Opengate 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

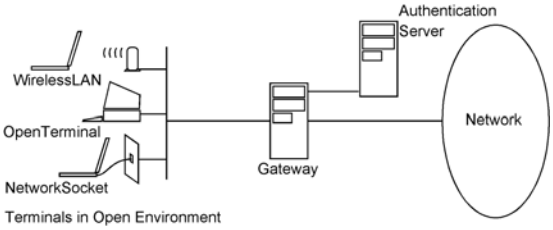
- needs
  - Occurrence of intrusion, disturbance, infringement
- Functions
  - Restriction of users
  - Record of usage
- Demand
  - Can be used easily
  - Can be controlled easily
  - Can be applied to various terminals
    - Public terminals for free use, network jack, wireless LAN
    - Windows,MacOS,Linux,...

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
  IPSJ Journal, Vol.42, No.12, pp.2802-2809(2001) (In Japanese)
- 2005.4 Publish a paper
  IPSJ Journal, Vol.46, No.4, pp.922-929(2005) (In Japanese)
- 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

.....
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

Allow from/to 192.168.0.11

Add at auth from 192.168.0.11
Delete at disuse

matching priority

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

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

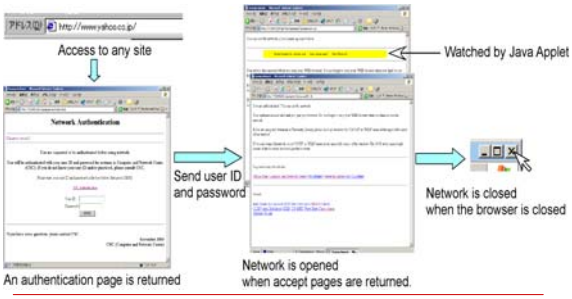
How to detect disuse

- 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)

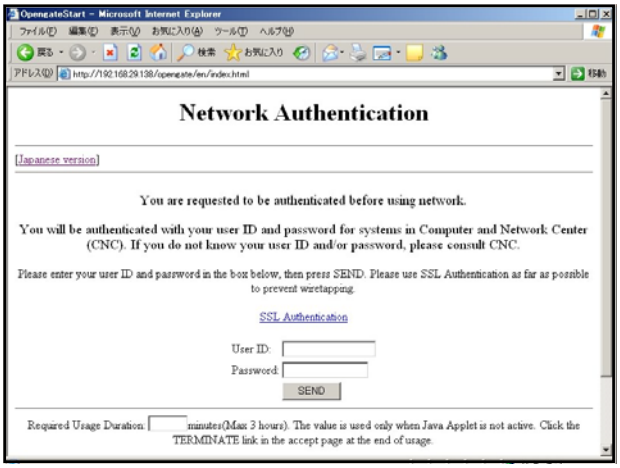
- By TCP connection with Java Applet sent to client
  - other methods are combined for terminals without Java

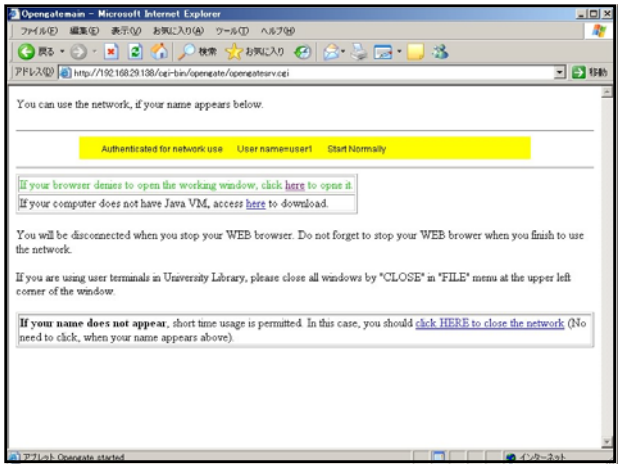
7

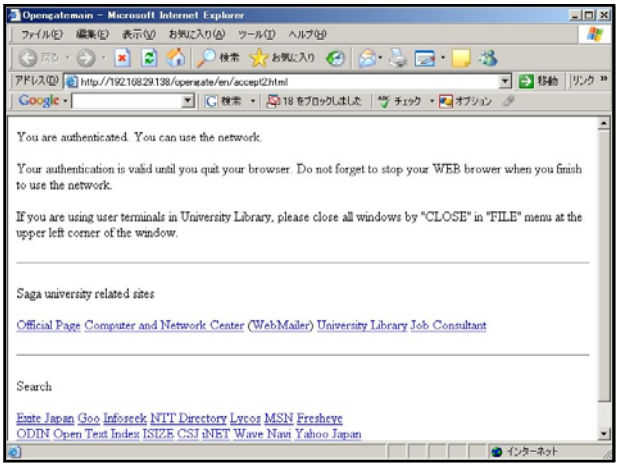
Usage procedure



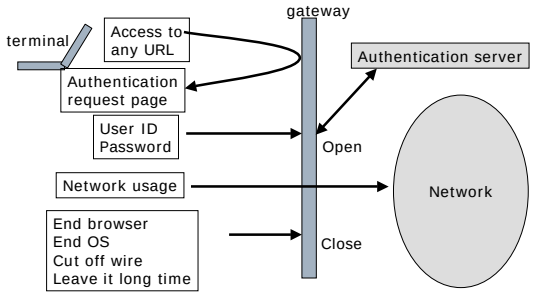
8





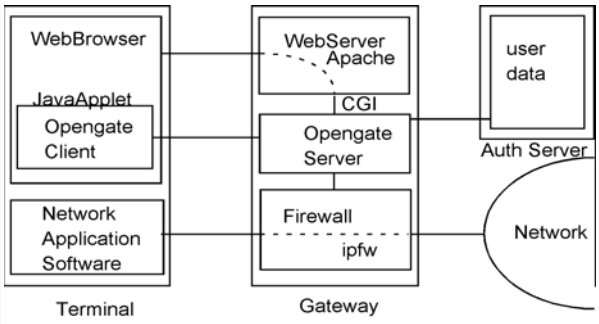


Action flow

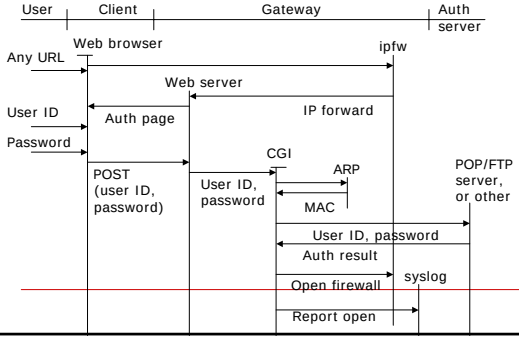


12

Software structure

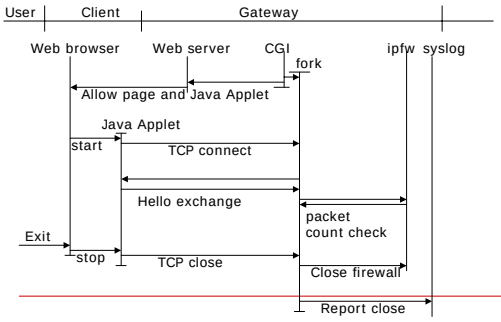


Process flow



14

Process flow (continue)



15

Elements of Opengate system

- Client machine
  - Used by user. Preferable to run Java Applet
- Gateway
  - Control the communication. CGI program, firewall and web server are run.
- Authentication server
  - Hold user information and reply to auth request
- Log server
  - Receive the usage log via syslog and record it

16

Client machine

- Need Web browser. Preferable to run Java Applet
- Need to use TCP/IP
- Need no address translation between gateway and client
- Applicable to wired and wireless LAN.
- Applicable to mobile PCs and public terminals
- Applicable to Windows, MacOS, Linux, FreeBSD, …

17

Open the network (allow to use)

- At entering right ID and password
- In default, all packets to/from the client address are allowed
- By using higher priority rules, can allow/deny specific packets
- By editing Perl script, can control more specific cases

18

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

19

Gateway

- OS
  - FreeBSD4.0 or later
- Hardware
  - compatible to above OS, need 2 or more Ether NICs
- Software(need)
  - Apache、ipfw
- Software (optional)
  - natd、DHCP、SSL、perl

20

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]

21

Example setting of authentication servers

When [user1] is entered in ID field

```
default:tc=rad

hg:address=pop.hoge.jp:protocol=pop3s
```

When [user1@lib] is entered in ID field

```
lib:protocol=ftp:address=192.168.0.1

rad:protocol=radius

pam:protocol=pam
```

22

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

23

Syslog output

Aug 30 11:04:26 ce-gate opengatesrv.cgi[526]:
Open 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]:
Close CLOS: user user1 from 192.168.0.11 at 12:34:56:78:9a:bc (00:01:22)

MAC address　User ID　period　IP address

Aug 30 11:07:36 ce-gate opengatesrv.cgi[1568]:
Deny DENY: auth-err, user xxxx from 192.168.0.11

Aug 30 11:09:21 ce-gate opengatesrv.cgi[55572]:
Error ERR in auth-comm: Ftp server is not normal 4

24

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
```

Firewall rule number | User ID | IP address

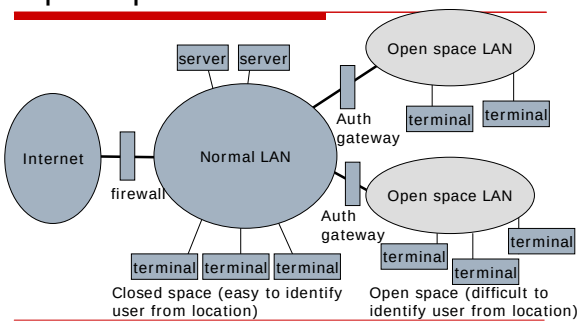
25

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)

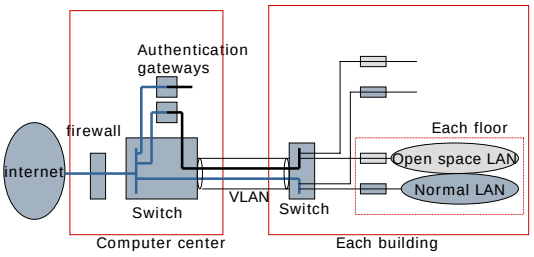
26

Open space LAN



27

Actual connection



28

Size of our open space LAN

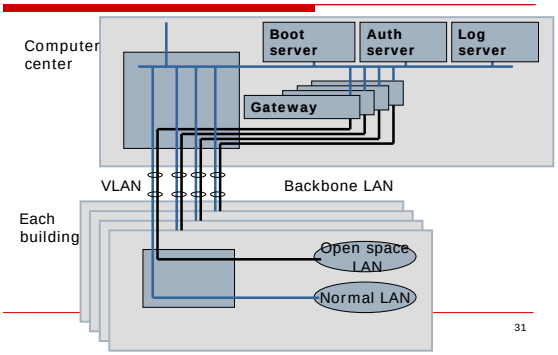
- 22 gateways: one for one or few buildings
- About 110 public terminals
  - Take in existing terminals in library, exercise room, employment bureau, ...
- About 730 Network jacks
  - All lecture rooms(two for each), library, student room, ...
- About 87 wireless access points
  - In or near lecture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

29

Stacked authentication gateways

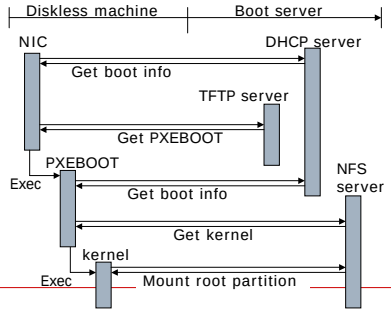
30

Servers and wiring



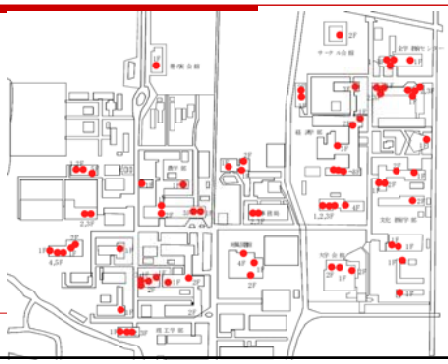
31

Diskless boot



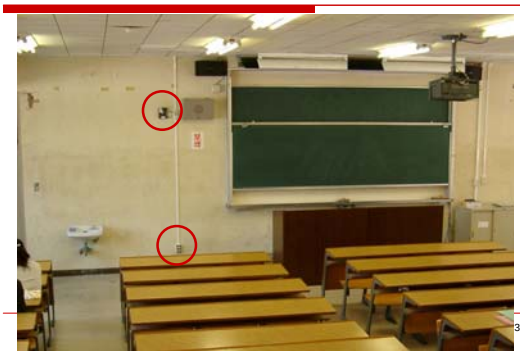
32

Wireless access points



33

Lecture room



34

Passage way

35

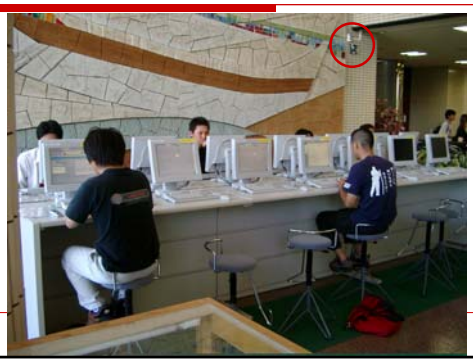
Hall

36

Library

37

library



38

library

39

Employment bureau

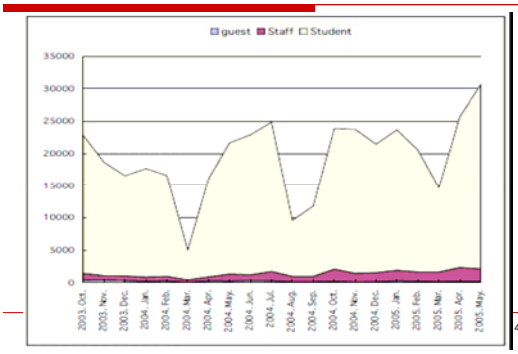
40

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

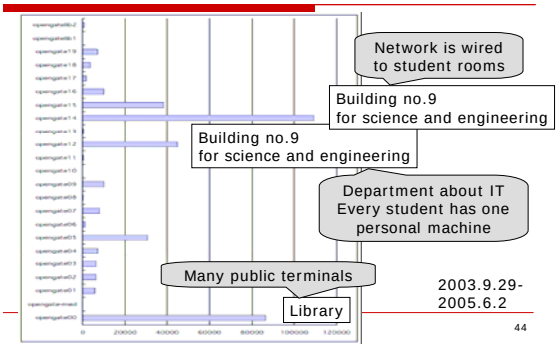
41

Change of user count



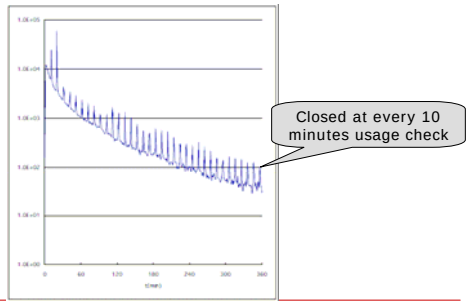
43

User count on each gateway



44

Histogram of connecting period



45

Present state and performance

- Present state
  - Usage is centered to gateways connecting to public terminals, student rooms, and note PCs
  - First half of 2004:140,000 connections, 6,000 users (Our university has 10,000 men)
  - Favorable comments on visitor's service
- performance
  - Gateway macchine: PemtiumIII 1GHz, 512MB memory, No HDD
  - Usage in programming exercise with 100 note PCs
  - DVTS video 40Mb,3hours
  - Stopped by NAT overflow with virus

46

Techniques employed in daily management

- Small remote sections are included into the LAN
  - Many students visit and want to use network
  - No power for network administration
  - No authentication request for staffs by firewall rules
- Countermeasure to virus
  - Virus infecting ports are closed using firewall
- At trouble of gateway machine
  - The subnet is led to other gateway machine
- To limit usage easier or harder temporally
  - Executed by manual firewall setting
- To exchange a group to open space LAN
  - The lines are connected to assignment port in switch
- To know risky usage
  - Gateway logs are investigated

47

Causes of troubles

- Client PC = majority
  - Miss setting of network(remain setting at home)
  - Hardware malfunction
  - Java is not installed (limited usage)
- Network devices
  - Hardware malfunctions of switches and antennas
- Server machine = minority
  - DHCP server is stopped
  - NAT processing is overflowed by virus packets
  - Hardware malfunction

48

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

49

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

50

Open source

- Open to public with GNU Public License

  http://www.cc.saga-u.ac.jp/opengate

  http://sourceforge.net/
  projects/opengateproject

51

Images of development sites

52

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

53

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

54