Internet Protocols EBU5403 Security + Network Management D4

Michael Chai (michael.chai@qmul.ac.uk)
Richard Clegg (r.clegg@qmul.ac.uk)
Cunhua Pan (c.pan@qmul.ac.uk)

	Part 1	Part 2	Part 3	Part 4
Ecommerce + Telecoms 1	Richard Clegg		Cunhua Pan	
Telecoms 2	Michael Chai			

Structure of course

- **Part A**
  - Introduction to IP Networks
  - The Transport layer (part I)
- **Part B**
  - The Transport layer (part II)
  - The Network layer (part I)
  - Class test (open book exam in class)
- **Part C**
  - The Network layer (part II)
  - The Data link layer (part I)
  - Router lab tutorial (assessed labwork after this week)
- **Part D**
  - The Data link layer (part II)
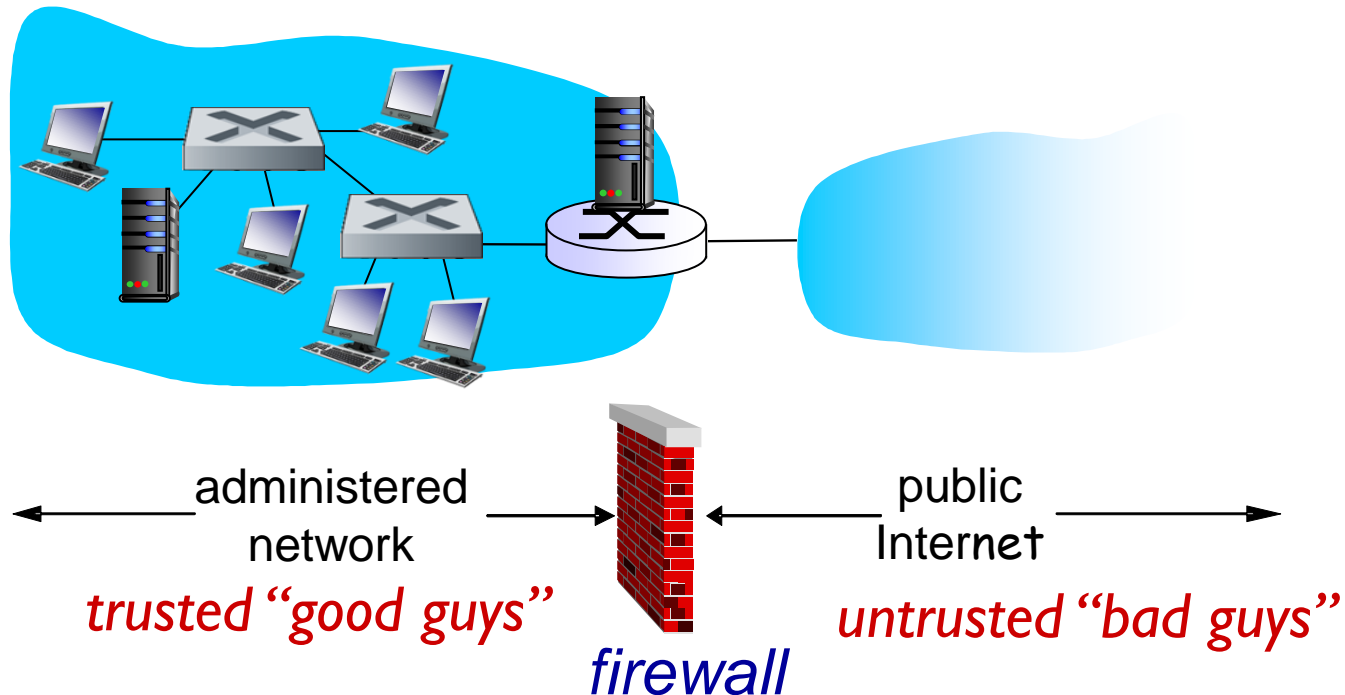 - Security and network management

Security and Network Management: outline

- Operational security: Firewalls and Gateway
- Network Management

Firewalls

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others

administered
network

trusted "good guys"

public
Internet

untrusted "bad guys"

firewall

Firewalls: why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections

prevent illegal modification/access of internal data

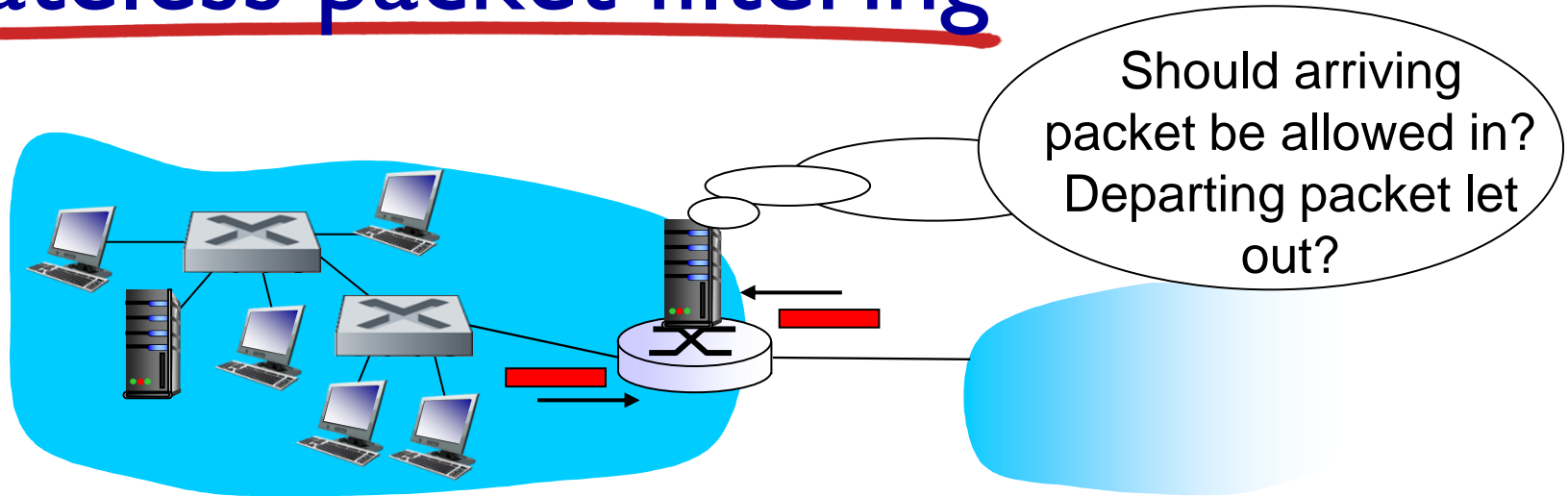- e.g., attacker replaces homepage with something else

allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering

Should arriving packet be allowed in? Departing packet let out?

- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- *example 1:* block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - *result:* all incoming, outgoing UDP flows and telnet connections are blocked
- *example 2:* block inbound TCP segments with ACK=0.
  - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

ACL: table of rules, applied top to bottom to incoming packets: (action, condition) pairs: looks like OpenFlow forwarding!

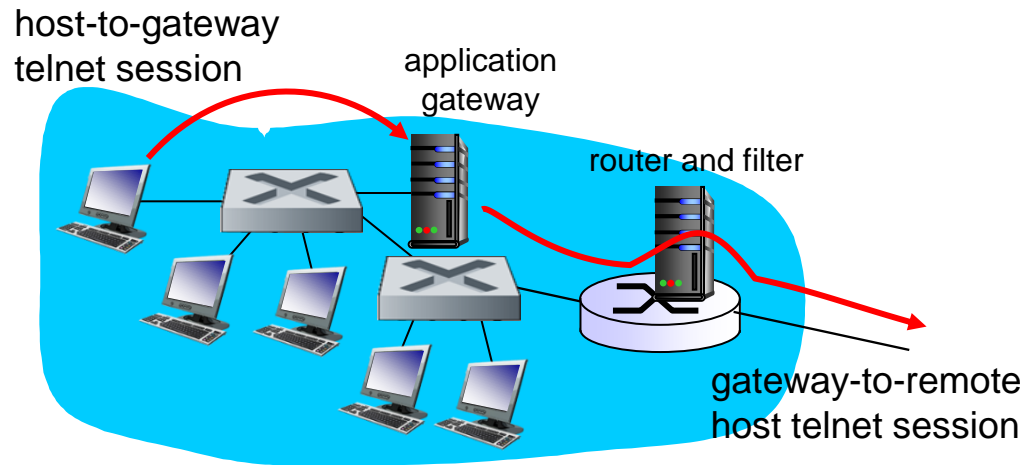| action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

- *stateless packet filter:* heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

Application gateways

- filter packets on application data as well as on IP/TCP/UDP fields.
- *example:* allow select internal users to telnet outside

host-to-gateway telnet session

application gateway

router and filter

gateway-to-remote host telnet session

1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.
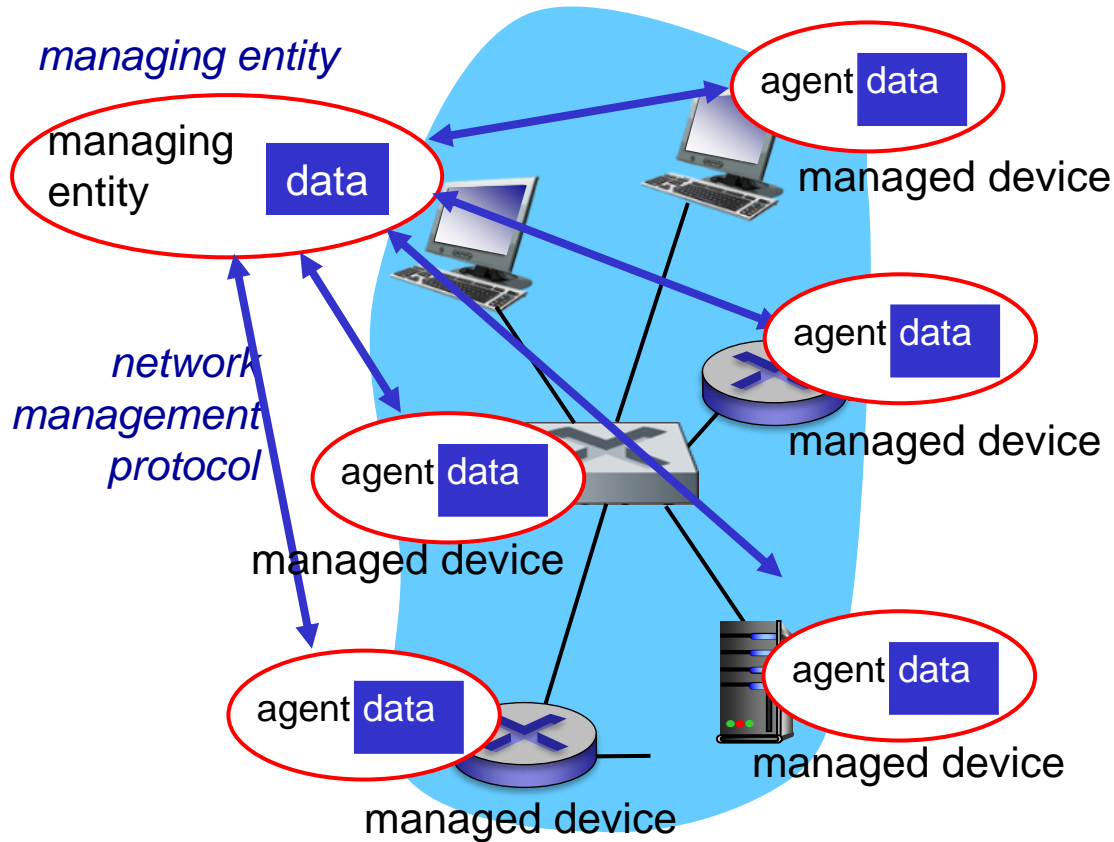
Security and Network Management: outline

- Operational security: firewalls and IDS
- Network Management

What is network management?

- **Autonomous systems (aka "network"):** 100s or 1000s of interacting hardware/software components
- How do we know when something is wrong?
  - Too much data on the network?
  - Router or switch is broken?
  - Part of network is slow or unreliable?
- Can't wait for user reports:
  - May take too long to process.
  - Might not have right cause ("my computer is working slowly").
  - May not spot some things (data back up is broken).
- Need automatic way to report on large number of hosts, switches and routers

Infrastructure for network management

definitions:

managing entity

managing entity

data

network management protocol

agent data

managed device

agent data

managed device

agent data

managed device

agent data

managed device

agent data

managed device

managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Network Management standards

OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol

- Internet roots
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

Simple Network Management Protocol (SNMP)
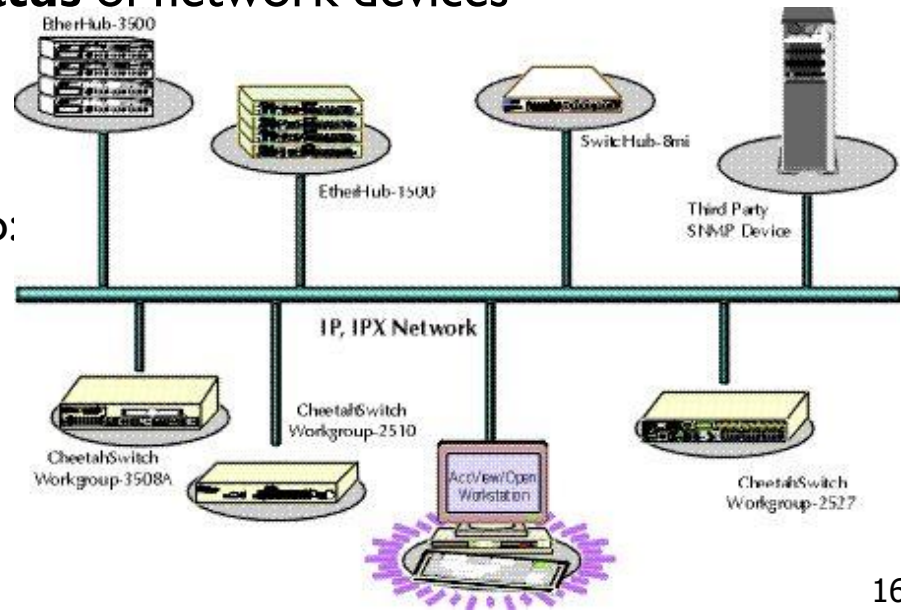
- ## What is it?
  - A Protocol that Facilitates the exchange of management information
  - between network devices.

- ## Why was it developed?
  - To **control and monitor status** of network devices

- ## How is it beneficial?
  - Enables network administrators to:
    - Manage network performance
   - Find and solve network problems
    - Plan for network growth

SNMP Basic Components

- Network Management station
  - Collects and stores management information, and makes this information available to NMS using SNMP
  - Could be a work station or PC

- Network Management System (NMS)
  - Executes applications that monitor and control managed devices

- Agent
  - A network-management software module that resides in a managed device

- Management Information Base (MIB)
  - Used by both the manager and the agent to store and exchange management information

Network Management Architecture

NMS

User Interface

Network Management Application

Management Station
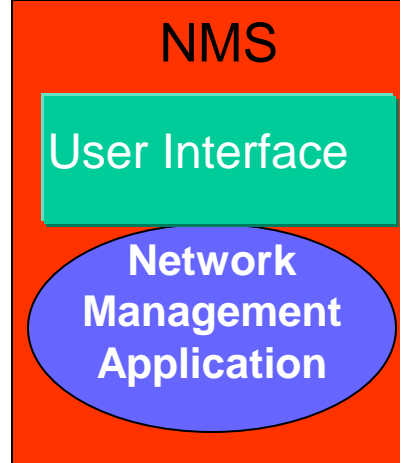
SNMP

SNMP
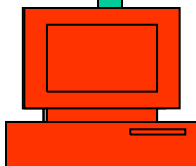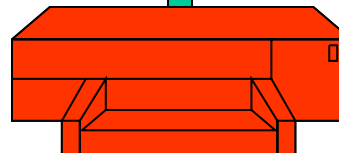
SNMP

AGENT

AGENT
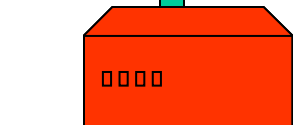
AGENT

MIB

MIB

MIB

Managed Devices

Host

Printer

Router

18

What have we learned?

- Operational security
  - Firewalls: Packet filtering and Access Control
- Network Management
  - Simple Network Management Protocol