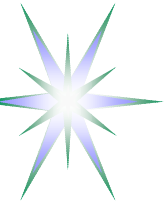
TechSec WG:
Related activities overview
and Fonkey Project update

TechSec WG, RIPE-46

September 3, 2003

Yuri Demchenko demch@NLnetLabs.nl

Erik Rozendaal <erik@NLnetLabs.nl>



Outline

- IODEF development at IETF INCH-WG
- PKI and other Security related developments at IETF
- Other developments in Application Security area
  - AA(A) – AuthN/AuthZ and Accounting
  - Network Identity management: Liberty Alliance vs WS-Federation
- Fonkey Project update

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-01.txt
  - To be updated before IETF-58
- 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
  - To be updated before IETF-58
- Planned implementation
  - CERT/CC AIRCERT project - http://www.cert.org/kb/aircert/
  - eCSIRT Project - http://www.ecsirt.net/
  - APCERT – very active, contribution to multilingual issues
  - GRID community (EGEE Project)

IODEF: implementation issues

- Implementation Guide – initial drafting
  - To address implementation issues
  - Technology issues: XML generation and parsing, XML Signature and Encryption, Key management, Information input/output
- Support tools for early implementers
  - Schema definition and Documentation
  - IODEF XML Library for Java
- Reference/Demo implementation to address
  - XML processing and XML Signature/ Encryption
  - Variables naming: for elements and attributes
    - Document vs system attributes

IETF PKIX WG - Public-Key Infrastructure (X.509)

PKIX-WG is wrapping up. The remaining problems and new drafts discussed at the meeting:

- Meet ISO/ITU development of PKI
- Algorithm and optimisation of path building for Cert verification and trust management: "it is easy to do but difficult to do well"
- X.509 PKC extension for IP addresses and Autonomous Systems (what is specifically important for S-BGP and so-BGP)
- Introduction of name comparison for international character sets (mandatory support stated in RFC3280 on X.509 PKC and CRL) creates a problem, e.g. when matching name in e-mail and Certificate
  - suggested solution to use “stringprep” algorithm developed by IDN WG for internationalised domain names (RFC3454)
- LDAP matching rules and LDAP Schema for attribute extraction – ML/UTF-8 again
- Multidomain PKI issue raised by Japanese Government PKI Project (draft-shimaoka-multidomain-pki-00.txt)
  - found also a case in US inter-university PKI deployment
- Russian Cryptographic algorithm (GOST) to be standardised for PKI

EESSI/ETSI for Europe

- European Electronic Signature Standardisation Initiative (EESSI) by ETSI - http://www.ict.etsi.org/EESSI/EESSI-homepage.htm
- EC published decision of OJ EU 15/7/2003 I 175/24 on set of standards for electronic signature use (in compliance with Annex II f to Directive 1999/93/EC) http://europa.eu.int/eur-lex/en/dat/2003/l_175/l_17520030715en00450046.pdf
  - CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements
  - CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
- Standards for electronic signature products (compliant with Annex III)
  - CWA 14169 (March 2002): secure signature-creation devices.
- Other useful documents, e.g.
  - “ETSI TR 102 044 Requirements for role and attribute certificates - http://webapp.etsi.org/action\PU/20021203/tr_102044v010101p.pdf

Enroll BOF (http://www.ietf.org/ietf/03jul/enroll.txt)

Addressed issues:

- Initial introduction model and enrolment for PK based network and application security solutions, e.g., enrolment of a user against a service provider
- There are no commonly accepted approaches and methods for initial introduction and enrolment for obtaining (more secure, long-term) credentials and problems with getting X.509 PKC
- Important deployment issue for many areas where PKI is used, including DNSSEC, ADSL, AuthZ/AuthN, etc.
- Discussed problems and proposed solutions:
  - "Imprint" vs "Leap-of-trust"
    - AuthN of previously unknown principal without relying on 3rd party
  - Shared Secrets Provisioning Protocol – few drafts by Bob Moskowitz
  - Machines vs human enrollement
    - all machine are controlled by humans

Lawful Intercept issues at IETF

Presentation related to Lawful Intercept in IP Networks by Cisco Fred Baker, former IETF chair

Cisco Architecture for Lawful Intercept In IP Networks
http://www.ietf.org/internet-drafts/draft-baker-slem-architecture-01.txt

- Cisco needs to answer their customers request to provide features for network surveillance and they provide these features in their equipment.
- Draft doesn't describe internal solution but describes functionality only
- European legislation on this issue
  Convention on Cybercrime, ETS No. : 185
  http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=17/07/03

Application Security and AA(A)

Authentication, Authorisation and Accounting (AAA) vs Authentication and Authorisation (AuthN/AuthZ)

- AAA is addressed by AAA-WG at IETF – currently focussed on mobile network problems - RFC2902-RFC2906
- AAAArch-RG at IRTF – focussed on deployment issues and accounting/billing
- AuthN/AuthZ and Network Identity management
  - Two competing technologies Liberty Alliance and WS-Federation
- **XML Security** as underlying technology for Application/Services oriented AAA technologies

Network Identity: Liberty Alliance vs WS-Federation

Identity Federation takes a place when multiple user/entity identities in different trust/administration domains are federated for SSO operations.

Liberty is a set of protocols that collectively provide a solution for identity federation management, cross-domain authentication, and session management - http://www.projectliberty.org/

- Three trust models based on Business or Trust agreements:
  - Pairwise Trust model (basic model for the Liberty Phase 1); Brokered Trust model; Community Trust Model
  - Circles of trust are initiated and controlled by user/principal

WS-Federation is the last published spec from WS-Security suite and is complimentary to WS-Trust and WS-Policy

- Developed by Microsoft, IBM, Verisign, BEA

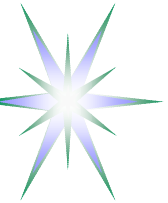
Fonkey Project Update

Fonkey Project at NLnet Labs - http://www.nlnetlabs.nl/fonkey/

- System to distribute cryptographic keys and reference/attribute information bound by Digital Signature

Project Status

- Current stage – initial design including technology overview and demo implementation
  - definition and pilot implementation of basic client-storage functionality, including Package format, Semantics of query language
  - XML Signature/Encryption tested
  - Key management tools tested
- Further development will depend on interest from community and available resources



Fonkey Target Applications

Fonkey is kept as simple as possible to create easily deployable infrastructure

- Analysis of target application allows to define specific requirements and necessary extensions to the generic/basic functionality

Target applications

- PGP Keyserver with extended payload
- Privilege Storage (bound to PK based identity)
- Other applications under discussion
  - Location Server for IIDS
  - Identity Server for Liberty Project applications – *under discussion*

Target Application: Extended PGP Keyserver

Reference - The OpenPGP HTTP Keyserver Protocol (HKP)

http://www.ietf.org/internet-drafts/draft-shaw-openpgp-hkp-00.txt

Specific requirements

- PGP key request via HTTP GET
  - Operations - {get, index, vindex, x-?}
  - Search - variable {key ID, V4 Fingerprint, V3 Fingerprint}
  - Modifier = {options {mr, nm}, fingerprint, exact
- PGP key publish via HTTP POST
  - OpenPGP Packet in an ASCII Armored format (RFC2440)

Benefits/new functionality with Fonkey

- Adding application oriented payload
- Flexible search for Key information
- Integration with other types of PK infrastructures

Design issues: Types of Package

Generic Package structure –
{Type, Public Key, Properties, Payload, Signature}

- **Key Package** – like generic package
  - Unique ID is defined by Public Key
  - Location by Public Key attributes/info
- **Named Package** – adds Name field to the generic package
  - Unique ID is defined by Name and Key
  - Location by Name
- **Signature Package** – adds Subject (ID of the package signed by this Signature) and References (to signed parts/portions)
  - Unique ID is defined by Public Key and Subject
  - Location by (Subject, Public Key) pair

Technology: Java Key management tools

Key management tools to generate, export or import server and client keys and certificates:

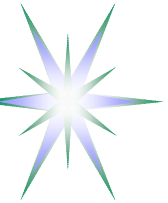
- Native Java key and certificate management tool ***keyrtool*** included as a standard tool in J2SE distribution that support X.509 public key certificates
- IBM KeyMan needed for creating mutual trust between two entities using a certificate chains (mutual certificates with attached lineage of public certificates with common trusted root) - http://www.alphaworks.ibm.com/tech/keyman/
- OpenPGP key tool - provides support for OpenPGP key encryption and signature; should be also installed with OpenPGP JCE Provider; both packages are available from The Cryptix Foundation Ltd. - http://www.cryptix.org/

Technology: XML Security packages for Java

XML Security packages available from Apache Jakarta and IBM:

- Apache XML Security library supporting XML Signature (XML Encryption is under development) - http://xml.apache.org/security/
- IBM xss4j Security suite that supports XML Encryption and Decryption Transform and aims to support XACML - http://www.alphaworks.ibm.com/tech/xmlsecuritysuite
- OpenSAML – http://www.opensaml.org/
  - Or as a part of Shibboleth - http://marsalis.internet2.edu/cgi-bin/viewcvs.cgi/
  - Note. SAML is an OASIS standard for AuthN/AuthZ tokens exchange

Note. XML Security requires implementation and use of the whole set of XML related technologies: XML parser (xerces), XSLT (xalan), XML Schema tools



Fonkey technology overview

Fonkey technology overview and demo will be available from the project web page - http://www.nlnetlabs.nl/fonkey/