Introduction to TCP/IP

TCP/IP protocol suite

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Problems in TCP/IP

Problems with authentication

"SYN" attacks

IP spoofing

Sequence guessing

Source routing

Connection hijacking

TCP/IP Security.

Problems in the TCP/IP Protocol Suite

Ferucio Laurenţiu Ţiplea

Department of Computer Science
"AL.I.Cuza" University of Iaşi
Iaşi, Romania

December 14, 2016

Outline

Introduction to TCP/IP

TCP/IP protocol suite

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Problems in TCP/IP

Problems with authentication

"SYN" attacks

IP spoofing

Sequence guessing

Source routing

Connection hijacking

1. *Introduction to TCP/IP*
   - *TCP/IP protocol suite*
   - *Internet Protocol (IP)*
   - *Transmission Control Protocol (TCP)*

2. *Problems in TCP/IP*
   - *Problems with authentication*
   - *"SYN" attacks*
   - *IP spoofing*
   - *Sequence guessing*
   - *Source routing*
   - *Connection hijacking*

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. *Introduction to TCP/IP*
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. *Problems in TCP/IP*
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

TCP/IP

Basic concept(s): (TCP/IP)

TCP/IP is a protocol suite. Its name comes from the two of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).

The main design goal of TCP/IP was to build an interconnection of networks, referred to as an internetwork or internet, that provided universal communication services over heterogeneous physical networks.

When written with a capital "I", the Internet refers to the worldwide set of interconnected networks. Therefore, the Internet is an internet, but the converse does not apply.

Nowadays, TCP/IP is the engine for the Internet and networks worldwide.

TCP/IP is modeled in four layers:

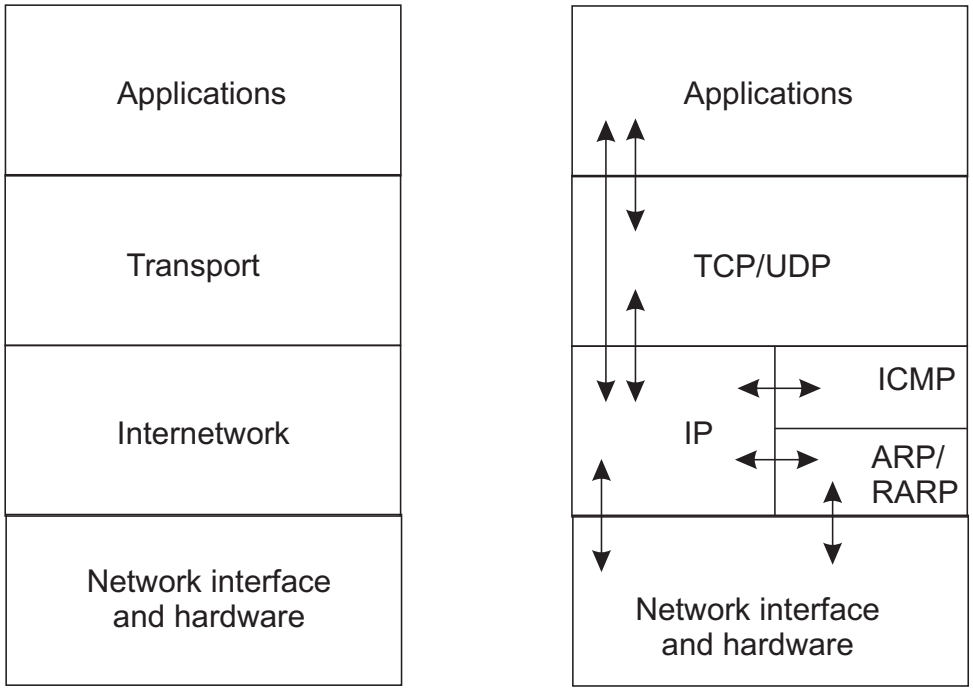

Figure: TCP/IP layers

TCP/IP layers: more details

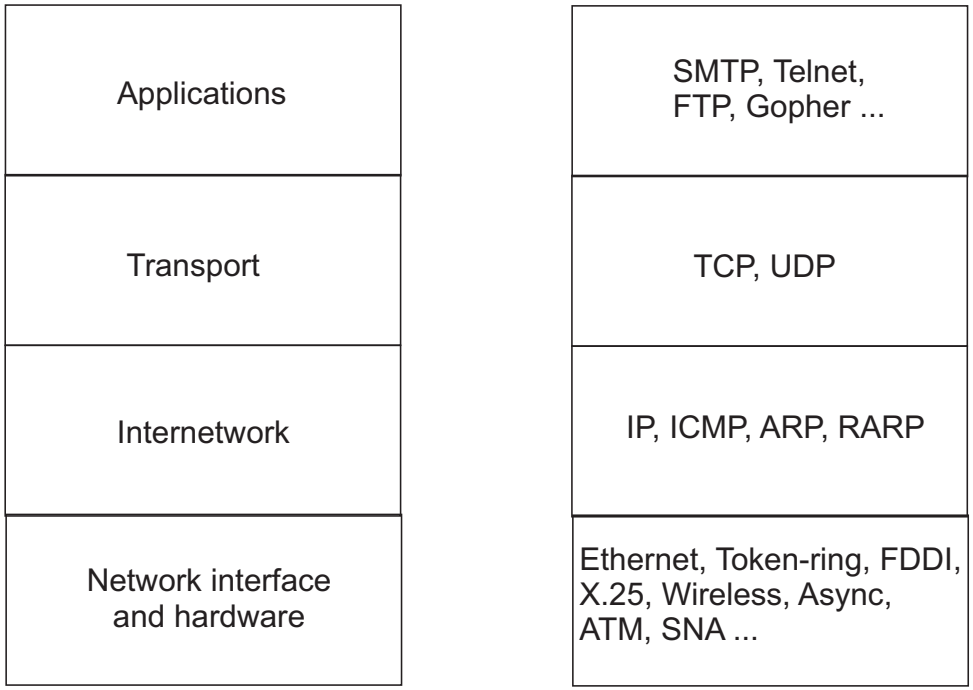

Figure: More details on TCP/IP layers

The client-server model

Most applications in the highest layer of the TCP/IP use the client-server model.

Basic concept(s): (client/server/application)

- *A server is an application that offers a service to internet users.*
- *A client is a requester of a service.*
- *An application consists of both a server and a client part, which run on the same or on different systems.*

Users usually invoke the client part of the application which builds a request for a particular service and sends it to the server part of the application using TCP/IP as a transport vehicle.

The client-server model

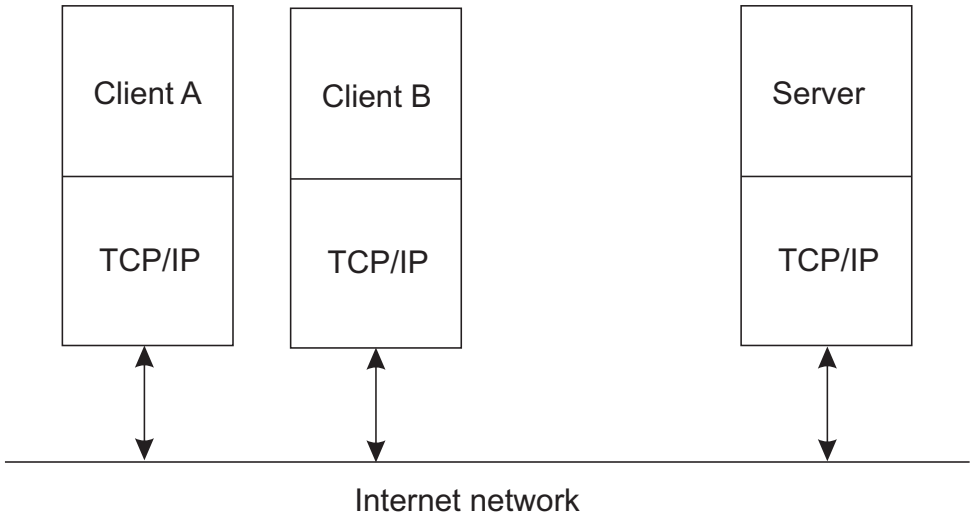

Figure: The client-server model

Request for Comments and Internet Standards

The Internet protocol suite is still evolving through the mechanism of Request for Comments (RFC). After an RFC has been published, all revisions and replacements are published as new RFCs.

When a protocol reaches the standard state it gets a Standard (STD) number. STD numbers do not change when the standards are updated.

To clearly indicate which version of a standard is used, both the standard number and the corresponding RFCs should be stated.

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. *Introduction to TCP/IP*
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. *Problems in TCP/IP*
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

Internet Protocol (IP)

IP is a standard protocol: STD 5, RFC 950, RFC 919, RFC 922, RFC 1349, RFC 3168, and RFC 3260.

Basic concept(s): (Internet Protocol (IP))

IP is a packet delivery protocol: its job is to route and send a packet to the packet's destination.

IP is:

- unreliable – packets may be lost, arrive out of order, or may be duplicated;
- best-effort – IP provides no guarantee whatsoever for the packets it tries to deliver; it only tries for a best-effort delivery;
- connection-less – there is no state maintained between two IP packets (datagrams).

IP assumes that higher level protocol will address all the anomalies occurred during packet delivery.

IP datagram

The unit of transfer in an IP network is called an IP datagram. It consists of an IP header and data relevant to higher-level protocols (IPv4):

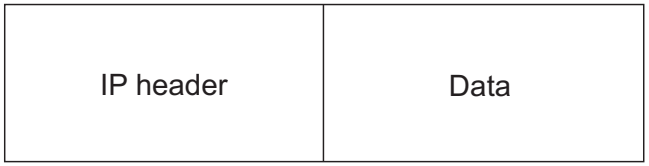

Figure: IP datagram

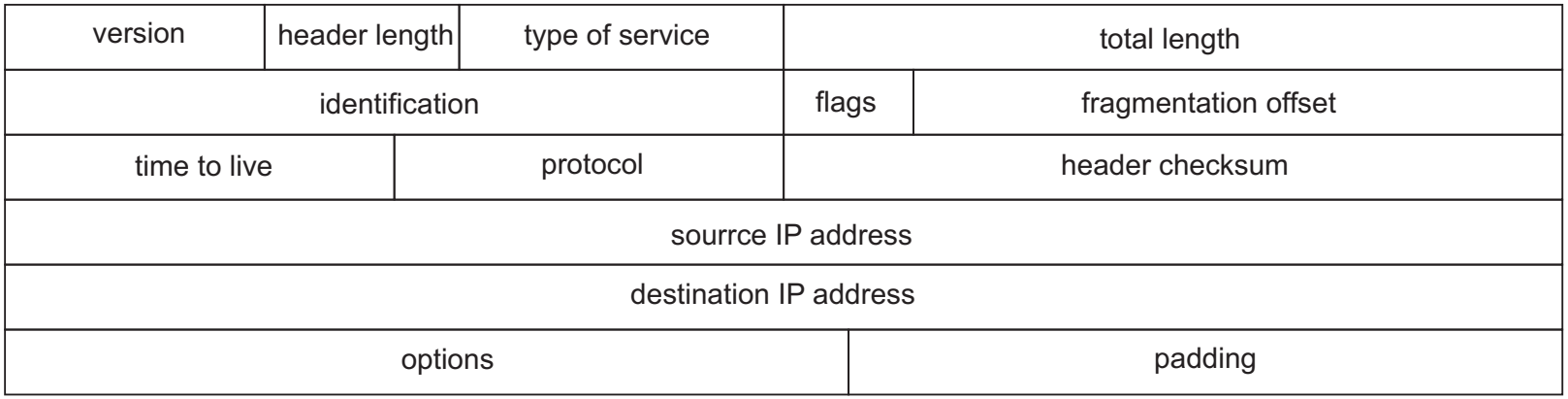

Figure: IP header

Fragmentation

IP can provide fragmentation and reassembly of datagrams. A few important facts about fragments are in order:

- maximum length of a datagram = 65,535 bytes;
- all IP host must support 576 byte datagrams without fragmentation;
- all fragments of a datagram have a header which is the original datagram's header;
- any fragment is treated as a normal datagram while being transported to the destination;
- the complete datagram is considered lost if one of its fragments gets lost (the remaining fragments are discarded by the destination host).

Outline

Introduction to TCP/IP

TCP/IP protocol suite

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Problems in TCP/IP

Problems with authentication

"SYN" attacks

IP spoofing

Sequence guessing

Source routing

Connection hijacking

1 Introduction to TCP/IP

- TCP/IP protocol suite
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)

2 Problems in TCP/IP

- Problems with authentication
- "SYN" attacks
- IP spoofing
- Sequence guessing
- Source routing
- Connection hijacking

Transmission Control Protocol (TCP)

TCP is a standard protocol: STD 7, RFC 793, RFC 1122.

Basic concept(s): (Transmission Control Protocol (TCP))

TCP offers seven major features:

- *connection-oriented;*
- *point-to-point communication;*
- *reliability;*
- *full duplex connection;*
- *stream data transfer;*
- *reliable startup;*
- *graceful shutdown.*

- connection-oriented – TCP provides a logical connection between pairs of processes, and then uses it for data transfer;
- point-to-point communication – each TCP connection has exactly two end points;

Transmission Control Protocol (TCP)

- reliability – TCP guarantees that the data sent across the connection will be delivered exactly as sent, without missing or duplicate data;
- full duplex connection – a TCP connection allows data to flow in either direction at any time;
- stream data transfer – TCP allows an application to send a continuous stream of bytes across the connection;
- reliable startup – TCP requires that two applications must agree to the new connection before it is established. Packets used in previous connections will not appear or otherwise interfere with the new connection;
- graceful shutdown – an application can open a connection, send data, then shut down the connection. TCP guarantees to deliver all the data reliably before closing the connection.

Ports

Each process that wants to communicate with another process identifies itself to the TCP/IP by one or more ports.

Basic concept(s): (port)

A port is a 16-bit number used by the host-to-host protocol to identify to which higher-level protocol or application program (process) it must deliver the incoming messages.

There are two types of ports:

- well-known ports;
- ephemeral ports.

TCP segment

A TCP atomic message is called a TCP segment. It consists of a TCP header followed by data (as in the case of IP datagrams).

16-bit sourrce port number								16-bit destination port number
32-bit sequence number								
32-bit acknowledgment number								
header length	reserved		URG	ACK	PSH	RST	SYN	FIN	16-bit window size
16-bit TCP checksum								16-bit urgent pointer
options (if any)								
data bytes (if any)								

Figure: TCP segment format

Each TCP segment is encapsulated into an IP datagram and sent across the Internet.

Flow control

In order to optimally use the network bandwidth, a transport protocols should use the window principle.

Basic concept(s): (window principle)

When a connection is established, each end of the connection allocates a buffer (window) to hold incoming data, and sends the size of the buffer to the other end. As data arrives, the receiver sends acknowledgments together with the amount of buffer space available. When the incoming data fill the receiver's buffer, the sender must stop sending new data until it receives a positive window.

Assuming that data is sent in packets, each packet should be assigned a timer so that the packet can be retransmitted in case that it did not reach the destination within some given amount of time.

TCP window mechanism

In TCP, the window mechanism works as follows:

- because TCP provides a byte-stream connection, sequence numbers are assigned to each byte in the stream. TCP divides this contiguous byte stream into TCP segments;
- the window size is expressed as a number of bytes and its initial value is determined by the receiver when the connection is established;
- each acknowledgment message includes the window size that the receiver is ready to deal with at a particular time.

Example

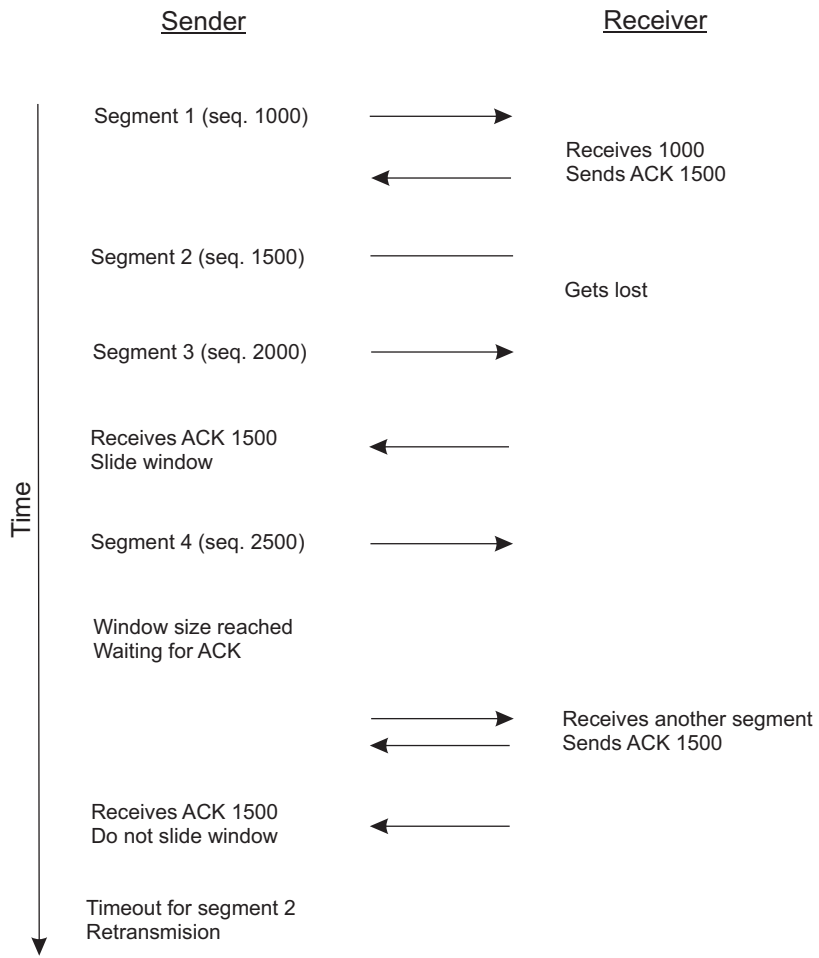

Figure: TCP window example: window size = 1500, segment = 500

TCP connection set up

TCP uses the three-way-handshake to set up a successful connection:

Protocol: (TCP connection set up)

1. $A \rightarrow B$: SYN, SEQ=x
2. $B \rightarrow A$: SYN, SEQ=y, ACK=x+1
3. $A \rightarrow B$: SEQ=x+1, ACK=y+1

The initial sequence numbers (x and y) are randomly chosen.

TCP connection release

The same three-way-handshake is used to terminate a connection:

Protocol: (TCP connection release)

1. $A \rightarrow B$: *FIN*
2. $B \rightarrow A$: *FIN, ACK*
3. $A \rightarrow B$: *ACK*

In the first step, A sends a segment with the FIN flag on and no data.

Outline

Introduction to TCP/IP

TCP/IP protocol suite

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Problems in TCP/IP

Problems with authentication

"SYN" attacks

IP spoofing

Sequence guessing

Source routing

Connection hijacking

1. *Introduction to TCP/IP*
   - *TCP/IP protocol suite*
   - *Internet Protocol (IP)*
   - *Transmission Control Protocol (TCP)*

2. *Problems in TCP/IP*
   - *Problems with authentication*
   - *"SYN" attacks*
   - *IP spoofing*
   - *Sequence guessing*
   - *Source routing*
   - *Connection hijacking*

Problems with authentication

Conventional IPv4 does not typically use authentication, and the lack of authentication with IP packets is a general weakness with TCP/IP.

Without authentication, there is no guarantee that a packet comes from where its source field claims it comes from. This is the the major issue in IP security, as the next sections will show.

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. Introduction to TCP/IP
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. Problems in TCP/IP
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

"SYN" attacks

Information Security
F.L. Tiplea
Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

SYN attacks take advantage of a flaw in how most hosts implement this three-way handshake. When host B receives the SYN request from A, it must keep track of the partially opened connection in a listen queue for at least 75 seconds. This is to allow successful connections even with long network delays. The problem with doing this is that many implementations can only keep track of a very limited number of connections (most track only 5 connections by default).

Attack: (SYN attack)

A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN+ACK the other host sends back. By doing so, the other host's listen queue is quickly filled up, and it will stop accepting new connections, until a partially opened connection in the queue is completed or times out.

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. Introduction to TCP/IP
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. Problems in TCP/IP
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

IP spoofing

IP Spoofing is an attack where an attacker pretends to be sending data from an IP address other than its own.

The IP layer assumes that the source address on any IP packet it receives is the same IP address as the system that actually sent the packet – it does no authentication. Many higher level protocols and applications also make this assumption, so it seems that anyone able to forge the source address of an IP packet (called "spoofing" an address) could get unauthorized privileges.

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. Introduction to TCP/IP
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. Problems in TCP/IP
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

Sequence guessing

The chance of guessing the correct initial sequence number (ISN) is exceedingly low due to the fact that sequence numbers used in TCP connections are 32-bit numbers.
However, if the ISN for a connection is assigned in a predictable way, it becomes relatively easy to guess. For instance, in BSD 4.2, the ISN for a connection is assigned from a global counter. This counter is incremented by 128 each second, and by 64 after each new connection (i.e., whenever an ISN is assigned).

Attack: (sequence guessing)

By first establishing a real connection to the victim, the attacker can determine the current state of the system's counter. The attacker then knows that the next ISN to be assigned by the victim is quite likely to be the predetermined ISN, plus 64. The attacker has an even higher chance of correctly guessing the ISN if he sends a number of spoofed IP frames, each with a different, but likely, ISN.

Outline

Introduction to TCP/IP
TCP/IP protocol suite
Internet Protocol (IP)
Transmission Control Protocol (TCP)
Problems in TCP/IP
Problems with authentication
"SYN" attacks
IP spoofing
Sequence guessing
Source routing
Connection hijacking

1. Introduction to TCP/IP
   - TCP/IP protocol suite
   - Internet Protocol (IP)
   - Transmission Control Protocol (TCP)
2. Problems in TCP/IP
   - Problems with authentication
   - "SYN" attacks
   - IP spoofing
   - Sequence guessing
   - Source routing
   - Connection hijacking

Source routing

The "option" field in the IP datagram allows the originating host to specify the path (route) that the receiver should use to reply to it.

Attack: (source routing)

The attack consists of specifying a route in the IP datagram option field that by-passes the real host and directs replies to a path it can monitor (e.g., to itself or a local subnet).

Outline

Introduction to TCP/IP

TCP/IP protocol suite

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Problems in TCP/IP

Problems with authentication

"SYN" attacks

IP spoofing

Sequence guessing

Source routing

Connection hijacking

1 Introduction to TCP/IP
- TCP/IP protocol suite
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)

2 Problems in TCP/IP
- Problems with authentication
- "SYN" attacks
- IP spoofing
- Sequence guessing
- Source routing
- Connection hijacking

Connection hijacking

Connection hijacking is a kind of man-in-the-midle attack.
When the sequence number in a received packet is not the same as the expected sequence number, the connection is said to be desynchronized. If the received packet is not the one expected but is within the current window, the packet will be saved on the premise that it will be expected later (various TCP mechanisms ensure that the expected packet will eventually arrive). If the received packet is outside of the current window, it will be discarded.
Thus, when two hosts are desynchronized enough, they will discard (ignore) packets from each other.

Attack: (connection hijacking)

An attacker located on the communication path between two desynchronized hosts can inject forged packets with the correct sequence numbers (and potentially modify or add commands to the communication).

Desynchronize hosts

The key to this attack is to desynchronize hosts. This can be done during connection set up or in the middle of a connection:

- to cause desynchronization during connection set up, the attacker resets a connection during the three-way handshake. After host B sends the SYN+ACK packet to host A, the attacker forges new packets from B (to A) in which the connection is first closed via the RST bit, and then a new three-way handshake is initiated with A – identical to the original, "real" handshake but with different sequence numbers. Host B now ignores messages from A (because A is using the attacker's new sequence numbers), and host A ignores messages from B (because A is expecting messages with the attacker's sequence numbers). The attacker then replicates new packets, with the correct sequence numbers, whenever A and B try to communicate. In doing so, the attacker may also modify the messages or inject his own;

Desynchronize hosts

- to cause desynchronization in the middle of a connection without closing the connection, only the sequence number counters should be altered. The Telnet protocol, in particular, provides an interesting mechanism to do this. Telnet allows special "NOP" commands to be sent. These commands do nothing, but the act of sending the bytes in the NOP command increments the expected sequence number counter on the receiver. By sending enough of these NOP commands, an attacker can cause the connection to become desynchronized. The attacker can then begin replicating new packets, with the correct sequence numbers.