

Security Workshop

2 - 4 July 2008, Port Vila, Vanuatu

In conjunction with PACNOG 4

APNIC Training


Presenters


- Cecil Goldstein
– <Cecil@apnic.net>
- Champika Wijayatunga
– <champika@apnic.net>

Network security fundamentals

Part I

Acknowledgements


- The content of this module is based on material provided by Merike Kaeo from Double Shot Security and the author of “Designing Network Security”.
- (merike@doubleshotsecurity.com), (<http://doubleshotsecurity.com>) and 
- **APNIC acknowledges her contribution and support with appreciation and thanks**
- Some material is also sourced from lecture material from the QUT Internetworking course (ITB524)



APNIC
Asia Pacific Network Information Centre

Objectives

- Provide information about basic security requirements for ISPs and NSPs
- Provide best practise guidelines to achieve device security



APNIC
Asia Pacific Network Information Centre

Assumptions

- Attendees are ISP/NSP network engineers
- Attendees have a role, commitment to network security

Security for an ISP

- An enterprise network security is relatively simpler comparing to an ISP's
 - Main objective: protecting the enterprise's network from outside intrusions
- An ISP's security concerns are much broader
 - Security measures will affect ISP's network operation
 - But security threats are real and need to be protected against
 - ISPs are very visible targets for malicious and criminal attacks
 - Must protect themselves
 - Must help to protect their customers
 - Must minimise the risk of their customers from becoming problems to others on the Internet

Reference: Cisco ISP Essentials, 2001 P49

Security for an ISP

- No network is ever fully secure or protected
- There is always a RISK factor
- ISPs need to know how to use tools to **build resistance**
 - Resist attacks and intrusion attempts to their network
 - Resist long enough for internal security procedures to be activated to track the incident and apply counters

Reference: Cisco ISP Essentials, 2001 P50

First of all...

- Introduction to security issues
 - Terms and definitions
 - Security goals and services
- Risk analysis and quantification

Basic terms and definitions

- Threat
- Vulnerability
- Risk
- Non-repudiation
- Authentication
- Data origin authentication
- Authorisation
- Integrity
- Confidentiality
- Audit

Threat

- Any circumstance or event with the potential to cause harm to a networked system
 - Denial of service
 - Attacks make computer resources (e.g., bandwidth, disk space, or CPU time) unavailable to its intended users
 - Unauthorised access
 - Access without of permission issued by a rightful owner of devices or networks
 - Impersonation
 - Identity theft
 - Worms
 - Viruses

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
 - Software bugs
 - Configuration mistakes
 - Network design flaw

Risk

- The possibility that a particular vulnerability will be exploited
 - Risk analysis: the process of identifying:
 - security risks
 - determining their impact
 - and identifying areas require protection

Risk management vs. cost of security

- Risk mitigation
 - The process of selecting appropriate controls to reduce risk to an acceptable level
- The level of acceptable risk
 - Determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy
- Assess the cost of certain losses and do not spend more to protect something than it is actually worth

Attack sources

- Active vs. passive
 - Active = Writing data to the network
 - Common to disguise one's address and conceal the identity of the traffic sender
 - Passive = Reading data on the network
 - Purpose = breach of confidentiality
 - Attackers gain control of a host in the communication path between two victim machines
 - Attackers has compromised the routing infrastructure to arrange the traffic pass through a compromised machine

Attack sources

- On-path vs. Off-path
 - On-path routers (transmitting datagrams) can read, modify, or remove any datagram transmitted along the path
 - Off-path hosts can transmit datagrams that appear to come from any hosts but cannot necessarily receive datagrams intended for other hosts
 - If attackers want to receive data, they have to put themselves on-path
 - How easy is it to subvert network topology?
 - It is not easy thing to do but, it is not impossible
- Insider or outsider
 - What is definition of perimeter/border?
- Deliberate attack vs. unintentional event
 - Configuration errors and software bugs are as harmful as a deliberate malicious network attack

What are security goals?

- Controlling data / network access
- Preventing intrusions
- Responding to incidences
- Ensuring network availability
- Protecting information in transit

Security services

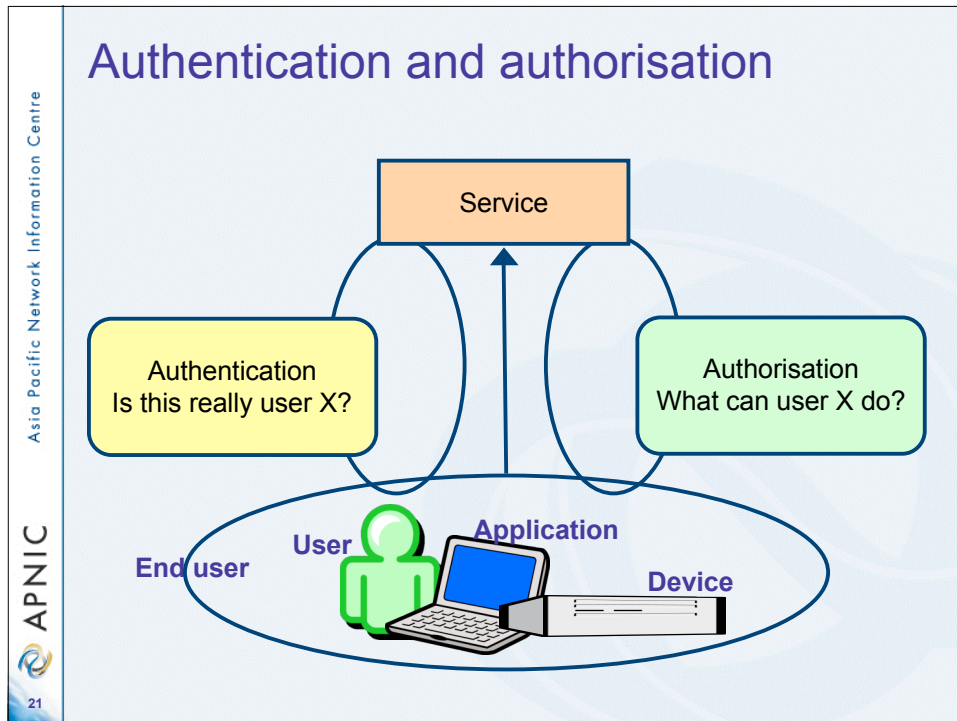
- Authentication
- Authorisation
- Access control
- Data integrity
- Data confidentiality
- Auditing / logging
- DoS mitigation

Authentication

- The process of validating the claimed identity of an end user or a device such as a host, server, switch, router, etc.
- Must be careful whether a technology is using:
 - User authentication
 - Device authentication
 - Application authentication

Authorisation

- The act of granting access rights to a user, groups of users, system, or program
 - Typically this is done in conjunction with authentication



Asia Pacific Network Information Centre

APNIC

22

Non-repudiation

- A property of a cryptographic system that prevents a sender from denying later that he or she sent a message or performed a certain action

Integrity

- Assurance that the data has not been altered except by the people who are explicitly intended to modify it

Confidentiality

- Assurance that data is not read or accessed by unauthorised persons

Availability

- A state in computing systems and networks in which the system is operable and can run services it is supposed to offer

Audit

- A chronological record of system activities that is sufficient to enable the reconstruction and examination of a given sequence of events

Encryption

- Cryptography
- Ciphers
 - Symmetric
 - Asymmetric
- Hash functions
- Digital signatures
- Applications
- Key management

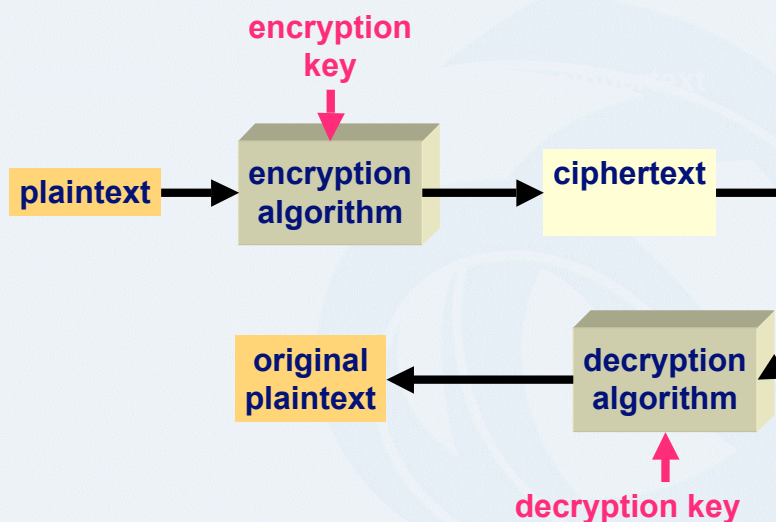
What is cryptography?

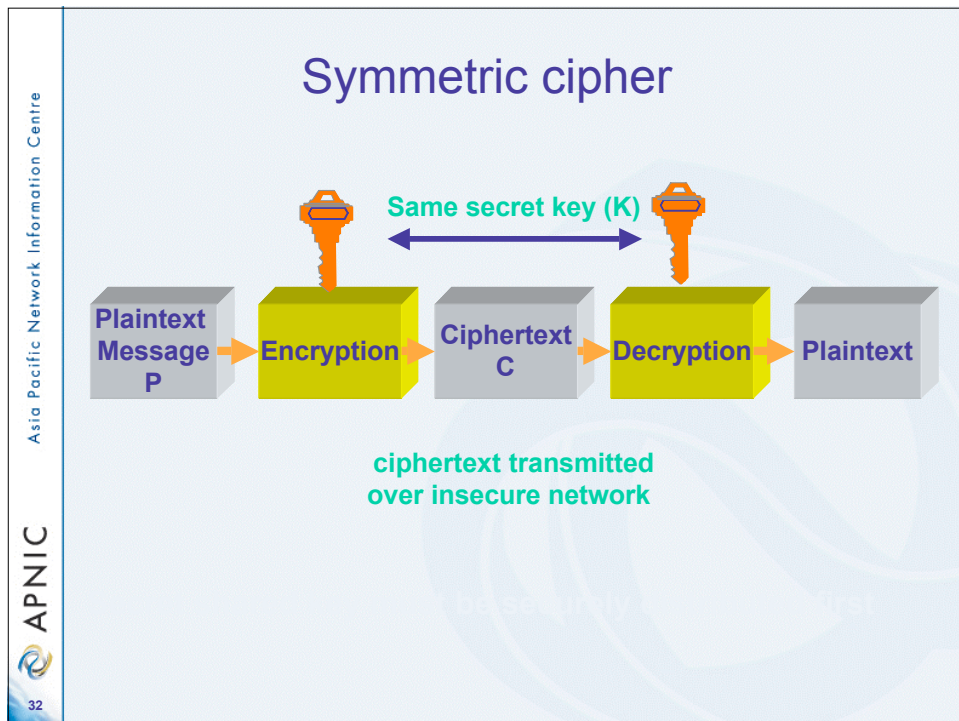
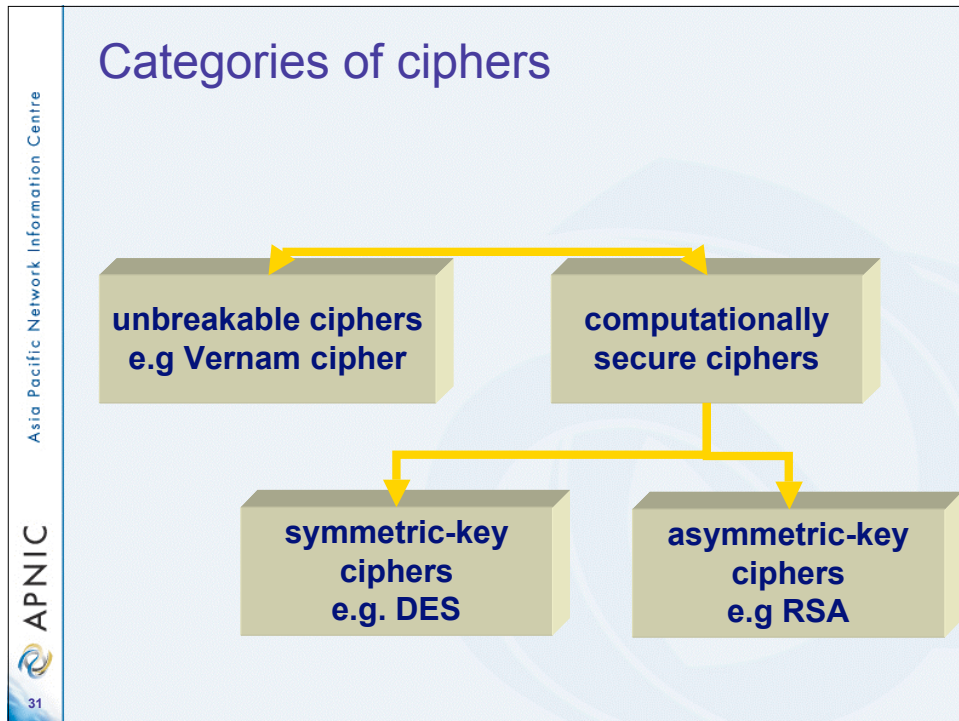
- Part of field of study known as **cryptology**
- Cryptology includes:
 - **Cryptography**
 - study of methods for secret writing
 - transforming messages into unintelligible form
 - recovering messages using some secret knowledge (key)
 - **Cryptanalysis**:
 - analysis of cryptographic systems, inputs and outputs
 - to derive confidential information

Terminology of cryptography

- **Cipher**
 - cryptographic technique (algorithm) applying a secret transformation to messages
- **Plaintext / cleartext**
 - original message or data
- **Encryption**
 - transforming plaintext, using a secret key, so meaning is concealed
- **Ciphertext**
 - Unintelligible encrypted plaintext
- **Decryption**
 - transforming ciphertext back into original plaintext
- **Cryptographic key**
 - secret knowledge used by cipher to encrypt or decrypt message

Cryptographic system



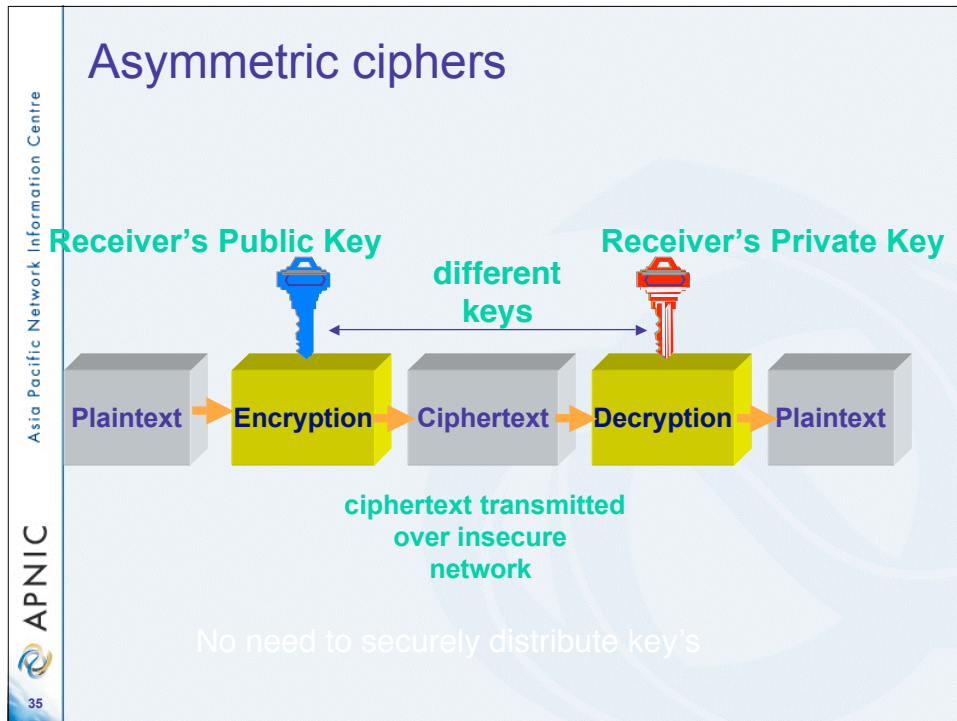


Symmetric ciphers

- Two categories:
 - Stream ciphers:
 - data is encrypted one bit at a time
 - Uses a keystream generator to produce pseudorandom key
 - Fast
 - No current standard
 - Eg RC4
 - Block ciphers:
 - Data is encrypted in blocks
 - EG DES has block size of 64 bits
 - Current standard: AES (Advanced Encryption Standard)

Asymmetric ciphers

- Two different keys (key pair):
 - A message encrypted with one key is decrypted using the other key
 - two keys are related
 - but it is *computationally infeasible* to derive one key from the other
- Each participant requires a pair of keys
 - encryption key K_{pub} (made public)
 - decryption key K_{priv} (kept private)
- Also known as public key cryptography
- Security depends on
 - algorithm strength
 - key size
 - protection measures of private key K_{priv}



Asia Pacific Network Information Centre

Asymmetric ciphers

- Everyone knows the public key
 - no need for secure means of public key distribution
- For **confidentiality**, anyone can encrypt a message for Alice using her **public** key K_{pub}
 - Encryption: $C = E(P, K_{pub})$
 - Only Alice knows her private key
 - so only Alice can decrypt encrypted message
 - Decryption: $P = D(C, K_{priv})$

C=ciphertext, E=encrypt, P=plaintext,
K=key, D=decrypt

APNIC 36

Asymmetric ciphers

- Role of public and private keys can be reversed for **authentication** and **non-repudiation**:
 - Alice encrypts a message using her private key, K_{priv}
 - Encryption: $C = E(P, K_{\text{priv}})$
 - Everyone knows Alice's corresponding public key, K_{pub}
 - Decryption: $P = D(C, K_{\text{pub}})$
 - Successful decryption means message must have been encrypted using Alice's private key

Example asymmetric cipher

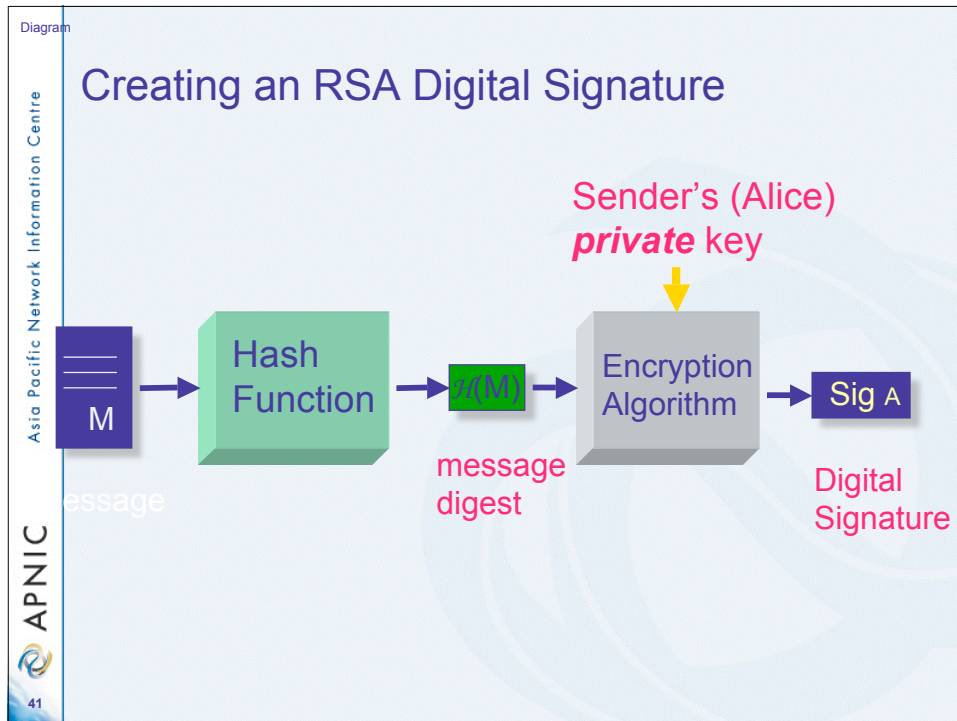
- *RSA algorithm* (1977)
 - Currently most widely used public key cryptosystem
 - Named after designers:
 - Rivest, Shamir, and Adleman
 - Based on difficulty of factoring large integers
 - Encryption and decryption involve exponentiation mod n
 - performed one data block at a time

Asymmetric ciphers

- Advantages:
 - Simple key exchange/distribution
 - public keys are not secret
 - so they don't need to be distributed over a secure channel
 - Any user need only have a single key pair
 - Rather than sharing a different key with every other user
 - Fewer keys needed – more scalable
- Disadvantages:
 - Complexity of operations greater than in symmetric ciphers
 - Longer keys required for equivalent security (*previous slide*)
 - Speed
 - Encryption/decryption is computationally intensive
 - so much slower than symmetric ciphers
 - Association between an entity and his public key must be verified
 - Trusted Certification Authority (CA) required
 - Digital certificates

Digital signature

- Used to provide:
 - Authentication
 - Integrity
 - Non-repudiation
- Uses public-key encryption
- Normal to sign a hash (condensed version) of document rather than signing whole document
 - For efficiency reasons
 - Particularly if messages are long

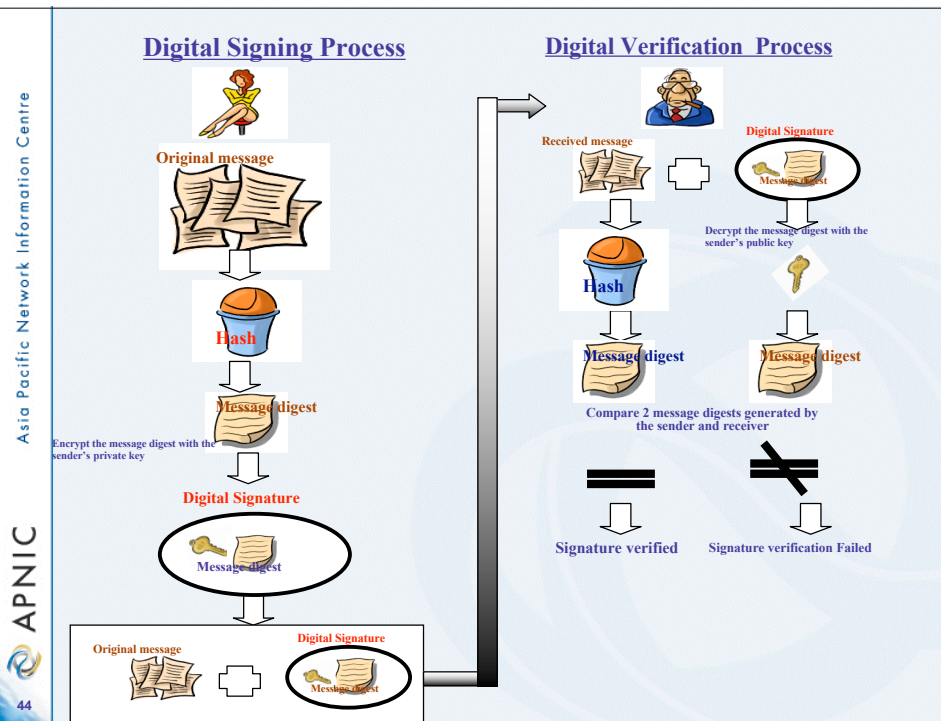
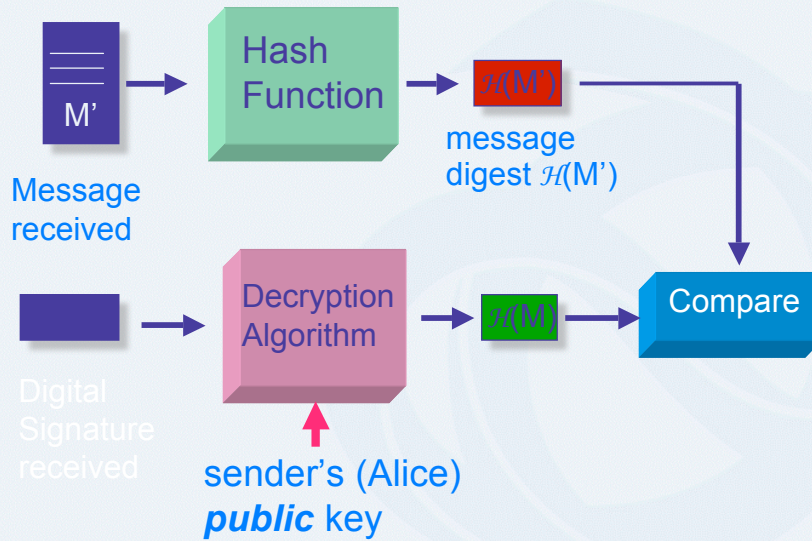


Authenticating message sender

- **Verifying an RSA Digital Signature:**
 - Bob (message receiver):
 - generates $H(M')$ from M' he received
 - determines $H(M) = D_{RSA}(Sig_A(M), K_{A_pub})$
 - compares $H(M')$ and $H(M)$
 - If $H(M')$ and $H(M)$
 - then integrity and authenticity of message are guaranteed
 - also sender cannot deny sending the message (non-repudiation)

Asia Pacific Network Information Centre
APNIC
42

Verifying an RSA Digital Signature

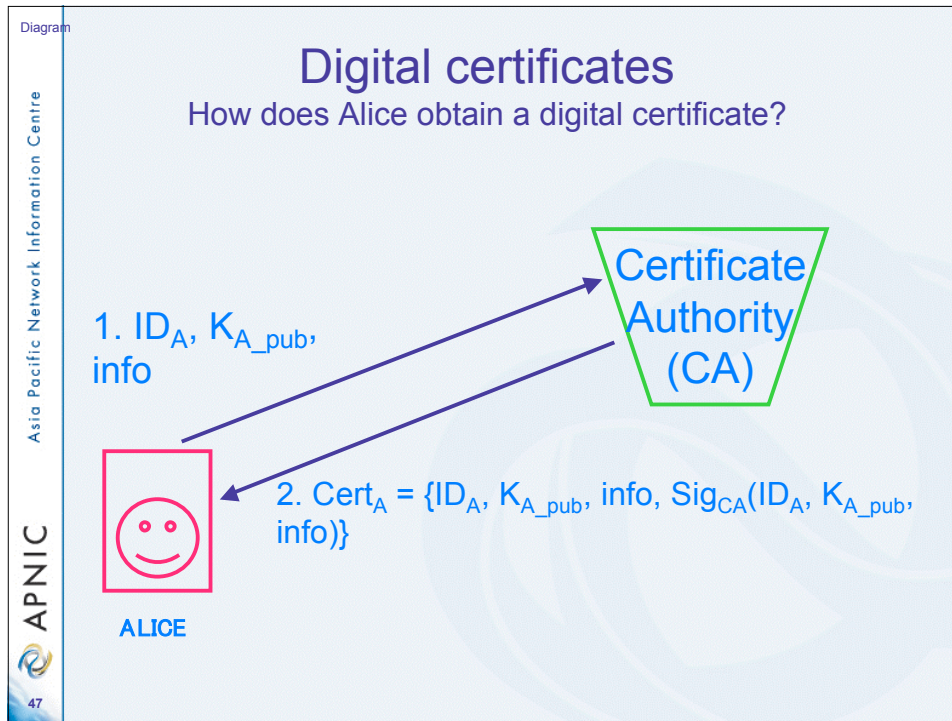


Digital certificates

- Digital certificates deal with the problem of
 - binding a public key to an entity
 - A major legal issue related to eCommerce
- A digital certificate contains:
 - user's public key
 - user's ID
 - other information e.g. validity period
- Certificate examples:
 - X509 (standard)
 - PGP (Pretty Good Privacy)
- Certificate Authority (CA) creates and digitally signs certificates

Digital certificates

- To obtain a digital certificate Alice must:
 - make a certificate signing request to the CA
 - Alice sends to CA:
 - her identifier ID_A
 - her public key K_{A_PUB}
 - additional information
 - Alice must supply proof that she is indeed Alice
- CA returns Alice's digital certificate, cryptographically binding her identity to public key:
 - $CertA = \{ID_A, K_{A_pub}, info, SigCA(ID_A, K_{A_pub}, info)\}$



- ## Non-repudiation
- provided using digital signatures:
 - If signature uses something known only to the signer
 - then only signer can have formed the signature
 - so signer cannot deny it
 - If Alice denies sending message:
 - Her private key can be tested on original plaintext to prove she must have sent it
 - Assumes no compromises of system, keys, etc
- APNIC Asia Pacific Network Information Centre
- 48

Network infrastructure security

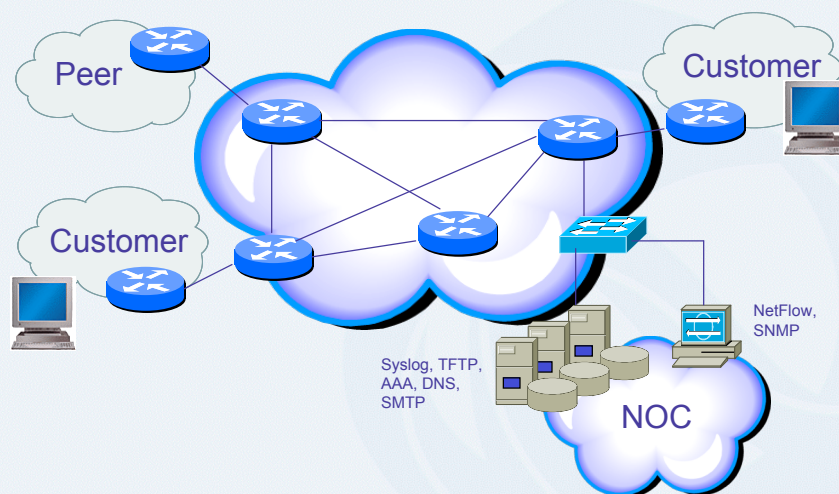
What are security goals?

- Controlling data / network access
- Preventing intrusions
- Responding to incidences
- Ensuring network availability
- Protecting information in transit

First step....Security policy

- What are you trying to protect?
 - What data is confidential?
 - What resources are precious?
- What are you trying to protect against?
 - Unauthorised access to confidential data?
 - Malicious attacks on network resources?
- How can you protect your site?

Network infrastructure security



Security services we need to consider

- User authentication
- User authorisation
- Data origin authentication
- Access control
- Data integrity
- Data confidentiality
- Auditing / logging
- DoS mitigation

How do large ISPs protect their infrastructure?

- Understand the problem
- Establish an effective security policy
 - Physical security
 - Logical security
 - Control / management plane
 - Control plane – process level on a router processor
 - Management plane – SSL, SNMP, CLI, AAA and etc.
 - Routing plane
 - E.g., BGP peer authentication
 - Data plane
 - E.g., Unicast Reverse Path Forwarding (RPF)
- Procedures for incident response
 - Assessing software vulnerability risk
 - Auditing configuration modifications

The security practices should include...

- Physical security controls
 - Media
 - Equipment location
 - Environmental safeguards
- Logical security controls
 - Subnet boundaries
 - Routing boundaries
 - Logical access control (preventative / detective)
- System and data integrity
 - Firewalls
 - Network services
- Data confidentiality

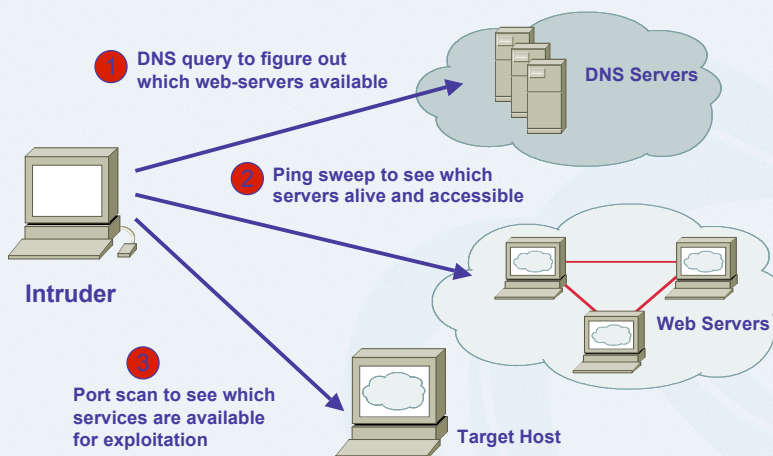
Cisco Technology Group view

- http://www.cisco.com/application/pdf/en/us/guest/products/ps6642/c1161/cdccont_0900aecd80313fee.pdf

The security practices should include...

- Mechanisms to verify and monitor security controls
 - Accounting
 - Management
 - Intrusion detection
- Policies and procedures for staff that is responsible for the corporate network
 - Secure backups
 - Equipment certification
 - Use of portable tools
 - Audit trails
 - Incident handling
- Appropriate security awareness training for users of the corporate network

Example active reconnaissance (spying) attempt



Threat consequences

- (Unauthorised) Disclosure
 - A circumstance of event whereby an entity gains access to data for which the entity is not authorised
- Deception
 - A circumstance or event that may result in an authorised entity receiving false data and believing it to be true
- Disruption
 - A circumstance or event that interrupts or prevents the correct operation of system services and functions
- Usurpation
 - A circumstance of event that results in control of system services or functions by an unauthorised entity

Disruption often caused by DoS and DDoS attacks

- TCP SYN
- TCP ACK
- UDP, ICMP, TCP floods
- Fragmented packets
- IGMP flood
- Spoofed and un-spoofed

DDoS is a huge problem

- Distributed and/or coordinated attacks
 - Increasing rate and sophistication
- Infrastructure protection
 - Coordinated attack against infrastructure
 - Attacks against multiple infrastructure components
- Overwhelming amounts of data
 - Huge effort required to analyse
 - Lots of uninteresting events

What if routers becomes attack target?

- It allows an attacker to:
 - Disable the router and network
 - Compromise other routers
 - Bypass firewalls, IDS systems, etc....
 - Monitor and record all outgoing and incoming traffic
 - Redirect whatever traffic they desire....

Router CPU vulnerabilities

- CPU overhead
 - Attacks on applications on the Internet have affected router CPU performance leading to some BGP instability
 - 100,000+ hosts infected with most hosts attacking routers with forged-source packets
 - Small packet processing is taxing on many routers...even high-end
 - Filtering useful but has CPU hit

Security device management

- Miscreants have a far easier time gaining access to devices than you think
- Ensure that the basic security capabilities have been configured
- In-band vs Out-of-band management trade off

Device physical access

- Equipment should be kept in highly restrictive environments
- Console access
 - Password protected
 - Access via OOB (Out-Of-Band) management
- Individual users authenticated
- Social engineering training and awareness

Logical access

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear texts (in config files)
- Never transfer passwords in clear texts (telnet Vs ssh)
- Authenticate individual users
- Restrict logical access to specified trusted hosts

Secure access to routers with passwords and timeouts

```
line console 0  
login  
password letmein  
exec-timeout 0 0
```

```
User Access Verification  
Password: <letmein>  
  
router>
```



NOT SECURE!

Secure access to routers with passwords and timeouts

```
line console 0  
login TACACS+ local  
exec-timeout 1 30
```

```
User Access Verification  
Password: <Ncr1pTd>  
  
router>
```



MORE SECURE!

Never leave passwords in clear-text

- **Password command**

- Will encrypt all passwords on the Cisco IOS with Cisco-defined encryption type “7”
- Use “command password 7 <password>” for cut/paste operations
- Cisco proprietary encryption method

- **Secret command**

- Uses MD5 to produce a one-way hash
- Cannot be decrypted
- Use “command secret 5 <password>” to cut/paste another “enable secret” password

Cisco IOS password encryption facts

- User passwords and most other passwords (NOT enable secrets) in Cisco IOS configuration files
 - Encrypted using a very weak encryption mechanism (reversible algorithm)
 - Never intended to resist a determined and intelligent attack
 - Designed to avoid password theft via simple snooping or sniffing

Reference: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00801d7efa.shtml

Cisco IOS password encryption facts

- Enable secret command
 - Hashed using the MD5 algorithm
 - Impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks)
 - Enable password command should no longer be used

Reference: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00801d7efa.shtml

Cisco IOS password encryption facts

- Configuration files
 - When you send configuration information in e-mail, you should sanitise the configuration from type 7 passwords

```
.....
hostname routerA
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default if-needed local
enable secret 5 <removed>
!
username jdoe password 7 <removed>
username headquarters password 7 <removed>
username hacker password 7 <removed>
```

Reference: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00801d7efa.shtml

Authenticate individual users

```

service password-encryption
enable secret 5 $1$mgfc$ISYSLeC6ookRSV7sl1vXR.
enable password 7 075F701C1E0F0C0B
!
username merike secret 5 $6$mffc$lmnGLeC67okLOMps
username staff secret 5 $6$ytjc$IchdLeC6o6klmR7s

line con 0
exec-timeout 1 30
login local
!
line vty 0 4
exec-timeout 5 0
login local
transport input ssh

```

Restrict access to trusted hosts

- Use filters to specifically permit hosts to access an infrastructure device
- Example

```

Access-list 103 permit tcp host 192.168.200.7 192.168.1.0 0.0.0.255
eq 22 log-input
Access-list 103 permit tcp host 192.168.200.8 192.168.1.0 0.0.0.255
eq 22 log-input
Access-list 103 permit tcp host 192.168.200.6 192.168.1.0 0.0.0.255
eq 23 log-input
Access-list 103 deny ip any any log-input
!
Line vty 0 4
Access-class 103 in
Transport input ssh telnet

```

Telnet is insecure

- Avoid using Telnet if possible
- Telnet sends username and password information across the wire in plain text format.
- Do not use telnet to gain access to any of your boxes (router-to-router could be exception for troubleshooting, but limit access in these instances)

Harvesting telnet passwords - sample

The image shows a Wireshark packet capture of a Telnet session. The packet list on the left shows several packets, with packet 79 selected. The packet details pane on the right shows the structure of the selected packet, which is a Telnet session establishment packet. The packet bytes pane at the bottom shows the raw data of the packet, with a red circle highlighting the password field. A red arrow points from the word "Password" to the highlighted password field in the packet bytes pane.

Filter: (ip.addr eq 202.12.29.165 and to.addr eq 203.119.0.107) and (tcp.port eq 23)

No.	Time	Source	Destination	Protocol	Info
70	18.038972	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [ACK] Seq=34 Ack=63 Win=64794 Len=0
71	18.242676	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=34 Ack=63 Win=64794 Len=1
72	18.247906	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [PSH, ACK] Seq=63 Ack=35 Win=64097 Len=1
73	18.422423	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=35 Ack=64 Win=64793 Len=1
74	18.428004	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [PSH, ACK] Seq=64 Ack=36 Win=64096 Len=1
75	18.539997	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [ACK] Seq=36 Ack=65 Win=64792 Len=0
76	18.714259	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=36 Ack=65 Win=64792 Len=2
77	18.840104	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [ACK] Seq=38 Ack=77 Win=64780 Len=0
78	19.129392	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=38 Ack=77 Win=64780 Len=1
79	19.337719	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [ACK] Seq=39 Ack=77 Win=64095 Len=0
80	19.533829	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=39 Ack=77 Win=64780 Len=1
81	19.736666	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [ACK] Seq=40 Ack=77 Win=64095 Len=0
82	19.943401	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=40 Ack=77 Win=64780 Len=1
83	20.144674	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [ACK] Seq=41 Ack=77 Win=64095 Len=0
84	20.158368	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=41 Ack=77 Win=64780 Len=1
85	20.360019	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [ACK] Seq=42 Ack=77 Win=64095 Len=0
86	20.562938	202.12.29.165	203.119.0.107	TCP	2042 → 2044 [PSH, ACK] Seq=42 Ack=77 Win=64780 Len=2
87	20.570384	203.119.0.107	202.12.29.165	TCP	2044 → 2042 [PSH, ACK] Seq=44 Ack=77 Win=64088 Len=2

Frame 79 (66 bytes on wire (528 bytes captured) on interface 0):

- Ethernet II, Src: Cisco-CF197F1 (00:09:08:0c:f9:7f), Dst: dellComp-Baidaid (00:06:1b:8a:da:1d)
- Internet Protocol, Src: 203.119.0.107 (203.119.0.107), Dst: 202.12.29.165 (202.12.29.165)
- Transmission Control Protocol, Src Port: 2044 (2044), Dst Port: 2042 (2042), Seq: 65, Ack: 38, Len: 12
- Source port: 2044 (2044)
- Destination port: 2042 (2042)
- Sequence number: 65 (relative sequence number)
- Next sequence number: 77 (relative sequence number)
- Acknowledgement number: 38 (relative ack number)
- Header length: 20 bytes
- Flags: 0x0018 (PSH, ACK)
- Window size: 4094
- Checksum: 0x08e9 [correct]
- Data (32 bytes)

0000 00 06 1b 8a da 1d 00 09 08 cf 57 f1 08 00 45 00W...E..
 0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0020 1d 31 07 04 07 fa 36 8a 3b 57 78 77 25 6b 10 186..;xwW.P..
 0030 0f fe 88 e9 00 00 0d 0a 50 61 73 77 6f 72 64Password
 0040 3a 20

Secure Shell (SSH)

- Username/password information is encrypted
- Flexible authentication methods
 - One-time password
 - Kerberos
 - Public key
- Allows secure tunneling
 - TCP port forwarding
 - Forward remote ports to local ones
- Uses TCP port 22

SSH support

- Two flavors of ssh, ssh1 and ssh2
- Use ssh 2 if possible
- In general the client connecting to your ssh server will either “speak” ssh1 or ssh2
- OpenSSH for UNIX
 - www.openssh.org
 - Supports both ssh1 and ssh2
- Putty client for windows
 - www.chiark.greenend.org.uk/~sgtatham/putty/

Using SSH on Cisco routers

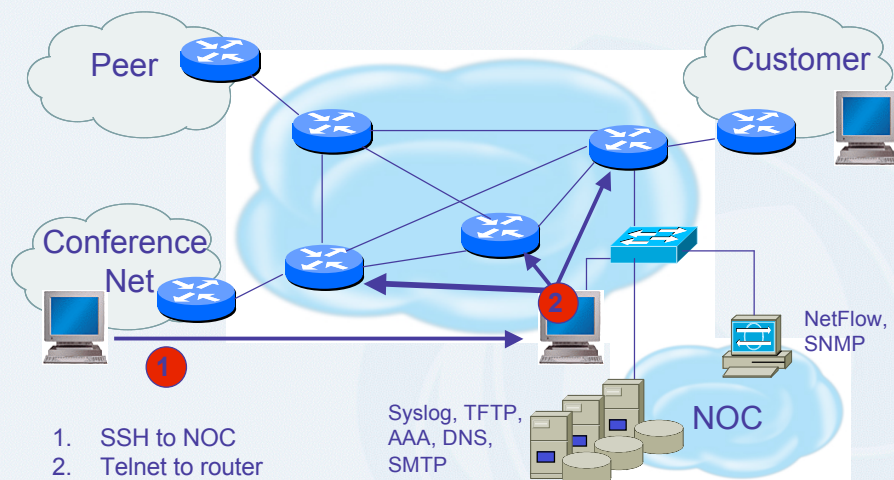
- Supported as of IOS 12.0S
- Ensure you have crypto image
- Set up SSH

```
Router(config)#crypto key generate rsa
```

- Add SSH as input transport

```
line vty 0 4  
  transport input ssh
```

Telnet using SSH 'Jumphost'



Securing routers

*“If you are not using it,
do not turn it on”*

Cisco ISP Essentials

Reference: Cisco ISP Essentials, 2001 P50

Turn off unused services

Interface-Specific Services

- no ip redirects
- no ip directed-broadcast
- no ip proxy-arp
- no ip source-route
- no ip mask-reply
- no cdp enable

Global Services

- no service finger
- no ip finger
- no service pad
- no service udp-small-servers
- no service tcp-small-servers
- no ip bootp server
- no cdp run

HTTP server

- Cisco devices support starting in IOS 11.1CC and 12.0S
- Explicitly disable if not using
`no ip http server`
- Example secure configuration

```
access-list 36 permit <router 1 IP address>  
access-list 36 permit <router 2 IP address>  
access-list 36 deny any  
ip http server  
ip http port 80  
ip http authentication aaa  
ip http access-class 36
```

Limiting device access

```
access-list 29 permit <NOC subnet>  
access-list 29 deny any  
line vty 0 4  
  access-class 29 in  
  exec-timeout 5 0  
  transport input telnet ssh  
  transport output none  
  transport preferred none  
  login local
```

- Define specific subnet or hosts which can have telnet or ssh access
- Note that authenticated login is also used

Disabling the AUX port

```
line aux0
login local
no password
transport input none
no exec
```

- Will not let anyone log in
- Use this if not using aux port for console access

Secure SNMP access

- SNMP is primary source of intelligence on a target network!
- Block SNMP from the outside
 - Access-list 101 deny udp any any eq snmp
- If the router has SNMP, protect it!
 - snmp-server community f00bAr RO 1
 - Access list 1 permit 127.1.3.5
- Explicitly direct SNMP traffic to an authorised management station.
 - Snmp-server host f00bAr 127.1.3.5

SNMP configuration

```
access-list 35 permit <SNMP-server IP address>  
access-list deny any  
snmp-server community try2brkme RO 35  
snmp-server trap-source loopback0  
snmp-server trap authentication  
snmp-server host <SNMP-server IP address> try2brkme
```

Syslog

- Event logs created by syslog daemon
- Unix
 - Configured in /etc/syslog.conf
 - facility.severity<Tab>destination-file-path
 - Possible values of for facility (Cisco) are local0
 - local7
 - debug, info, notice, warning, err, crit, alear, emerg, and none
 - Usually log stored in /var/log
- Windows based syslog server
 - <http://www.kiwisyslog.com>

Ref: <http://www.ciscopress.com/articles/article.asp?p=426638&rl=1>

Secure logging infrastructure

- Syslog sends its information in clear text
 - A sniffer on the network easily capture the messages
 - Syslog messages should be sent on a separate network using a second network interface, if possible
 - Also IPsec tunnel can be used to encrypt the traffic to the syslog server
- Syslog uses UDP
 - If possible, use syslog over TCP
- Centralise logging location good for net admins but also for attackers
 - Regularly update the syslog server with the latest service packs and security patches

Ref: <http://www.ciscopress.com/articles/article.asp?p=426638&rl=1>

Infrastructure access logging

- Logging servers should be physically and logically secure
- Accept messages only from trusted hosts
- Encrypt log messages

Secure logging infrastructure

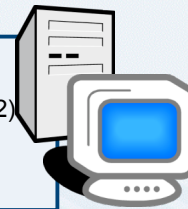
- Log enough information to be useful but not overwhelming
- Create backup plan for keeping track of logging information should the syslog server be unavailable
- Remove private information from logs
- How accurate are your timestamps?

Timestamp issues

```
unix% tail cisco.log
Feb 18 21:48:26 [10.1.1.101.9.132] 31: * Mar 2 11:51:55 CST:
% sys-5-CONFIG_1: Configured from console by vty 0 (10.1.1.2)
unix% data
Tue Feb 18.21:49:53 CST 2005
unix%
```

```
Version 12.2
Service timestamps log datetime
localtime show-timezone
!
Logging 10.1.1.2
```

```
Router> sho clock
*11:53:44.764 CST Tue Mar 2 1993
Router>
```



NTP

- Need to synchronize timestamps
- Network Time Protocol (NTP)
 - External source
 - Upstream ISP, Internet, atomic clock, GPS
 - Internal source
 - Router can act as stratum 1 timesource

```
access-list 15 permit 192.168.66.0 0.0.0.255
access-list 17 permit 192.168.1.1
access-list 17 permit 192.168.3.1
!
ntp source loopback0
ntp access-group peer 17
ntp access-group serve-only 15
ntp server 192.168.3.1
ntp server 192.168.1.1 prefer
```

NTP

- Routers with inaccurate and unsynchronised time
 - Trouble with correlating log files
 - Affect to perform accounting, fault analysis, network management and time-based AAA authentication and authorisation
- Four different modes to operate
 - Client
 - Server
 - Peer
 - Broadcast

Ref: <http://www.oreilly.com/catalog/hardisco/chapter/ch10.html>

Banner....what's wrong?

banner login ^C

Martini

2.5 ounces vodka

1/5 ounce dry vermouth

Fill mixing glass with ice, add vermouth and vodka, and stir to chill. Strain into a Martini glass and garnish with an olive or lemon twist.

RELAX....INDULGE....

Get Off My Router!!

^C

Better device banner

!!!! WARNING !!!!

You have accessed a restricted device.

All access is being logged and any unauthorised access will be prosecuted to the full extent of the law.

System image and configuration file security

- Careful of sending configurations where people can snoop the wire
 - CRC or MD5 validation
 - Sanitise configuration files
- SCP should be used to copy files
 - TFTP and FTP should be avoided
- Use tools like 'rancid' to periodically check against modified config files

Bare minimum device security

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through ssh
- Disable device access methods that are not used
- Shut down unused interfaces
- Shut down unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners
- Test device integrity on a regular basis

Need for an Information Policy

- Before it can address network security, an organisation must:
 - assess risks – identify organisational threats and estimate their likelihoods
 - Identify and implement a set of protection mechanisms and procedures which match perceived risk to value and use of information assets – risk mitigation
 - develop a clear policy for information access and protection
- A **security policy** needs to specify
 - who has access to each piece of information (access control)
 - rules for giving information to others
 - how the organisation will handle violations
 - How the organisation will handle compromises
 - Disaster recovery plan (redundancy, backups)
 - How to react to, and mitigate a malicious event (NSP-SEC, Certs, filters)

Need for an Information Policy

- Establishing a policy and educating employees is important because:
 - People are usually the weakest link in any security scheme
 - A worker who is malicious, careless, or unaware of the information policy can compromise the best security
- *There is no such thing as “perfect security”*

Network security and infrastructure fundamentals

Part II

Acknowledgements

- The contents of this module is based on material provided by:
 - Merike Kaeo from Double Shot Security and the author of “Designing Network Security”.
 - (merike@doubleshotsecurity.com), (<http://doubleshotsecurity.com>)
 - Barry Green (bgreene@cisco.com) and
 - Philip Smith (pfs@cisco.com), Cisco Systems
- **APNIC acknowledges their contributions and support with appreciation and thanks**
- Some material is also sourced from lecture material from the QUT Internetworking course (ITB524)

Monitoring and managing access

AAA, TACACS and RADIUS

AAA

Authentication, Authorisation, and Accounting (AAA) network security services

- AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way for performing authentication, authorisation and accounting.
 - It provides the primary framework for access control on routers and access servers
 - Identifies who can access the network or network server
 - What the user can do
 - Provides records of accounting information about the user's activity for analysis.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfaaa.htm

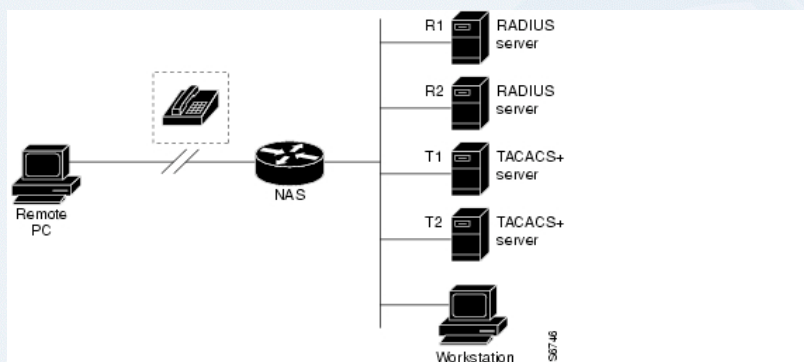
AAA

- Authentication
 - Provides the method of identifying users
- Authorisation
 - Provides the method for remote access control
- Accounting
 - Provides the method for collecting and sending security server information used for billing, auditing, and reporting

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfaaa.htm

Typical AAA network configuration

- a typical AAA network configuration that includes four security servers:
 - R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.



http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfaaa.htm

AAA configuration process

1. Enable AAA
 - **aaa new-model** global configuration command.
2. If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
3. Define the method lists for authentication by using an AAA authentication command.
4. Apply the method lists to a particular interface or line, if required.
5. (Optional) Configure authorization using the **aaa authorization** command.
6. (Optional) Configure accounting using the **aaa accounting** command.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfaaa.htm

TACACS+

- Terminal Access Controller Access Control System (TACACS)
- Protocol spec is defined by RFC 14
- TCP port 49
- Client/server protocol
 - Client typically a NAS
 - Server typically on UNIX or Windows NT
- Separates authentication, authorisation and accounting

TACACS+ Authentication

- Not mandatory
- Arbitrary length and content allows any authentication method to be used
- Three packets types
 - START
 - REPLY
 - Accept / Reject / Error
 - CONTINUE

TACACS+ Authorisation

- Single request/response pair
- Request contains fixed set of fields
 - Authenticity of user or process
 - Arguments that describe services and options for which authorisation is requested
- Can customise service
 - Example: time restriction on login or IP access list on PPP connections

TACACS+ Accounting

- Account for server
- Auditing tool for security services
- Three type of records
 - Start
 - Stop
 - Update

TACACS+ Transactions

- Transactions between client and server are authenticated through use of shared secret
- Transactions are encrypted

RADIUS

- Remote Authentication Dial In User Service (RADIUS)
 - A protocol for carrying authentication, authorisation, and configuration information between Network Access Server and a shared Authentication server
 - Protocol spec is defined by RFC 2865, which obsoletes RFC 2138
 - RADIUS uses UDP 1812 (1645)
 - RADIUS encrypts only the password in the access – request packet, from the client to the server

Reference: RFC2865

RADIUS

- Client / server protocol
 - Client typically SAN
 - Server typically on UNIX or Windows NT
- A RADIUS server can act as a proxy client to other RADIUS or authentication servers

RADIUS Authentication

- Supports variety methods of authentication
- Three message types
 - Access-request
 - Access-accept
 - Access-reject
 - Can be accompanied with optional text message which can indicate reason for refusal

RADIUS Authorisation

- Coupled together with authentication
- Access-accept response includes a list of attribute-value pairs which describe parameters to be used for the session
 - Service type (shell or framed)
 - Protocol type
 - IP address (static or dynamic)

RADIUS Accounting

- Can be used independently of authentication / authorisation
- Data can be sent at start and end of sessions, indicating amount of resources used during a session

RADIUS Transactions

- Transactions between client and server are authenticated shared secret
- Only user passwords are encrypted between client and server

Asia Pacific Network Information Centre

APNIC

119

Point Protection

119

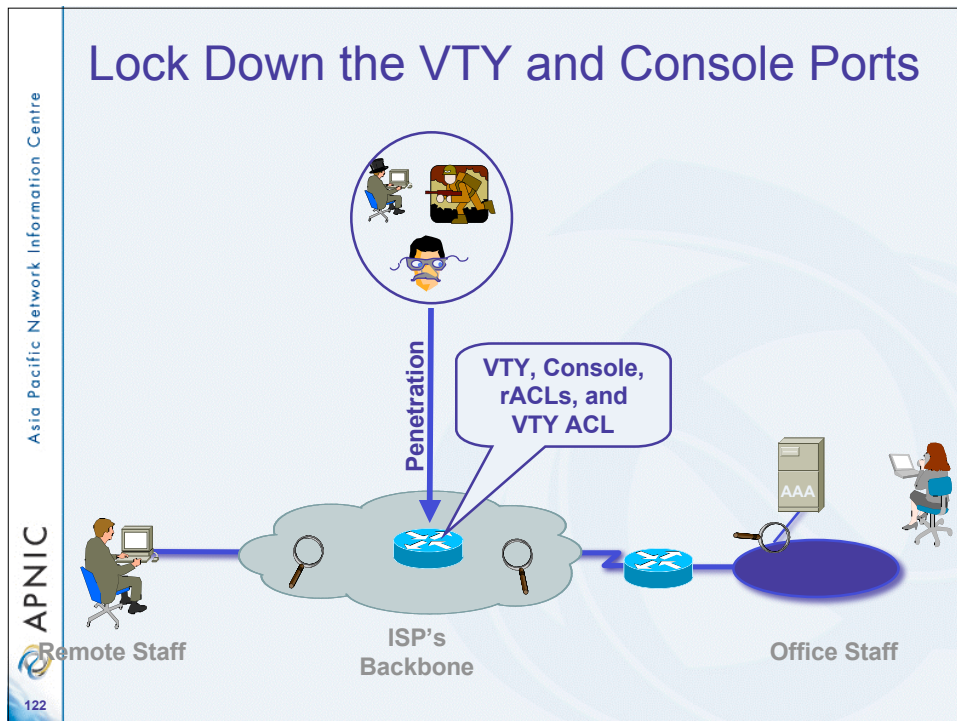
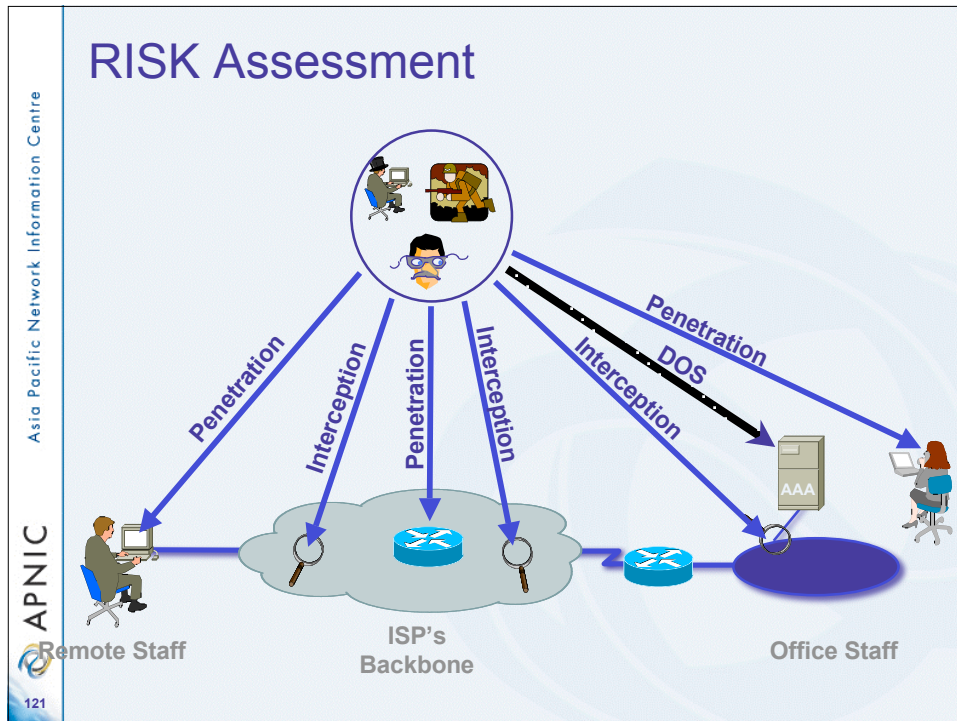
Asia Pacific Network Information Centre

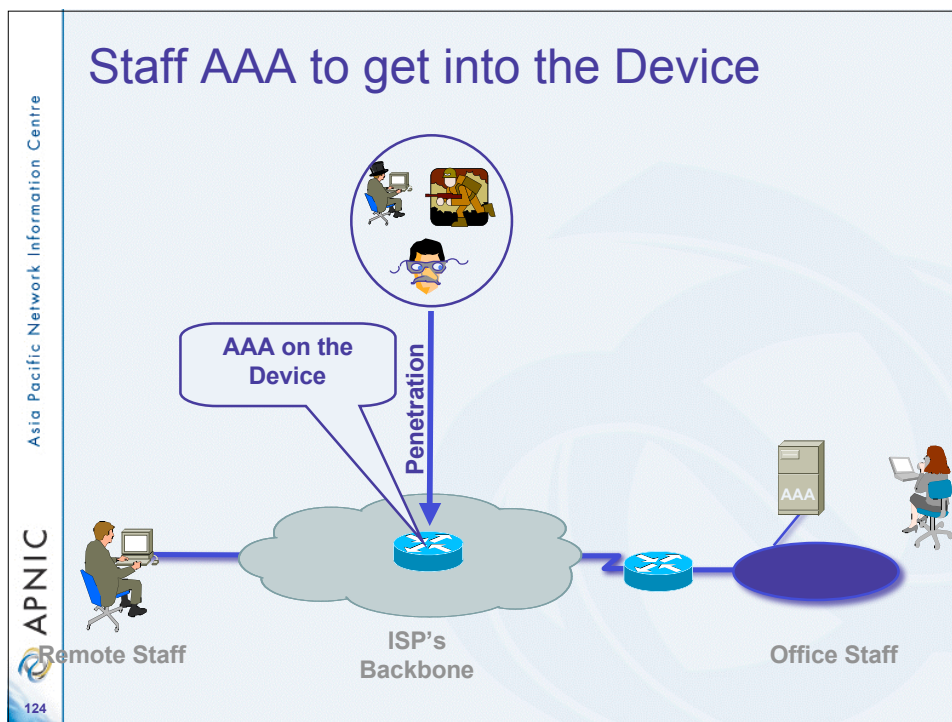
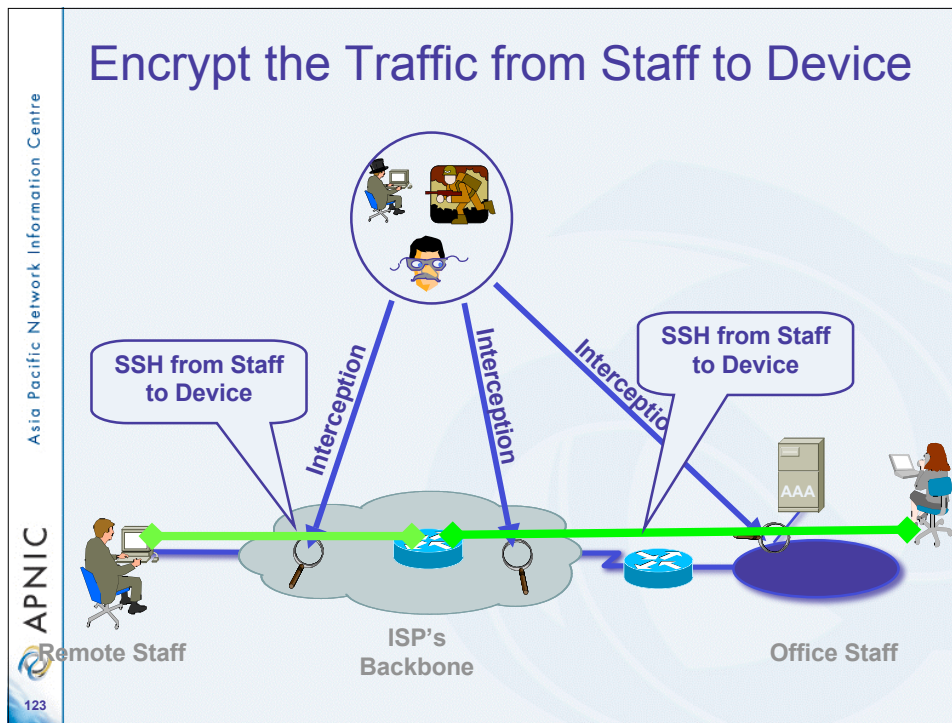
APNIC

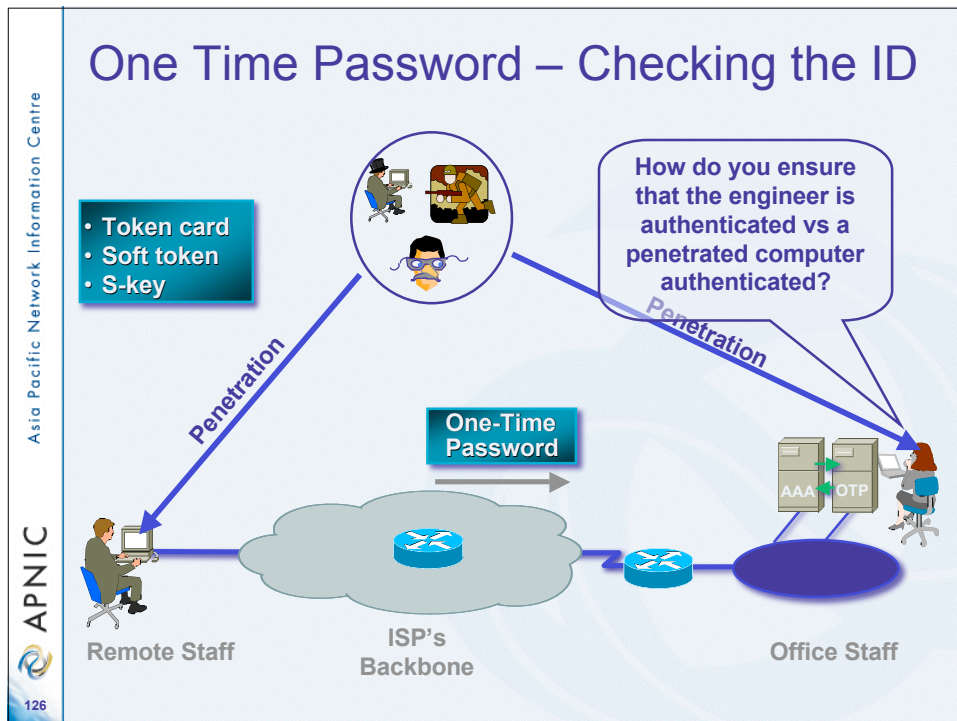
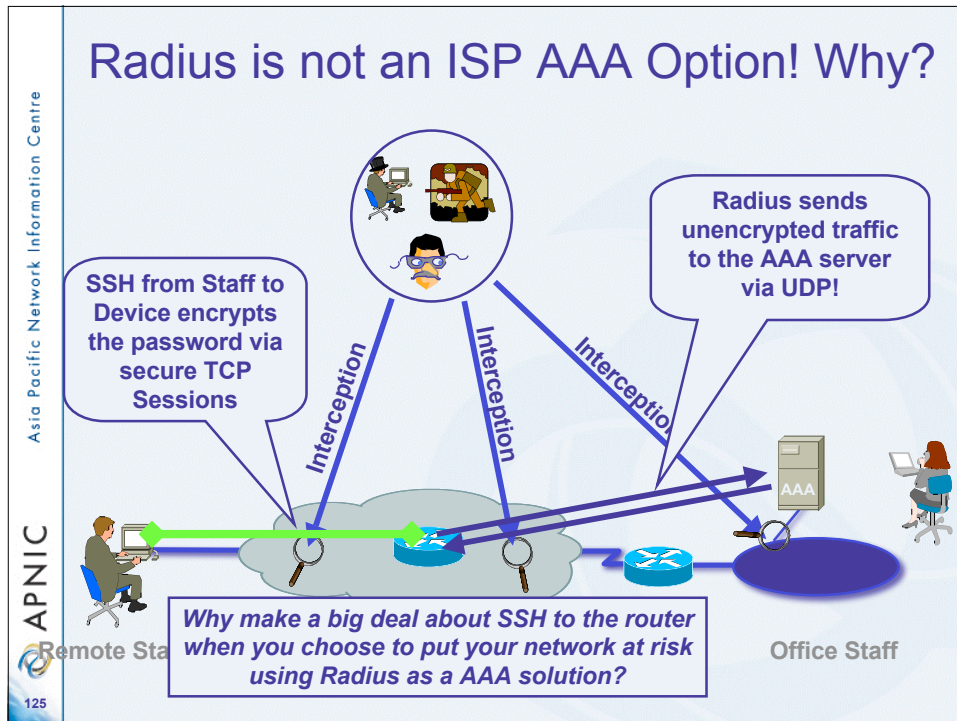
120

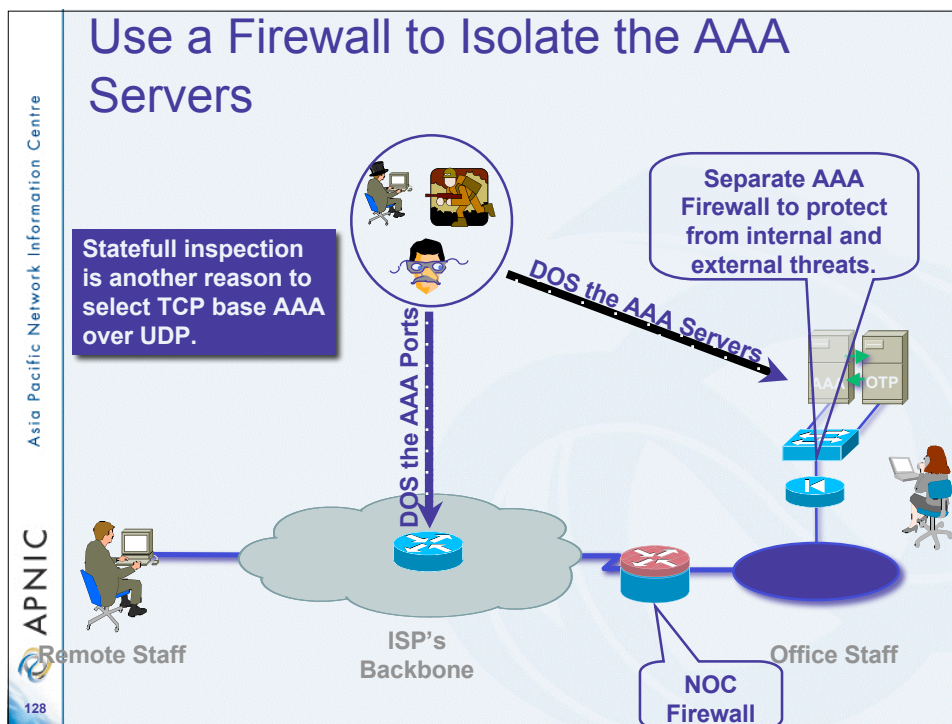
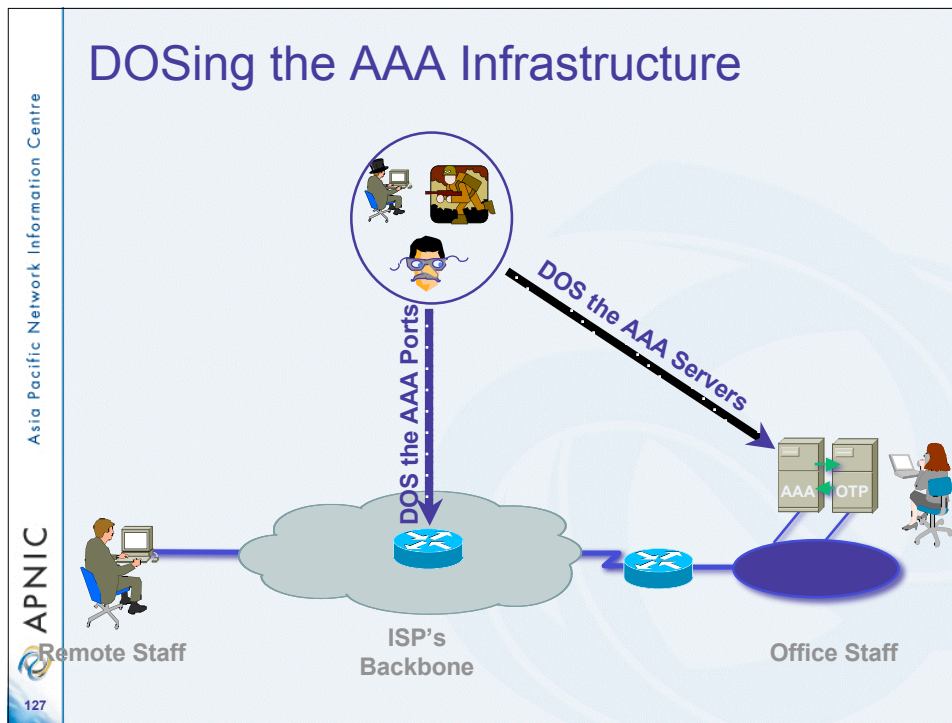
Check List

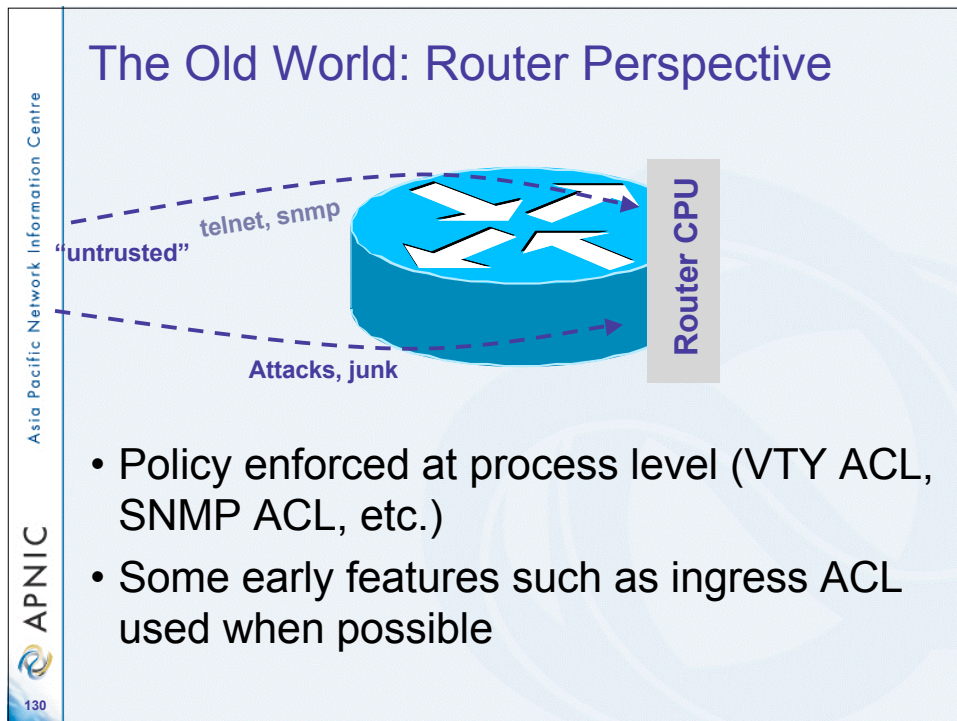
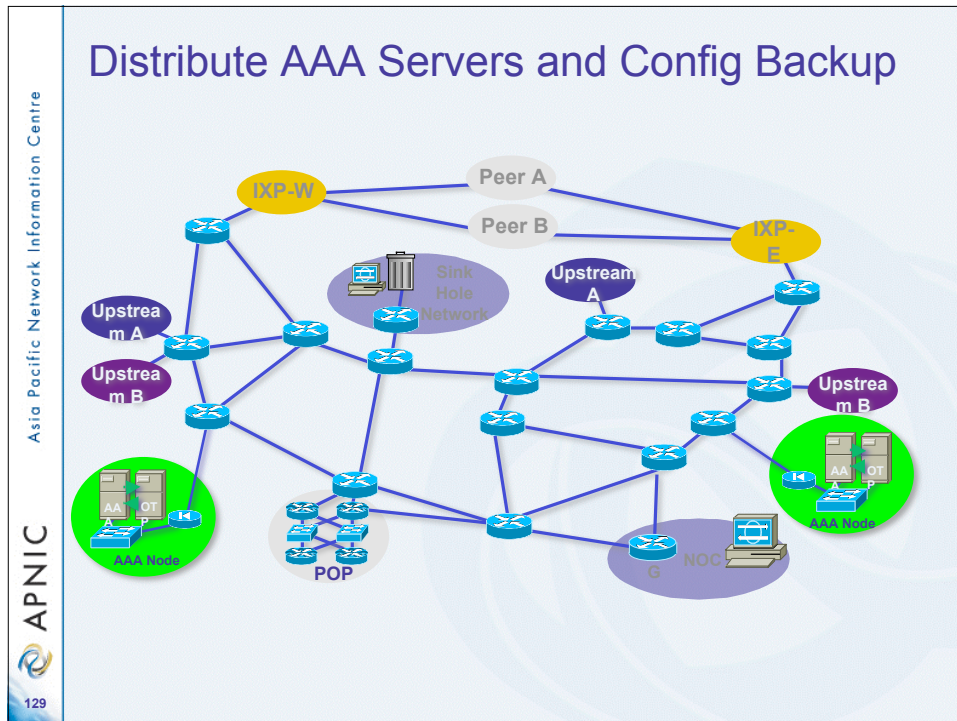
- AAA to the Network Devices
- Controlling packets destined to the network devices
- Config Audits





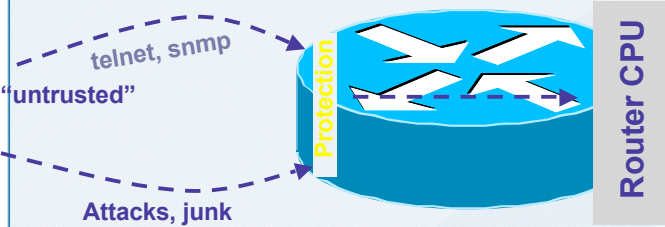






Asia Pacific Network Information Centre

The New World: Router Perspective



- Central policy enforcement, prior to process level
- Granular protection schemes
- On high-end platforms, hardware implementations

APNIC

131

Asia Pacific Network Information Centre

Watch the Config!

- There has been many times where the only way you know someone has violated the router is that a config has changed.
- If course you need to be monitoring your configs.

APNIC

132

Config Monitoring

- **RANCID - Really Awesome New Cisco config Differ (but works with lots of routers)**
<http://www.shrubbery.net/rancid/>
<http://www.nanog.org/mtg-0310/rancid.html>
- **Rancid monitors a device's configuration (software & hardware)**
- **Rancid logs into each of the devices in the device table file, runs various show commands, processes the output, and emails any differences from the previous collection to staff.**

Lab

- AAA
- TACACS
- RADIUS

Access Control Lists (ACLs)

What is an Access control list (ACL)

- ACLs define a series of rules or filters that are applied to traffic either entering or leaving an interface.
- Standard access-lists only filter on the source IP address.
- Extended access-lists can filter on
 - source and destination IP addresses
 - source and destination port numbers
 - protocols

Applying ACLs

- When an access list is configured it is applied to an interface.
- Each interface can have one list for incoming and one list for outgoing traffic.
- When a list is applied to an interface, it should contain permit filters for acceptable traffic since if a packet does not comply with one of the rules, it will be dropped even if it is not implicitly rejected.

Defining ACLs

- Access lists are defined in global configuration mode and applied in interface mode.
- Access lists are given a number;
 - 1-99 for standard lists,
 - 100-199 for extended lists
 - Can also be named ACLs
- The general syntax is:
 - access-list <number> <deny|accept>
<protocol> <source ip> <source port> <dest
ip> <dest port>

Defining addresses in an ACL

- Addresses are given as
 - any - refers to any IP address; that is, all IP addresses are filtered
 - host a.b.d.c - a specific host address
 - a.b.d.c A.B.D.C - a block or range of addresses.
 - The first 4 octets gives the network id and the second defines the block, much like a mask defines the netid, but in reverse.
 - For example, 212.12.2.3 0.0.0.0 means an exact match on all 4 octets;
 - 212.12.2.3 0.0.0.255 means match the first 3 octets exactly but match any value in the fourth octet;
 - 212.12.8.0 0.0.7.255 means match any address in the block 212.12.8.0 to 212.12.15.0 (the bits that are set to 1 define the range, ie the number of addresses. The third octet = 7, that is, the first 3 bits are set to 1, so the range in the third octet are all the addresses covered by the first 3 bits; that is $8+(0 \text{ to } 7) = 8$ to 15; and in the fourth octet, the range is 0+(0 to 255.)

ACL Notes

- using IP for the protocol refers to all traffic using IP
- rules (filters) in a list are processed from top to bottom until a match is found.
 - Specific rules should therefore be placed first.
 - The last rule is an "implicit deny", that is, anything that cannot be matched is denied.
 - An appropriate default permit should therefore be placed last.
 - Single filters cannot be removed. The whole list must be reconfigured. You can keep the rules in a text file and then edit this
 - If creating a named ACL, the name must unique across both standard and extended ACLs

What ACLs do?

- Filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces
 - Based on the criteria/rules specified in the access lists
- ACL criteria/rules
 - Source address of the traffic
 - The destination address of the traffic
 - The upper-layer protocol
 - Other information

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacsl.htm#xtocid2689513

Why you should configure ACLs?

- To provide security for your network
 - If there is no ACL then all packets passing through your router will be allowed into all parts of your network
- To restrict contents of routing updates
- To provide traffic flow control

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacsl.htm#xtocid2689513

When should ACLs be configured?

- Should be used in “firewall” routers
- You can also use ACLs on a router positioned between two parts of your networks
- To provide security benefits
 - configure ACLs on border routers (routers situated at the edges of your networks)
 - This will provide a basic buffer from the outside network, or from a less controlled area of your own network into a more sensitive area of your network

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacsl.htm#xtocid2689513

Overview of ACL configuration

- 1st step
 - Create ACL
- 2nd step
 - Apply ACL to interfaces

Cisco IOS ACL commands

- Creating numbered standard and extended IP ACLs

Command	Purpose
Router(config)# access-list <i>access-list-number</i> { deny permit } <i>source</i> { <i>source-wildcard</i> }	Defines a standard IP ACL using a source address and wildcard
Router(config)# access-list <i>access-list-number</i> { deny permit } any	Defines a standard IP ACL using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255.
Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol</i> <i>source</i> <i>source-wildcard</i> <i>destination</i> <i>destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>]	Defines an extended IP ACL number and the access conditions.
Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol</i> any any	Defines an extended IP ACL using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.
Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol</i> host <i>source</i> host <i>destination</i>	Defines an extended IP ACL using an abbreviation for a source and source wildcard of source 0.0.0.0, and an abbreviation for a destination and destination wildcard of destination 0.0.0.0.

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r46docs/r46mls/aclcfg.htm>

Cisco IOS ACL commands

- Applying the ACL to an interface
 - ACLs can be applied on either the inbound or the outbound direction of an interface

Command	Purpose
ip access-group { <i>access-list-number</i> <i>name</i> } { in out }	Controls access to an interfaces

<http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r46docs/r46mls/aclcfg.htm>

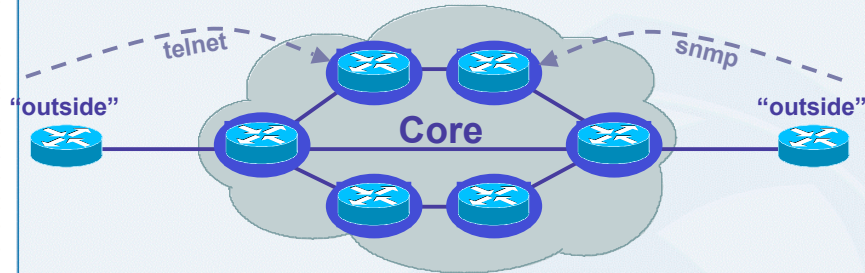
Example - Cisco IOS ACLs

- `access-list 100 permit tcp any host 171.16.23.1 eq 80`
- `access-list 100 deny ip any any`
- A packet is addressed to 171.16.23.1 80
 - The packet is permitted
- A packet addressed to 171.16.23.1 21
 - The packet is denied.
- A packet addressed to 171.16.23.2 80
 - The packet is denied.

<http://www.cisco.com/univercd/cc/td/doc/product/orig/15400/r46docs/r46mls/aclcfg.htm>

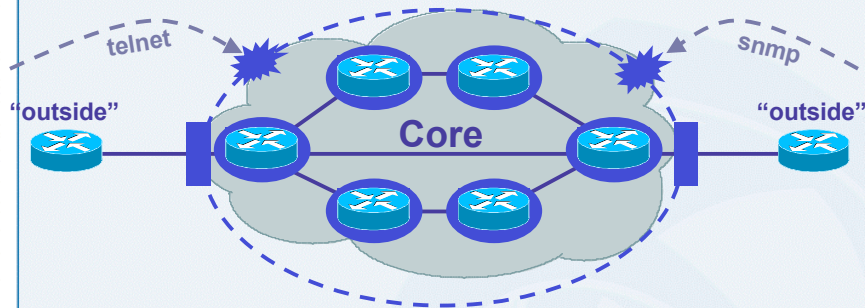
Edge protection

The Old World: Network Edge



- Core routers individually secured
- Every router accessible from outside

The New World: Network Edge



- Core routers individually secured PLUS
- Infrastructure protection
 - Routers generally NOT accessible from outside

Infrastructure ACLs

- Basic premise: filter traffic destined TO your core routers
 - Do your core routers really need to process all kinds of garbage?
- Develop list of required protocols that are sourced from outside your AS and access core routers
 - Example: eBGP peering, GRE, IPSec, etc.
 - Use classification ACL as required
- Identify core address block(s)
 - This is the protected address space
 - Summarization is critical → simpler and shorter ACLs

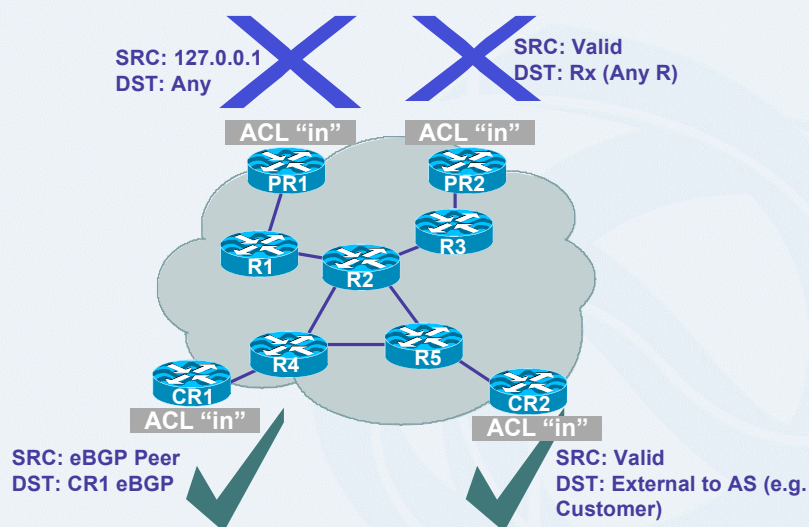
Infrastructure ACLs

- Infrastructure ACL will permit only required protocols and deny ALL others to infrastructure space
- ACL should also provide anti-spoof filtering
 - Deny your space from external sources
 - Deny RFC1918 space
 - Deny multicast sources addresses (224/4)
 - RFC3330 defines special use IPv4 addressing

Infrastructure ACLs

- Infrastructure ACL must permit transit traffic
 - Traffic passing through routers must be allowed via permit IP any any
- ACL is applied inbound on ingress interfaces
- Fragments destined to the core can be filtered via fragments keyword

Infrastructure ACL in Action



Iterative Deployment

- Typically a very limited subset of protocols needs access to infrastructure equipment
- Even fewer are sourced from outside your AS
- Identify required protocols via classification ACL
- Deploy and test your ACLs

Step 1: Classification

- Traffic destined to the core must be classified
- NetFlow can be used to classify traffic
 - Need to export and review
- Classification ACL can be used to identify required protocols
 - Series of permit statements that provide insight into required protocols
 - Initially, many protocols can be permitted, only required ones permitted in next step
 - Log keyword can be used for additional detail; hits to ACL entry with *log will increase CPU utilization*: impact varies by platform
- Regardless of method, unexpected results should be carefully analyzed → *do not permit protocols that you can't explain!*

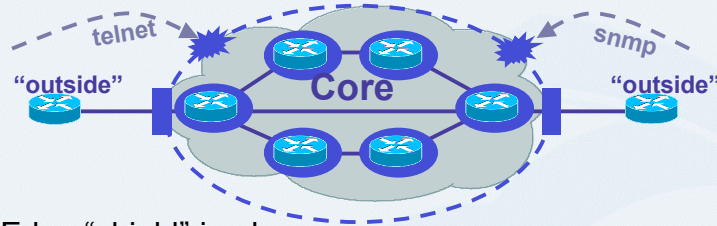
Step 2: Begin to Filter

- Permit protocols identified in step 1 to infrastructure only address blocks
- Deny all other to addresses blocks
 - Watch access control entry (ACE) counters
 - Log keyword can help identify protocols that have been denied but are needed
- Last line: permit ip any any ← permit transit traffic
- The ACL now provides basic protection and can be used to ensure that the correct suite of protocols has been permitted

Steps 3 and 4: Restrict Source Addresses

- Step 3:
 - ACL is providing basic protection
 - Required protocols permitted, all other denied
 - Identify source addresses and permit only those sources for requires protocols
 - e.g., external BGP peers, tunnel end points
- Step 4:
 - Increase security: deploy destination address filters if possible

Infrastructure ACLs



- Edge "shield" in place
- Not perfect, but a very effective first round of defense
 - Can you apply iACLs everywhere?
 - What about packets that you cannot filter with iACLs?
 - Hardware limitations
- Next step: secure the control/management planes per box

Questions ?

Thank you

