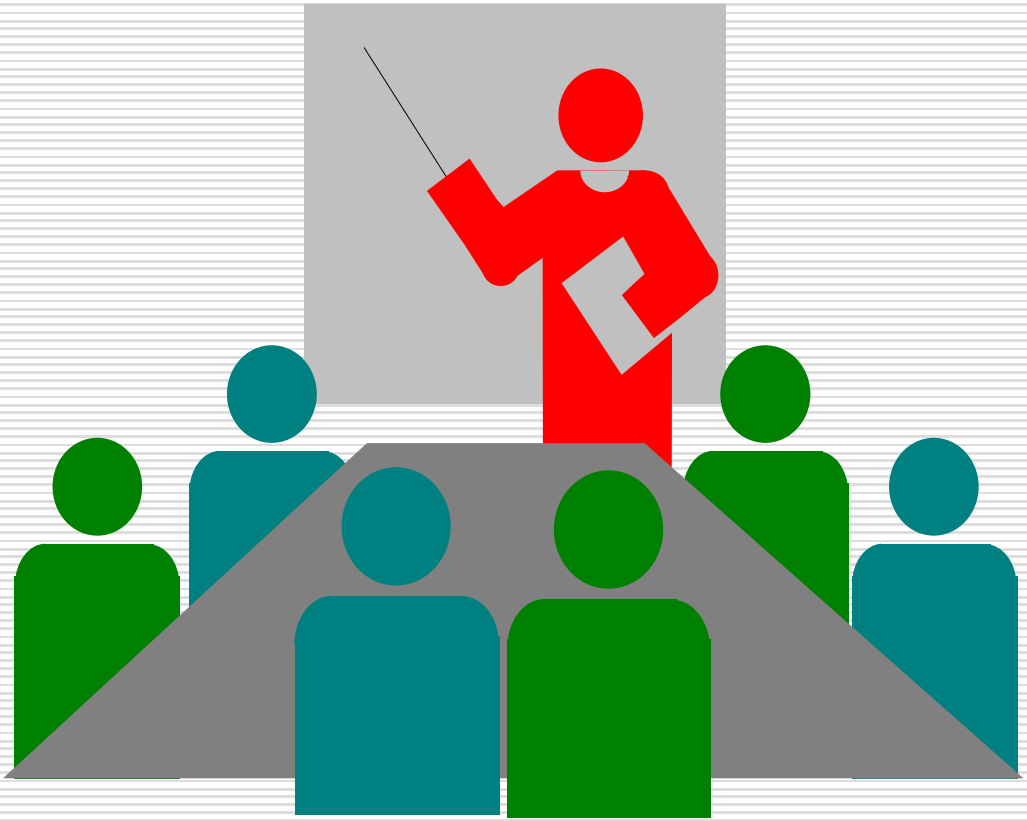
Vulnerability and Exploit Description and Exchange Format (VEDEF)

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

Vulnerability & Exploit DEF

- The Current Situation
- Activities by TF-CSIRT WG
- Proposed Way Ahead
- Questions ?

The Current Situation



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

Vulnerability and Exploit DEF

- The *de facto* standard for storage of Vulnerability information is Mitre's Common Vulnerabilities and Exposures (C
- 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 5 existing initiatives in this area
  - Varying degrees of activity in their development
  - Being proposed by differing regions / communities
  - No real efforts towards their deconfliction

VEDEF – Current Initiatives

Organisation	Initiative	Status
EISPP*	Common Format for Vulnerability Advisories	FP5 funding expired January 2004
RUSCERT*	Common Advisory Interchange Format (CAIF)	Last updated during February 2004
OpenSec	Advisory and Notification Markup Language (ANML)	Last updated during January 2003
OASIS	Application Vulnerability Description Language (AVDL)	Last updated during April 2003
	Classification Scheme for Web Security Vulnerabilities	No progress since 1st meeting June 2003

* Previous TF-CSIRT involvement

Basic Information Requirement

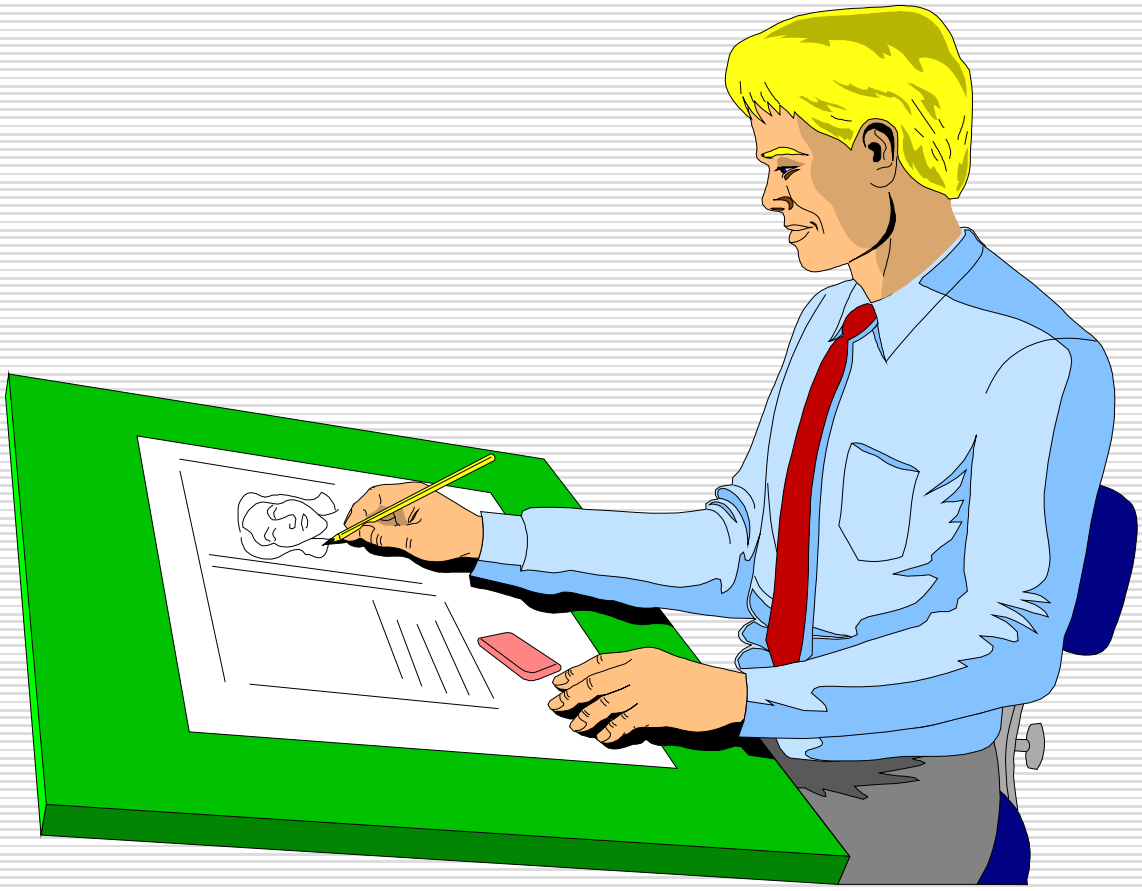
- Description of the platform(s) affected
- Description of the nature of the problem
- Description of the likely impact if the Vulnerability and/or Exploit were, accidentally or maliciously, triggered
- Available means of remediation
- Disclosure restrictions

VEDEF Outline Deliverables

Series of Documents establishing consolidated Best Practice for Vulnerability and/or Exploit description

- Functional requirements of data format for collaboration between Vendors, CSIRTs, and end users
- Specification of the extensible, data language to describes the data formats to satisfy the requirements
- Guidelines for implementing the WG data format, with a set of sample Vulnerability and/or Exploit reports and their associate representation in the data language

Activities by TF-CSIRT WG



TF-CSIRT

- European Task Force (TF) on Computer Security Incident Response Teams (CSIRT)
- Created, and supported, by TERENA (Trans-European Research and Education Network Association – http://www.terena.nl)
- Membership heavily involved in generation of Incident Object Description and Exchange Format (IODEF)
  - Led to RFC3067
- Working Group established to pursue VEDEF, co-chaired between NISCC and Cisco

TF-CSIRT VEDEF WG Status

- Charter published
- Review of external activities completed
  - EISPP
  - CMSI(I)
  - CAIF
  - IETF

VEDEF – Options with EISPP

- Initial effort supported by EU
  - FP5 funding
  - Expired January 2004
- Many of those involved with EISPP are also TF-CSIRT members
- Version 2.0 of the XML Common Format for Vulnerability Advisories now published

VEDEF – Options with CMSI (I)

Common Model of System Information

- Produced by a group of TF-CSIRT members
- Produces Machine Readable data
- Proposes central repository of XML data structure
- Proposes Vendors should maintain their own proprietary part of the model
- Has been used in EISPP v2.0

VEDEF – Relationship to CAIF

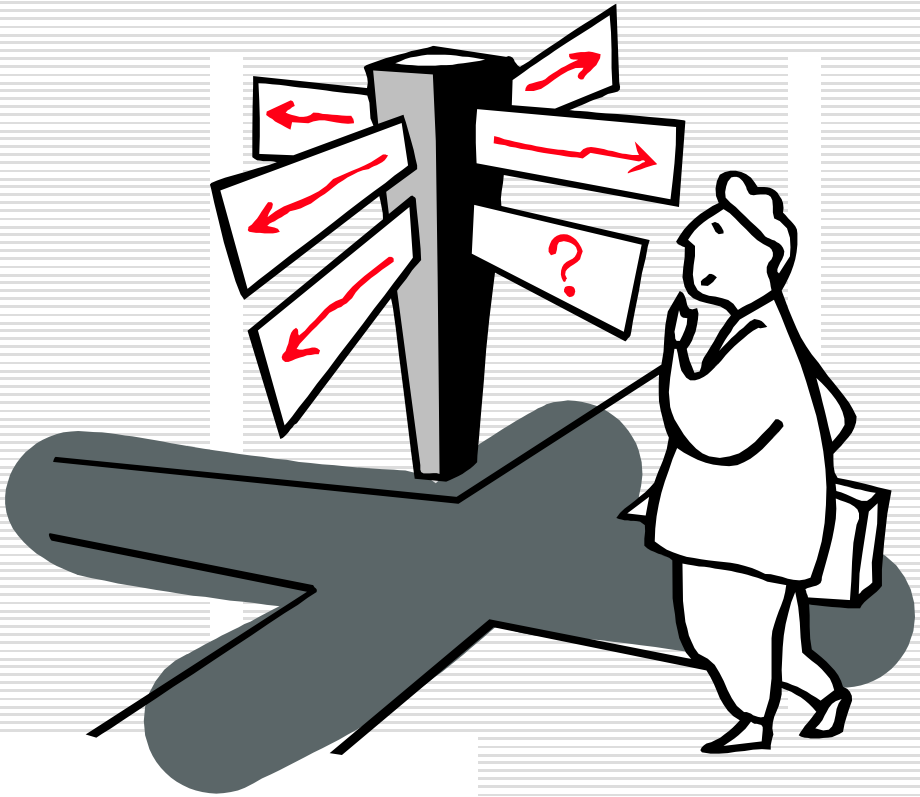
- Briefed to TF-CSIRT by RUS-CERT (University of Stuttgart) in 2002
- Largely dormant since
- Became active again in February 2004
- Updated version scheduled to be presented at FIRST Annual Conference in June 2004

VEDEF – Options with IETF

- Initial discussions held with Security Area Directors
  - Informal guidance is that IETF would not wish to charter new Working Group
  - Probable way ahead would be to use Extended Incident Handling (INCH)
  - Would require change to Charter

→ *INCH WG Interim Meeting at FIRST Annual Conference*

Proposed Way Ahead



Baseline for VEDEF Development

- Select underlying Vulnerability Format to be developed
- Needs to be evolved with :
  - CMSI(I) to formalise the System / Proprietary Information
  - Additional consideration of how to cover other (generic) Exploits types (e.g. Web Applications)
  - Ensure that (as far as practicable) nomenclature etc. is aligned with IODEF / RFC3067

VEDEF – Next Steps

- FIRST Annual Conference
  - → *INCH WG Ad Hoc Meeting (Sunday 13th June)*
  - Presentation on CAIF (Tuesday 15th June)
  - Proposed Birds of Feather (BOF) on VEDEF (Tuesday 15th June)
- Activate TF-CSIRT Working Group to draft 1st document (Requirements)
- Agree Requirements document at September TF-CSIRT Meeting (Valetta MT)

Summary - VEDEF WG Project Plan

Milestone	Activity
May-04	Agreement of "Best of Breed" candidates for development
Jun-04	***Presentations to IETF INCH and FIRST***
Sep-04	Initial Draft for TF-CSIRT of the requirements specification
Oct-04	**Initial Internet-Draft (I-D) of the requirements specification**
Nov-04	**Submit requirements I-D to IESG as Informational**
Jan-05	Initial Draft for TF-CSIRT of the data language specification
Feb-05	**Initial I-D of the data language specification**
Mar-05	**Submit data language specification I-D to IESG as Standard**
May-05	Initial Draft for TF-CSIRT of the implementation guidelines and examples document
Jun-05	**Initial I-D of the implementation guidelines**
Jul-05	**Submit implementation guidelines 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; Secretary
+44-20-7821-1330 x 4561;Direct
Facsimile : +44-20-7821-1686

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