

# AI<sup>3</sup> Operation

---

SOI-ASIA OW 2002  
Achmad Husni Thamrin



# Agenda

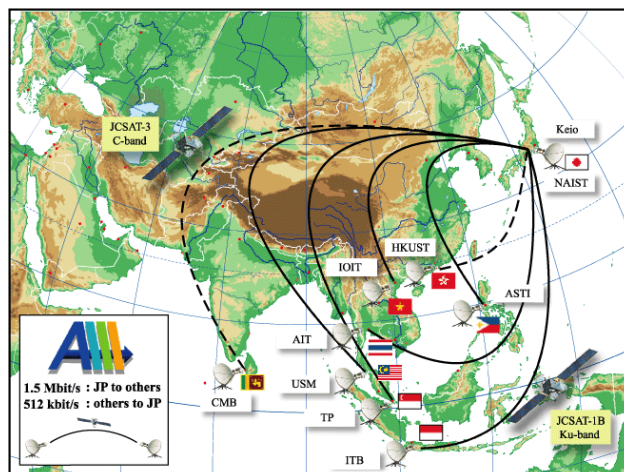
---

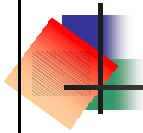
- AI<sup>3</sup> Overview
- Internet Operation (Security)
- AI<sup>3</sup> Secure Network Operation

## About AI<sup>3</sup>

- Asian Internet Interconnection Initiatives Project
- <http://www.ai3.net/>
- Internet satellite network test bed
- Doing research and operation
- Partners in several countries -- including your institution

## Testbed Map (before SOI-ASIA)

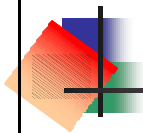




## SOI-ASIA and AI<sup>3</sup>

---

- SOI-ASIA is a partner of AI<sup>3</sup>
- AI<sup>3</sup> serves the infrastructure for SOI-ASIA
  - Satellite bandwidth
  - IP Address space
  - Internet connectivity (using UniDirectional Link Routing)

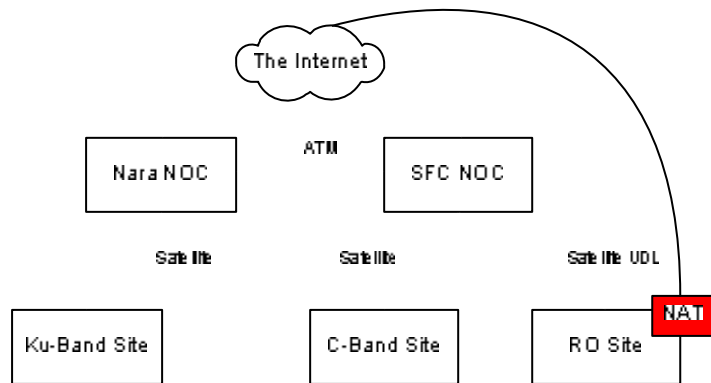


## AI<sup>3</sup> Network (Internal View)

---

- Generally we say
  - SFC NOC
  - Nara NOC
  - Ku-Band site
  - C-band site
  - UDL/RO site

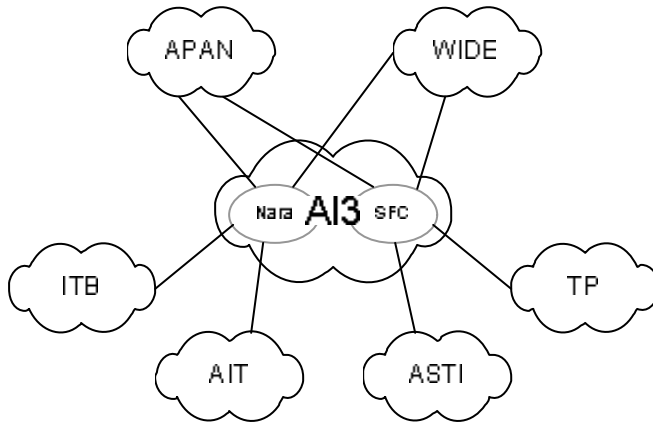
## AI<sup>3</sup> Network Configuration



## AI<sup>3</sup> Network (External View)

- The Internet is an interconnection of Autonomous Systems (AS)
  - Each AS has its own (routing) policy
  - Each AS is identified by AS number
- Directly connected ASes are called Peers
- AI<sup>3</sup> is AS4717

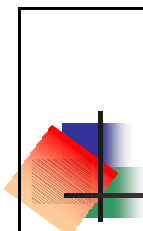
## AI<sup>3</sup> Network (External View) 2



## AI<sup>3</sup> Network Address

- IP address space
  - 202.249.24.0 - 202.249.26.127
- Allocated by JPNIC
- Administrative Contact
  - Prof. Suguru Yamaguchi (Director General)

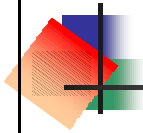
```
%whois -h whois.apnic.net 202.249.24.0
```



## Internet Operation

---

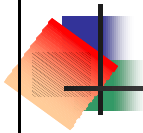
- Non-security (technical) Problems
  - Setup, upgrade, and configure
  - H/W failure and replacement
- Security Problems



## Security Problems

---

- Illegal Access
  - Other people log into your host without your permission
- Denial of Service Attack
  - Attempt to paralyze your hosts (servers) or links
- Fraud
  - E-commerce



## Who are The Culprits

---

- Outsiders
  - Launching attacks to your network
  - Fraud
- Insiders
  - Launching attacks to your network or somewhere in the Internet
  - Fraud



## Who are The Victims

---

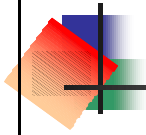
- The victims are You – the operators, and Your Organizations
  - I am just like you – we are operators
- By Outsiders:
  - You loss your connectivity/data/etc.
- By Insiders:
  - You receive claims from somebody



## A Worst Case Example

---

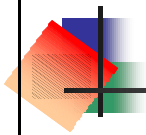
- Somebody broke into your hosts then launched attacks using them
- You received claims for something that you (someone in your organization) did not do
- Who's to blame? You? The Culprits?



## What To Do

---

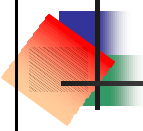
- Secure Your Networks
  - From outsiders
  - From (naughty) insiders



## Network Security

---

- Negative Deliverables
  - You can't know whether your network is secure or not
  - When you had a break in, then you know that your network is insecure.

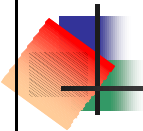


## Be Informed in Security Issues

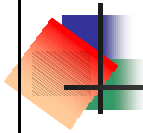
---

- You should be an informed operators
- Being informed -> more secured network
- You can find good sites providing the latest security issues and how to fix them

[http://www.cert.org/nav/index\\_red.html](http://www.cert.org/nav/index_red.html)



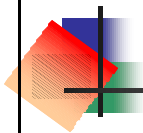
---



## AI<sup>3</sup> Secure Network Operation

---

- We had our incidents
- We always make efforts to have our network secure
- We expect no less from you for your network



## Security Policy

---

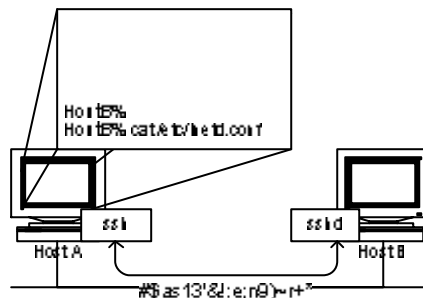
- Always use SSH
  - RSA authentication, not password
- Never run unnecessary services
- Never use NAT for web access
  - Web clients always use proxy (Squid)
- Always update hosts with the latest known bug-free software

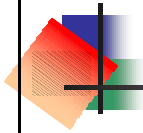
## Two “must do” points

- Always install SSH
- Disable everything that you will not use
  - Edit `inetd.conf` and `rc.conf`

## SSH: Secure Shell

- SSH gives you a secure remote shell using encryption
- Illustration: admin doing ssh from host A to host B

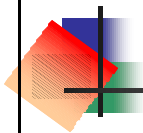




## SSH Authentication

---

- Password
- RSA
- Challenge-Response (One time password)
- Kerberos
- rhost



## RSA Authentication

---

- Using a public/private key pair
- You create a public/private key pair
- Put your public key in servers that you want to connect to
- Keep your private key in your host
  - Safeguard your private key
- To connect to a server, you input your private key's passphrase



## Practice

---

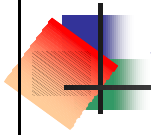
- SSH using password
  - create an account for your left neighbor
- SSH using RSA
  - create key pair
  - put to authorized\_keys
  - connect
  - change pass phrase



## SSH Using Password

---

- Create an account for your left neighbor  
**#adduser**
- Try to login using your new account  
**%ssh -l <your\_acc>**  
**<neighbor\_host>**
  - You will be asked to input password



## SSH Using RSA (1)

- Create a key pair
  - In your local host as your account (not root)
  - Input your passphrase
    - There is no way to recover lost passphrase, create new key pair



## ssh-keygen -t rsa

```
> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/testssh/.ssh/id_rsa):
Created directory '/home/testssh/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/testssh/.ssh/id_rsa
Your public key has been saved in /home/testssh/.ssh/id_rsa.pub
The key fingerprint is:
58:62:ee:f7:33:05:14:3c:74:38:ed:61:7a:a2:1e:0b testssh@
>
>
```



## SSH Using RSA (2)

---

- See your private and public keys
  - .ssh/id\_rsa
  - .ssh/id\_rsa.pub
- Safeguard your private key
- Put your public key to your account on neighbor's host



## SSH Using RSA (3)

---

- On your neighbor's host
  - Create directory .ssh  
`%mkdir .ssh`
- On your local host
  - Copy your public key to neighbor's host  
`%scp .ssh/id_rsa.pub  
<your_acc>@<neighbor_host>:.ssh/  
id_rsa.pub`



## SSH Using RSA (4)

---

- On your neighbor's host
  - Add your public key to the authorized keys

```
%cat .ssh/id_rsa.pub  
>> .ssh/authorized_keys
```



## SSH Using RSA (5)

---

- On your local host as root
  - SSHD configuration
    - Enable RSA authentication
    - Disable password authentication
    - /etc/ssh/sshd\_config

```
RSAAuthentication yes  
PasswordAuthentication no  
PubkeyAuthentication yes
```
  - Reconfig your SSHD

```
# ps -xa|grep "/usr/sbin/sshd"  
#kill -HUP <sshd PID>
```



## SSH Using RSA (6)

---

- Try login to your neighbor's host  
`%ssh -2 -1 <your_acc.>`  
`<neighbor_host>`
- Now you are asked for passphrase



## Authentication: Password vs RSA

---

- Password
  - Everyone who knows your password can use your account
- RSA
  - Everyone who has your private key and knows your passphrase for that key can use your account
- RSA auth. is better than password auth.

## NAT:

# Network Address Translation

---

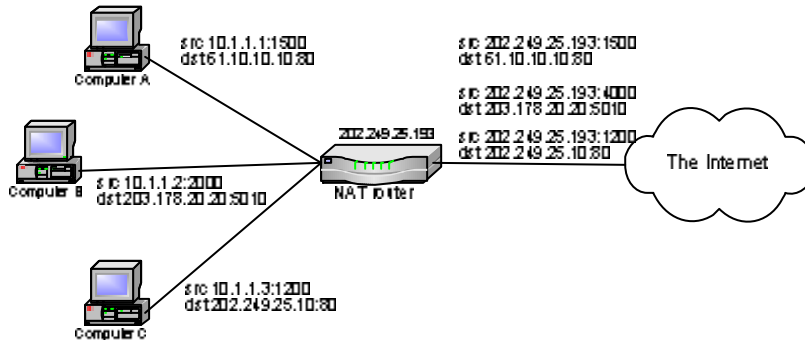
- You use NAT from private network to connect to the Internet
  - 10/8
  - 172.16/12
  - 192.168/16
- NAT translates your private IP addresses to (a) global IP address(es) and vice versa

## Why You Need NAT

---

- You don't have enough global IP addresses for your network
  - The usual reason
- You want to hide your network from the outside
  - You can use firewall

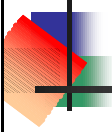
# How NAT Works



# NATD Limitations

- No Log File
- We can't see who accesses what at a particular time
- Log file is important for tracing
  - If an insider launched attacks/committed frauds





# Questions, Please

---

husni@ai3.net