Open Gate and Open space LAN in Saga University

Y. Watanabe, H. Eto, M. Otani, K. Watanabe, S. tadaki

Jus symposium 2005 (translated from Japanese)

Open Campus Network

Request
- In open space such as lecture room and lounge
- Public terminals used freely by students
- Network jack used freely by students
- Wireless LAN (spread later)

Realization
- Settle separated open space LAN
- Develop user authentication system
- Opengate

Network user authentication system

- needs
  - Occurrence of intrusion, disturbance, infringement
- Functions
  - Restriction of users
  - Record of usage
- Demand
  - Can be used easily
  - Can be controlled easily
  - Can be applied to various terminals
    - Public terminals for free use, network jack, wireless LAN
    - Windows, MacOS, Linux, ...

History

- 1999.8 Development of scratch version of Opengate
- 2000.6 Field test in the computer center
- 2000.9 Field test in a remote practice room
- 2001.1 Start service in the Library
- 2001.4 Start campus wide service
- 2001.12 Publish a paper
- 2005.4 Publish a paper
- 2005.5 Release Version 1.0, Add to SourceForge

Network user authentication system - Opengate

- Control the firewall on the gateway from a CGI

Basic action: add / delete firewall rules

- Allow from/to 192.168.0.11
- Add at auth from 192.168.0.11
- Delete at disuse

- 10000 allow ip from 192.168.0.11 to any
- 10000 allow ip from any to 192.168.0.11

- 60000 fwd localhost tcp from any to any http
- 65535 deny ip from any to any

Forward web access to local server (if not matched to previous rules)

All packets are denied (if not matched to previous rules)

Matching priority
How to detect disuse

- By TCP connection remained => difficult at mail and web usage
- By some physical detection => difficult at public terminals
- By an agent installed => difficult at user terminals (lots of users, various environments)
- By TCP connection with Java Applet sent to client
  - other methods are combined for terminals without Java

Usage procedure

**Network Authentication**

- You are required to be authenticated before using network.
- Your will be authenticated with your user ID and password for systems in Computer and Network Center (CNC). If you do not know your user ID and/or password, please consult CNC.
- Please enter your user ID and password in the text box, then press [OK]. Please use SSL Authentication as far as possible to prevent wiretapping.

SSL Authentication:

- User ID:
- Password:

Required Usage Duration:
- measured by [h] hour(s). The value is used only when Java applet is not active. Click the [TIMEOUT] link in the second page at the end of usage.

**Action flow**

- Terminal
  - Access to any URL
  - Authentication request page
    - User ID
    - Password
  - Open
  - Network usage
  - End browser
  - End OS
  - Cut off wire
  - Leave it long time

**Network**

- Authentication server
Software structure

Process flow

Process flow (continue)

Elements of Opengate system

Client machine

Open the network (allow to use)
Close the network (deny to use)

- When Java Applet is enabled
  - Exit the web browser or OS (normal user action)
  - Fail the periodic hello exchange (cut off wire)
  - No packets in a long time (left public terminal as is)
- When Java Applet is disabled
  - Time limit passed (user can indicate it in auth page)
  - No packets in a long time (left public terminal as is)
  - Command ‘arp’ reply varied MAC (PC is exchanged)
  - User clicks the link for termination

Gateway

- OS
  - FreeBSD 4.0 or later
- Hardware
  - compatible to above OS, need 2 or more Ether NICs
- Software
  - need
    - Apache, ipfw
  - optional
    - natd, DHCP, SSL, perl

Authentication server

- protocols
  - POP3, POP3S, FTP, RADIUS, PAM
- configuration
  - Describe server information in configuration file
- Selection of server
  - When UserID only [user] is entered in ID field
    => user [user] is authenticated by default server
  - When UserID and serverID [user@serv]
    => user [user] is authenticated by sever [serv]

Example setting of authentication servers

- default: tc=rad
- hg: address=pop.hoge.jp: protocol=pop3s
- lib: protocol=ftp: address=192.168.0.1
- rad: protocol=radius
- pam: protocol=pam

Installation

- Reconstruct kernel including firewall ipfw
- Install related softwares check these
  - Apache, ipfw, natd, DHCP, SSL, perl, ...
- Check set/unset of firewall rules manually
- Configure Apache and ipfw to forward any web pages matching to no priority rules
- Install opengatesvr.cgi and configure
- Set auth server and check the whole action
- Documents and test programs in archive

Syslog output

Aug 30 11:04:26 ce-gate opengatesrv.cgi[526]: OPEN: user user1 from 192.168.0.11 at 12:34:56:78:9a:bc
Aug 30 11:05:48 ce-gate opengatesrv.cgi[533]: CLOS: user user1 from 192.168.0.11 at 12:34:56:78:9a:bc ( 00:01:22 )
Aug 30 11:07:36 ce-gate opengatesrv.cgi[1568]: DENY: auth-err, user xxxx from 192.168.0.11
Aug 30 11:09:21 ce-gate opengatesrv.cgi[55572]: ERR in auth-comm: Ftp server is not normal
Usage status displayed by UNIX command ‘ps’

ps -x | grep opengate

525 ?? I 0:00.24 opengatesrv.cgi:
10000,user1,192.168.0.11

533 ?? I 0:00.01 opengatesrv.cgi:
10002,user2,192.168.0.15

Merits

- Easy to use
  - Auth page is displayed with any URL request
  - Network is closed with browser termination
  - No client program is installed
- Easy to manage
  - only the gateway machine is needed to maintain
  - Compatible to various authentication protocols (pop, pops, ftp, radius, pam)
  - Can be added easily to existing network
- Applicable to various clients
  - Wired/wireless connection, public/mobile terminals, windows/macintosh/linux/freebsd, ...
  - Require Only a web browser (Java preferably)

Open space LAN

Actual connection

Size of our open space LAN

- 22 gateways: one for one or few buildings
- About 110 public terminals
  - Take in existing terminals in library, exercise room, employment bureau, ...
- About 730 Network jacks
  - All lecture rooms(two for each), library, student room, ...
- About 87 wireless access points
  - In or near lecture rooms, library, ...
- About 10,000 users
  - Students, teachers, officers, guests

Stacked authentication gateways
Servers and wiring

- Computer center
- Boot server
- Auth server
- Log server
- Gateway
- VLAN
- Backbone LAN
- Each building
- Open space LAN
- Normal LAN

Diskless boot

- Diskless machine
- Boot server
- NIC
- DHCP server
- Get boot info
- PXEBOOT
- TFTP server
- Get kernel
- Mount root partition

Wireless access points

Lecture room

Passage way

Hall
Operation

- For user belonging to our university
  - Use with ID of computer center
  - No application form for usage
  - No guidance without general computer literacy

- For user visiting to our university
  - Library guest, conference, short stay staff, et al.
  - Prepare authentication server for guest
  - Prepare application form including preprinted ID and password
  - If applied, allow to use network in some period, but not to login to internal servers
Change of user count

User count on each gateway

Histogram of connecting period

Present state and performance

Techniques employed in daily management

Causes of troubles
Costs

- money
  - One PC for every subnet
  - Distribute network wire and/or wireless access points
- Man power
  - At starting: Install FreeBSD+Firewall, Apache, DHCP, CGI etc.
  - At daily: No operation when no trouble
    - Server is stopped: reboot server, or connect wire to other server and examine the server without hurry
    - Finding wrong usage: checking logs
    - Found security hole in system software: need to reconstruct the system when serious
  - Maintenance of user authentication data properly
    - very troublesome job => Need to use existing data

Our developments related

- Key logger in a public terminal
  - Authentication at booting with Opengate
- Easier interface
  - Opengate client program by Java
- Compatible to IPv6
  - Want to open IPv4 and IPv6 at once
  - Develop Opengate compatible to IPv6
- Examine other environment for development
  - Opengate on Java Servlet

Open source

- Open to public with GNU Public License
  - http://www.cc.saga-u.ac.jp/opengate
  - http://sourceforge.net/projects/opengateproject

Images of development sites

- Open Source Technology Center
  - http://www.cc.hit-u.ac.jp/opengate

Other techniques employed elsewhere

- Switching of VLAN => Need many switches
- Usage of VPN => Low performance, limited clients
- Registering MAC => Need client data maintenance
- Hold SSH connection at usage => Difficult to use
- Checking by HTTP REFRESH => Closing delay
- IEEE802.1X => Limited clients
- Various appliances => Cost, flexibility

Reference link sites

- Practice of open access floor (tentative name) - Nagoya Univ. (in Japanese)
  - http://www.cc.hit-u.ac.jp/monban/ref.html
- PortalSoftware - Personal Telco
  - http://wiki.personaltelco.net/index.cgi/PortalSoftware