CMPS 10 Lecture Notes: Lecture 20 (3-10-2016)
LAST DAY!

Today's Lecture: Answering Questions!
1.) Why is torrenting so hard for the police to stop.
2.) How to hack?
3.) What did you want to teach that the curriculum wouldn't let teach?

- The curriculum didn't really cause any problems. But the thing is that many classes are made difficult when there is a really big variance in terms of the background of the students. So this class is, in some sense, the epitome of this. This class has many people from many different backgrounds, so it's tough to pick a way to talk about it that doesn't simultaneously make some people bored while others still struggle.

4.) The Dark Web?

- Well, public key cryptography. The fact that people can have a dialog in front of everyone in plain sight and yet still no one else is able to understand it.
  - public key cryptography is what enabled the commercial web.
    * and the commercial web is essentially what made the web the major thing that it is today. Without commercial side of it, its possible that it wouldn't have seen the growth that it had.

5.) AI, HCI, How computers can use Natural Language.

- Maybe we will get to this if we have time!

Secret Sharing.

One of the nicest ideas in Computer Science: Secret Sharing.

- Imagine that we have a safe, and the safe has a lot of key holes.
- You have a secret. And you want to distribute it, but perhaps in a very specific way.
  - You have 8 key holes, 8 different keys, give one key to each of 8 different people. And make it so that ANY three people, it doesn't matter who they are, then they can open the safe if they are all together.
  - This concept is realizable with information. That is, we can do this WITH information.
- Imagine that you have a Document. And for simplicity, let's say that your document is 900 bits.
  - Let's say that your document is your will. But you don't want to announce your will to everyone ahead of time. You want to make it so that three of your kids have to get together to figure it out.
    * So, we want to make it so that you give 300 bits to each of your kids. And you want it to be so that any three can get together to piece together the whole thing.
      · BUT we can't just split the document up into chunks, because even then people would be able to get some information out of their personal chunk. We want the information that each individual has to be gibberish on its own, but only makes sense when combined with the work of others.
- So if we are dealing with illegal file sharing:
  - Someone makes an announcement that says "I would like pieces corresponding to this song." And the different computers have different parts of the song, but they are all just fragments. They don't appear to be recognizable.

AKAMAI

- A company that works with other companies. Takes files, spreads it from all over the world. So when you try to download something, the bits come from everywhere.

MP3 and DSL was a huge thing towards leading to music piracy.

- And this in some ways led to death of music industry.

- Teacher used to work at Microsoft in Seattle. His neighbor John was the vice president of Excel.
  - Apparantly there was a huge internal fight about whether "Microsoft Office" should exist (the thing that links Word, Excel, Power Point, etc.)
    * John was strongly in favor of not linking office. But they did link it, and it made Microsoft a lot of money. And because of that, John essentially had to quit.
    * His wife was also very wealthy. And so then they said well we can enjoy our lives now. But his wife said no I like my career and so they divorced.
      · So now he lives in wind surfer paradise, "Hood River Oregon" where a desert and a river create a neat bit of wind!
- Teacher's other neighbor was the guy who thought it would e a good idea to put software on CDs.
  - CDs, originally, were not meant for music. It was because it was a far faster, more convenient way of distributing software.
    * So people had CD Readers. they couldn't write CDs but they could write them.
    * So you could put a CD into your computer and "rip" it, store it in your hard drive.
      · And then you would use a file sharing program, which would take the "document" and split it up into the fragments that it then can be distributed it.
      · So your computer would now have fragments of all of these songs.
    * You could get a list of thousands of computers from a Master computer that would tell you who all had fragments of the document you wanted.
      · So the illegal part was that master database. They were the ones that had the illegal information.
      · So the logical conclusion: make the master database distributed as well! So now, making databases that even had fragments of things became illegal as well. So they way it is done now is basically through a shake down. People who do this illegal thing have a small chance of having a massive penalty, and a huge legal team, facing them.

Why Do We Have Laws?

We'll get more technical about the previous topic in a second, but there is another thing that it is fun to think of in a more quantitative way: Why do we have laws?

- To regulate people? But why do we want to regulate them?
  - So they don't impact other people negatively? Ah, but we still negatively impact each other all the time and we consider that to be perfectly fine.
    * for example: Breathing is a good idea. Not breathing is bad. So why don't we have a law about it?
      · Because a law that mandates breathing is an unnecessary law.
- To what question are laws the answer?
  - Why do we have a law against robbing?
    * there are two possible societies: one in which everyone robs, and one in which no one robs. are these two situations the same? Are they symmetric?
      · Hopefully we can agree that a society in which no one robs is better than a society in which everyone robs. Hopefully we can just accept this point for a moment.
      · So why do we have laws against robbery if that's the case?
  - Let's look at the example of roads.
    * Roads in some other countries are just crazy, people go every which way. Roads in most countries have two sides: one side people go in one direction, the other side people go in the other direction.

Imagine two curves: Robbery is a U-shape and No Robbery is an upside-down-U.

- And a little metal ball that represents the state of society.
  - with Robbery, the ball is at the bottom of a valley formed by the U.
  - with No Robbery, the ball is at the top of a hill formed by the upside-down-U.

        * when in a valley, it is impossible to escape from it. It is stable (i.e. you are gonna STAY in a robbery filled world. Even if 99 percent of everyone said "ok, starting tomorrow, no more robbing" if as little as 1 percent keep on robbing, it's gonna encourage everyone else to go back to robbing again too).
        * When on a hill, it is very unstable. (i.e., you are gonna have a couple of people who start robbing and then everyone else is like "wait, what am I a sucker" and it all literally goes down hill from there and now you've ended up in a robbery world again).

- Nash Equillabrium
    - There is a game. Players of the game can choose to rob or not to rob.
        * A collective action is an equilibrium if it has the following property:
            · You pick an action. And you are told no one else will change their action. Will you change yours? And if you say "no, I wouldn't change" then that is an equilibrium.
            · Nobody stealing is *not* an equilibrium (you are told no one else is stealing and you aren't stealing either. Will you change yours? Teachers says people will say "yes" so not equilibrium since you changed your answer).
            · So laws essentially say for these non equilibrium cases "alright, you can
            · there are many situations in which the pursuit of individual self interest lead to situations that are bad for everyone, sometimes produces globally good outcomes, sometimes produces globally bad outcomes.
            · Laws disincentivize people from moving away from the globally good equilibrium.

There are a lot of ads on the internet.

- If we wanted to pay 10 dollars to cover all of our ad costs, it leads to a problem, because who do we pay the money to?
- The ad filled internet is a valley world. We are trapped here. It would require a lot of force to get us out.

Laws exist for one reason: when the pursuit of individual self interest leads to outcomes that do not promote social welfare, whereas there exists equilibriums that are much better for society.

- and of course people can disagree about specific equilibriums. And hence that is where politics do.
    - But then there are other things that we all agree are good if we could get there. But we can't get there because it requires too much collaboration.

Ok, back to secret sharing.

- Let's say we have 100 bits.
- and the bits are going to be sent to us through a Channel (and the channel can be the aether, can be a copper wire, whatever).
    - And now we are told that 5 of our 100 bits are going to be erased.
        * So we will get 95 bits and 5 question marks.
            · Is there something we can do so that we can recover what the originally intended message was.
- Maybe we could send the exact same message again two times?
    - Ah, but what is to protect us from the same bit getting erased both times?
        * What if we sent 6 messages? Maybe that wold be better but that's awfully wasteful.

So, let's imagine that we have a good channel and a bad channel.

- the good channel is expensive, and the bad channel is cheap.
- And we want to transmit 100 bits.
    - Imagine that the cheap channel is made up of sockets. And we put each bit in a socket. But then there are also objects on the 'expensive' side, and each object on the expensive side are connected to a small number of objects on the cheap side.
    - to make life easy, let's say that each object on the left is connected to an equal number of objects on the right, and vice versa.

        * This pattern of connections is known to both the sender and receiver, and it is designed before information transmission happens. So you can think of this as their secret.
            · For each of the expensive objects, it will count the number of 0s residing in the sockets its connected to. If even, it will be a 0. If odd, it will be a 1.
    - And so the 'socket' information gets sent on the poor quality channel, and the 'even or odd' value gets sent on the high quality channel.
        * So information than gets sent to us in the following form: 100 bits from poor channel, 20 bits from high quality channel.
            · So we take our 100 bits, we place them there and they get sent to us, but we also compute those 20 bits by counting in the specific location that we're talking about, is the number of 0s odd or even, and that gets sent on the 'good' channel.
- Now imagine that you say that the bits in the poor quality channel have a chance to get erased with some probability, say 5 percent.
    - So if you get 100 bits, on average there will be 5 question marks.
        * How does this help us?
    - What you are hoping, is that there exists a question mark and a square so that for the square there is exactly one question mark.
        * Because if that's the case you can determine if you should have an odd number of 0s or an even number.
            · So you can decode that information.
            · But what makes it really cool?
            · Because in that same picture, there may well have been a different square that had two question marks. But now that you've solved one of the bits for a different guy, now you can also solve it for other guys.
            · this cascades! It's a little bit like solving a crossword puzzle! As you write more entries it becomes easier and easier to solve other entries.

Ah, but now you might be saying, you don't REALLY have a perfect channel.

- So you just use recursion! You apply the proctection bits to other projection bits! You keep on protecting and protecting! It narrows! And so you can ultimately use a very small number of bits to protect more and more. And then at the end, you can just send your six extra copies of four bits or whatever, and you don't care because it's so small.

It turns out that you do not want it to be regular. You want there to be a skew between the protected bits.

- Imagine that we are given a cigarette lighter, and we are asked to burn the cigarette lighter.
- You could go up to a tree and hold your cigarette lighter, but it probably wouldn't work.
    - Instead what you would do is gather some pine needles, and then some small branches, and then you gather bigger branches of wood, and then you are creating this structure, and then you light the pine needles, and then from there you are able to burn just about everything.
- the analogy with this, is if we make everything regular, there is a pretty good chance in which every square will have two or more question marks.
    - So instead what we say, is we say that there are some question marks that participate in fewer connections.
        * It gives us a place to start. There will be some squares, by virtue of the fact they only depend on a few bits, will only have one question mark. And these are the pine needles. By the time you've figured out how to burn all of the pine needles, now you can solve for the squares with slightly more connections, and so on and so on.
        * That idea alone saves about 5 to 10 percent of your iPhones battery, because your iPhone needs to spend a lot of time unpacking the bits it gets from the phone.
            · You need to strip the information away to solve the original intent.
            · Because the code was regular, we had to send a lot more information. If there was no square that had exactly one question mark, you would have to end up making a lot of guesses, which ends up burning a tremendous amount of battery.

            - Designing such patterns is essentially a completely solved problem. And most of the insights come from physics.
            - We can speak in the efficiency of burning of the code; the pine needle analogy is remarkably apt.
            - Things connect, and it is a very nice thing to see things connect.
            - Math is typically the thing that connects everything.

Some small company created multi touch

- But multi touch is what enabled the iPhone to have gesture based input
  - And THAT is what enabled us to ditch the keyboard.
    * Which leads to a nice big screen.
      - When lets us actually see things better.

And there are more exciting technologies on the way.

- If virtual reality happens, especially in the holographic form, humanity as we know it will change.
- Language is the most important thing we've created so far, and VR is getting us to that point.
  - We're getting better and better at it, but we still might not get there.

A Form of Hacking

Teacher is afraid we didn't get to the hacking question. But he very much encourages us to look up:

- CRISPR CAS9
  - JENNIFER DUDNA (this may be a misspelling, professor of bio chemistry at Berkeley).
  - This is hacking the biological world. Take a mechanism that exists in bacteria, to be able to modify DNA in adult cells pretty much in any way she pleases. Roughly speaking this is an enzyme, one is a working part, the other is a socket.
    * Take any fragment of DNA, load it into a cell. What this complex will do is enter it into a cell, and start scanning for that pattern, and if it does it, it cuts the DNA at that place. From the point of view of a molecular biologist, this is the promised land. We think this is going to transform medicine. But there is a big patent fight for the centuries.
    * Great video that explains how this works. Watch it on YouTube. It's remarkable. It's worth seeing. and very fresh, 2 to 3 years old. Assuming you are reading these notes on a computer, just click on the underline above to watch in on You Tube right now!

And that's that! Thanks for the great quarter everyone!