EISPP - Overview

- EU-funded (5th framework programme, IST-2001-35200)
- Duration: June 2002 to January 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)
- Objectives:
  - **CERT cooperation on security advisories**
  - (Provide security advisories and related services to SMEs)

EISPP - Motivation

The number of vulnerability announcements has increased dramatically over the last few years.

Consequences:

- CERTs that write advisories for their own constituencies are spending more and more resources on this
- CERTs that ‚only' collect and forward advisories to their constituencies are flooding their constituencies
- CERTs that are coordinating vulnerability response can only react to the most important vulnerabilities

⇒ EISPP (European Information Security Promotion Programme) wants to lay foundations for a co-operation in writing advisories.

EISPP - Process

- Creation of common infrastructure (until April '03)
  - Common exchange format for advisories
  - Exchange/Access to advisory data
- Experimentation phase (April '03 - Sept. '03)
  - Experimentation with various cooperation models
  - Request feedback from European/international CERT community
- Evaluation (Sept.'03 - Jan. '04)
  - Enhancement of common exchange format
  - Roadmap for European CERT-cooperation with respect to security advisories

EISPP - Results Overview

The results of EISPP relevant for improving CERT co-operation on vulnerability handling / advisory creation are:

- **Common Advisory Format**
  - V1.2 available from http://www.eispp.org/documents.htm
  - V1.3 ready until end of January 2004
- **Roadmap for establishing CEISNE**
  - CEISNE = Co-operative European Information Security Network of Expertise
  - Available as **"CEISNE Model and Processes"** from http://www.eispp.org/documents.htm

EISPP - Results
Common Advisory Format

- EISPP Advisory Format V1.3 devloped with feedback/involvement of German CERT community
- EISPP Advisory Format V1.3 will be used within the German CERT community
- ⇒ **EISPP Advisory Format about to become de-facto standard** used by a significant number of CERTs within Europe
- German CERT community working on a standardized system for categorizing system information (which systems are affected?)
  - Can be used as add-on to EISPP format
  - Should also be useful in conjunction with other advisory formats (cf. the CVE initiative)

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. Initiate structured information exchange regarding vulnerabilities on a broad basis
  2. Use information exchange as vehicle for advancing common advisory format
  3. Small-scale co-operation on advisories becomes possible between CERTs using the common format
  4. Use small-scale co-operation as stepping stone for initiating *coordinated* co-operation between CERTs "that fit to each other"

EISPP - Conclusions

- Vulnerability handling and advisory creation requires more and more effort
- Increased co-operation between CERTs necessary to keep up with growing volume of vulnerabilities
- Co-operation and coordination between some CERTs can grow out of structured information exchange between large number of CERTs
- EISPP's roadmap towards CEISNE describes a process for establishing a co-operative network
- The EISPP advisory format, an important corner stone of an infrastructure that supports close co-operation, is well on its way towards a de-facto standard within Europe