A federated framework for secure videoconference

Daniel Kouril, Michal Prochazka
Acknowledgement

- This work is funded by
  - CESNET Development Fund
  - Masaryk University
Outline

- Introduction
- PKI - Digital certificate
- OpenVPN
- Secured videoconferencing
- Federated Online CA
- CAT
- Federated framework
- Conclusion
Introduction

- Problems with making applications federation-aware
  - Closed-source applications
  - Prohibited by the licence
  - Sometimes it is not possible
- Today's federations are mainly focused on the web environment
- Most of videoconferencing applications are non-web
- Missing authorization or it is based on the shared password
- Several groups need secure and close collaborative environment
  - people from medical env., secret research, ...
- Users are not IT professionals, do not bother them with security technologies
Digital certificate

- Has defined structure – X.509
- Issued by trusted certification authority
- PKI is not user-friendly but in some cases it is widely used
  - SSL, SSH, HTTPs, ...
- Holds public information:
  - Issuer of the certificate
  - Holder of the certificate
  - Public key of the holder
  - Issue data and expiration date
- Additional information in form of extensions
  - CRL, OSCP responder, Policy, ...
Example of the certificate

Certificate:

Data:

Version: 3 (0x2)
Serial Number: 1119039755 (0x42b3310b)
Signature Algorithm: sha1WithRSAEncryption
Issuer: DC=cz, DC=cesnet-ca, CN=CESNET CA
Validity

Not Before: Aug 29 12:34:16 2007 GMT
Not After: Sep 29 13:04:16 2008 GMT
Subject: DC=cz, DC=cesnet-ca, O=Masaryk University, CN=Daniel Kouril
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
17:87:b1:c8:90:56:2a:1b:3e:cb:0c:8e:eb:ef:fa:
4c:11:6c:c6:cb:9e:3e:04:8c:bd:07:5c:63:0c:2a:
7e:59:01:63:7b:75:bfe:5e:7f
Exponent: 65537 (0x10001)

X509v3 extensions:
X509v3 Key Usage: critical
  Digital Signature, Key Encipherment, Data Encipherment
X509v3 Certificate Policies:
  Policy: 1.3.6.1.4.1.8057.1.2.2.2.0
X509v3 Subject Alternative Name:
  email:kouril@ics.muni.cz
X509v3 CRL Distribution Points:
  DirName:/DC=cz/DC=cesnet-ca/CN=CESNET CA/CN=CRL2
  URI:http://www.cesnet.cz/pki/crl/cn=CESNET%20CA,dc=cesnet-ca,dc=cz.crl

X509v3 Authority Key Identifier:

X509v3 Subject Key Identifier:
OpenVPN

- Creates VPN tunnel on the application level of ISO/OSI
- Creates virtual network adapter on the client
- Firewall and NAT traversal
- Capable of creating bridged or routed tunnels
- Supports IPv6
- Supports Linux, *BSD, Mac OS X, Windows, Solaris
- Primary authentication by the digital certificates
- Variety of approaches for AuthN/AuthZ
  - PAM, scripts, username/password, static key
- Transparent for the applications
### OpenVPN - Latency

**Table 1.** Measured comparison between direct communication and communication through various VPN modes as implemented by OpenVPN.

<table>
<thead>
<tr>
<th></th>
<th>no VPN</th>
<th>UDP VPN</th>
<th>TCP VPN</th>
<th>TCP VPN + HTTP proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>pchar latency [ms]</td>
<td>3.51</td>
<td>3.69</td>
<td>3.94</td>
<td>3.93</td>
</tr>
<tr>
<td>iperf jitter [μs]</td>
<td>6</td>
<td>6</td>
<td>9</td>
<td>13</td>
</tr>
<tr>
<td>pchar capacity est. [Mb/s]</td>
<td>39.8</td>
<td>35.2</td>
<td>20.1</td>
<td>19.8</td>
</tr>
<tr>
<td>iperf packet loss @ 30 Mb/s [%]</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>iperf CPU idle @ 30 Mb/s [%]</td>
<td>48.9±0.2</td>
<td>41.7±0.4</td>
<td>44.5±0.4</td>
<td>42.6±0.4</td>
</tr>
</tbody>
</table>
Secured Collaborative Env.

- User needs digital certificates from the CA
  - Users have problems with acquiring the certificate
  - Need to manage users
- Videoconference uses Mbone tools (VIC, RAT)
  - Can't be used behind the NAT - uses UDP and RTP
- OpenVPN server
  - Assignes public IP but does not route them outside of the tunnel
    - prevent IP collision at the client's network
  - Applications are accessible only through the tunnel
  - Process authN and authZ
- Installation package for the users
Federated Online CA

- Combines RA and CA together
- Clients are authenticated at theirs home institution
- Automated and less administrative work
- We are operating two types of Online CA
  - based on GridShib [http://gridshib.globus.org](http://gridshib.globus.org)
  - based on OpenSSL and Perl scripts
- Issues short and mid lived certificates
- Puts SAML response from IdP into the certificate
Federated Online CA

- CESNET has OnlineCA in pre-production mode
  - Uses HSM
  - Can provide unlimited number of different CAs based on different profiles
  - We are discussing design of API to the Online CA
- SAML Single Sign-on Browser/Artifact Profile
  - Security Analysis of the SAML Single Sign-on Browser/Artifact Profile (Thomas Groß)
Current Status

- Modification to the OpenVPN
  - enhanced authN based on the digital certificates
  - added support for processing SAML extensions
- Functional federated OnlineCA
  - AuthZ is transferred in form of attribute inside the certificate as an extension
  - Private key is not encrypted
    - do not bother us due to short live time of the certificate
    - allows easy integration with the applications
- Installation package for videoconferencing tools
Framework design
CAT

- Common Access Toolkit for Federations
- General framework which allows integrate applications into the federation
  - Secure and authenticated tunnel from application to the server
- One of the main purpose is to make authN/authZ transparent for the user
- GUI tool for managing credentials for users
  - acquiring, translating, deleting, checking validity
Network Identity Manager

http://web.mit.edu/kerberos/
Network Identity Manager
Network Identity Manager

Obtain new credentials

Identity | Kerberos v5 | Kerberos v4 | KCA Certificate | My Cred

<table>
<thead>
<tr>
<th>czTestFed</th>
</tr>
</thead>
<tbody>
<tr>
<td>O federaci : Politika : Kontakty : Nápověda</td>
</tr>
</tbody>
</table>

Zvolte Vaši domovskou organizaci

Přístup ke zdrojů může získat server 'mizar.ics.muni.cz' vyžaduje autentikaci.

METACentrum

Zvolit

Welcome

Získat certifikát

Help

EuroCamp '08 - Stockholm
Federated Framework

- General framework - client software independent
  - Transparent security from appz and user point of view
    - Appz do not need to solve AuthN and AuthZ
  - Minimal requirements on the network configuration
    - only one specific stream which has to be enabled on the firewalls
    - NAT traversal, HTTP proxy support
  - Clients' machines could be managed
Related Work

- Adobe Connect
  - Commercial tool for collaboration
  - Flash based => run inside the browser
  - AuthN/AuthZ only by username/password
  - Ongoing work on make it Shibboleth SP
  - During testing we have discovered some problems
    - missing fine graind access rights
    - interruptions
    - some bugs in UI
Future Work

- Use Stunnel/OpenSSL TLS/DTLS
  - it doesn't require administrative rights
  - allow to make per port tunnels
This is the end ...
Ithanet eInfrastructure

Ithanet is a Euromediterranean network of research centres conducting molecular and clinical research of thalassaemia and related haemoglobinopathies.

- OpenVPN + UDP Packet reflector + MBone tools
- Public IP addresses are assigned inside the tunnel, but they are not routed outside
  - protection against IP collision at the connected institutions
- Client installation package for Win2000/XP
  - easy to install, easy to use (one click to start/stop the conference)
- X.509 based AuthN - OTP used to obtain the certificate