Open-source Public Key Infrastructure

Open-source Public Key Infrastructure (PKI)

Simos Xenitellis
University of London
S.Xenitellis@rhbnc.ac.uk
Open-source Public Key Infrastructure

**Agenda**

*We are going to discuss about*

- open-source software
- public key cryptography
- PKI functionality

*about*

- available standards
- open-source PKI implementations

*and finally about*

- critic on OS PKI design

3rd August 2000, LBW2000
Open-source Public Key Infrastructure

**Open-source**

is

- a new trend
- a new software development model
- is based on the almost zero distribution costs
- quick initial distribution
- not expensive life-cycle

**In short**

- availability of source code
- covered by suitable unencumbered licence
Open-source Public Key Infrastructure

Public Key Cryptography

In a nutshell

- one key to encrypt (public)
- another to decrypt (private)
- the two have strong math relationship

Algorithms

- RSA
- El Gamal
- Elliptic curves

can

- encrypt/decrypt
- sign/verify
Example of Public Key Cryptography: RSA

Setup

- Find strong primes p and q.
- Set $n = p * q$
- Pick e co-prime with $(p-1)(q-1)$ (65 is ok)
- and find d so that $(d * e) \mod ((p-1)(q-1)) = 1$

the keys are

- Public: $n$ and $e$
- Private: $d$

and they can do

- encrypt: $c = m^e \mod n$
- decrypt: $m = c^d \mod n$

can also sign/verify

3rd August 2000, LBW2000
Both parties create a key pair

- I give you my public key
- you give me your public key

To send a message to you

- I encrypt it with your public key

To read the received message

- you decrypt with your private key

Public keys can be stored on servers
Let's do business

Well

- the idea looks nice
- could it fit some requirements?
- what are those requirements?

The requirements

- an organisation can have own repository of certificates
- ability to attach properties to public keys
- allow possible recovery of ’forgotten’ keys
- have bigger entities to ’verify’ somehow user keys
Creation of a Certification Authority

In the beginning, the CA was created

- generates public/private key pair
- generates certificate request (attach pub. key and descr. of CA)
- make a certificate out of the certificate request (sign)
- gives that certificate, the root CA certificate to everyone
- keeps private key very private (in a box?)
Client sign-up

Then, clients start to sign up

- user creates own certificate request
- sends over to RA to authorise [optional]
- if RA says ok, sends over to CA
- CA signs the request, thus creating a Certificate
- CA publishes Certificate to a repository
- user can be contacted securely
Open-source Public Key Infrastructure

**Why PKIs?**

To improve Internet Security

- S/MIME
- TLS (a.k.a. SSL)
- IPsec

To provide

- confidentiality
- data integrity
- data-origin authentication
- non-repudiation

3rd August 2000, LBW2000
The history of that X.509

X.509 is

• a specification for certificates
• but demasiado generic (can accommodate all cert needs)

History

• Part of X.500 (directory services)
• X.500 has slow adoption, X.509 continues development
• Passed 3 major revisions, now X.509v3
• Meanwhile, PEM implementation showed deficiencies
• Along the revisions, fields were added
• ISO/IEC/ITU and ANSI X9 standard

3rd August 2000, LBW2000
Still X.509 Certificates were lacking
Formed PKIX Working Group (Oct95)
Specified Internet PKI profile
In detail

- for X.509 v3 PKCs
- for X.509 v2 CRLs

Gone through 11 drafts
Now it’s official, RFC2459

certificate profile

describes what fields to use on X.509 and how
PKIX Definitions

Certificate

- Public Key Certificate
- Attribute Certificate

Authority

- Certification Authority
- Attribute Authority
- and maybe Registration Authority

End Entity
PKIX Definitions (cont’)

Infrastructures

• Public Key Infrastructure (PKI)
• Privilege Management Infrastructure (PMI)

Documents

• Certificate Policy (CP)
• Certification Practice Statement (CPS)
Open-source Public Key Infrastructure

More PKIX

Keep in mind these too

• Management protocols (online interaction with managmt. entities)
• Operational protocols (delivery of certs/crls)
• Certificate Policy and Certification Practice Statement
• Time-stamping and data-certification services
Common Data Security Architecture (CDSA)

CDSA is a

- cross-platform
- interoperable
- extensible

security infrastructure

for an Internet applications environment

Status

- Brought to you by Intel
- Endorsed by the The Open Group
- Open-source implementation by Intel
- ...for win only
- But Bull is doing a Linux implementation!
- To be delivered on 24th August 2000
- all the above are about CDSA 2.0
More on CDSA

Crypto

- Comes in CSPs, Cryptographic Service Provider
- Can use either hardware or software CSP
- an OpenSSL CSP is available!
- hmm, hardware accel. crypto card? Bull sells such a thing

Misc

- Ability for secure net-booting (integrity-wise)
- self-integrity check support
Types of Certificates

Why plural

- Certs need not only bind name and public key

Types

- identity certificates
- attribute certificates
- credential certificates

PKIX does 1 and 2
Implementations #1

pyCA and OpenCA

- set of CGI scripts
- OpenSSL for crypto needs
- run ok on Unix/Unix-like
- support Netscape
- no strict compliance with PKIX
- allow RAD testing/implementation

pyCA at www.pyca.de
OpenCA at www.openca.org
OSCAR

- Open Secure Certificate ARchitecture
- comes from DTSC, Australia
- good support for X.509v3, crypto, PKCS, PKIX
- very good Netscape support
- source code available, but can’t redistribute/sell freely
- should open license, me thinks
Open-source Public Key Infrastructure

**Implementaions #3**

**Mozilla Open Source PKI Projects**

**Provides two libraries**

- NSS, Network Security Services
- PSM, Personal Security Manager

**Comments**

- For integration with Netscape/iPlanet products
- License is MPL or GPL, you choose
- Crypto still in trouble
- Not much PKIX compliance, getting better
- Crypto must get fixed, then go fast
Implementations #4

MISPC or Minimum Interoperability Specifications for PKI Components

- Brought to you by NIST (it’s .gov)
- CD-only distribution (still waiting for it)
- That has source code (excl. crypto)
- Only for Windows
- Has some PKIX support
- No crypto for US, yet
- Part of the FPKI
- Gloomy future, me thinks
Open-source Public Key Infrastructure

**Implementations #5**

Jonah, the reference implementation from IBM

PKIX compliance with

- RFCs 2459, 2510, 2511 and LDAPv2 draft

Comments

- they verified the PKIX docs, found errata, gave feedback
- no crypto for US
- uses CDSA 1.2
- does not compile on linux
- are selling it now
- pulled it back on licensing issues (regarding the CDSA)
- is freeware, me says they changed their mind
Open-source Public Key Infrastructure

Open-source PKI vision

To be

- based on the (evolving) PKIX standards
- used as a open-source reference model for PKIX
- based on CDSA 2.0
- available in server mode implementation
- available in CGI mode implementation (RAD)
- integrated with the MUSCLE project (smartcards)
- used for Single Sign-On (SSO) and PAM
El Fin

We are going to discuss about

- open-source software
- public key cryptography
- PKI functionality

about

- available standards
- open-source PKI implementations

and finally about

- critic on OS PKI design

for more, check out http://ospkibook.sourceforge.net