Proposal: Information Flow on the Internet

Jeremy Foote
jdfoote@u.northwestern.edu

Overall Goal

The goal of this session will be for students to gain an intuitive understanding of some of the technologies that underlie the Internet, such as packets, packet routing, encryption, VPN, Tor, man-in-the-middle attacks, and government surveillance. Each of these technologies will be explained, and then enacted through an in-class packet routing exercise.

This proposal is based on feedback from the previous class that I taught. I have tried to make the discussion much more about the technical aspects of the Internet rather than the social implications.

IP Addresses and Packets

We will talk a little bit about the history of the Internet - how computer internetworking started, and how decisions were made in the early days.

We will discuss what IP addresses are - how they are assigned, why websites have access to them, and what sort of information can be gleaned from them. We will also talk about how TCP/IP works - with an explanation of packets and headers.

At this point, I will introduce an activity borrowed from Aaron Shaw's class. I will use envelopes with content in them to represent packets. As the class moves along, we will adjust the activity based on the topic we are teaching. I haven't worked out all of the details, but I think I might have one student act as "Gmail", one student act as an email sender, another as an email receiver. The other students will be nodes in the network, and we can show how information moves around and is copied during a simple email transaction.

In this initial portion of class, we will also show the importance of the decentralized nature of the Internet and discuss the "dumb network" implementation. If there is enough time, it would also be good to talk about cookies here.

Encryption and Man-in-the-middle

We will discuss the opportunities for packet sniffing and man-in-the middle attacks. One student will now be assigned the role of a nefarious node who is stealing usernames and passwords as they are passed through, and another student will be the NSA, which will store a copy of all of the packets that come through, and will subpoena Google for access to the emails on its servers. I will ask the students how they could stop others from seeing their messages.

We will talk about what encryption is, and how it works at a packet level. This section could easily be expanded to explain public key encryption, SSL, and certificates.

Proxies, VPN, and Tor

We will talk about another limitation of TCP/IP. The NSA student will now be a despotic government, who wants to know everyone who visits an anti-government website. We will talk about how even encrypted information still contains a header, which lets men-in-the-middle to know who has been where, and we will talk about how to possibly solve that problem.

I'll see if students can come up with solutions, and then we will talk about the way that proxies, VPN, and Tor each work, and the advantages and disadvantages of each. This would probably be a good place to reinforce the benefits and drawbacks of the inherent anonymity of the Internet.

Philosophical Musings

If there is time, I'd love to talk about how the design decisions of the Internet were made to solve the small, initial problems of the network, but they have had incredible ramifications. Perhaps we could end with discussion about what sorts of technological decisions being made now might have similar long-term consequences (e.g., self-driving car regulations, gene manipulation, etc.)