I. Announcements

II. Building WWW on top of the internet
   a. URL (Uniform resource locator) – gives location
   b. HTTP (hypertext transfer protocol) – talks to server
   c. HTML (hypertext markup language) – how we describe information for display
   d. Browser – program to control this
   e. Embellishments
      i. Pictures, sounds, movies, loadable software, ...
   f. When you click on a URL
      i. Client opens TCP/IP connection to host
         1. Sends request GET /filename HTTP/1.0
      ii. Server returns
         1. Header information
         2. HTML
         3. Since server returns the text, it can be created as needed
      iii. URL format can be service://hostname/filename?other_stuff
         1. Can encode data (forms), request to run program on server (cgi-bin),
            anything else, ...
      iv. Forms and programs
         1. Common gateway interface (CGI)
            a. Run program on server to send info back to client
            b. Can get more sophisticated than mere forms
      v. Programs can be in Javascript, Java (applets), plug-ins, ActiveX, ...

III. Modes of communication
   a. Landline to landline call
   b. Cell phone to landline call
   c. Skype to cell phone call
   d. Gmail to your neighbor

IV. How does the web track you?
   a. Web beacon
      i. Send email to someone@somewhere.org
      ii. Include embedded image of URL
         http://comewhere.org/bug.jpg?someone@somwhere.org
      iii. When email is read, the image is requested via the URL
      iv. Part after ? is ignored (to give the jpg which may not be noticeable in your email reader)
      v. But complete URL is stored in server’s log files
      vi. So they know when you opened the email
      vii. Often used by spammers to test email addresses
   b. Tracking pixels
      i. Add a single pixel to your image
         1. Have pixel come from a tracking URL
         2. Each time the page is drawn, the tracking pixel has to be drawn and so
            the tracking URL has to be reached.
c. Cookies
   i. http is stateless
      1. but we’d like it to have memory at times
      2. cookies provide this memory
   ii. cookie is a chunk of text sent by server and stored on client
      1. stored in browser when running
      2. stored in file system when not running
   iii. when client connects to a domain, cookie is sent back to server
      1. sent back only to where it came from and sent as is
      2. pretty benign so far
V. Cookies getting more complicated
   a. Tracking pixels
      i. Enable cookies to be stored among many server sites
      ii. You fetch a page; it loads a tracking pixel from doubleclick
      iii. This gives doubleclick access to your cookies
      iv. Doubleclick sends back a suitable advertisement
      v. Doubleclick remembers what you did on the site
      vi. Next time, doubleclick can track you a little bit better
   b. More advanced cookies
      i. Flash cookies
         1. Cookie like mechanism shared by all sites that use flash
      ii. Super cookies
         1. Used e.g. on cell phones by ATT/Verizon
            a. Your phone sends an http: request to visit a web site
            b. Verizon injects an HTTP header to provide identification of you
               i. Described as trusted Verizon network
            c. Website knows your ID without knowing who you are
            d. This is enough to effectively serve ads
            e. Ads are more relevant to the consumer
         2. Once discovered; ATT announces it is no longer attaching hidden
            internet tracking codes to data transmitted from users’ smartphones
            (11/2014)
         3. FCC ruling (3/2016)
            a. 3/2013 Verizon started injecting supercookies into messages
            b. 12/2014 Noticed that Verizon was injecting information without
               informing consumers
            c. 1/2015 Verizon acknowledged that they were doing this but
               that they were of little value to third party advertisers;
               however, a Verizon advertising partner was found to be using
               supercookies to override consumers’ choices
            d. 3/2015 Verizon updated its privacy policy to disclose what they
               had been doing and offered consumers the ability to opt out.
            e. FCC fined Verizon $1.35M and asked them to adopt a 3 year
               compliance program.
iii. HTML canvas fingerprinting
   1. Your browser, operating system, etc. tell a lot about you. You are more unique than you would expect.

c. Defenses
   i. Addons like AdBlock, FlashBlock, Cookie Monster, Ghostery, NoScript
      1. But companies can retaliate
         a. Yahoo restricting email accounts if ad blocker detected
         b. Facebook blocking ad blockers, ad blockers working around Facebook, ....

VI. Creepy or not creepy
   a. Apple tracks you via wifi; att tracks you via cell towers
      i. Apple knows what wifi networks are near you because it's on your phone
      ii. ATT knows what cell towers are near you because they are aware of you

VII. Security and privacy and nuisance issues
   a. Eavesdropping
      i. Encryption helps
   b. Masquerading
      i. Can be handled by authentication in both directions
   c. Spam
      i. Iconic message is from Nigeria asking you to accept their inheritance
      ii. 269B sent daily
      iii. Clickthrough rate North America 3.1%
      iv. Open rate North America 34.1%
      v. Percentage of Americans who check email – in bathroom 42%, in bed 50%, while driving 18%
      vi. 65% of emails are spam (175B per day)
      vii. Seems innocuous but 65% is a lot, though the number is decreasing (malware being shifted elsewhere)
   d. Worms
      i. Work their way across the internet entering machine after machine, usually without human knowledge
            a. Believed to have been developed by US and Israel
            b. Attacked sites in Iran
               i. The uranium enrichment plant at Natanz
               ii. Destroyed roughly 1/5 of centrifuges causing them to spin out of control
            c. First publicly known attack of cyber warfare
   e. Viruses
      i. Spread like worms but have the power to corrupt functions on your machine
      ii. Anna Kournikova virus (2001)
         1. AnnaKournikova.jpg.vbs
      iii. Have the virus get into the kernel and have it take some control
iv. Have it get into boot sequence so that it can regenerate itself when the machine restarts.

v. Rootkit is a Trojan horse – changes systems software so that
   1. Evidence of attacks is hidden
   2. Attackers have backdoor access to systems

vi. Rootkit runs with same powers as malware detection
   1. May have been installed as part of software you thought was secure or through email attachment or bad click

vii. Can set up **Keylogger**
   1. Software that gets into your machine, records every key stroke and mouse click and sends it back to the source → passwords, URLs visited,

f. Phishing
   i. Fake website mimics real web site and attempts to get your credit card or other info
      1. Fancy bear (Russian cyber hackers) spear phished Podesta telling him to change his google password at https://bit.ly/1PibSU0

   g. Pharming
      i. Like phishing but more extensive; may involve DNS cache poisoning or fake sites
      ii. Phishers drop a couple lines in the water and wait to see who will take the bait. Pharmers are more like cybercriminals harvesting the Internet at a scale larger than anything seen before.

h. Pagejacking
   i. Detours visitors from legitimate sites to copycat webpages; often redirecting them to pornographic sites

   j. Flybox
      i. Don’t try this at home

   k. Ransomware
      i. Cryptolocker (2013); I’ve encrypted your disk; send bitcoins or cash within 3 days or I will destroy the key

k. Denial of Service
   i. Botnets
      1. Build a network of computers
         a. Maybe get in through virus propagation
         b. Maybe get in through back doors left open
         c. Botnet takes control of the bots and turns them into zombies
         d. Can involve hundreds of thousands of devices
      2. Botnets spend their time
         a. Finding machines to convert to zombies
         b. Sending spam
         c. Sending viruses
         d. Sending spyware
         e. Sending lots of requests to DNS server (or amazon or .. ) to shut them down
         f. Clicking on ads to boost revenue (clickfraud)
ii. Example from last year
   1. 10/16 Botnets attacked Dyn, an internet infrastructure company that supports Twitter, Amazon, Reddit, Tumbler, Spotify and Netflix among others
      a. Used IoT devices' DVRs and cameras made by a Chinese hi-tech company XiongMai
         i. Doors to telnet and ssh were left open
         ii. Found 515,000 such devices by scanning the internet
      1. On Monday, a massive botnet, made up of 100,000 infected computers and other internet connected devices, was found by Daniel Cohen, head of RSA’s FraudAction business unit, for sale on the Alpha Bay marketplace.
      2. A botnet of this size could be used to launch DDoS attacks in addition to automated spam and ransomware campaigns. The price tag was $7,500, payable in bitcoin. The anonymous vendor claimed it could generate a massive 1 terabit per second worth of internet traffic.
      3. Bringing down Dyn DNS service at around that time required 1.2 TB (so 10x as much)

VIII. A few workarounds
   a. Ten minute mail or hushmail
   b. Tor for onion routing
      i. You pick 3 nodes from a list of Tor sites
         1. Triple Encode your message
            a. First person takes off one layer which tells them where to send it
            b. Second person does the same
            c. Third person takes off third layer and then delivers it
         2. Messages can come back the same way