



# Security Issues

**Dr Steven Furnell**

Network Research Group

University of Plymouth

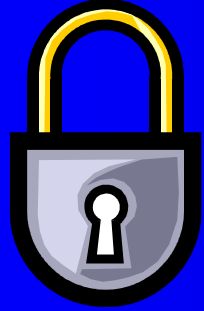
Plymouth

United Kingdom

# Session Content

- IT security concepts
- Authentication approaches
- Firewall technologies

# IT Security concepts



# What is security?

Computer security is the protection of a company's assets by ensuring the safe, uninterrupted operation of the system and the safeguarding of its computer, programs and data files.

Prof. Harold J Highland  
State University of New York

# Why we need security

- The Internet is host to numerous threats:
  - Viruses, worms, Trojan Horses
  - Hacking, Denial of service attacks
  - Masquerading, spoofing
  - Fraud, data theft, malicious damage
- The impacts of these can be far-reaching . . .

# Some notable incidents

- The Love Bug (May 2000)
  - A worm program distributed via email, using automation features of Microsoft Outlook
  - Estimated to have been received by around 90% of computers worldwide
    - notable victims included the Pentagon, the UK Parliament and the BBC
    - numerous others shut down their email systems to avoid infection
  - Estimated to have caused at least \$7 billion in damage

## Notable incidents (cont.)

- Denial of Service (February 2000):
  - Widespread distributed DoS attack
  - Utilised tools such as Tribal Flood Net (TFN), and Trinoo - freely available on the Internet.
  - Affected numerous popular sites, including Amazon.com, eBay and CNN.
  - Significant impact : e,g, within a few minutes, the Amazon.com web site became 98.5% unavailable to legitimate users
  - average performance of the net was “degraded by as much as 26.8%” (Keynote, USA)

# Notable incidents (cont.)

- Defacement of web sites



UK Labour Party (Dec. 1996)



RSA Securty (Feb. 2000)

# Security requirements

- Security involves the maintenance of:
  - Confidentiality
  - Integrity
  - Availability
  - Accountability

# Confidentiality

- Prevention of unauthorised information disclosure.
- Data access must be restricted to authorised entities with a legitimate “need to know”.
- Seriousness of disclosure often dictated by whether it occurs to an unauthorised member of the same organisation or a total outsider

# Integrity

- May refer to systems and data.
- Users must have confidence that :
  - the same information can be retrieved as was originally entered;
  - internal system processes work as expected / claimed.
- May be compromised as a result of accidental error or malicious activity.

# Availability

- The property of being accessible and usable on demand by an authorised entity
- Encompasses :
  - prevention of unauthorised withholding of information or resources;
  - safeguards against system failure.
- Seriousness of denial of service generally increases depending upon the period of unavailability

# Accountability

- The property that ensures that actions of an entity may be traced uniquely to that entity
- Encompasses :
  - Staff activity
  - System behaviour
- Related to the issue of non-repudiation

# Types of Security



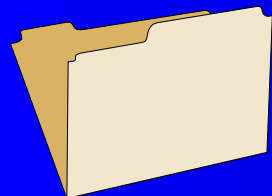
## Physical

- e.g environmental protection



## Logical / System / Technical

- e.g. authentication, secure communications



## Procedural / Personnel

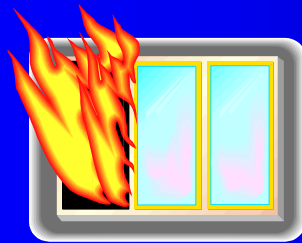
- e.g security policy

# Terminology

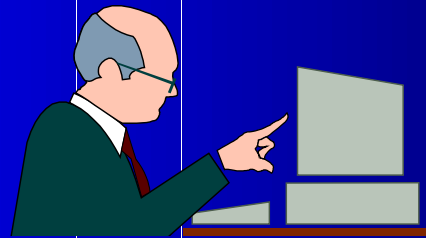
- *Asset*
  - Everything and everybody forming part of an information system.
- *Threat*
  - A potential violation of security (ISO 7498-2)
- *Vulnerability*
  - The likelihood of a threat to become a reality

# Threats

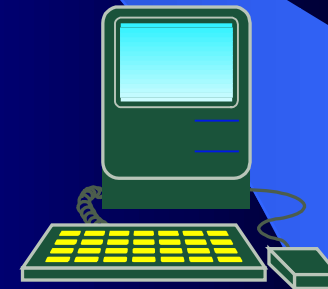
Accidental or Deliberate



**Physical**  
e.g. fire,  
flood,  
power failure;



**Human**  
e.g. operator errors,  
misuse of resources,  
hacking, viruses.



**Equipment**  
e.g. CPU,  
network,  
storage failure;

# More Terminology

- *Risk*
  - Threats and vulnerabilities of a particular asset
- *Countermeasure*
  - A mechanism or procedure used to reduce one or more elements of risk
- *Impact*
  - The effect of a failure to preserve confidentiality, integrity and/or availability.

# Impact Types

The effects of a failure to preserve CIAA :

- Disclosure
- Denial
- Destruction
- Modification

} relate to *availability*

with particular consequences

# Consequences

- Financial Loss
- Embarrassment
- Breach of Commercial Confidentiality
- Breach of Personal Privacy
- Legal Liability
- Disruption to activities
- Threat to personal safety

# Handling Risk

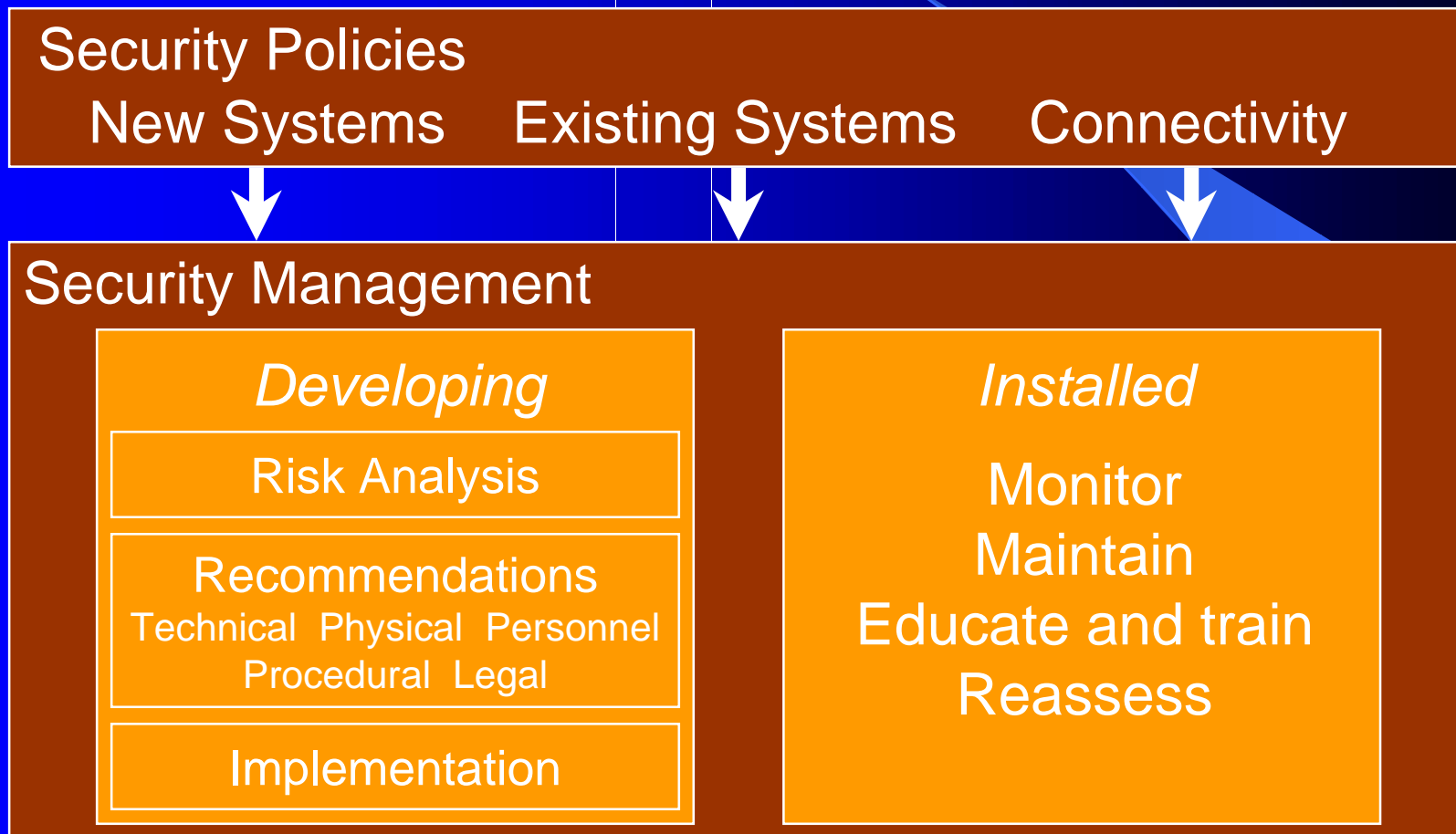
- Removal System is modified so that a particular feature, and the associated risk, is removed.
- Reduction Security measures are used to reduce risk to an acceptable level
- Retention Nothing is done - the risk is small and insignificant
- Transfer The system is unchanged, but the risk is transferred to another party (e.g. via an insurance policy).

# Management need to know . . .



- What is at risk
- the cost incurred if the risk becomes a breach
- safeguards that can be implemented to reduce risk
- the cost of the safeguards
- the risk reduction that will result from implementation of specific safeguards

# Managing Security



## Managing Security (cont.)

- Monitor effectiveness of the technical measures
- Monitor compliance by staff, via manual and computer records
- Maintain protection by acting upon monitored information where necessary
- Provide general and specialist training for all staff
- Periodically reassess whether countermeasures are still relevant to current threats
- Ensure that new systems are developed / procured in accordance with policy

# Conclusion

- 100% security is not an achievable goal
- Security costs money :
  - Must determine the appropriate level of countermeasures for the assets requiring protection;
  - Require a means to address the problem in a consistent and structured manner.
  - Baseline security helps, but is not a total solution.

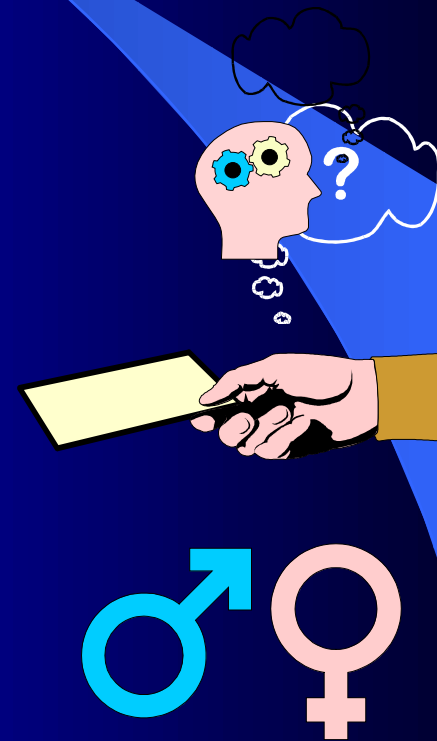
# Approaches to authentication

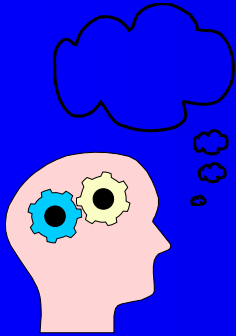
# User Identification & Authentication

- Users must be *identified* to enable :
  - user-specific access controls;
  - individual accountability for activities.
- Claimed identities must be *authenticated* :
  - first line of system protection;
  - safeguards against abuse by external parties or unauthorised insiders;

# Authentication Strategies

- Three main approaches to authentication :
  - Something the user *knows* (e.g. password or PIN)
  - Something the user *has* (e.g. a card or other token)
  - Something the user *is* (i.e. a biometric characteristic)





# Traditional Passwords

- Most commonly used means of authentication in IT systems
- *Advantages*
  - ✓ Conceptually simple for designers and users.
  - ✓ Can provide effective protection if used correctly.
- *Disadvantages*
  - ✗ Protection often compromised by users.

# Password Weaknesses

- Passwords are often :
  - badly selected (and easily guessed) :
    - dictionary words;
    - personal data (names, car registration etc.).
  - written down;
  - shared with colleagues;
  - infrequently changed;
  - the same on multiple systems;
  - only required at the start of a session.

# Improving Password Systems

“Use them like a toothbrush.  
Change them often and don’t share  
them with friends”

Cliff Stoll

*IT security expert and  
author of “The Cuckoo’s Egg”*

# Improving Password Systems

- Encourage better selection
- Password ageing
- Password filtering
- Prevention of password reuse
- System generated passwords
- One-time passwords

***Decreases user-friendliness?***



# Token-based Authentication

- Based upon possession of physical identifier.
- Examples : *Magnetic cards;*  
*Smart cards;*  
*Radio transmitter devices.*
- May be combined with secret knowledge to create 2-stage authentication.



# Token-based Authentication (cont.)

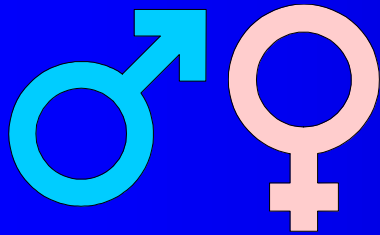
- *Advantages*

- ✓ Avoids masquerade potential of passwords;
- ✓ Users cannot share their access privileges;
- ✓ Increased awareness of likely compromise;
- ✓ An attacker must counterfeit or steal a token before gaining access;
- ✓ Illegal possession of a token can be used as evidence of an attempt to gain unauthorised access.



# Token-based Authentication (cont.)

- *Disadvantages*
  - ✗ More expensive to implement (esp. large scale);
  - ✗ Tokens can still be lost or stolen;
  - ✗ Combining with secret knowledge reintroduces some of the disadvantages of that approach.



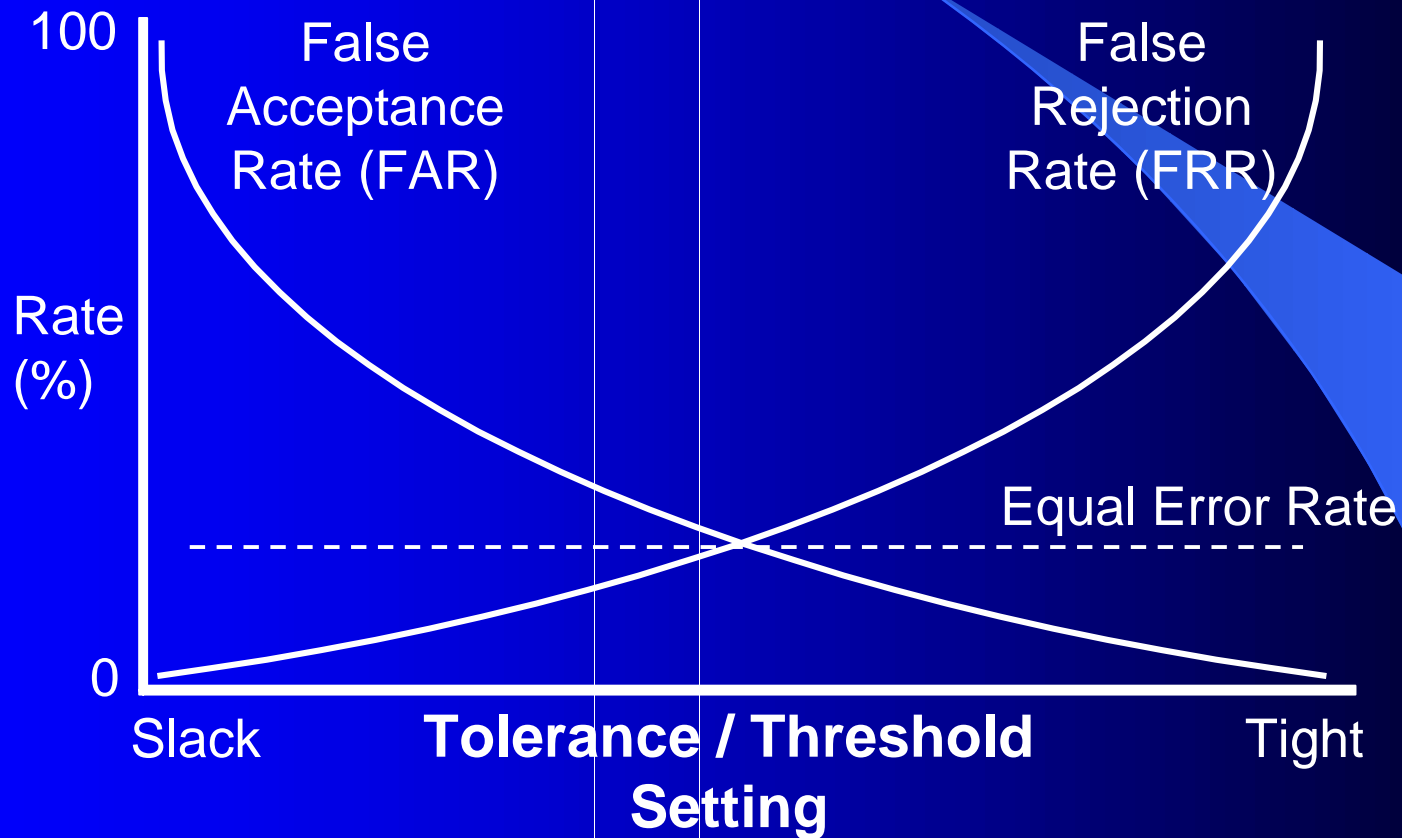
# Biometric Approaches

Physiological	Behavioural
<ul style="list-style-type: none"><li>• Fingerprints</li><li>• Hand geometry</li><li>• Vein checking</li><li>• Faceprint</li><li>• Facial thermogram</li><li>• Iris scanning</li></ul>	<ul style="list-style-type: none"><li>• Voice recognition</li><li>• Signature verification</li><li>• Keystroke analysis</li><li>• Mouse dynamics</li></ul>

# Error Rates

- False Acceptance Rate (FAR)
  - errors where impostors are falsely believed to be legitimate users;
  - also known as Impostor Pass Rate (IPR).
- False Rejection Rate (FRR)
  - errors where the system falsely identifies the legitimate user as an impostor;
  - also known as False Alarm Rate (FAR!).

# FAR and FRR relationship



Increasing end-user rejection →

# Firewall Technologies

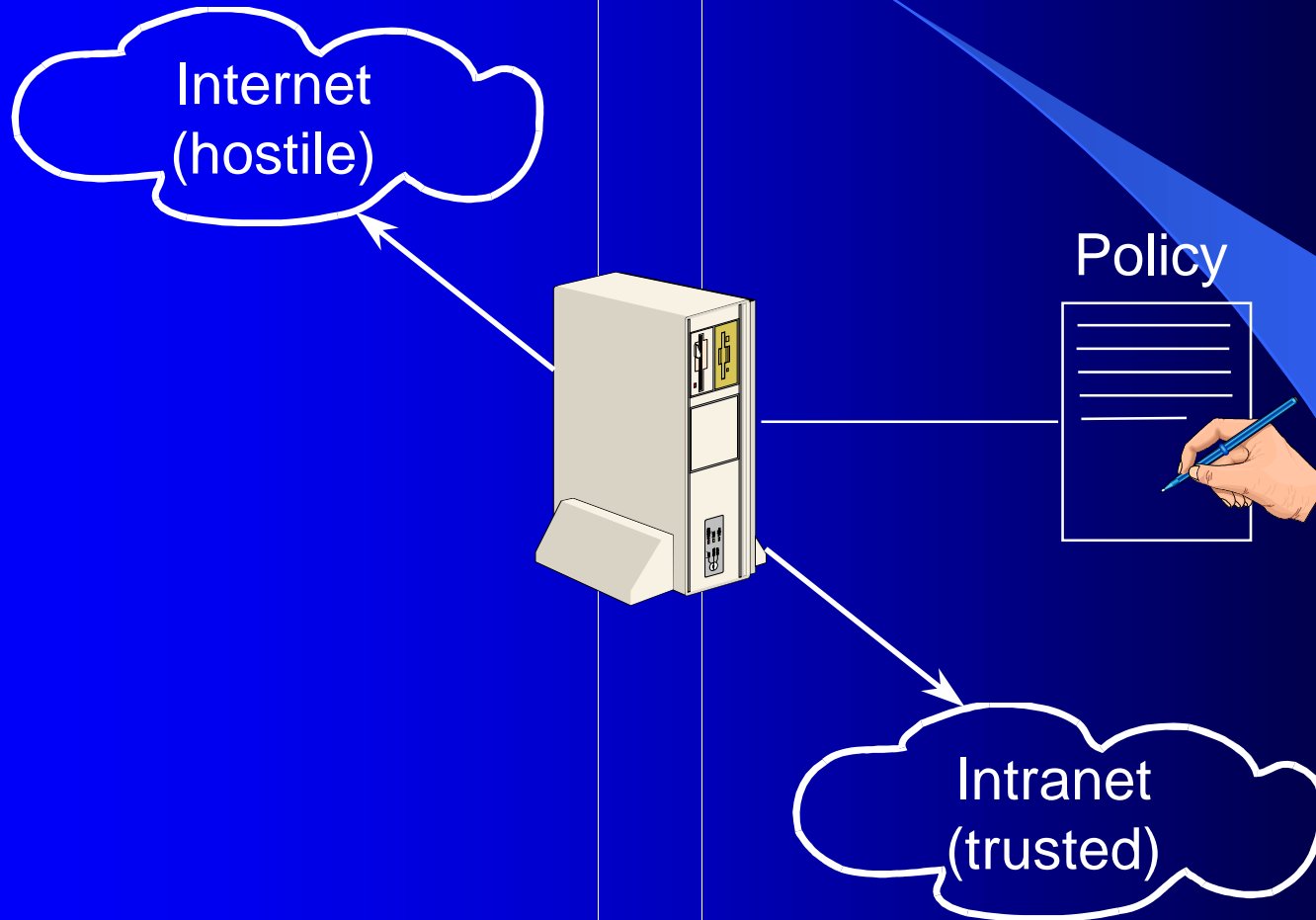
# Introduction

- Allowing a business / company intranet completely open access to / from the Internet may lead to :
  - hackers attempting to gain unauthorised access;
  - competitors attempting to impede the business electronically;
  - disclosure or modification of business information.
- Require some kind of (selective) barrier

# The Firewall Concept

- Purpose of firewall :
  - Control access to or from a protected network;
  - Implements network access policy
    - connections pass through firewall and are examined / evaluated.
- May be implemented in :
  - router; PC; host; collection of hosts.
- Normally located at a high-level gateway
  - e.g. site's Internet connection
- Firewall system AKA “Bastion Host”

# The Firewall Concept (cont.)



# The need for Firewalls

- Traditionally rely on security of individual hosts



- As number of hosts increases :
  - less manageable;
  - more chance of administrative mistakes / lapses.
  - reduced likelihood of uniform security
- Firewall helps to increase overall security of the subnetwork

# Grades of Firewall Security

(Source : Network & Internet Security)

Function



Firewall Security Enhancement

No  
Access

Filters  
Gateways  
Name Service  
Mail Handling  
Confidentiality  
Data Integrity

Filters  
Gateways  
Name Service  
Mail Handling  
-----  
Secure OS

Filters  
Gateways  
Name Service  
Mail Handling

Filters  
Gateways

Filters

Open  
Internet  
Access

No  
Security

Grades of Firewall

Complete  
Security



# Packet Filtering Firewall

- Operates at IP packet level
- Filters packets as they pass between router interfaces
- A number of packet features may provide basis for filtering :
  - source / destination IP addresses
  - source / destination port numbers

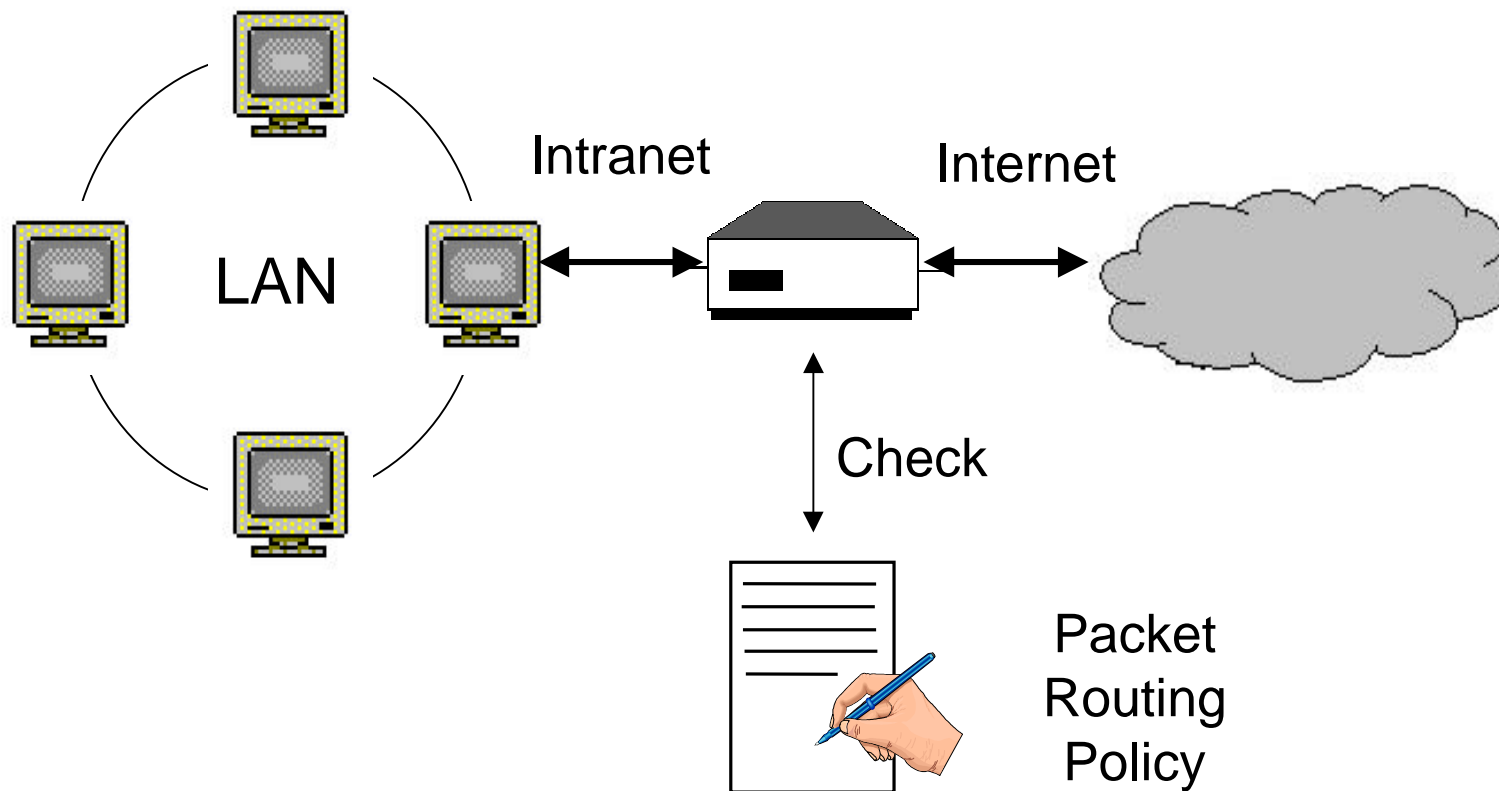
# Packet Filtering Firewall (cont.)

- Source IP address :
  - can control which machines on the internal network may access the Internet;
  - can control which machines from outside may access the internal network.
- Destination IP address :
  - on incoming packets, can filter what machines can be contacted for which services (e.g. WWW / email servers);
  - on outgoing packets, can control which sites internal users can access.

# Packet Filtering Firewall (cont.)

- Source and Destination port numbers :
  - Many standard Internet services are offered via “well known” destination ports, e.g. :
    - HTTP = port 80;
    - SMTP = port 25;
    - FTP = port 21;
    - Telnet = port 23;
    - RPC = port 111.
  - Can control the accessibility of specific services.

# Packet Filtering Firewall (cont.)



# Packet Filtering Advantages

- Functionality is part of standard router configuration software
  - no special hardware / software required.
- Flexible
- Fast
- Installation requires no action on the part of users

# Packet Filtering Disadvantages

- Filtering rules are complex to specify, especially when selective blocking of services required.
- Usually no testing facility to enable correctness of rules to be verified;
- Routers may not provide logging capability, so dangerous packets may not be detected until a break-in has occurred.

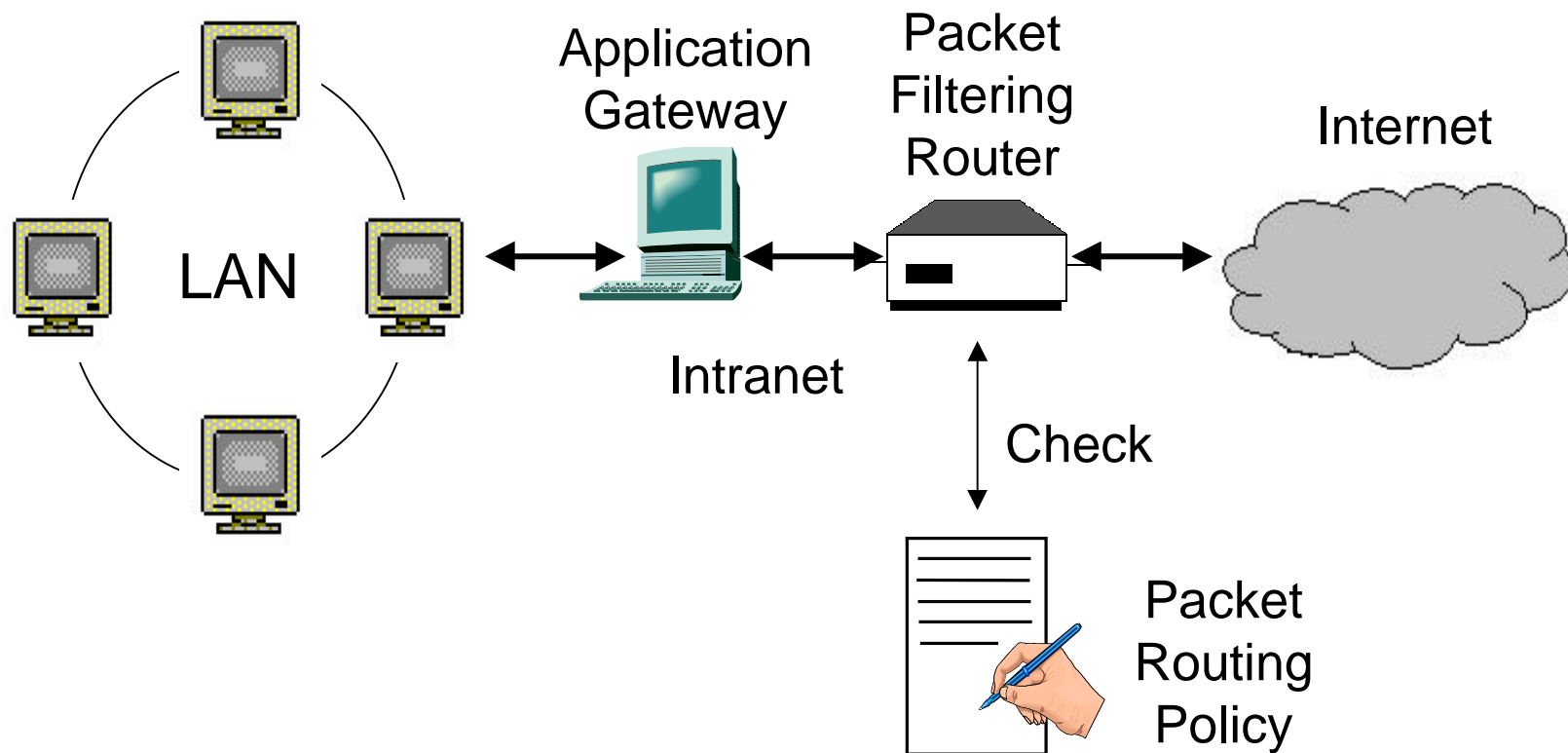
# Packet Filtering Disadvantages (cont.)

- May not be able to filter based upon TCP/UDP source port - may lead to holes in protection.
- Difficult to filter RPC services because the ports used are assigned randomly (therefore, cannot block RPC without potentially affecting other traffic).
- Some routers do not have the capability to filter according to the interface a packet arrived at (i.e. inbound / outbound), complicating the specification of rules.

# Application Gateway Firewall

- Provides a *proxy* between external systems and hosts offering services on an internal network
  - users connect to the proxy as a *gateway* to the internal network;
  - no longer have direct connections to internal machines.
- Allows more fine-grain control of connections.
- Can be used in conjunction with packet filtering router
  - ↳ directs all permitted connections towards the application gateway machine.

# Router & Application Gateway Firewall



# Application Gateway Process

E.G. For establishing a TELNET connection :

- user TELNETs to application gateway and enters name of an internal host;
- gateway checks user's source IP address - accepts or rejects according to access criteria in place;
- user may need to authenticate him/herself;
- proxy creates TELNET connection between gateway and internal host;
- proxy service passes bytes between the 2 connections;
- application gateway logs the connection.

# Application Gateway Advantages

- Allows through only those services for which there is a proxy
  - all other services completely blocked.
- Allows protocol to be filtered
  - e.g. allow FTP, but deny use of *put* command
- Information hiding
  - names of internal systems need not be known to outsiders. DNS only needs to know of application gateway

# Application Gateway Advantages (cont.)

- Robust authentication and logging
  - application traffic can be pre-authenticated before reaching internal hosts;
  - can be logged more effectively.
- Cost effectiveness
  - hardware / software for authentication and logging need only be located at the application gateway.

# Application Gateway Advantages (cont.)

- Less complex filtering rules
  - packet filter need only allow application traffic destined for the gateway and reject the rest;
  - easier than filtering and directing to a number of specific systems.

# Application Gateway Disadvantages

- Client-Server protocols (e.g. TELNET) require two steps for inbound and outbound connections.
- Requires modified user behavior or modified client :
  - e.g. for TELNET, either :
    - user must connect (but not login) to firewall rather than direct to host; OR
    - use a modified TELNET client that deals with the firewall transparently.

# Firewall Management

- Generate policy :
  - determine Internet access requirements;
  - regularly review as user needs change.
- Breach monitoring :
  - maintain and analyse logs.
- Continual improvement :
  - update in light of attacks;
  - regular, independent penetration testing.



# Firewall Advantages

- Protection from vulnerable services
- Controlled access to site systems
- Concentrated security
- Enhance privacy
- Logging and statistics on network use
- Security policy enforcement



## Firewall Disadvantages

- Restricted access to desirable services
  - likely to block services that users want (e.g. TELNET, FTP etc.)
- Implementation may demand major restructuring
  - topology may not lend itself to firewall
  - cost of introducing firewall may exceed cost of vulnerabilities
  - alternative solutions may be appropriate



## Firewall Disadvantages (cont.)

- Potential for back doors
  - e.g. unrestricted modem access
  - administration should ensure no means to bypass firewall
- Little protection from insider attacks
  - firewall designed to prevent outsiders from accessing sensitive data
  - many attacks would not need to use the firewall



## Firewall Disadvantages (cont.)

- Viruses
  - May be downloaded in program files or incoming emails
- Throughput
  - Firewall represent a potential bottleneck as all connections must pass through it
- “All eggs in one basket”
  - security concentrated in one spot
  - compromise could be disastrous

# Conclusions

- Increasingly common form of protection in Internet / Intranet scenario
- Can be implemented at varying levels
  - compromise between strength and flexibility
  - none represent a complete security solution
- Require careful configuration and management
  - i.e. cannot just install it and forget about it