Federated Identity Management at CERNET

Youjun Huang

2015-09-22 ChengDu
1. Roaming access requirements
2. CerID Design
3. Cross-Domain Roaming Authentication
4. Deployment Experience and Lessons
5. CerID User Management Platform
6. Next Work
Full Network Roaming Support User Access System

- A subproject of CNGI-CERNET2 network support projects
- A basic support platform for carrying out IPv6 commercial trial
- Deployed in 100 universities to carry out IPv6/IPv4-based network roaming access
- Implement of access control, mobile roaming, billing and business management for campus networks
Authorized users of the campus network can access the networks of member universities with a unified identity to achieve trusted access, roaming and billing by wired or wireless networks.
Network User Authentication - Roaming Access Requirements

- Fine-grained access control, such as switch port
  - Security Event Tracking
  - Resource Access Control
- Minimizing administrative costs
  - Client: compatibility with different platforms
  - Administrator: software development, distribution, and configuration
- Integration with other applications: SSO
  - Unified user name and password
  - Single login and access multiple applications
- Supporting cross-domain access
  - Applications outside the campus network
  - Roaming authentication among different campus networks
CerID design
Overview of Existing Roaming

- GSM Roaming
  - GSM roaming mechanisms
    - GSM (Global System for Mobile Communications), allowing users to achieve global roaming with a mobile phone
  - GSM roaming policy
    - Zoning
    - Location Identification
    - Assigning a temporary roaming number
Overview of Existing Roaming

- Mobile IP Roaming
  - designed to meet the mobile nodes to maintain their connectivity during moving, and including two versions of IPv4 and IPv6
- Three functional entities
  - MN (Mobile Node)
  - HA (Home Agent)
  - FA (Foreign Agent)
Overview of Existing Roaming

• EDUROAM
  – From the university's wireless network roaming certification program in Europe
  – Promoting wireless network sharing service for the EU education and academic units
  – Built on RADIUS tree structure and proxy function
    • Top—level RADIUS Server
    • National RADIUS Server
    • Institutional RADIUS Server
Requirements of access and roaming of CNGI-CERNET2 trial commercial

- GSM: Complicated distribution mechanism
- Mobile IP: The network must support mobile IP technology
- EDUROAM: No unified central management system
Mechanism of access and roaming

• Different mechanisms of access and roaming for different users:
  – Local campus network user
  – Unified roaming user
  – Other ISP/ICP user
Mechanism of access and roaming

- Central database +AAA
  - CerID Binding: consistency password
  - Certification Request
  - Billing request

- Local Gateway
  - Local authentication
  - Network account

- Remote Gateway
  - Remote authentication
  - Unified CERID

Authentication for local campus network user
Mechanism of access and roaming

Authentication for unified roaming user
Mechanism of access and roaming

Central database +AAA

Billing Request

Any Gateway

Green Channel User → Unified CERID

Local authentication

authentication for other ISP/ICP user
System Design - Guidelines

1. Combination of flexibility and practicality
2. Combination of centralized management and scalability
3. Combination of IPv4 & IPv6
4. Combination of innovation and industrialization

Kernel
Theories
Modules
System Design - Principles

1. REGISTRY/REGISTER(Data centralization/Business distribution)
2. CERID central and local identities
3. Unified central database maintenance, providing ISP/ICP a unified interface
4. Business interacting with the central database only when required (roaming)
### System Design - CERID

CerID: Prefix (type) + Variable-length coding + Suffix (optional extension)

<table>
<thead>
<tr>
<th>类别 (Type)</th>
<th>前缀代表的用户类型</th>
<th>用户标识编码长度</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VIP</td>
<td>7位</td>
</tr>
<tr>
<td>2</td>
<td>机构网用户</td>
<td>11位</td>
</tr>
<tr>
<td>3</td>
<td>移动互联网用户</td>
<td>11位</td>
</tr>
<tr>
<td>4</td>
<td>预</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>中央匿名用户</td>
<td>11位</td>
</tr>
<tr>
<td>6</td>
<td>中央普通用户</td>
<td>11位</td>
</tr>
<tr>
<td>7</td>
<td>预留给中小学用户</td>
<td>13位</td>
</tr>
<tr>
<td>8</td>
<td>本地临时用户</td>
<td>11位</td>
</tr>
<tr>
<td>9</td>
<td>预</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>预</td>
<td></td>
</tr>
</tbody>
</table>
Interaction with the user account of the campus network system – CERID Generation Tool

- Configuration database information
  - Database connection
  - Tables associated with user information
- Query the user list by the conditions
- Generate CERID and password based on user list
- Save CERID user info into file or database
Roaming access control location

- Web-based authentication on export gateway (Allow Out)
  - Intranet freedom, anonymous access
  - Used widely at the enterprise network and campus network
- Port authentication at access switch (Allow In)
  - Port Control
  - Used by some colleges
Interaction with the data link of the campus network system – Green Channel

• Support for the green channel
  • export gateway (Allow Out)
  • access switch (Allow In)
  • support IPv4/IPv6
System characteristics

- Roaming Access Authentication: the advantages of the Web and 802.1X
  - No special client, good compatibility
  - No software development and distribution
  - Realization fine-grained port authentication

- Access authentication and web-based SSO
  - Simplify user operations
  - Simplify user management

- Applications outside the campus network can use the result of the campus network authentication

- Roaming among the different campus networks
Cross-Domain Roaming Authentication
SSO of Web application

Interface provided by authentication server:
User's browser retained a ticket with NAA signature (Cookie)
- MAC
- User ID
- IP Address
- MAC Address
- Campus Name
- ...
- Signature by Web Portal

(10) HTTPS Response (ticket)
**SSO of Web application**

- Web App redirects the requests to Portal, and Portal takes the iTicket as a parameter of the URL and redirects it to App.
Cross-domain SSO

[Diagram showing the relationship between different components such as ASP, ISP1, Transit ISP, Trust Server, ISP2, SW/ AP/ GW, and PC.]
Cross-domain Access of Web applications

- Trust Server (Trust) signing the certificate for the authentication server, providing transit service

PC (browser) → Web portal → Trust Server (CERNET) → Third-party applications (Web application)

- (10) HTTPS Response (ticket)
- http://webApp
- http://webApp? appTicket signed by NAA
- <trustTicket > signed by Trust Server
- <appTicket > signed by Trust Server
Cross-domain Roaming Billing System - Technical realization

- Providing four user connection patterns
- When a user roaming to other CNGI-CERNET2 campus network, taking the local RADIUS server as a proxy, transiting to the home RADIUS server for authentication, and billing locally after authentication
- Each RADIUS server in campus networks required to unified registration to form a AAA platform supporting full-network roaming
- Configuring the Roaming authentication through a unified interface
Cross-domain Roaming Scenarios

- Two scenarios of central users roaming
- Two scenarios of local users roaming
CERID: Campus Network and Unified Login
Deployment Experience and Lessons
Results of System Implementation

- **CERID-based Unified Identity Solutions**
  proposed and designed CERID coding scheme, providing basic services for unified identity and full network roaming, and allowing visitors to access and use the network free among the various units to achieve the wired and wireless credible roaming.

- **Cross-domain full network roaming authentication and billing Solutions**
  proposed and designed a series of roaming management solutions such as cross-domain authentication, roaming billing, accounting, and user management etc.
Experience – External Interfaces

• Radius interface
• SOA interface supporting single user or SAVI server address to connect or disconnect the network
• Reading the network-access records in database to provide users with billing, query, self-service
• Obtaining all the online information of certain user or all users by IP or user’s name
• Querying some information for Network administrator:
  – getOnlineUserByLogin: get online info by user name
  – getOnlineUserByIp: get online info by IP
  – getOnlineList: get all online info
• Providing the interface specification & API Code for web app
• Web-based authentication service interface specifications & API Codes
Lesson – the benefit of the campus network

- SIP Server & Gateway Joint R&D Technology
  - Billing solution based on SIP server and gateway joint
  - How to motivate the campus network to share user account
  - How to motivate the campus network to share data link
CERID User Management Platform
SSO in Baidu

tieba.baidu.com
zhidao.baidu.com
image.baidu.com
v.baidu.com
map.baidu.com
baike.baidu.com
wenku.baidu.com

login

https://passport.baidu.com/v2/api/?login

Parameters in Request

Set-Cookies in Response

BDUSS=J-xlP1UuHCOFZydEc2MV1CcElYQmVtNn1XTThLVNGUHi3RC1VakN05XZPYYjFTQUFQBOF8BJCQAAAAAABAAACB5EB4A2Z3
httponly PTOKEN=73965835fc69b6557fd8451de4a0f8b52; expires=Sun, 13-Feb-2022 08:24:15 GMT; path=/; domain=
httponly STOKEN=01379fe11ff278e6102713bc0623a002; expires=Sun, 13-Feb-2022 08:24:15 GMT; path=/; domain=
httponly SAVEUSERID=deleted; expires=Tue, 27-Nov-2012 08:24:15 GMT; path=/; domain=passport.baidu.com; httponly USERNAME1TYPE=1; expires=Sun, 13-Feb-2022 08:24:15 GMT; path=/; domain=passport.baidu.com;
SSO in Netease

Parameters in Request

- noRedirect: 1
- password: a....c
- product: 163
- saveLogin: 0
- type: 1
- username: lz...@163.com

Set-Cookies in Response

- NTES_SESS=X3L_IrbDv7VBzWPhGu71DZ3uW66bwvXMk5KqiiDYBfFJAZ_WA7Kw6g6VcZYq0
- HttpOnly_S_INFO=1385532681|0|3&100#1385532681
- P_INFO=lzg...@163.com|1385532681|0|113,1126,beijing1385532426,easyread#beijing1385532426,http://www.163.com
- T_INFO=869A853D2F7ED299656622D5EF93FB,FQ,http://www.163.com
- HttpOnly_ANTICSRF=8a2f4adfff5da972e580e793c114091; path=/; domain=1.163.com
SSO in Sina

http://weibo.com/

http://news.sina.com.cn/

http://video.sina.com.cn/

http://finance.sina.com.cn/

http://mail.sina.com.cn/

...
SSO in CERUMP

- 手机教育网
  http://m.edu.cn

- 教育网导航
  http://top.edu.cn

- CERID社交平台
  http://s.id.edu.cn

- 慢速网站反馈系统
  http://e.m.edu.cn/ssfs

- Cerpark微创业乐园
  http://www.cerpark.com:8081
第一届下一代互联网技术创新大赛

主管单位：教育部科技发展中心
主办单位：赛尔网络有限公司
协办单位：CERNET网络中心 《中国教育网络》杂志

时间：2015年9月至12月
Social function
CERID Applications - Real-time Hot Board

one 10G 80 Billion, 1.5P
CERNET Annual Conference Registration

- CERID Registering and Binding
  - Register new CERID
  - Bind existing CERID

- 2015-11 NanChang
CERID User Management Platform

User Register
User Login
Password reset

Integrated applications

- 微创业乐园
- 慢速网站反馈
- 手机教育网
- 教育网导航

http://www.cerpark.com:8081
http://e.m.edu.cn/ssfs/
http://m.edu.cn/
http://top.edu.cn/
Possible integration with the Internet2 system

- Having a unified account, but no single sign-on at some universities
- Single sign-on system in same domain:
  - CAS: Centralized Authentication System
  - Kerberos: Traditional Applications, MS Windows Domain
- Federated SSO: Internet2 SHIB
- eduRoam: RADIUS
Next Work

1. Make central database covering more universities with CERID generation tool
2. CERID deep integration with ICPP, CANS and CERNET Annual Conference
3. Take CERID into DNS, DHCPv6, and build them into virtual machine template of OpenStack
Contact Information

huangyj@cernet.com
Mobile Phone: 13810566737
Office Phone: 010-62603512
Thank you!