Class 29: Trick-or-Treat Protocols

CS150: Computer Science
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/evans

This Week in CS150

- Today:
  - Networking and the Internet
  - Trick-or-Treat Protocols
- Wednesday:
  - How to make a dynamic web site using HTML, SQL, Python
- Friday: Return to Models of Computation

Who Invented the Internet?

Who Invented Networking?

What is a Network?

A group of three or more connected communicating entities

Beacon Chain Networking

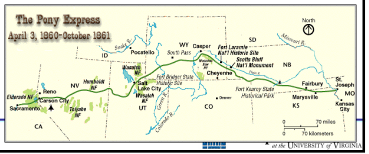
Thus, from some far-away beleaguered island, where all day long the men have fought a desperate battle from their city walls, the smoke goes up to heaven; but no sooner has the sun gone down than the light from the line of beacons blazes up and shoots into the sky to warn the neighboring islanders and bring them to the rescue in their ships.

Iliad, Homer, 700 BC

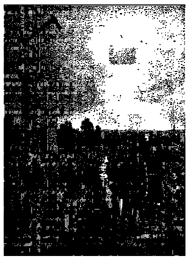
Chain of beacon's signaled Agammemnon's return (~1200BC), spread on Greek peaks over 600km.

Pony Express

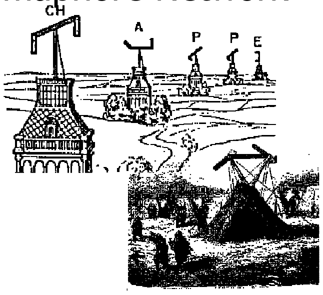
- April 1860 – October 1861
- Missouri to California
  - 10 days
  - 10-15 miles per horse, ~100 miles per rider
- 400 horses total (not per station like Kahn's)



Chappe's Semaphore Network



First Line (Paris to Lille), 1794



Mobile Semaphore Telegraph
Used in the Crimean War 1853-1856

Measuring Networks

- **Latency**

  Time from sending a bit until it arrives

  seconds (or *seconds per geographic distance*)
- **Bandwidth**

  How much information can you transmit per time unit

  bits per second

Latency and Bandwidth

- Napoleon's Network: Paris to Toulon, 475 mi
- Latency: 13 minutes (1.6s per mile)
  - What is the delay at each signaling station, how many stations to reach destination
  - At this rate, it would take ~1 hour to get a bit from California
- Bandwidth: 2 symbols per minute (98 possible symbols, so that is ~13 bits per minute
  - How fast can signalers make symbols
  - At this rate, it would take you about 9 days to get *ps7.zip*

Improving Latency

- Less transfer points
  - Longer distances between transfer points
  - Semaphores: how far can you see clearly
    - Telescopes can help, but curvature of Earth is hard to overcome
  - Use wires (electrical telegraphs, 1837)
- Faster travel
  - Hard to beat speed of light (semaphore network)
  - Electrons in copper travel about 1/3rd speed of light
- Faster transfers
  - Replace humans with machines

How many transfer points between here and California?

```
] tracert cs.berkeley.edu
Tracing route to cs.berkeley.edu [169.229.60.28]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  router137.cs.Virginia.EDU [128.143.137.1]
  2   <10 ms   <10 ms   <10 ms  carruthers-6509a-x.misc.Virginia.EDU [128.143.222.46]
  3   <10 ms   <10 ms   <10 ms  uva-internet.acc.Virginia.EDU [128.143.222.93]
  4   <10 ms   <10 ms   <10 ms  192.35.48.42
  5
  6
  7
  8
  9
 10
 11
 12
 13
 14
 15    70 ms    70 ms    70 ms  vlan199.inr-202-doecev.Berkeley.EDU [128.32.0.203]
 16     *        *        *     Request timed out.
 17    70 ms   100 ms    70 ms  relay2.EECS.Berkeley.EDU [169.229.60.28]

Trace complete.
```

```
> (define meters-to-berkeley (* 1600 3000))  ;; 3000 miles * 1600 meters/mi
> (define seconds-to-berkeley 0.070)
> (define speed-to-berkeley (/ meters-to-berkeley seconds-to-berkeley))
> speed-to-berkeley ;;; meters per second
68571428.57142857
> (define speed-of-light 300000000) ;;; 300 000 000 meters per second
> (/ speed-of-light speed-to-berkeley)
4.375
```

The Internet latency today is about ¼ the best physically possible!

Improving Bandwidth

- Faster transmission
  - Train signalers to move semaphore flags faster
  - Use something less physically demanding to transmit
- Bigger pipes
  - Have multiple signalers transmit every other letter at the same time
- Better encoding
  - Figure out how to code more than 98 symbols with semaphore signal
  - Morse code (1840s)

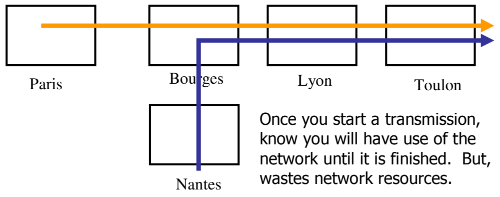
Morse Code

Represent letters with series of short and long electrical pulses

A	B	C	D
• –	– • • •	– • – •	– • •
E	F	G	H
•	• • – •	– – •	• • • •
I	J	K	L
• •	• – – –	– • –	• – • •
M	N	O	P
– –	– •	– – –	• – – •
Q	R	S	T
– – • –	• – •	• • •	–
U	V	W	X
• • –	• • • –	• – –	– • • –
Y		Z	
– • – –		– – • •	

Circuit Switching

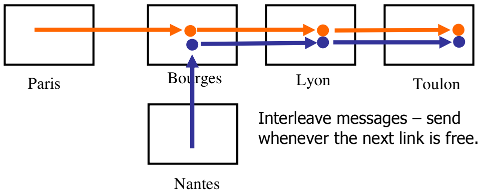
- Reserve a whole path through the network for the whole message transmission



Once you start a transmission, know you will have use of the network until it is finished. But, wastes network resources.

Packet Switching

- Use one link at a time



Interleave messages – send whenever the next link is free.

Circuit and Packet Switching

- (Land) Telephone Network
  - Circuit: when you dial a number, you have a reservation on a path through the network until you hang up
- The Internet
  - Packet: messages are broken into small packets, that find their way through the network link by link

internetwork

A collection of multiple networks connected together, so messages can be transmitted between nodes on different networks.

Okay, so *who* invented the Internet?

"Trick or Treat" Protocols

"Trick or Treat" Protocols

- Trick-or-Treater must convince victim that she poses a credible threat
- Need to **prove** you know a trick, **without revealing** what it is
  - Revealing the trick gives victim opportunity to prevent it

Tricker's License

Virginia

TRICKER'S LICENSE

DOE, JANE Q
ANYWHERE STREET
RICHMOND, VA 2322
RICHMOND CITY

CUSTOMER NO. 123-45-6789

CLASS NONE

ENDORSEMENTS NONE

DOB 01-01-1982

EXPIRES 01-31-2006

ISSUED 03-12-1999

COURT CODE

ORGAN DONOR

UNDER 21 UNTIL 01-01-2003

UNDER 18 UNTIL 01-01-2000

Jane Doe

Cryptographic Hash Functions

One-way

Given h, it is hard to find x such that $H(x) = h$.

Collision resistance

Given x, it is hard to find $y \neq x$ such that $H(y) = H(x)$.

Example One-Way Function

Input: two 100 digit numbers, x and y

Output: the middle 100 digits of $x * y$

Given x and y, it is easy to calculate

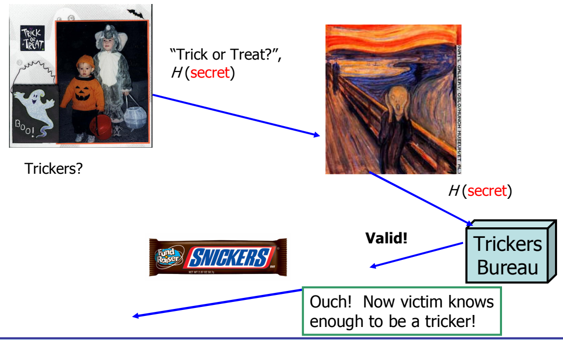
$f(x, y)$ = select middle 100 digits $(x * y)$

Given $f(x, y)$ hard to find x and y.

A Better Hash Function?

- $H(x) = \text{encrypt}_x(0)$
- Weak collision resistance?
  - Given x, it should be hard to find $y \neq x$ such that $H(y) = H(x)$.
  - Yes – encryption is one-to-one. (There is no such y.)
- A good hash function?
  - No, its output is as big as the message!

Trick-or-Treat



"Trick or Treat?", *H* (secret)

Trickers?

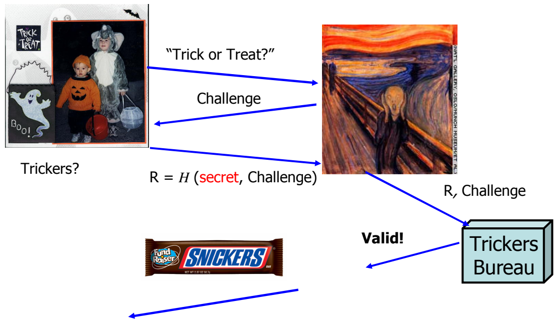
H (secret)

Valid!

Trickers Bureau

Ouch! Now victim knows enough to be a tricker!

Trick-or-Treat



"Trick or Treat?"

Challenge

Trickers?

R = H (secret, Challenge)

R, Challenge

Valid!

Trickers Bureau

Problem Set 7

http://www.HooRides.net

Charge

- Next class:
  - Who invented the Internet?
  - How to make a dynamic web application
  - Password Authentication (similar to Trick-or-Treat)
- Before Wednesday:
  - Read through PS7 handout