IS53012A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2017-18 (since 2007)

Part I

Network security

Outline

Network Security

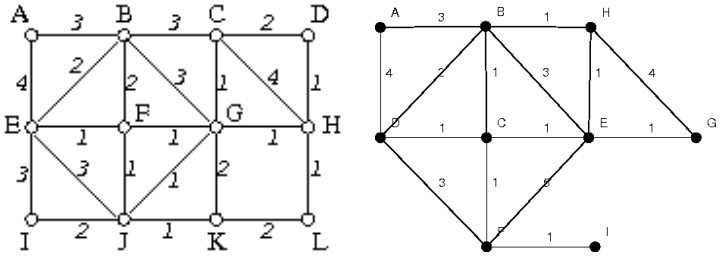
1. Fastest developing area
2. Similarity to and difference from a single application
3. Threats against networked applications
4. Confidentiality, integrity and availability in network settings
5. Weakness and strength of a network
   - A single point failure and fault tolerance
   - Great strength in the middle and fragility at the perimeter
6. To focus on the security issues, we work on simplified and abstract network models

Abstract network models

- A simple network consists of n nodes
  1. a server (host): the processor
  2. a client (workstation): end-user's devices
  3. communication media (hardware and software, 'links') in between that enable the communication
- Many routine communication activities are hidden from the end users.

Example of a network abstraction

Connected weighted graphs $G = (V, E)$, where V is the set of vertices and E the set of edges:



Network security

single point of failure as one link is broken

resilience or fault tolerance unlikelihood of failure of the entire network due to redundancy

network topology configuration in terms of nodes and connections, logical shape of the network

boundary A boundary distinguish an element from outside of a network, but the Internet is boundaryless

ownership difficult to know who is the owner of particular part of the network.

control (installing) depicting, configuring and administrating the networks.

1. Is it part of network A?
2. Who is the administrator who is responsible?
3. Who decides the version of the network software that is in use?

Models

OSI
application
presentation
session
transport
network
data link
physical

TCP/IP
application
transport
internet
network access

Hybrid
application
transport
network
data link
physical

Characteristics

- boundary: distinct an element of the nodes and connections
- anonymous ownership: due to the information hidden
- control: arbitrary host
- mode of communication: digital and analogue, and one-way or dual
- media: cable (unshielded twisted pair, coaxial cable), optical fibre, wireless, microwave, infrared, satellite

Media	Capacity	Coverage	
twisted pair	$<$ 10 Mbps	300 feet	
coaxial cable	100 Mbps	1500 feet	
optical fibre	1000 Mbps	2.5 miles	
wireless	1–10 Mbps	$\approx$ 10 meters	
microwave	100 Mbps	30 miles	straight line
infrared		9 miles	straight line
satellite		22,300 miles	

Models of layers

1. TCP/IP model (4 layers)

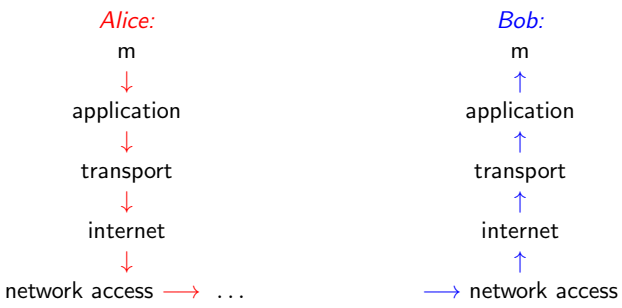
Layer	Activity
application	user interaction, addressing
transport	sequencing, reliability, error detection and correction
internet	flow control and routing
network access	communication on physical medium, bit transmission

2. ISO OSI Model (7 layers)

Layer	Activity
application	user data and programs
presentation	standardised data, blocking, text compression
session	sessions or logical connections, recover messages
transport	flow control, error detection and correction
network	routing, message blocking and packets
data link	transmission error recovery, separate packets into frames
physical	communication on physical medium, bit transmission

Protocols

network protocol an agreement to allow abstract levels of communication
protocol stack a layer architecture for communications



Internet protocols

internet protocol (IP) A packet multiplexer
IP packets a bundles of data
characteristics Unreliable datagram service
- no guarantee for deliveries
- no control of the source address and open for *IP spoofing* (cheat, fake)
- can drop packets regardless of traffic
- intermediate hops can fragment packets and all the reassembles are done at the destination
- no proper ways to handle the overlapping fragmented packets

IP addresses
1. Addresses in IP version 4, 32 bits, 25 bits for network and 7 bits for host address for broadcasting;
2. Addresses in IPv6 version 6, 128 bits, 25 bits for network and 7 bits for host address for broadcasting

CIDR Classless inter-domain routing

Transport protocol

- Stream Control Transmission Protocol (SCTP)
- capable for multiplex several independent streams on a SCTP connection
- four-way handshake at connection establishment time
- record making within each stream
- optional unordered message delivery
- multi-homing of each connection

Questions and discussion

1. What makes a network vulnerable?
   - anonymity An attacker can be made anywhere in the world; difficulties in computer-to-computer authentication;
   - multi-points attack difficult to trace origins of an attack
   - sharing difficult for access controls
   - complexity of systems difficult for reliable security if not impossible, a single operating system is hard enough
   - unknown perimeter difficult to identify boundary, difficult to control malicious users
2. Who would attack networks?
   - psychological traits and hacking
   - motive
   - opportunity
   - method

Attacks

IP spoofing attackers send packets with a faked return addresses

directed broadcast

denial of service simply over use of a service, straining software, hardware, or network links beyond their intended capacity

- on a network link
- on a network layer
  - Killer and ICMP packets
  - SYN-ACK packet attacks: another type of DNS attack, e.g. Telnet (to establish a virtual connection, called a "session")
  - Application-level attacks - Spam

Mainly due to

- protocol weaknesses
- programming bugs in servers
- inappropriately helpful humans

Classes of attacks

Attacks	Defences
steal passwords	password file encryption
password guessing	restrict the number of failed logins, report the failed login to the users
dictionary attacks	cryptography matching guessed passwords against the stolen ones
Social engineering	a. A security guard does not allow the access to the centre computer for a reboot b. "Just change the password on my login on your computer; it has been a while since I have used it." "... no problem." c. A visitor's username and password d. Past employee's account etc. etc.

Protocol failures

- TCP sequence number attack
- human errors
- inappropriate assumptions
- insecure foundation

Exponential attacks

viruses attach to other programs
Do not get virus without communicating with an affected host, but can be forwarded

worms Programs travelling by themselves

Denial-of-service attack

DoS Overuse of a service: straining software, hardware, or network links beyond their intended capacity

DDoS Distributed Denial-of-Service: use many hosts on the Internet; more difficult than DoS to trace back.

SYN flood Use TCP protocol suite, making the session-oriented nature of these protocols work against victims

Botnets Bots are programs that receive commands from *bot controllers* using protocols such as IRC (Internet Relay Chat) and HTTP and lunch spam or DNS attacks from the bots.

Attacks on the network layer

ICMP packets Internet Control Message Protocol (ping, echo, destination unreachable, source quench)

SYN packet attacks, SYN flood Sending many SYN requests but never responding with ACKs.

Application level attacks e.g. Spam

Distributed denial-of-service attack (DDoS) February 2000

1. install a zombie program on as many machines as possible
2. install a master program
3. wait for his moment
4. when the time comes, send a message to the master including the address of the target.
5. zombies flood the target with enough traffic to cause the problem.

Questions and discussion

1. What are the assets?
   - infrastructure
   - application programs
   - data
2. What are the threats?
   - similarity, protocols
   - connectivity
   - software flaws
3. What are the threat agents?
4. What are the controls?
5. What are the challenges and uncontrolled risk?

Part II

Defence and control

Outline

Defence options

1. live with the standard services (trust or not)
2. build new software that is likely to be secure
3. find a way to tame those unsafe but useful services

Services

- Inetd — network services, does not run as a root, but runs an instantiation for each incoming connection, suitable for low volume networks
- ssh — terminal and file access, provides end-to-end encryption, configuration details are important
- Syslog — useful for managing various logs, runs as root (user datagram protocol) UDP packets

Network administration tools

network monitoring

`tcpdump`

`ping, traceroute and dig` not purpose built for security: `dig` (domain information groper) is for DNS (Domain Name System) queries

`chroot` Unix DTE (Domain and Type Enforcement) in Linux

Jailing the Apache web server

samba an SMB (Server Manage Block) implementation

Firewalls

fire wall a device, software, or arrangement or equipment that limits network access;

- can be software or hardware, included in many devices such as routers, modems, wireless base stations and IP switches
- a client shim (a software layer) in Windows, or a set of filtering rules implemented in a Unix kernel in various popular operating systems

Categories

Three categories:

1. packet filters, 1988, first generation firewalls, DEC (Digital Equipment Corporation)
2. circuit gateways, 1980–90, second generation, AT&T Bell Laboratories
3. application gateways, 1991, third generation, Purdue University, AT&T Bell Laboratories

Types

1. packet filtering gateways or screening routers
2. stateful inspection firewalls
3. application proxies
4. guards
5. personal firewalls

Packet filtering gateway I

Packet filters, e.g. `iptables` - administration tool for IPv4 packet filtering and NAT, in Linux

- simplest, most effective type for some situations
- work by dropping packets with 'disagreed' source or destination addresses or port number
- usually take place at incoming or outgoing interface, or both
- the administrator makes a list of the *acceptable* computers and services and a stop-list of *unacceptable* computers or services
- this allows an easy means to permit or deny access at the host or network level

Packet filtering gateway II

Weakness

- may not be flexible enough to realise a security policy
- easy to make a mistakes with the permission tables
- not always easy to derive a logical expressions on packet fields
- have to implement the expressions in vendor's syntax
- not easy for authentication since the source addresses in packets can be forged.

Stateless firewalls I

A dynamic filtering, firewall structure at network layer.

- examine a packet based on the header information
- inspect one packet at a time and decide to accept or reject it
- only packets matching a known *connection state* will be allowed by the firewall
- track each connection and traverse all interfaces of a firewall
- the contents of the packet up through the application layer may also be inspected

Stateless firewalls II

Advantages

- can track the sequence of packets and
- conditions from one packet to another

Weakness

- Only inspect the header information but not the inside the packets
- cannot deal with the complex and flawed application

Application proxy I

Application proxy gateway, or bastion host: A program/device that simulates the effects of an application so the application receives only requests to act properly.

- runs pseudo applications, e.g. legitimacy of a mail transformation
- two headed: to the insider as if it is the outside connection, while to the outside it responds just as if the insider application would.

Application proxy II

Example

- An online price list that shows a list of products and prices can be seen from outside, and outsiders cannot change the list nor access to other information than the prices.
- A school wants to monitor the web sites accessed by the students via its Intranet
- A company wants to provide information from its databases but to restrict queries that contains too many values
- A institution wants to encrypt the data portion of all emails to addresses of its divisions

Guard I

A sophisticated firewall

- receives protocol data units, interprets them and passes through the same or different protocol data units that achieve the same result or a modified result
- A guard decides that services to preform on the user's behalf in accordance with its available knowledge, e.g. the user's identity, previous interactions.
- No clear cut to distinct a guard from a proxy.

Guard II

Advantages:

- The degree of control can only restricted by what is computable
- finer application level control

Weakness:

- More difficult for implementation due to the complex
- Easy to be exposed to errors
- Slower than filtering
- less flexible and slow upgrade than stateful inspection firewalls

Personal firewalls I

An application program that runs on a workstation to block unwanted traffic, usually from the network

- screen the data accepted by a single host
- can compensate for the lack of a regular firewall
- define a personal security policy, e.g. a list of personally accepted web sites for download software
- can generate logs for later review or re-examination for anything slipped by firewalls

Personal firewalls II

Advantages:

- can be effective and efficient
- easy to combine with a virus scanner

Weakness:

- run on the same computer that it tries to protect
- powerless for undetected attack that would disable or reconfigure the firewall for the future, not very effective for 'always-on' connections

Comparison of firewall types I

PF: Packet Filtering,
SI: Stateful Inspection,
AP: Application Proxy;
G: Guard;
PF: Personal Firewall
1: simple,
2: medium complex,
3: complex,
4: most complex

Comparison of Firewall Types

		PF	SI	AP	G	PF
Complexity		1	2	3	4	2
	addresses	Y	Y	Y	Y	Y
	protocol type	Y	Y	Y	Y	Y
Screen	data		Y	Y	Y	
	packet data			Y	Y	
	full text				Y	
	conection rules	Y				
	header or data		Y			
based on	proxy behaviour			Y		
	message content				Y	
	packet, header					
	and data				Y	

Comparison of firewall types II

	PF	SI	AP	G	PF
Auditing	difficult	possible	+ activity	+ activity	+ activity
Weakness	tricky configuration	signature attack only	addressing rules	limit assurance	need experience

Firewall problems

- inadvertent problems
- intentional subversions
- handling IP fragments
- the FTP problem
- testing firewalls