UC Berkeley EECS
Sr Lecturer SOE
Dan Garcia

The Beauty and Joy of Computing

Lecture #16
Internet II

Heartbleed Bug!

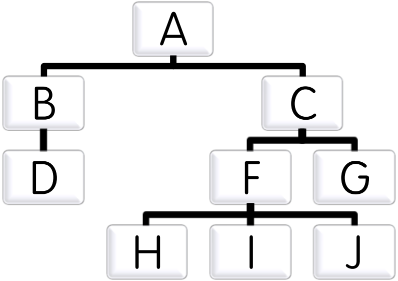
About one year ago, a bug of incredible magnitude was uncovered. It was an incredibly serious security hole (aka vulnerability) in OpenSSL, which provides security and privacy for the Internet (web, email, IM, VPNs, etc). You'll read about it next week.

`heartbleed.com`

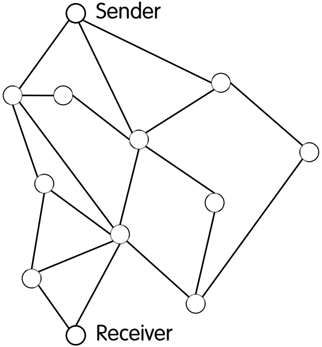
Internet: Hierarchical & Redundant

Definitions

Hierarchical

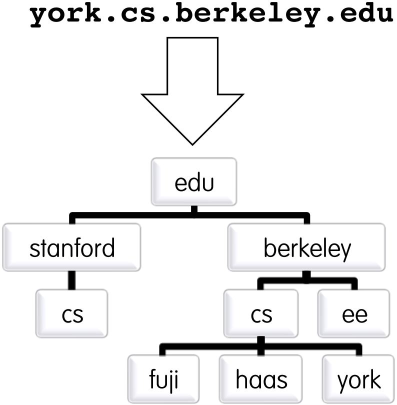


Redundant



Hierarchical

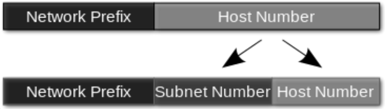
- The Internet and the systems built on it are Hierarchical
  - Domain Name Syntax (DNS)
  - IP addresses
- Benefits
  - Helps systems scale



en.wikipedia.org/wiki/Domain_Name_System

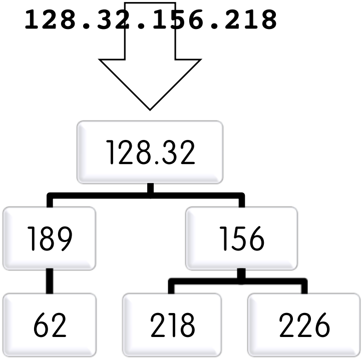
Hierarchical

- The Internet and the systems built on it are Hierarchical
  - Domain Name Syntax (DNS)
  - IP addresses
- Benefits
  - Helps systems scale



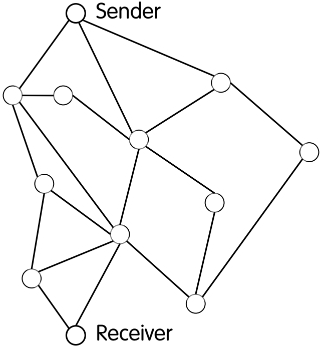
york.cs.berkeley.edu

128.32.156.218



Redundant

- The Internet and the systems built on it are Redundant
  - Routing (i.e., more than one way to get there)
- Benefits
  - Fault tolerance (i.e., more reliable)
  - Helps Internet scale to more devices, people

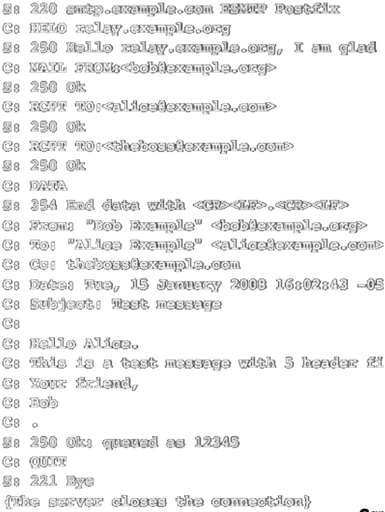


Internet: Widespread Growth, Use. How?

en.wikipedia.org/wiki/Open_standard#Protocols

Widespread Growth, Use. How?

- Interfaces and protocols enable widespread use of the Internet
- Open standards fuel the growth of the Internet.
  - "Open" = not owned by company
  - Standards for packets and routing include transmission control protocol/Internet protocol (TCP/IP).
  - Standards for sharing information and communicating between browsers and servers on the Web include HTTP and secure sockets layer/transport layer security (SSL/TLS).



```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -05
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fi
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

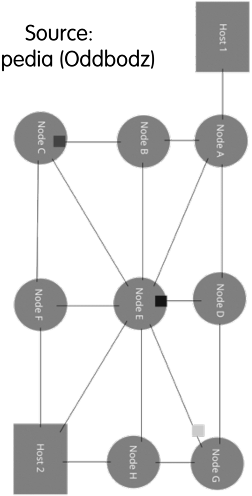
Garcia

en.wikipedia.org/wiki/Packet_switching

Packet-Switched System

- The Internet is a packet-switched system through which digital data is sent by breaking the data into blocks of bits called packets, which contain both the data being transmitted and control information for routing the data.

Source:
Wikipedia (Oddbodz)

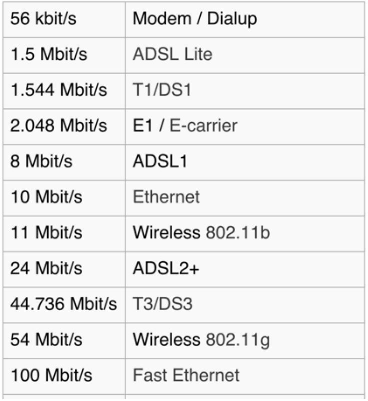


The data packets take different routes to their destinations.

en.wikipedia.org/wiki/Network_performance#Bandwidth

Bandwidth and Latency

- The size and speed of systems affect their use.
  - E.g., Netflix on dialup? Nope.
- Bandwidth
  - a measure of bit rate—the amount of data (measured in bits b) that can be sent in a fixed time. Usually b/s
- Latency
  - the time elapsed between the transmission and the receipt of a request. Usually ms.



56 kbit/s	Modem / Dialup
1.5 Mbit/s	ADSL Lite
1.544 Mbit/s	T1/DS1
2.048 Mbit/s	E1 / E-carrier
8 Mbit/s	ADSL1
10 Mbit/s	Ethernet
11 Mbit/s	Wireless 802.11b
24 Mbit/s	ADSL2+
44.736 Mbit/s	T3/DS3
54 Mbit/s	Wireless 802.11g
100 Mbit/s	Fast Ethernet

(Cal) Clicker Question

What has the highest bandwidth?

a) Wireless networks
b) Wired networks
c) Your hard drive and your computer
d) Your CPU and its scratch space
e) A truck of MicroSD cards going next door

Internet
Cyber security

en.wikipedia.org/wiki/Computer_security
en.wikipedia.org/wiki/Web_of_trust

Cyber Security

- DNS was not designed to be completely secure
- Implementing cybersecurity has software, hardware, and human components
- Phishing, viruses, and other attacks have human and software components
- Cyber warfare and cyber crime have widespread and potentially devastating effects
- Distributed denial-of-service attacks (DDoS) compromise a target by flooding it with requests from multiple systems
- Antivirus software and firewalls can help prevent unauthorized access to private data

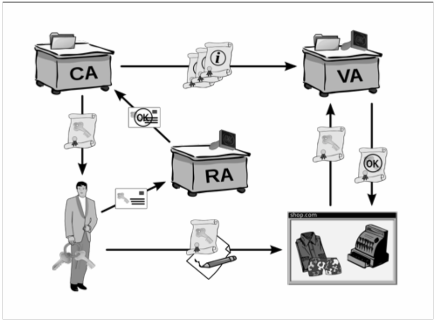
Edward Snowden. Wikipedia *(Hic et nunc)*

en.wikipedia.org/wiki/Public_key_infrastructure

Cryptography

- Cryptography is
  - essential to many models of cybersecurity
  - has a mathematical foundation
- Open standards help ensure cryptography is secure
- Symmetric encryption is a method of encryption involving one key for encryption and decryption
- Public key encryption (not symmetric) is an encryption method that is widely used because of the functionality it provides
- Certificate authorities (CAs) issue digital certificates that validate the ownership of encrypted keys used in secured communications and are based on a trust model
- The trust model of the Internet involves trade-offs.

Public Key Infrastructure. Wikipedia *(Chrkl)*



www.youtube.com/watch?v=3QnD2c4Xovk

Public Key Encryption