The Internet and Sockets
Computer Security
Tom Chothia

This Lecture
• How the Internet works.
  – Some History
  – TCP/IP
• Some useful network tools:
  – Nmap, WireShark
• Some common attacks:
  – “The attacker controls the network”

Before the Internet
• Life was solitary, poor, nasty, brutish and short.
• Computer Networks:
  – local networks,
  – telephone line connections,
  – leased line.

The Start 1969
• The US Defense Advanced Research Projects Agency (then ARPA now DARPA) gives research grants to universities to buy computers.
• They decide to link their computers.
• But how?

But if everyone just sends a small packet of data, they can both use the line at the same.
IP Addresses

- Every computer has an IP address.
  e.g. 147.188.193.15

- Every router on the Internet keeps a list of which connection it should use for which addresses.

Transmission Control Protocol

- 1974: daily traffic more than 3 million packets a day. Many are getting lost.

- TCP is a protocol than runs on top on IP, if an IP packet gets lost. It requests that it is resent.

- TCP/IP becomes allows Inter network connections. So in 1977:
The ARPAnet

- 1969 the birth of the ARPAnet.
- 1971 E-mail @
- 1977 the ARPAnet becomes a Inter-network.
- 1978 first Spam message send. Admin assures users this will never happen again

Domain Name Servers (DNS)

- Remembering IP address is hard.
- So people associate names with addresses. e.g. news.bbc.com → 212.58.226.141
- A hierarchy of servers list handle requests
- The route for most of Europe is RIPE based in Amsterdam.

The Internet

- 1988 The Morris Worm, CERT formed.
- 1989 The Web: HTTP and HTML.
- 1992 The first ISPs and Mosaic the first web browser.
- 1994 Yahoo
Ports

- To allow multiple connections TCP uses “ports”
- A TCP “Socket” connection is defined by: (destination IP, destination port, source IP, source port)
- The destination port normally depends on the service: WWW runs on port 80, ssh on port 22, dns on 53
- The source port is normally chosen at random.

Nmap: http://nmap.org/

A network scanning tool: tells you which ports are open.

> nmap 127.0.0.1

Many other functions (see man nmap)

MAC addresses

Every computer has a unique media access control address (MAC address)

To use IP you need a protocol that sends IP packets to MAC addresses,
- wi-fi (802.11)

MAC addresses not secure: easy to change, snoop, steal,…

The Internet Protocol Stack

Internet communication uses a stack of protocols.

Each protocol uses the protocol below it to sent data.
The Stack, Most of the Time:

Applications
TCP
Internet Protocol
IP address
Ethernet
MAC address

WireShark www.wireshark.org

A network protocol analyzer.

It records all Internet traffic, so it can then be viewed and analysed.

Excellent for debugging, protocols and finding out how Internet applications work.

Who can monitor and alter my traffic?

Anyone on the route a the packet takes:

IT Services, ISPs, Governments, ...

but also..

Hubs vs Switches

Local area networking equipment may be:

- Hubs (also unencrypted wi-fi, WEP):
  - 
  - 
- Switches (also WPA)
  - 
  -

DHCP & ARP

Dynamic Host Configuration Protocol:

- (MAC address). Not stored long term.

Address Resolution Protocol (ARP)

- Lets router find out which IP address is being used by which machine.

ARP spoofing lets one machine steal the IP address of another on the same network.
Domain Name System

DNS used to turn domain names into IP addresses.
• “Authoritative name servers” store all IPs for a particular domain.
• Local servers cache domain details.

“DNS spoofing”/“DNS cache poisoning” lets an attacker insert a false record.

“The Attack Owns The Network”

The Internet was not designed with security in mind.

Traffic may be monitored or altered.

All good security products assume that the attacker has complete control over the network (but can’t break encryption)

This Lecture

• How the Internet works.
  – Some History
  – TCP/IP
• Some useful network tools:
  – Nmap, WireShark
• Some common attacks:
  – “The attacker controls the network”

Next Lecture

• How to make communication secure.
• How to authenticate who you are talking too.
• This is done with the symmetric crypto, public key crypto, certificates and hashes that you have already seen.