

# Securing Your Network

SOI-ASIA Operators Workshop 2004

## Objective

- Get the basic skills to secure your networks
- Know the AI<sup>3</sup> security policy

## Network Security

- Preventing and detecting unauthorized use of your computers and networks
- Why you have to care for network security
  - protect your data
  - prevent your network to be used as a source of attacks
- What you can do
  - secure your hosts and networks
  - keep up to date to the latest security threats

## Securing Your Hosts

- Account security
- Network servers
- Firewall
- Secure shell

## Account Security

- No group and shared accounts
  - An account should correspond to only one person
- “Good” password
  - Mix alphanumeric + sign characters
- Password ageing
- Limit who can access to root
  - wheel group + sudo access
- Do not log on as root
  - Log on as your account, then su to root
- Never leave idle console

## Network Servers

- Disable unnecessary network servers
- Make sure that the network servers do not have vulnerabilities
  - keep up to date

## Lab Work Ex. 1 Ex. 2

## Firewall

- Block packets
- Rule based: protocol, source & destination address & port, other flags
- First match
- Example:  
0500 allow tcp from 10.0.0.0/8 to 10.1.1.1 80  
0600 deny tcp from any to 10.1.1.1 80

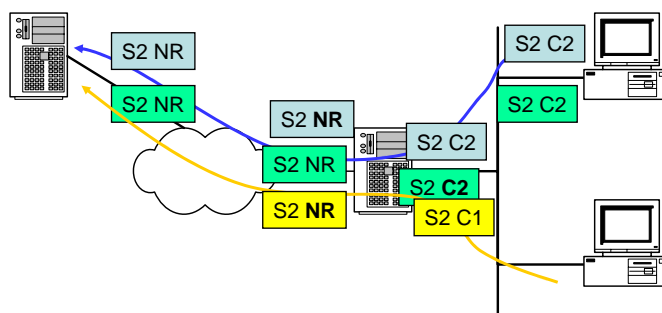
## Lab Work Ex. 3

### Secure Shell

- A secure way for remote access
- Default remote access method
- More security by limiting access only from certain hosts
  - use firewall
- But, sometimes a vulnerability is found
  - patch ASAP!!

## Lab Work Ex. 4

### Network Address Translation



## NAT is Dangerous

- Masquerade source address
- No log file
- If an attack is launched from behind NAT, difficult to track the culprit

## AI<sup>3</sup> Security Policy

- Refuse anything except the ones defined
- Use firewall on border routers
- Share security info via [ai3-ix@ai3.net](mailto:ai3-ix@ai3.net)
- Run port scan and SSH version check regularly
- PC hosts must use SSH only
- Zebra beasts can be accessed from localhost only
- Limit access via NAT only to authorized clients
- Avoid NAT for web access, use Squid