EISPP
A Status Report

Bernd Grobauer
Siemens CERT
EISPP Overview (I)

• "EISPP" stands for European Information Security Promotion Programme
• Started in June 2002, running for 18 months
• Project partners:
  • Private-sector CERTs:
    • Callineb (Sweden)
    • CERT-IST (France)
    • EsCERT (Spain)
    • Siemens CERT (Germany)
  • ISPs: I-Net (Italy)
  • IT-Security-Organisations: CLUSIT (Italy)
• Details under http://www.eispp.org
EISPP Overview (II)
CERT Co-operation on Advisories: Objectives

- Define common advisory format
- Build initial infrastructure for co-operation
- Experiment with co-operation models
- Collect feedback/requirements on
  - Advisory format
  - Co-operation model

⇒ Prepare „CEISNE“ (Co-operative European Information Security Network of Expertise)
  - Revised advisory format
  - Co-operation model / Agreement
CERT Co-operation on Advisories: Progress

- Common advisory format defined, available and used
- Initial infrastructure for co-operation in place since end of March
- Experiments with co-operation models are running since beginning of April
- Collection of feedback/requirements in progress
  - EISPP Workshop associated with 9th TF-CSIRT meeting
  - Bilateral contacts with various CERTs
EISPP Advisory Format

- Presentation-independent, structured data format
- Defined as XML format
- Supports multiple-language content
- Version 1.2 available from http://www.eispp.org
- All EISPP CERTs use common format for advisory production
EISPP Infrastructure

- Automated exchange of advisory data in common format using SMTP („push“ modell) ⇒ replicated database of advisory information
- Optional „pull“ modell via http or mail-request
- Discussion about advisories via mailing list
- Initial assessment:
  - replicated database works well, but
  - we lack a central site for
    - harnessing data (e.g., create common overview)
    - structured discussion / sharing of expertise
Advisory Co-operation Model (I): Desiderata

- Common, unanimous classification of vulnerabilities
  - Now: CERTs use proprietary classification schemes
  - Vision: Common classification scheme as basis for communication and joint classification

- Division of labor
  - Now: for writing security advisories, the same work is done in parallel at many CERTS: collection and analysis of data, authoring
  - Vision: wide spectrum for possible collaboration

- Pooling of expertise
  - Now: a CERT can support systems for which it has in-house expertise
  - Vision: network of CERTs allows one CERT to draw on expertise of other CERTs
Advisory Co-operation Model (II): First findings

• Common, unanimous classification of vulnerabilities
  • we have common classification scheme, but
  • often different assessments need to be resolved in discussion

• Division of labor
  • Re-use of advisory data or « one-for-all » models hampered by different advisory styles
    • Concise vs detailed
    • Update vs. New advisory
  • Workshop result: concentrate first on information sharing

• Pooling of expertise
  • Division of fields of expertise too big a step?
  • Information sharing in common areas of expertise as first staring point?
CERT Co-operation on Advisories: Objectives

- Define common advisory format
- Build initial infrastructure for co-operation
- Experiment with co-operation models
- Collect feedback/requirements on
  - Advisory format
  - Co-operation model

⇒ Prepare „CEISNE“ (Co-operative European Information Security Network of Expertise)
  - Revised advisory format
  - Co-operation model / Agreement
CEISNE: First ideas

- Informal co-operation based on a code of conduct
- Central site for sharing advisory data?
  - Parts (title, abstract, classification, standard vuln-ids)
  - Full advisories
    - in proprietary format
    - in EISPP advisory format

⇒ Benefits
  ⇒ Overview over important vulnerabilities
  ⇒ Advisory-driven information-sharing
  ⇒ „contact forum“ for closer co-operation on advisories