

COMP202-08B Computer Communications

Lecture 2 – Internet communications basics

Matthew Luckie
mluckie@cs.waikato.ac.nz



28 July 2008

Specified Labs

- Lab 1 (Linux) shared with COMP204
- G.B.20 (Linux) shared with COMP501
- Supervised lab sessions will probably be held
 - Mon 2-4pm
 - Wed 10-12pm
 - Wed 3-4pm ??

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O HOKIANGA

28 July 2008

2

Lecture outline

- Internet addressing, naming, and numbering basics

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O HOKIANGA

28 July 2008

3

Communications

- There are many ways of communicating between computers
 - Infra-red beaming, e.g. TV, video, stereo remotes, cell phones
 - Dial up modems
 - Serial cables
 - Firewire
 - USB
 - Bluetooth
 - Various wireless systems (WiFi)
- Ethernet-based methods are the most common

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O HOKIANGA

28 July 2008

4

Communications

- Computers on a network need to be identified somehow
 - To be able to accurately direct messages to them
 - Think of it like identifying houses in the postal system
- We identify computers by their address
- There are a number of addressing schemes
 - Internet Protocol version 4 (IPv4) addressing
 - Internet Protocol version 6 (IPv6) addressing
 - Ethernet MAC addressing
 - Bluetooth MAC addressing
 - ... and many, many more.

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O HOKIANGA

28 July 2008

5

IPv4

- The addressing scheme used most on the Internet is IPv4
- Each system on the Internet has at least one IPv4 address; some have more than one
- An IP address is a 32 bit number, written as four one-byte values
 - e.g. 130.217.250.39
 - This presentation format is known as a dotted-quad.
- Question: what is the range of numbers between each dot? Why?

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O HOKIANGA

28 July 2008

6

IPv4

- Question: How many addresses are there in the IPv4 *address space*?
- Answer: $2^{32} = 4,294,967,296$

IPv4

- Question: why not just use a 32 bit number instead of a dotted-quad?
- Answer:
 - More difficult to remember
 - E.g. 130.217.250.39 => 2,195,323,431
 - Often easier to remember four small numbers than a large one.

IPv4

- At the time IPv4 was specified, it was not conceived that we would need more than 4 billion addresses
- Due to inefficiencies in the allocation system, as well as the massive growth over the last 20 years, we will run out of addresses to allocate shortly.

Friendly names

- It is not practical to remember the addresses of each of the computers on the Internet we want to communicate with
- Many addresses also have a name associated with it
 - sorcerer.cs.waikato.ac.nz : 130.217.250.39
 - icanhascheezburger.com : 72.233.69.8
 - www.nzherald.co.nz : 202.175.131.11
 - www.trademe.co.nz : 203.57.145.2

Friendly names

- The system for *resolving* (looking up) friendly names to give an IP address is known as the
 - **Domain Name System (DNS)**

Communicating

- We don't communicate with a computer as such
- Rather, we communicate with a piece of software running on the computer
 - E.g. to browse to www.google.com we actually want to talk to google's web server software
- This is achieved by using a **port number** to identify the application

Port Numbers

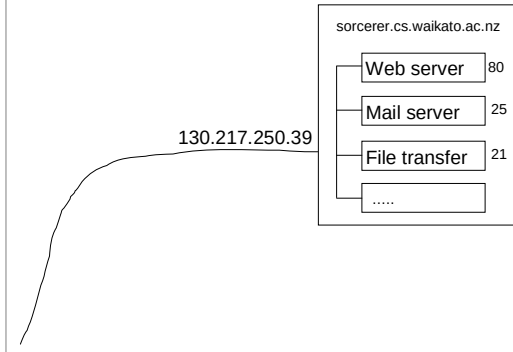
- A port number is a 16-bit number
- Some applications have well known port numbers
 - 80 is used for web
 - 53 is used for DNS
 - 21 is used for file transfer protocol (FTP)
 - 110 is used for POP email
 - 25 is used to send mail

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

23

Wrapping it all up



© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

24

Wrapping it all up

- DNS names map to IP addresses
- IP addresses identify systems on the Internet
- Applications run on a port

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

25

Determining network addresses on your computer

- Windows : use the command "ipconfig"
- Linux, MacOS X, ... : use the command "ifconfig"
 - /sbin/ifconfig

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

26

```
cms-r1-17:[102]~>/sbin/ifconfig
```

```
eth0 Link encap:Ethernet HWaddr 00:19:B9:19:2A:9E
      inet addr: 130.217.252.17 Bcast:130.217.255.255
      Mask:255.255.0.0
      inet6 addr: fe80::219:b9ff:fe19:2a9e/64 Scope:Link-Local
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Ethernet interface, number zero

IP address

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

27

In the news

NZ Herald, 15 July 2008

Conviction would harm hacker's future – judge

A young Whitianga computer hacker walked free from court today after a judge said a conviction would have harmed his prospects.

He was allegedly the mastermind of a "botnet" coding group said to have infected a million computers and caused millions of dollars of damage

© THE UNIVERSITY OF WAIKATO - TE WHARE WAIKATO O WAIKATO

28 July 2008

28

Botnets

A botnet is created by

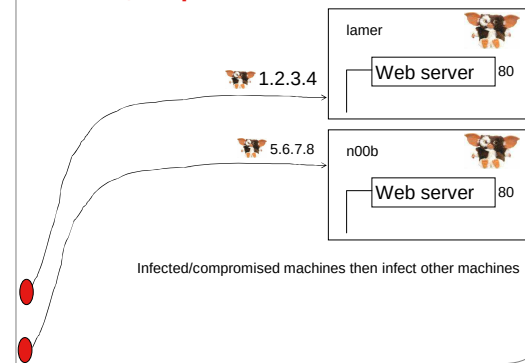
1. exploiting flaws in application services running on computers to have it run different application code
 - i.e. 'infect' it with malicious code
2. have some way of controlling a large number of these infected machines
 - Often have infected machines congregate in a special chat room to then be issued with instructions
 - But more than one way to organise a botnet

© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

29

Botnets, Step 1

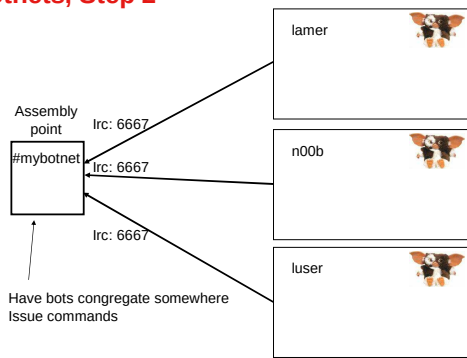


© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

30

Botnets, Step 2



© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

31

Botnets

- Step 3: Profit
- Step 4: Get caught.
- Let's say the FBI shuts down the server where they congregate.
- How might you reassemble the bots?

© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

32

Botnets

- Have the assembly point controlled in DNS.
- Change the IP address to which the friendly name resolves, and have the bots reassemble there.
- E.g.
 - assemblypoint.mybots.biz → 192.168.55.4
 - Hacker finds the machine at 192.168.55.4 is taken offline
 - Hacker then changes DNS entry
 - assemblypoint.mybots.biz → 172.18.4.4

© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

33

Summary

- Friendly names
- IP addresses
- Application ports
- Next lecture: using this knowledge to build a simple network application

© THE UNIVERSITY OF WINNATO - TE WAKA WAKANGA CHAKAKATO

28 July 2008

34