CS 60: Computer Networks

Sergey Bratus, Spring 2017
Lectures: Life Sciences Center 200, in the **3B** time slot. X-Hour will only be used when announced.
My office is Sudikoff 065, office hours by appointment.

Objective: To develop an understanding of TCP/IP protocol stacks, the software that runs the Internet. To understand the implementation of TCP/IP protocols from the ground up, starting at the link layer (Ethernet, ARP) and going up through IPv4, IPv6 and TCP to application protocols such as DNS and HTTP. To use the standard Berkeley sockets layer, and understand how it functions under the hood, including raw sockets. To analyze TCP/IP packets on the wire, understand the functionality of firewalls and intrusion detection systems; to understand and craft non-protocol-compliant packets used in attacks on network devices.

Pre-requisites: CS 50. You will be writing and reading a lot of C code in a Unix environment, using Unix libraries, GDB, and command line tools; you will be expected to be comfortable with these.

OS and HW: Linux and Mac OS X. It may be possible to develop the same code on Windows, and I will accept working solutions, but the TA won't be able to support it and your mileage *will* vary.

Course directory: `http://www.cs.dartmouth.edu/~sergey/cs60/` Lecture notes and other reading materials will be posted in the course directory after each class, and emailed to the class list.

Grades: 70% labs (homework), 30% final project. The 70% credit for labs will be divided among labs according to difficulty, varying between 10%–15% per lab.

Lecture topics: (these topics do not directly correspond to the lectures; rather, they follow the grounds-up succession of protocols we will deal with)

- Link-layer connectivity: what your computer needs to know to get to the Internet. Ethernet and ARP.
- IP networks: global addressing scheme for the Internet; basics of IP routing. How your packets get from here to where you want them to go and back again, and how you can trace their path.
- IP protocol, the packet-level view. The 20 bytes that connect the world and need firewalls.
- An overview of UDP and TCP: datagrams and streams, and their uses on the Internet. Berkeley sockets as the Internet API.
- Firewalls. Linux Netfilter/IPtables and BSD PacketFilter (PF). Network Address Translation (NAT) and other routing and traffic-shaping features of a Linux box.
- Internals of TCP. Three-way handshake, sliding window, push and urgent data, closing a connection, and rejecting connections. TCP flow control and gotchas. Slow start, exponential back-off, and alternatives.
- From sockets to packets and back. OS TCP/IP stacks under the hood. Linux *skbuff*s and BSD *mbuff*s.
- DNS, the basic protocol and the (in)famous bug(s) that broke the Internet.
- HTTP and an overview of HTTPS. Certificate authorities and their failures. Famous bugs in SSL/TLS implementations.
- Stealing and crafting packets. Packet-level attacks on TCP/IP stacks, past and present.
- IPv6: the protocol your smartphone is probably using.
- Intrusion Detection/Prevention systems (IDS/IPS) and evading them.
- Global IP routing: what ISPs do and how they do it.
- Virtual Private Networks and how to build one.

Textbook: TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition), by Kevin R. Fall and W. Richard Stevens, Addison-Wesley, 2011, `https://www.amazon.com/TCP-Illustrated-Protocols-Addison-Wesley-Professional/dp/0321336313`

Additional Reading:

How can an internet work and how does the Internet work, Stanislav Shalunov, `http://www.mccme.ru/computers/Shalunov-inet.pdf` (free PDF online). This old book provides a concise overview of what matters in the design of Internet protocols, and why their designers made the choices they did.

The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, by Charles M. Kozierok, `http://www.tcpipguide.com/`. Free material is available online: `http://www.tcpipguide.com/free/`, very handy to look up an explanation of a particular protocol feature.

IPv6 for IPv4 Experts (draft), by Yar Tikhiy, `https://sites.google.com/site/yartikhiy/home/ipv6book` (free PDF online). Don't worry, you will be enough of an IPv4 expert to read this book :)

Beej's Guide to Network Programming: Using Internet Sockets, by Brian "Beej Jorgensen" Hall, `http://beej.us/guide/bgnet/` (free PDF and HTML online)