EISPP – A First Attempt on Prevention Co-operation

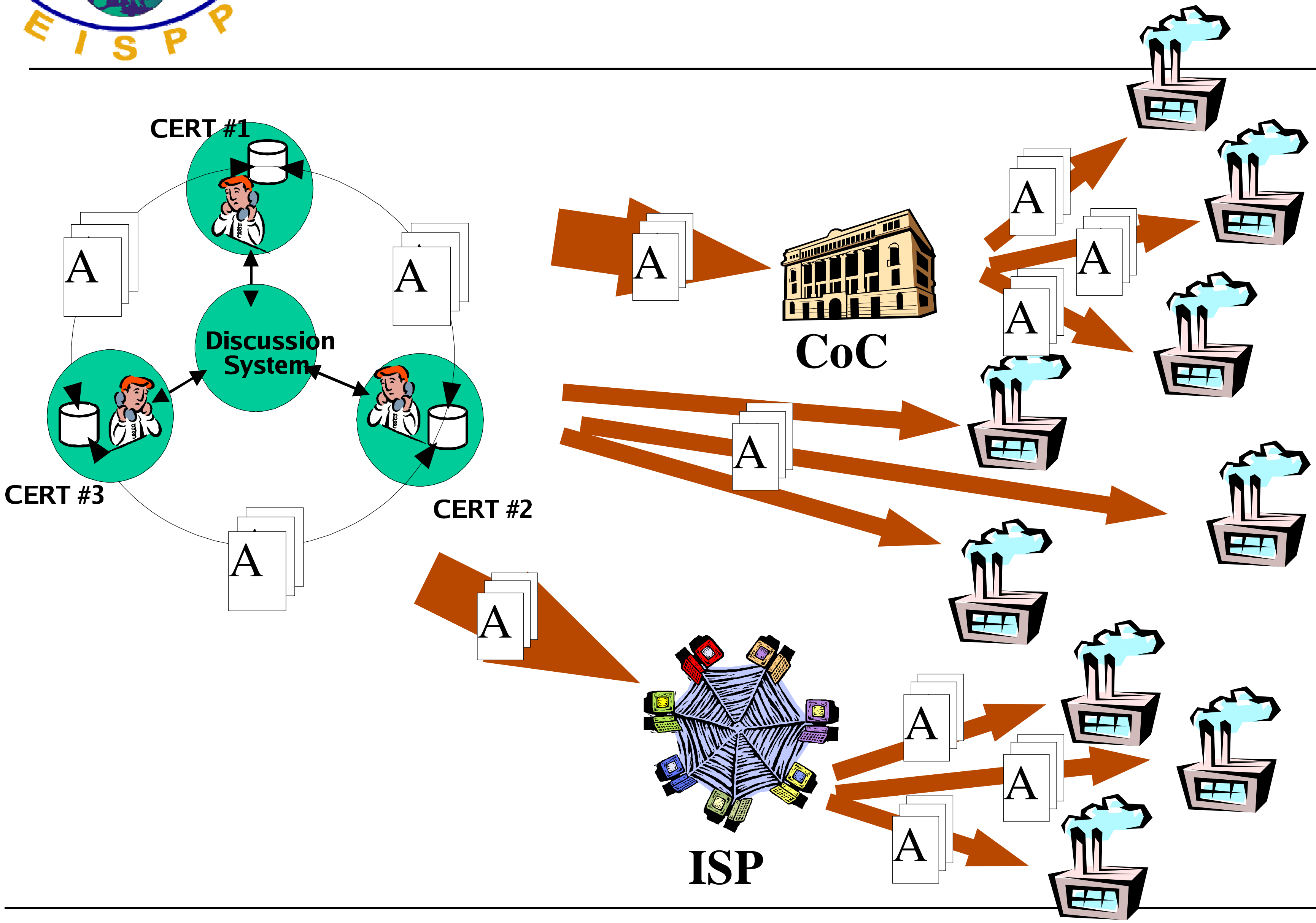
Bernd Grobauer

Siemens CERT

What is EISPP?

- **EISPP stands for "European Information Security Promotion Programme"**
- **Funded through European Union IST Program**
- **Founding members:**
  - Private-sector European CERTs:
    - CERT-IST (France)
    - EsCERT (Spain)
    - SBS BT-Ignite (Great Britain)
    - Siemens CERT (Germany)
  - ISPs: I-NET (Italy)
  - Security professional organization: CLUSIT (Italy)
- **Details: see http://www.eispp.org**

Vision of EISPP



This talk

- **Three workpackages in EISPP:**
  - WP 3: CERT co-operation w.r.t. security advisories
  - WP 4: Distribution of tailored security advisories to SMEs
  - WP 5: Added value to security advisories for SMEs
- **This talk focuses on WP 3:**

  ① Definition of an advisory co-operation model (⇒ CERT network)

  ② EISPP exchange format for security advisories
- **Objective of presentation here at FIRST TC:**
  - Receive feedback
  - Get ***you*** interested into EISPP's activities (network, exchange format)

Advisory Co-operation Model: 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: Issues

- **How fast can unanimity on vuln. classification be reached?**

  (In-depth discussion vs. timely advisory creation)

- **How similar must the advisory styles of participating CERTs be?**

  (concise vs. comprehensive, update of old advisory vs. issuing new adv.)

- **Where and to which extent is division of labor possible?**

  (collection of data, analysis, joint authoring, reuse of finished advisory,...)

- **To which extent is division of expertise possible?**

- **What is a possible legal framework/agreement for the cooperation?**

  (code of conduct, quality of service, ...)

Approach of EISPP to Co-operation Model

- **Basis of co-operation (– March '03):**
  - advisory exchange format
  - Infrastructure:
    - Cross access to advisory databases
    - System for discussion/co-operation
- **Trial period (April '03 – Sept. '03):**
  - EISPP CERTs experiment with possibilities for co-operation
- **Evaluation of trial period (Sept '03 – Dec. '03)**

  ⇨ processes/policies defining co-operation model

  ⇨ model agreement for CEISNE (Co-operative European Information Security Network of Expertise)

This talk

- **Three workpackages in EISPP:**
  - WP 3: CERT co-operation w.r.t. Security advisories
  - WP 4: Distribution of tailored security advisories to SMEs
  - WP 5: Added value to security advisories for SMEs
- **This talk focuses on WP 3:**
  - ① Definition of an advisory co-operation model (⇒ CERT network) ✔
  - ② EISPP exchange format for security advisories
- **Objective of presentation here at FIRST TC:**
  - Receive feedback
  - Get ***you*** interested into EISPP's activities (network, exchange format)

Advisory Exchange Format: Significance for EISPP Co-operation

- **Provides common vuln. classification scheme**
- **Automatically approximates advisory styles**
- **Basis for EISPP cross-access infrastructure**
    - search/manipulate advisories with own toolset
    - only way to scale up co-operation
- **Essential for close collaboration**
    - joint authoring
    - re-use of parts or even whole advisory

Requirement: Format must support tailoring of advisories

Advisory Exchange Format: Design Decisions

- **Presentation-independent, structured data format**
  - Supports tailoring
  - Eases authoring, maintenance, re-use
  - Basis for additional features (fine-grained search, ...)
- **Defined as XML format**
  - Formal description aides standardization
  - Standard tools (XML-editor, XML-parser, XSLT-stylesheets) can be used
- **Supports multiple-language content**
  - Supports tailoring for international audience (essential in European context)

Advisory Exchange Format: Overview over Contents

- Identification Data
- History Data
- System Information
- Vulnerability Classification
- Problem Description
- Solution
- Standard Vulnerability Ids
- Additional Resources

Advisory Exchange Format: Related Work

- **CAIF (Common Advisory Interchange Format) being developed at RUSCERT**
  - For the time being, only “Requirements Document” available
  - RUSCERT already uses prototype of CAIF
- **Common ground between CAIF and EISPP Format:**
  - CAIF requirements document taken into account for EISPP design:
    ⇨ Both formats likely to be compatible to some extent
  - EISPP Format will be developed further
  - Possibility for future co-operation: system classification model
- **Difference between EISPP Format and CAIF:**

  EISPP Format about to be used in five countries

  ⇨ EISPP Format is a living standard

This talk

- **Three workpackages in EISPP:**
  - WP 3: CERT co-operation w.r.t. security advisories
  - WP 4: Distribution of tailored security advisories to SMEs
  - WP 5: Added value to security advisories for SMEs
- **This talk focuses on WP 3:**
  - ① Definition of an advisory co-operation model (⇒ CERT network)
  - ② EISPP exchange format for security advisories
- **Objective of presentation here at FIRST TC:**
  - Receive feedback
  - Get ***you*** interested into EISPP's activities (network, exchange format)

What *I* would like to take home

- **Questions, questions, questions**
- **Feedback, feedback, feedback:**
  - Your thoughts about the advisory exchange format
    - Could you imagine using it?
    - If so, under which circumstances?
    - If not, why not?
  - Your thoughts about a CERT network for co-operation on security advisories
    - Could you imagine participating?
    - If so, under which circumstances?
    - If not, why not?
  - ...

What you can take home

- **EISPP strives for CERT co-operation w.r.t. authoring security advisories**
- **To that end, EISPP is definining/experimenting with:**
  - an XML exchange format for security advisories
  - well-defined processes for co-operation
- **EISPP advisory exchange format soon to be used in five countries ⇨ a *living* standard**

Ask yourself:

- Could my CERT profit from using the EISPP exchange format?
- Could my CERT profit from participating in a CERT network for co-operation on security advisories/pooling expert knowledge?