



EISPP - Overview

- EU-funded (5th framework programme, IST-2001-35200)
- Duration: June 2002 to January 2004
- „*Successful conclusion*“ of project acknowledged by EC in February 2004
- Project partners:
 - Private-sector CERTs:
 - Cert-IST (France)
 - EsCERT (Spain)
 - Siemens CERT (Germany)
 - Callineb (Sweden)
 - ISPs: I-Net (Italy)
 - IT-security organizations: CLUSIT (Italy), InetSecure (Spain)
- Objectives:
 - **CERT cooperation on security advisories**
 - (Provide security advisories and related services to SMEs)



EISPP - Results Overview

Publicly available are:

- **Final Project Report**
 - Sums up motivations, project development and results
- **Common Advisory Format**
 - an XML-based exchange format for advisories
- **"CEISNE Model and Processes"**
 - CEISNE = Co-operative European Information Security Network of Expertise
 - Describes a roadmap for establishing close co-operation between European CERTs
- All documents available from
<http://www.eispp.org/documents.htm>



EISPP - Results

Common Advisory Format

Frequently asked questions:

- What is the EISPP Advisory Format?
- Is it useable?
- What is the future of the EISPP Advisory Format?
- What about related work?



EISPP Advisory Format

What is it?

- Exchange format for advisories to be used for co-operation between advisory issuers
- Definition:
 - Syntax: defined as XML-DTD
 - Semantics: defined via documentation that explains the format and its intended use



EISPP Advisory Format

Is it usable? (I)

- EISPP format is in productive use by five organizations in four European countries:
 - four EISPP CERTs
 - DFN CERT (not part of EISPP consortium) adopted EISPP format a few months ago
- Stable version 2.0 of EISPP format defined in co-operation between EISPP members and German CERT working group with special focus on co-operation regarding vulnerability classification
- Weak point: EISPP format (such as any other structured format) requires adequate tool support
 - ⇒ switching to EISPP requires some work
 - **Solution:** Adopt EISPP format gradually, moving from a bare-bones version of EISPP via EISPP light to full compliance (cf. Section 6 of the format description)



EISPP Advisory Format

Is it useable? (II)

```
<EISPP-Advisory version="2.0" issuer="ACME-CERT" xml:lang="en" date="2004-01-01">
  <Id_Data>
    <ref_num>ACME-2004-0001</ref_num>
    <title>
      <FreeText>Buffer Overflow in Foo package on Bar system</FreeText>
    </title>
  </Id_Data>
  <Vulnerability_Class>
    <vulnerabilities>
      <vulnerability>
        <risk_ratings>
          <risk schema="ACME" rating="high"/>
        </risk_ratings>
      </vulnerability>
    </vulnerabilities>
  </Vulnerability_Class>
  <System_Information>
    <information type="system_info">
      <FormattedText>Foo v1.3 on BAR OS</FormattedText>
    </information>
  </System_Information>
  <Description>
    <description type="complete_advisory">
      <FormattedText>
        A <em>buffer overflow</em> vulnerability has been discovered in the
        Foo package on the Bar system. Find more information
        <a href="http://www.foo-vendor.org/security/advisories/04/001">here</a>.
      </FormattedText>
    </description>
  </Description>
</EISPP-Advisory>
```

- Here, the EISPP format is used as a sort of wrapper for an advisory
- Even though almost none of the EISPP features have been used, this is already useful: EISPP-enabled tools can process it
- Features can be introduced gradually



EISPP Advisory Format

What is its future?

EISPP format is gaining momentum:

- Co-operation of EISPP partners continues
- Co-operation within Germany:
 - closer co-operation between DFN CERT and Siemens CERT as nucleus
 - EISPP format supported by „Deutscher CERT Verbund“ as basis for co-operation between interested German CERTs:
 - Project: Create a central database
 - for collecting EISPP advisories from different issuers
 - to provide tools necessary for making use of advisory collection (e.g., automated grouping)
 - Project: Design a common model for exchanging machine-readable information about affected systems (cf. yesterday's presentation about CMSI)
- Plans for co-operation between Latin-American CERTs and esCERT on basis of the EISPP format
- EISPP format as TF-CSIRT's format ...?



EISPP Advisory Format

What about related work?

Initiatives	Standardization Approach	Participants
CAIF	IETF (planned)	RUS-CERT
EISPP	None (yet; de-facto European standard)	EISPP (Callineb, Cert-IST, DFN-CERT, esCERT, Siemens-CERT)
WAS / AVDL	N/K	OASIS
ANML	N/K	OpenSec

} focus on presentation rather than co-operation?

} dormant/
much less mature

Source (for the stuff in blue): Ian Bryant's email on TF-CSIRT list regarding VEDEF



EISPP - Results

Roadmap towards CEISNE

- Experimentation within EISPP showed that
 1. CEISNE can only succeed if number of participants reaches 'critical mass'
 2. Close co-operation requires bilateral agreements between CERTs
 3. Successful co-operation within CEISNE requires **central** tool support
- CEISNE can only be a facilitator of co-operation providing a "market place" for finding co-operation partners and adequate supporting tools.
- The roadmap describes, how CEISNE could be established under the auspices of TF CSIRT and/or the Trusted Introducer
 1. Advance common advisory format and initiate structured information exchange regarding vulnerabilities on a broad basis
 2. Small-scale co-operation on advisories becomes possible between CERTs using the common format
 3. Use small-scale co-operation as stepping stone for initiating *coordinated* co-operation between CERTs "that fit to each other"



Carrying EISPP's results into TF-CSIRT

The members of the EISPP consortium ask the TF-CSIRT teams to:

- adopt a common advisory format
 - A common format is required to enable further works in that area
 - ⇒ get VEDEF working group started (with EISPP format as basis?)
- Start a discussion regarding the roadmap for closer CERT-cooperation proposed by the EISPP project:
 - decision on a common format is an important first step
 - central support for co-operation has to follow (cf. project of German CERT community)
 - Possibility of a further TI-service?