Asia Pacific Network Information Centre

APNIC

APNIC Training

Security Tutorial

21 July 2009 – Chennai, India

In conjunction with

SANOG

Asia Pacific Network Information Centre

APNIC

Network security fundamentals

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”.

- **APNIC acknowledges her contribution and support with appreciation and thanks**

- Some material is also sourced from lecture material from the QUT Internetworking course (ITB524)

Objectives

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

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

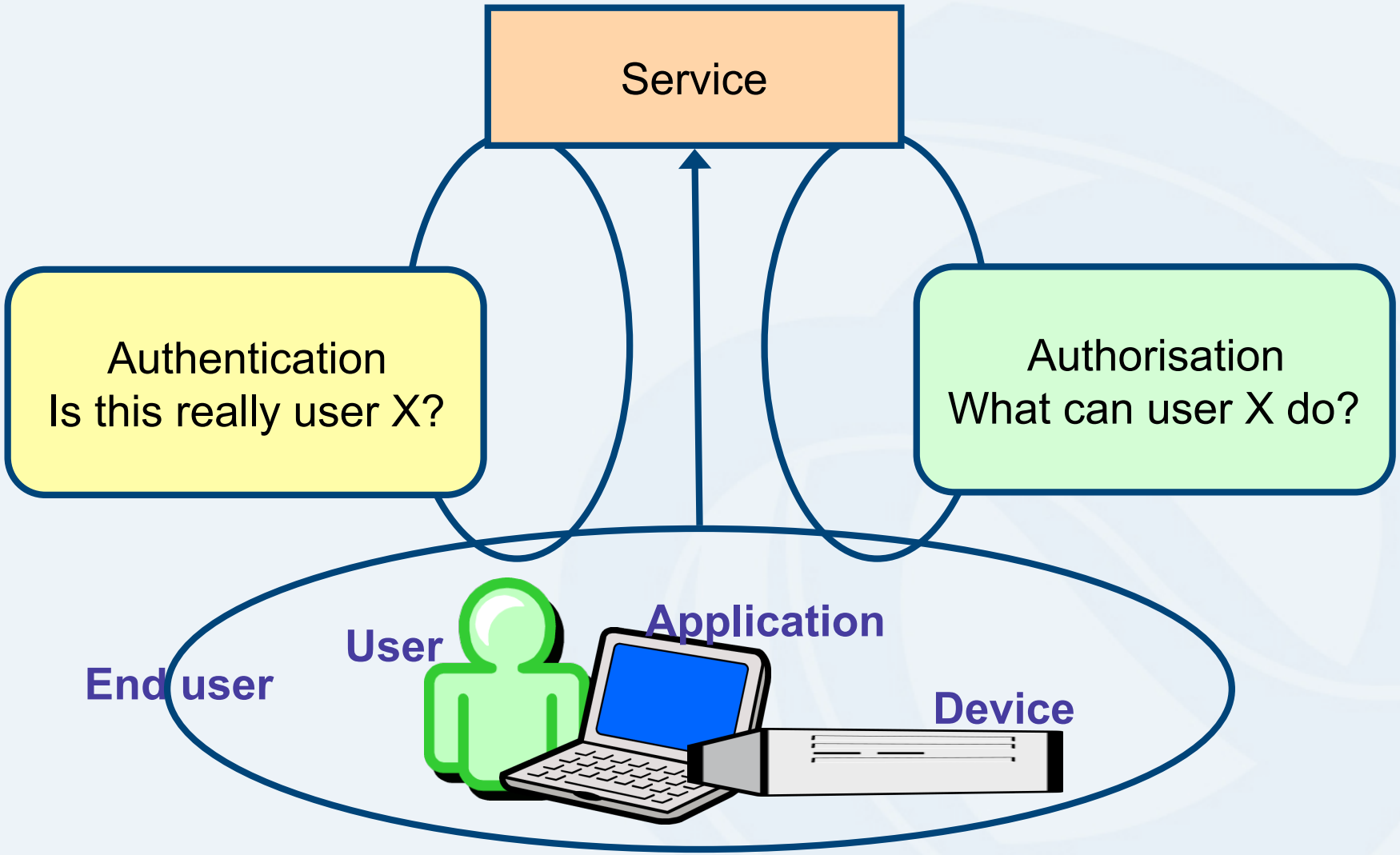
Authentication

- 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

Authentication and authorisation



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

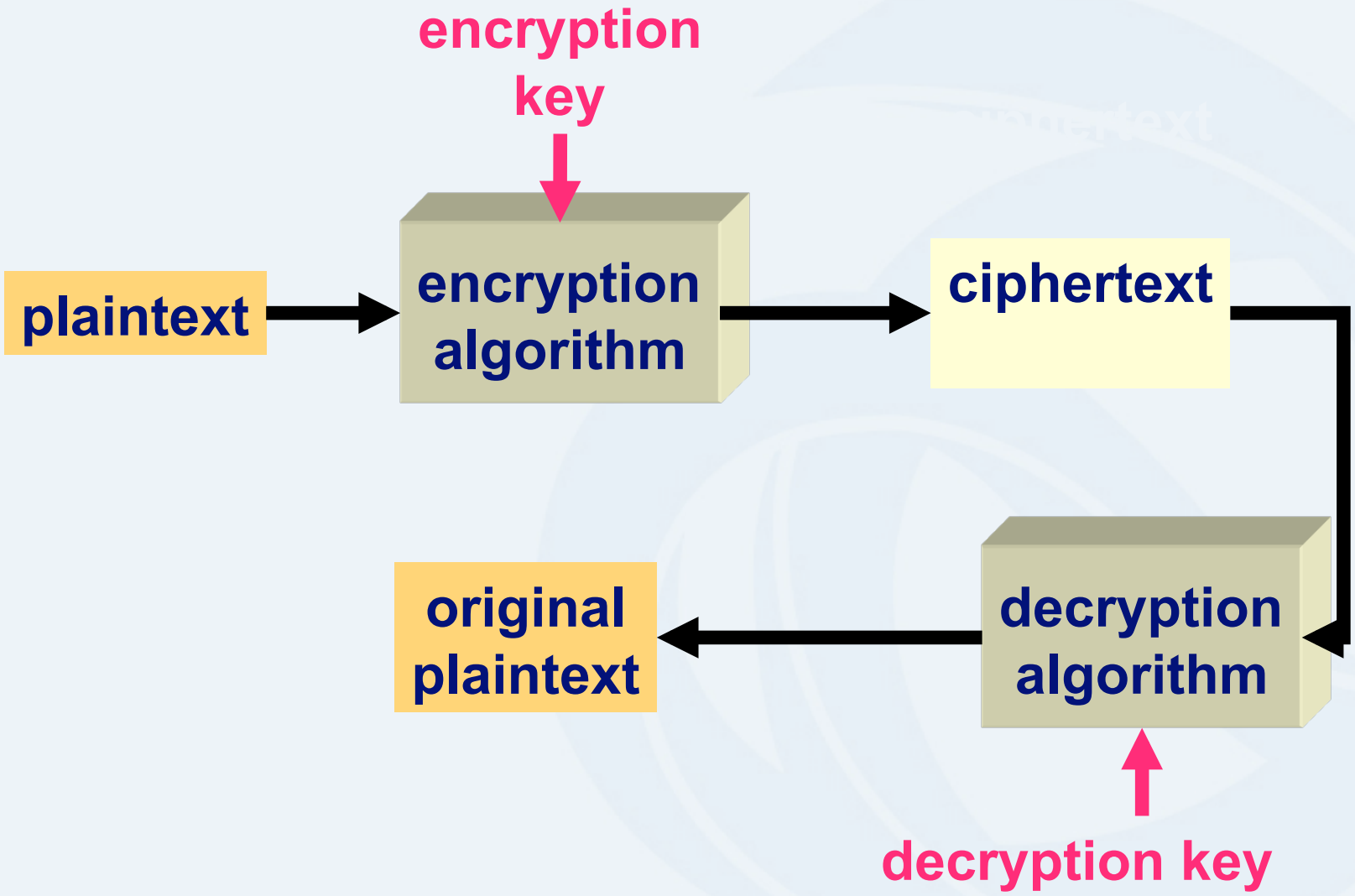
What is cryptography?

- 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

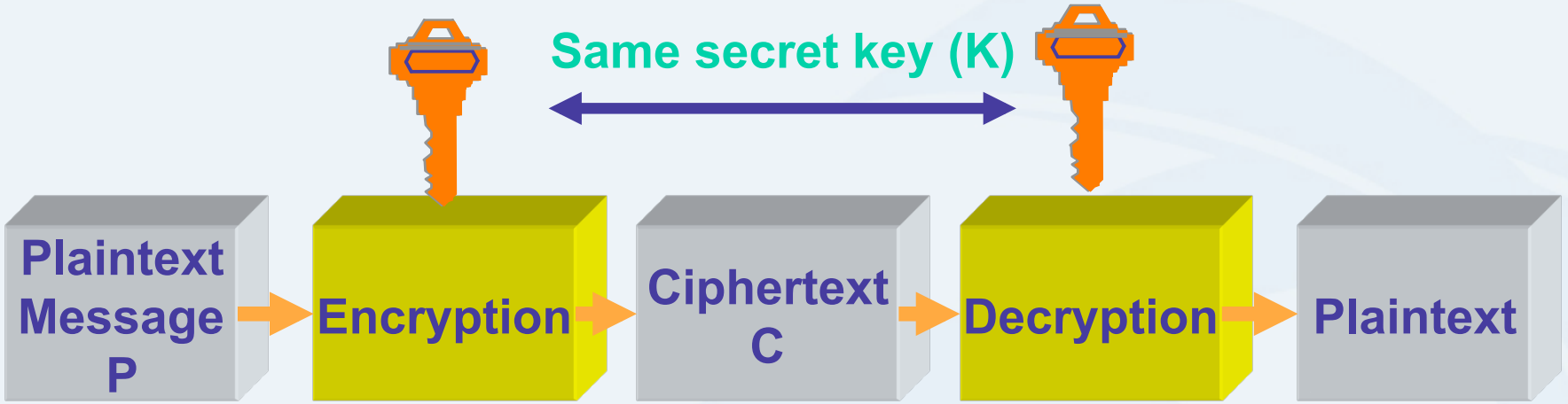
Terminology of cryptography

- 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 cipher



ciphertext transmitted over insecure network

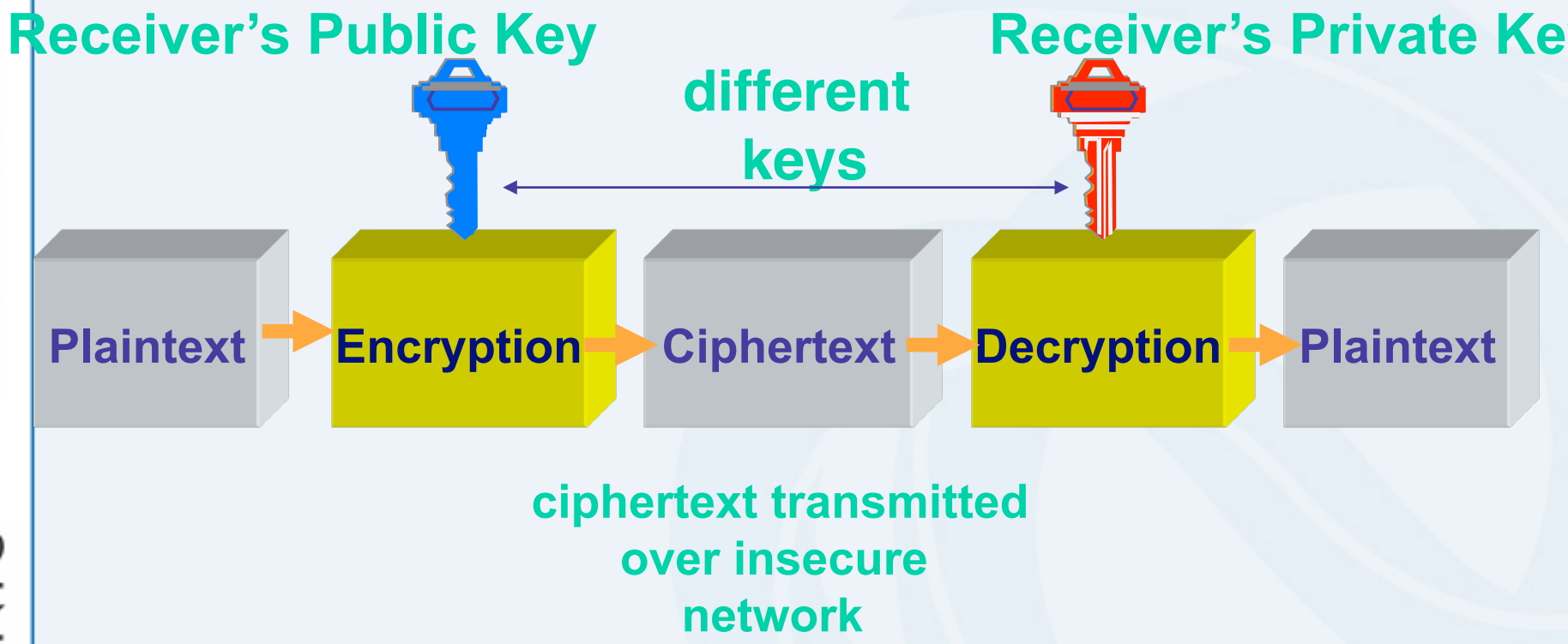
Symmetric ciphers

- 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
    - 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 $\mathbf{K_{pub}}$ (made public)
  - decryption key $\mathbf{K_{priv}}$ (kept private)
- Also known as public key cryptography
- Security depends on
  - algorithm strength
  - key size
  - protection measures of private key $\mathbf{K_{priv}}$

Asymmetric ciphers



No need to securely distribute key's

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

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: $C = E(P, K_{priv})$
  - Everyone knows Alice's corresponding public key, K_{pub}
    - Decryption: $P = D(C, K_{pub})$
    - 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

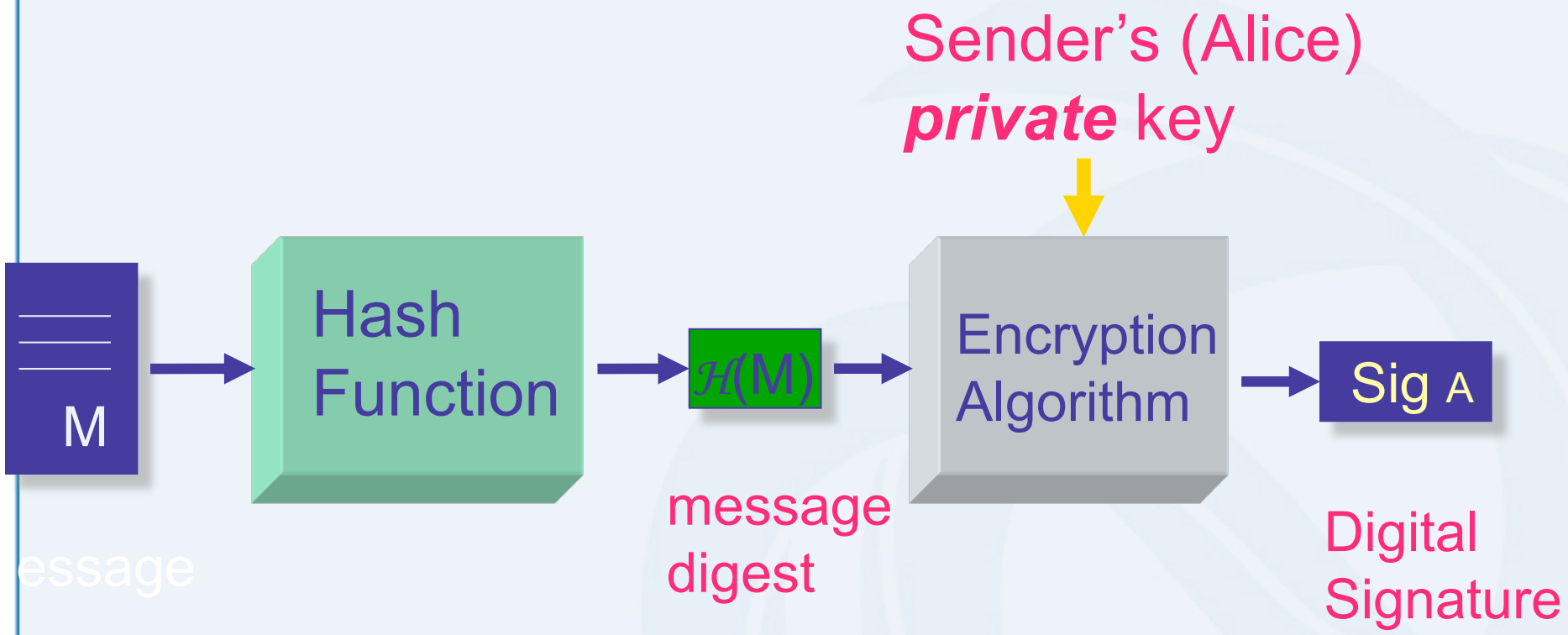
Asymmetric ciphers

- 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

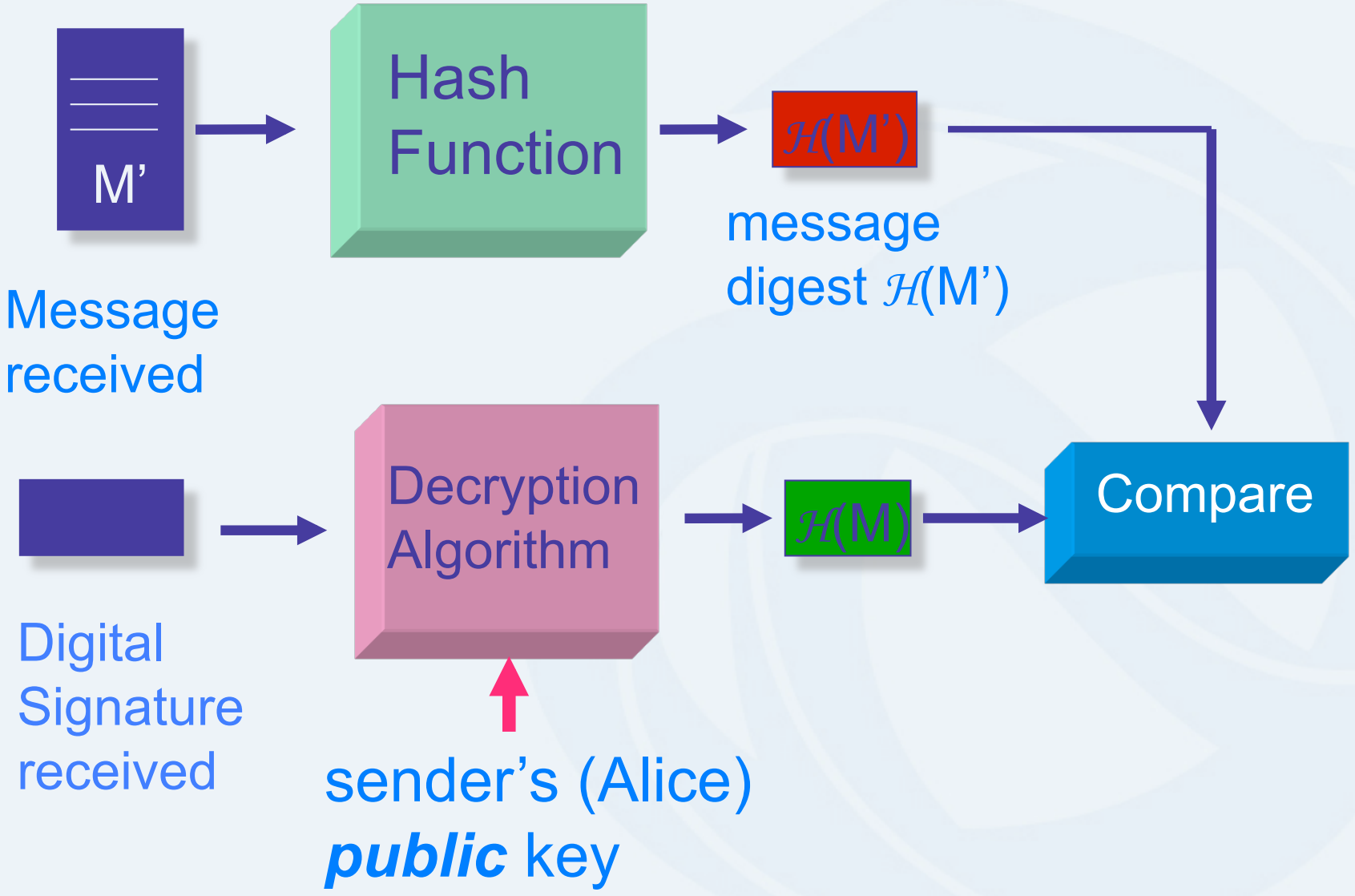
Creating an RSA Digital Signature



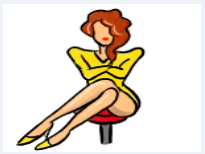
Authenticating message sender

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

Verifying an RSA Digital Signature



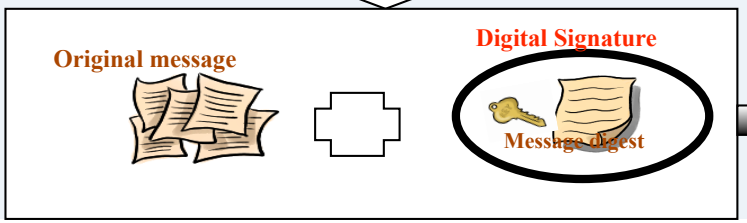
Digital Signing Process



Original message

Encrypt the message digest with the sender's private key

Digital Signature



Digital Verification Process

Received message

Digital Signature

Decrypt the message digest with the sender's public key

Message digest

Message digest

Compare 2 message digests generated by the sender and receiver

Signature verified

Signature verification Failed

Digital certificates

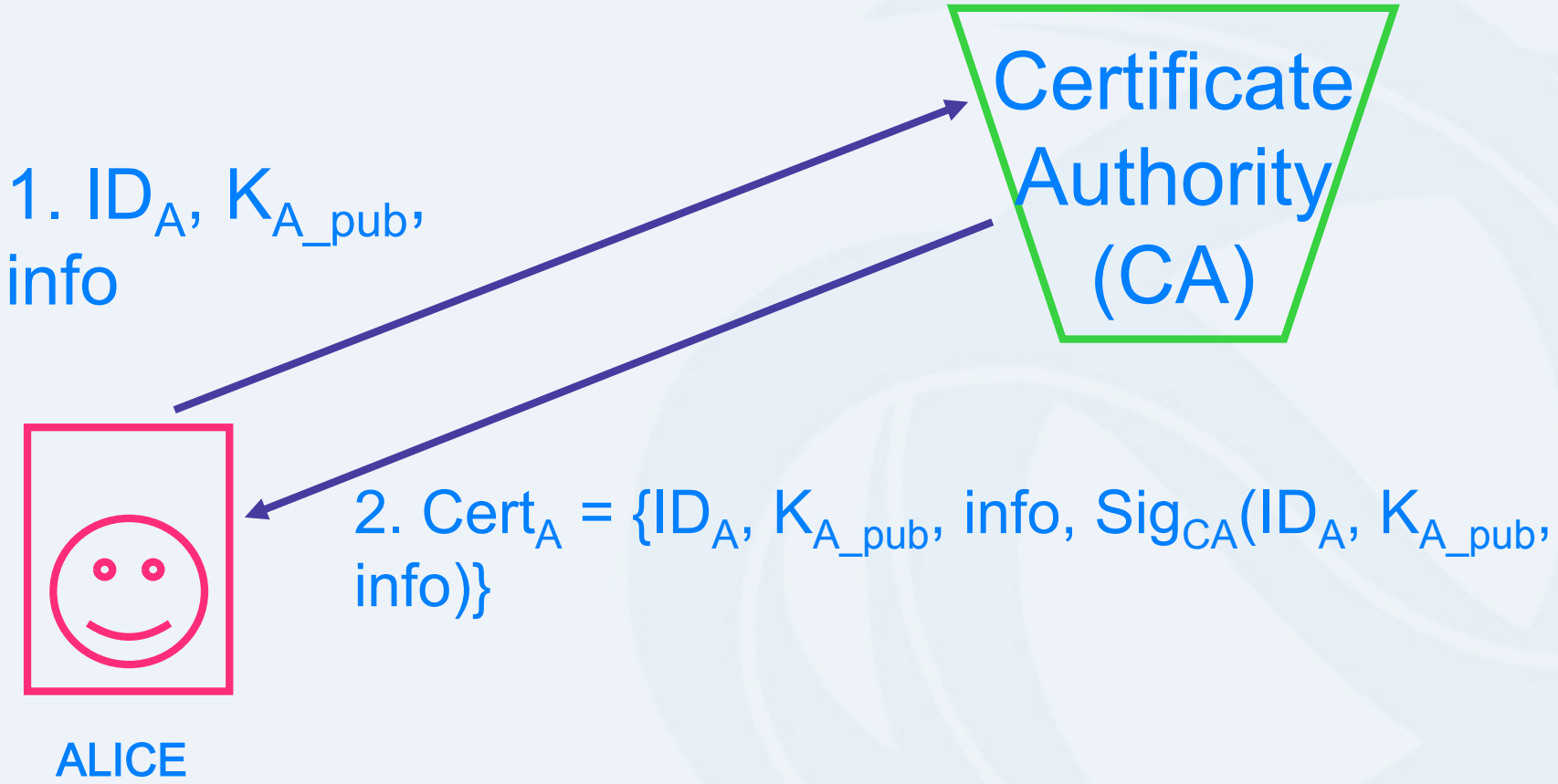
- Digital certificates deal with the problem of
  - binding a public key to an entity
  - A major legal issue related to eCommerce
- A digital certificate contains:
  - user's public key
  - user's ID
  - other information e.g. validity period
- Certificate examples:
  - X509 (standard)
  - PGP (Pretty 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:
  - $Cert_A = \{ID_A, K_{A\_pub}, info, Sig_{CA}(ID_A, K_{A\_pub}, info)\}$

Digital certificates

How does Alice obtain a digital certificate?



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

Network infrastructure security

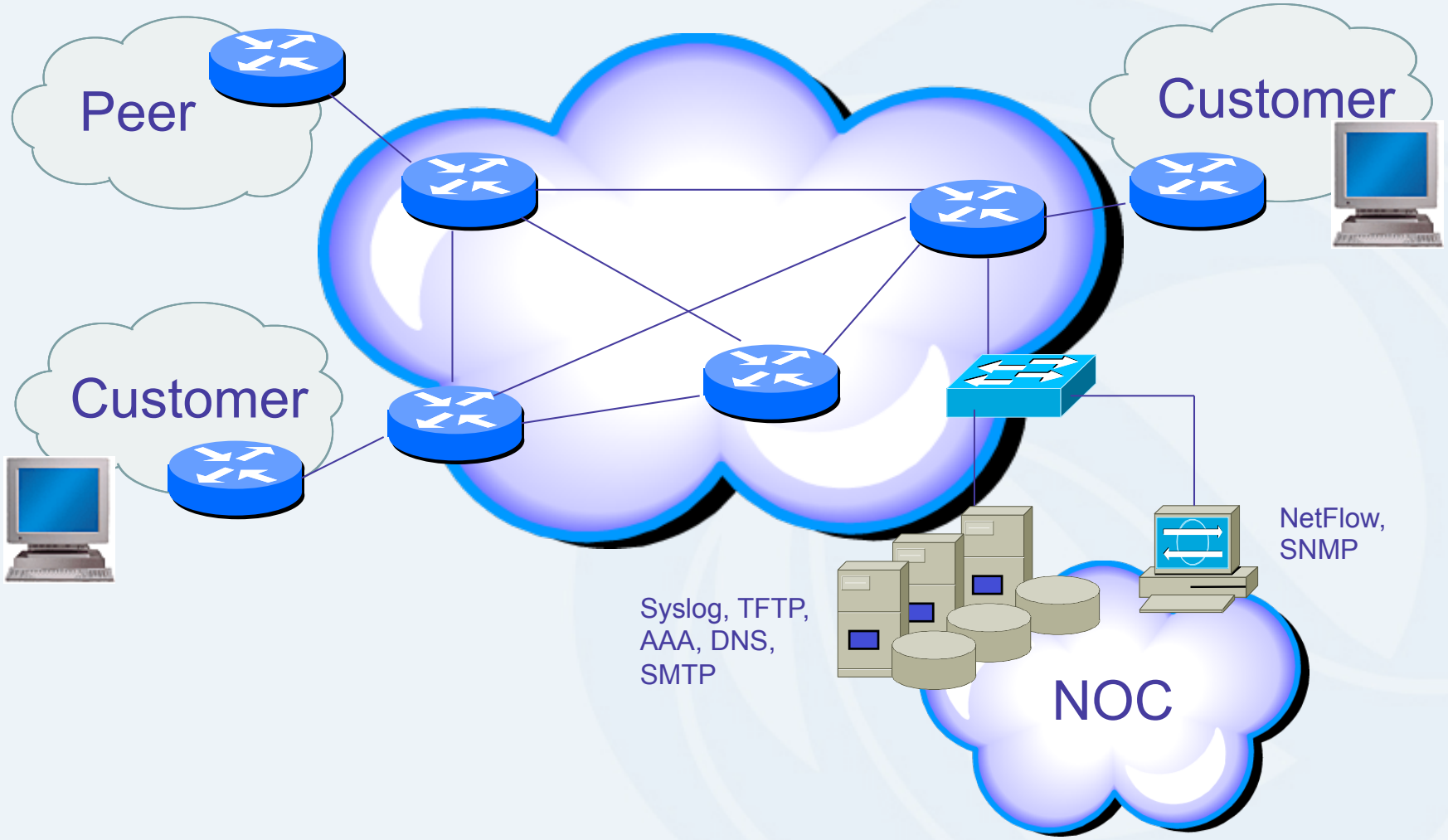
What are security goals?

- 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., BPG 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

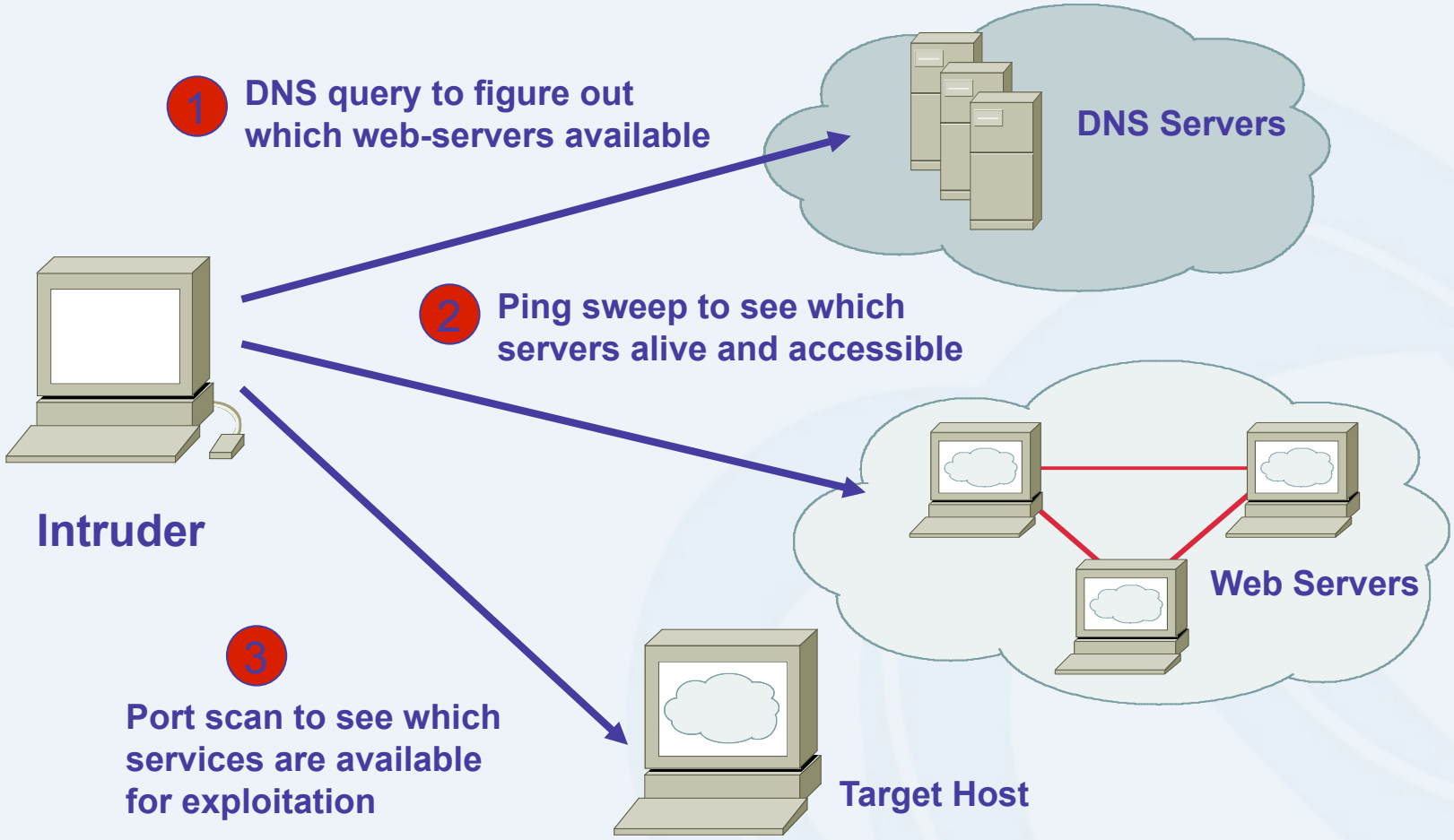
Cisco Technology Group view

- 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

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

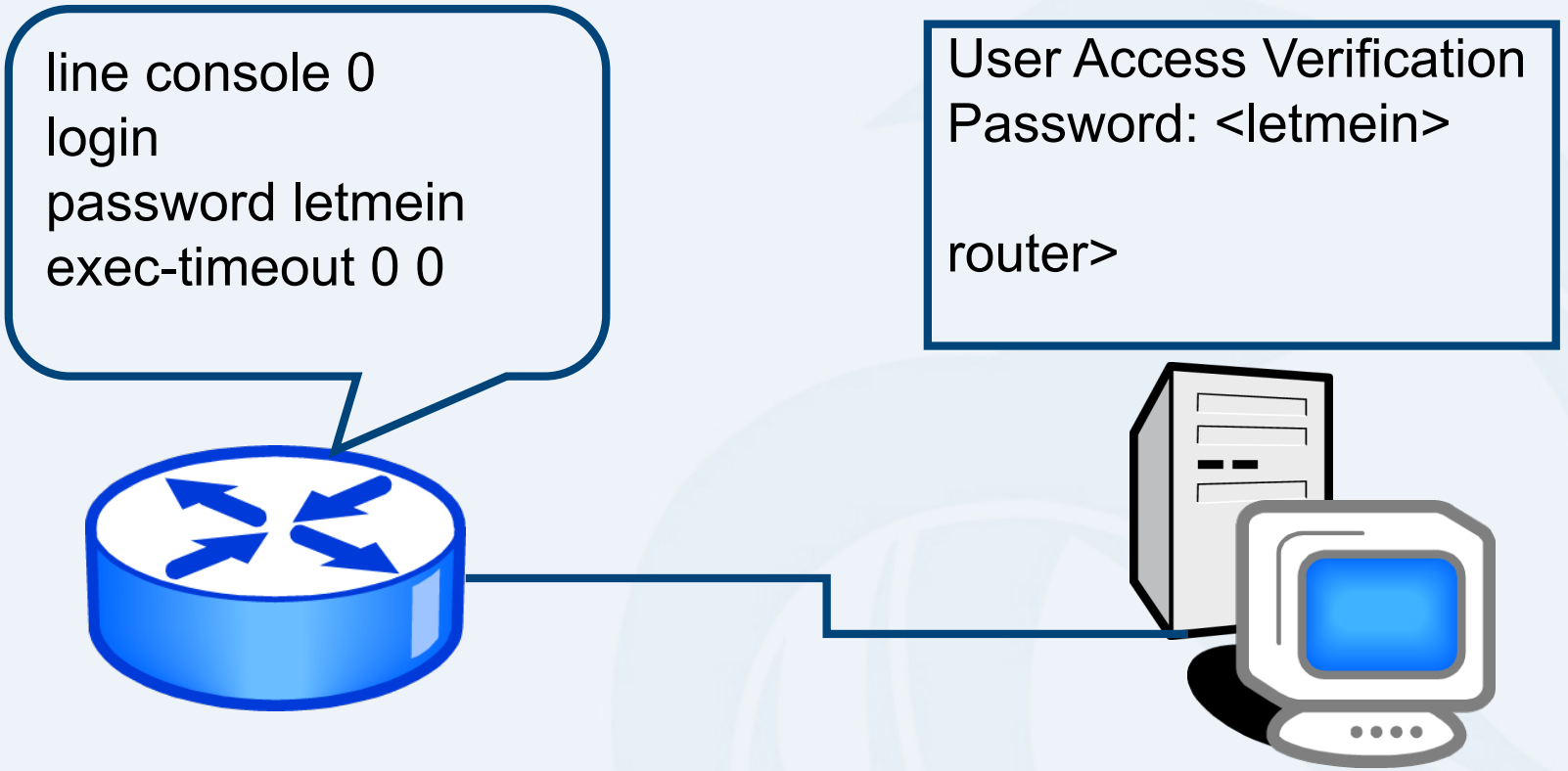
Device physical access

- 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

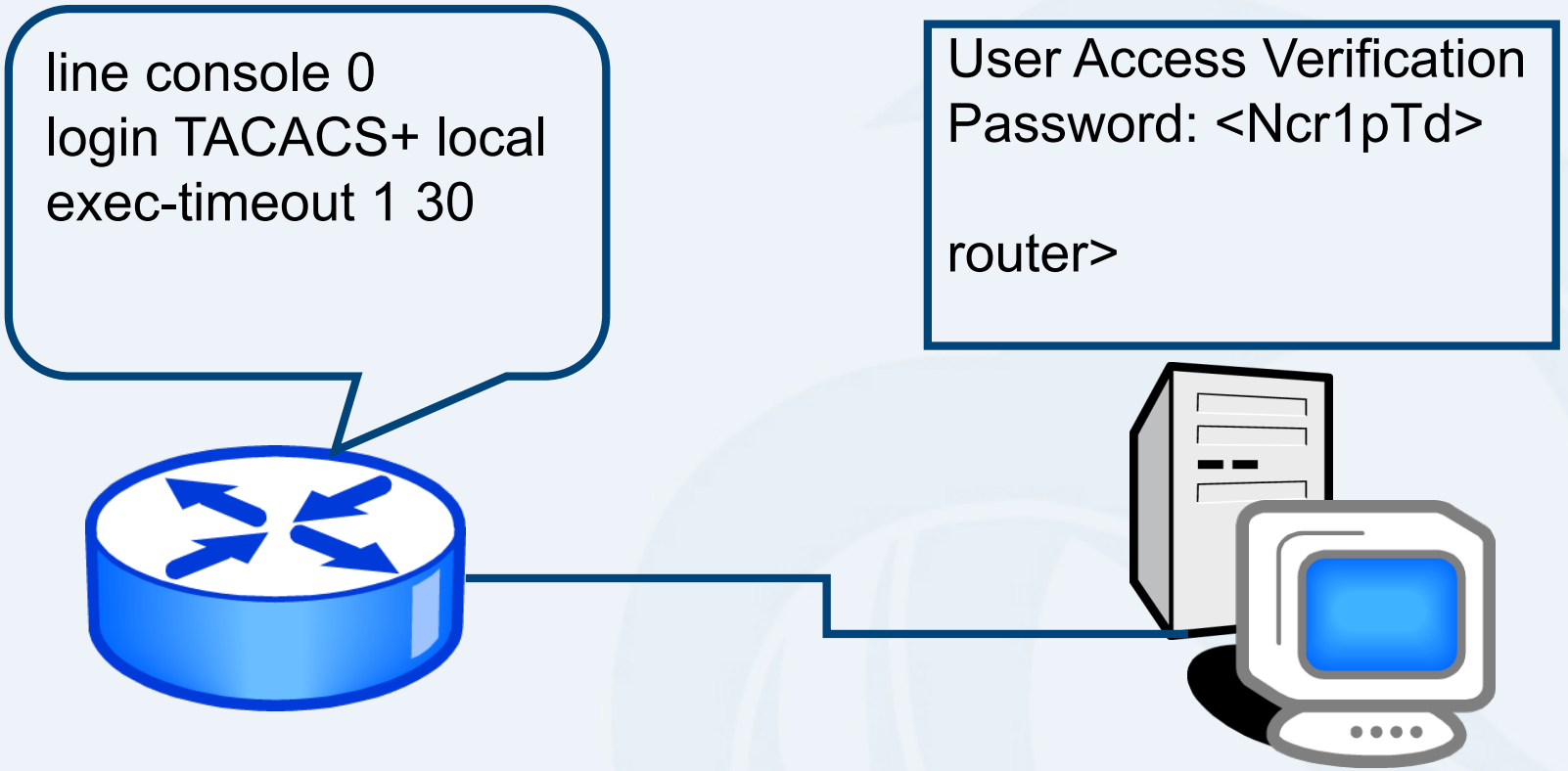
- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear texts (in config files)
- Never transfer passwords in clear texts (telnet Vs ssh)
- Authenticate individual users
- Restrict logical access to specified trusted hosts

Secure access to routers with passwords and timeouts



NOT SECURE!

Secure access to routers with passwords and timeouts



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$lSYSLeC6ookRSV7sI1vXR.
enable password 7 075F701C1E0F0C0B
!
username merike secret 5 $6$mffc$lmnGLeC67okLOMps
username staff secret 5 $6$ytjc$lchdLeC6o6klmR7s

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

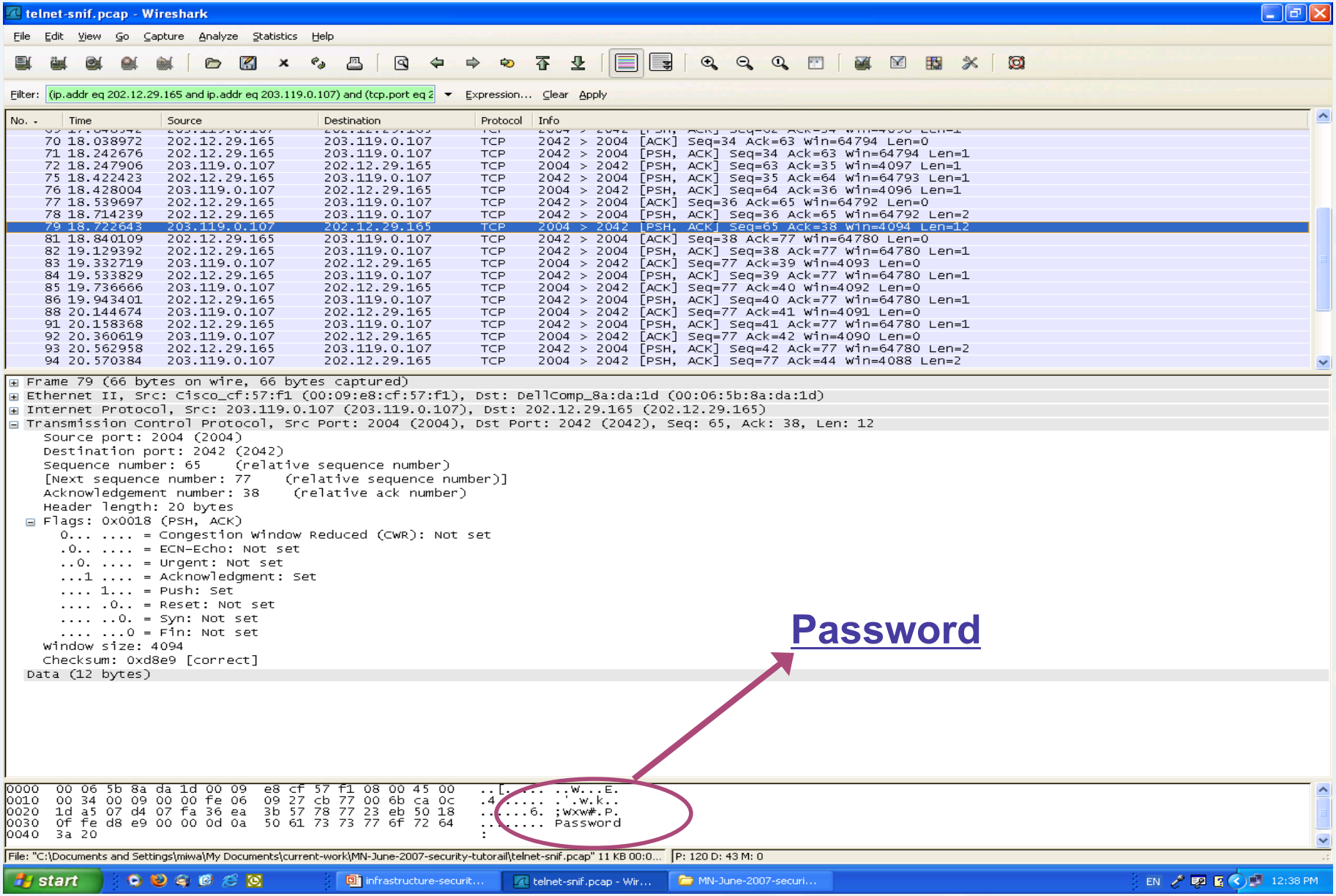
- Use filters to specifically permit hosts to access an infrastructure device
- Example

```
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



Password

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 poossible
- 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

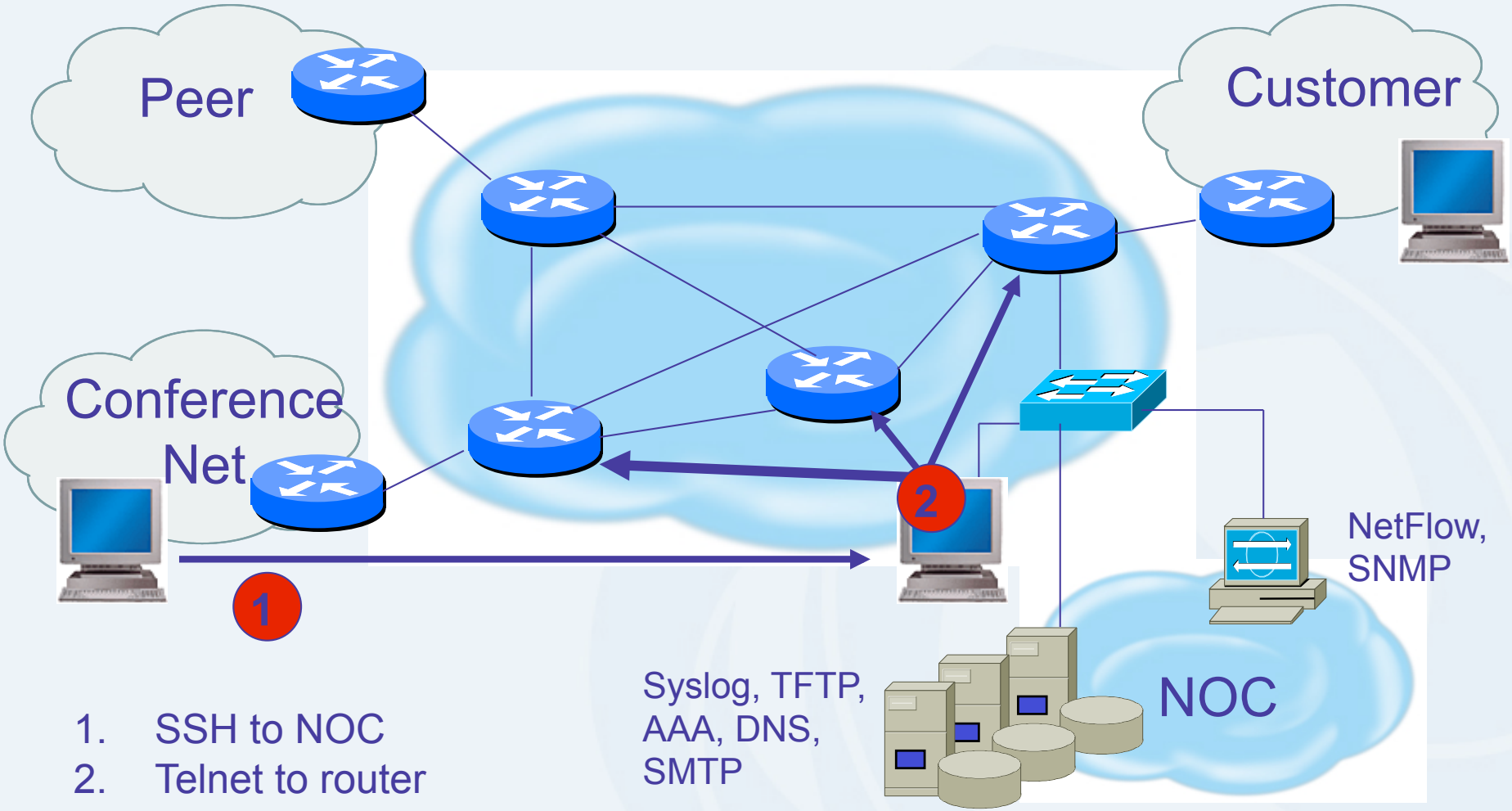
- Supported as of IOS 12.0S
- Ensure you have crypto image
- Set up SSH

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

- Add SSH as input transport

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

Telnet using SSH ‘Jumphost’



1. SSH to NOC
2. Telnet to router

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 fO0bAr RO 1
  - Access list 1 permit 127.1.3.5
- Explicitly direct SNMP traffic to an authorised management station.
  - Snmp-server host fO0bAr 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

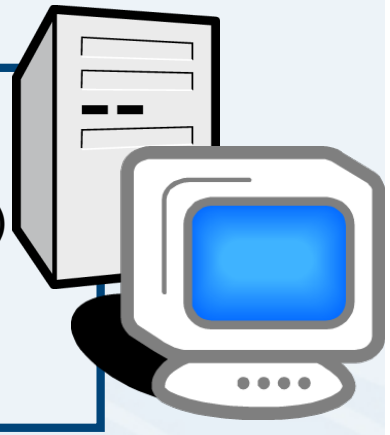
- Logging servers should be physically and logically secure
- Accept messages only from trusted hosts
- Encrypt log messages

Secure logging infrastructure

- Log enough information to be useful but not overwhelming
- Create backup plan for keeping track o 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/hardcisco/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 vodoka, 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"*

Questions?