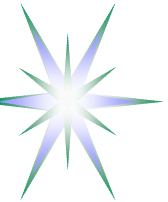
TechSec WG:
Related activities overview
Information and discussion

TechSec WG, RIPE-45

May 14, 2003

Yuri Demchenko <demch@NLnetLabs.nl>



Outline

- TechSec WG liaison with CSIRT community
  - Results and developments in CSIRT community
- Other possible areas of interest
  - PKI and AuthN/AuthZ developments
- Discussion: Interest from RIPE community and possible forms

Developments in CSIRT community

- TF-CSIRT – Task Force for Computer Security Incident Response Team Coordination for Europe - http://www.terena.nl/tech/task-forces/tf-csirt/
- TI – Trusted Introducer Service - http://www.ti.terena.nl/
- Training for new CSIRT members – TRANSITS project http://www.ist-transits.org/
  - Next training course – May 2003
- CHIHT - Clearinghouse of Incident Handling Tools - http://chiht.dfn-cert.de/
- BCP working group to assist new CSIRTs with focus for East European countries
  - Mailing list archive - http://hypermail.terena.nl/csirt-bcp/
- Prospects for closer cooperation - TF-CSIRT meetings:
  - 29-30 May, 2003 Warsaw
  - 27-28 September, 2003 Amsterdam

IETF INCH WG (INCident Handling)

INCH WG - http://www.ietf.org/html.charters/inch-charter.html

Status and recent developments

- Requirements for Format for INcident Report Exchange (FINE)
  http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-00.txt
  - To be updated before IETF-57
- The Incident Data Exchange Format Data Model and XML Implementation Document Type Definition
  http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-01.txt
- Planned implementation
  - CERT/CC AIRCERT project - http://www.cert.org/kb/aircert/
  - eCSIRT Project - http://www.ecsirt.net/
  - Interest from AP region, GRID community (EEGE Project)

Registry services for CSIRTs

- Trusted Introducer for CSIRTs
  - Formal procedure of accreditation
  - Special information services for members, i.e. maintained trust relations
  - Accredited teams – more than 30 (NRENs, Com, Gov)
  - Not limited by region and type of CSIRT
- FIRST (Forum for Incident Response Security Teams)
  - More than 120 teams
  - No formal procedure, no accreditation, no maintained trust relations
- IRT Object in RIPE NCC database

IRT Object in RIPE NCC database

- Initiative by TF-CSIRT and RIPE NCC – two years project
  - RIPE NCC document ripe-254 - http://www.ripe.net/ripe/docs/irt-object.html
- Purpose to allow search for IRT/CSIRT responsible for specific IP address space
  - Prospectively by automatic tools
- Registration procedure:
  - Individual CSIRTs via ISP/LIR or
  - by Trusted Introducer Service, also considerably by FIRST
- Number of IRT objects created – total 16
  - By TI maintainer – 9
  - By ISP/CSIRT - 7

PKI related development by IETF, ETSI and others

- X.509 PKI is a basic technology for trusted secure communications, protocols and services
- IETF PKIX WG - Public-Key Infrastructure (X.509) http://www.ietf.org/html.charters/pkix-charter.html
  - Profiles and Identitfies: PK Certificate, Qualified Cert, Attribute Cert for AuthZ/PMI, Proxy Certificate, etc.
  - Using LDAP for PKI
  - Protocols and services for PKI management, e.g. CVP (Certificate Validation Protocol), OCSP (Online Certificate Status Protocol), Timestamping, etc.
- European Electronic Signature Standardisation Initiative (EESSI) by ETSI - http://www.ict.etsi.org/EESSI/EESSI-homepage.htm
  - Number of practical documents are published, e.g. “ETSI TR 102 044 Requirements for role and attribute certificates - http://webapp.etsi.org/action\PU/20021203/tr_102044v010101p.pdf
- Next joint meeting between IETF PKIX and EESSI at IETF57 in Vienna

PKI and AuthN/AuthZ (AA) services

- PKI also creates a basis for AuthN/AuthZ services and Identity management
  - They are intending to become “killer”-applications for PKI
- IETF Standards
  - An Internet Attribute Certificate Profile for Authorization (RFC 3281) – defines AC for X.509 role-based Privilege Management Infrastructure (PMI)
  - RFC2902-RFC2906 – Authentication, Authorisation, Accounting Framework – mostly oriented for mobile communications
- ITU-T Rec. X.812(1995) | ISO/IEC 10181-3:1996, Information technology - Open systems interconnection - Security frameworks in open systems: Access control framework
- OASIS developments
  - SAML (Security Assertion Markup Language)
  - XACML (eXtensible Access Control Markup Language)
  - Web Services Security (actually SOAP Security)

Existing OpenSource solutions for AA and PMI

- PERMIS (PrivilEge and Role Management Infrastructure Standards Validation Project) - http://sec.isi.salford.ac.uk/permis/
- SPOCP (Simple POlicy Control Protocol) - http:/www.spocp.org/
- Internet2 PubCookie/WebISO - http://middleware.internet2.edu/webiso/
- Shibboleth AuthZ Service - http://shibboleth.internet2.edu/
- A-Select (AuthN and SSO) - http://a-select.surfnet.nl/

Liberty Alliance Project (LAP) and Network Identity

Liberty is a set of protocols that collectively provide a solution for identity federation management, cross-domain authentication, and session management.

- New set of LAP specifications Version 1.1 was published in April 2003 - http://www.projectliberty.org/
  - Using SAML and Web Services technology
- The Liberty architecture contains three actors: Principal, Identity provider, and Service provider
  - Circles of trust are initiated and controlled by user/principal

Liberty Identity and Protocol

Liberty protocol provides federation of Principal's identity between the Identity provider and the Service provider.

- Principal is *authenticated* to the Identity provider
- Identity provider provides an authentication assertion to the Principal
- Principal can present the assertion to the Service provider
  - Principal is then also authenticated to the Service provider if the Service provider trusts the assertion.
- An *identity federation* is said to exist between an Identity provider and a Service provider when the Service provider accepts authentication assertions regarding a particular Principal from the Identity provider

Discussion – Interest from RIPE community

- Provide information on PKI and AA/Identity development
  - Including BCP and Use cases
- Provide training courses – in support of the proposed RIPE NCC PKI based Secure service model
  - PKI basics
  - Setup own Certification Authority
  - Using PKI for Authentication and Authorisation
- Any other suggestions?