“Intuitive” Protocols

From the ‘Best of Beta’, Emily announces that her name is Emily, and considers the nature of the Internet.

Upon dwelling upon the core of the Internet, and the fact that its nothing more than a very large, very distributed system, I always begin to feel a gentle, yet unshakable, sense of sadness creep over me; kind of like when you first realise that the world is not a fair place and that kitten on the box may never reach its treat, or that Keanu Reeves will almost certainly make more money than you over arbitrary time scales.

Facial expressions are for the weak.

The Internet is such a core utility in our lives, but an eternally confusing one. Whenever people try to “explain” the core protocols and connections that make up distributed, weblike, systems, they always lean towards “intuitive”, “approachable” arguments. Interestingly, no matter how they spin it, these kinds of intuitive arguments are not intuitive. A successful intuitive explanation must invoke experiences that someone would have in real life, and I have never had a real-life experience that has resembled any form of common distributed or Internet protocol.

For example, let’s suppose that I am having a nice conversation with a friend. If that conversation was similar to HTTP, it would go something like:

Emily. Alex, I would like today’s `xkcd`.

Alex. OK, here it is.

Emily. Alex, I would like last week’s comic.

Alex. Yeah, it’s here.

Emily. Alex, I want the comic with Knuth being a ninja.

Alex. … Give me a moment to find it.

Emily. Let me tell you again that I want the `xkcd` comic with Knuth being a ninja.

Alex. … Here.

[Hours pass.]

Emily. Alex, do you have the `xkcd` comic with the ghost and the eternal passage of time?

Alex. 404 FILE NOT FOUND. GO AWAY.

And that, children, is how you lose friends forever.

What’s the Gossip?

But maybe something less concrete, more conceptual, is necessary for the real intuitive explanation experience. Gossip protocols are ostensibly modeled off, you guessed it, gossip, so sound as if they can be easily explained. So let’s pretend that I’m at a party and am meeting someone for the first time:

Emily. I announce that my name is Emily.

Oz. *(to Beth)* I verify that she announced that her name is Emily.

Andy. *(to Beth)* I verify that she announced that her name is Emil.

Beth. *(to Oz)* I verify that she announced that her name is Emil.

Oz. *(to Beth)* I verify that she announced that her name is Emily!

Beth. I VERIFY THAT SHE ANNOUNCES THAT HER NAME IS EMIL!

Andy. I VERIFY THAT SHE ANNOUNCES THAT HER NAME IS EMIL!

Oz. I ANNOUNCE THAT YOUR NAME IS EMIL.

Emily. I announce that my name is Emily!

Oz. *(to Andy)* She announces that her name is Emily.

Andy. *(to Beth)* She announces that her name is Emily.

Beth. *(to Oz)* She announces that her name is Emily.

Emily. Who are you?

Oz, **Beth**, **Andy.** … YOU ANNOUNCE THAT YOUR NAME IS EMILY.

Emily. I ANNOUNCE THAT YOU ARE BORING.

Oz. I ANNOUNCE THAT YOU ARE BORING.

Emily. I announce that I am leaving.

Have I mentioned that I don’t like gossip parties?

An Ottoman And A Hard Place

Last but not least, we have the old “favourite”, known as Byzantine Fault Tolerance. The name itself should give it away as being an unintuitive idea, as neither you, nor I, nor the NSA, are Byzantine Generals, and the attack at dawn is a ruse anyway, so we can get a few hours peace before lunch. So, lets all suppose I am in the basement, and want to go to lunch with a few friends. This is what the experience would look like if it resembled a BFT protocol:

Emily. I announce my desire to go to lunch.

Beth. I verify that I heard that you want to go to lunch.

Andy. I also verify that I heard that you want to go to lunch.

Chris. YOU DO NOT WANT TO GO TO LUNCH.

Emily. OH NO. LET ME TELL YOU AGAIN THAT I WANT TO GO TO LUNCH.

Chris. YOU DO NOT WANT TO GO TO LUNCH.

Beth. CHRIS IS FAULTY.

Chris. CHRIS IS NOT FAULTY.

Andy. I VERIFY THAT BETH SAYS THAT CHRIS IS FAULTY.

Beth. I VERIFY MY VERIFICATION OF MY CLAIM THAT ANDY CLAIMS THAT I KNOW CHRIS.

Emily. I AM SO HUNGRY.

Chris. YOU ARE NOT HUNGRY.

Andy. I DECLARE CHRIS TO BE FAULTY.

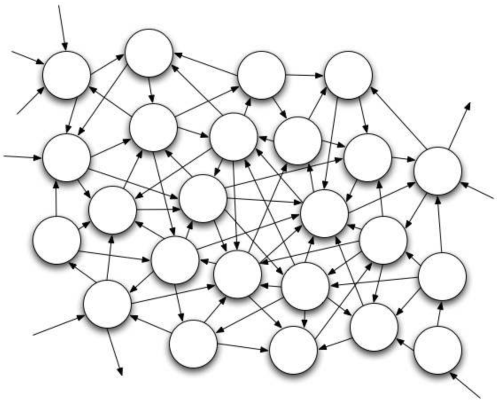
Chris. I DECLARE ANDY TO BE FAULTY.

Emily. I DECLARE EMILY TO BE SLIPPING INTO A DIABETIC COMA.

Andy. I have already left for lunch.

On Coherence

Ultimately, we need to stop obsessing over distributed systems and how they do or don't talk to each other. I don't blame people for being interested in this hideously complex, excruciatingly irrational field, in the same limited sense that I do not blame drug addicts for wanting to acquire and then consume cocaine. The desire to make computers communicate, and then make that communication fast and reliable is a powerful one, growing with the Internet in size and scale. However, unfortunately, this addiction, if left unchecked, will inescapably lead to madness and/or reports containing no less than 453 pages of diagrams (with appendices, containing the proofs), and these reports will *still* be incoherent to the educated expert.



As you can see, we removed the labels for simplicity.

Even if we break the will of the machines with formal proofs, and restrictive protocols, and cryptography, we will never be able to put ourselves inside the computer. And as such, we will be left helpless and crying as the Internet explodes and the computers decide that gossip was overrated after all.

▪ *Emily Olorin*

The Security Society of UNSW

The Security Society of UNSW is a newly-formed group of students who are passionate about computer security. Our plan is to run lots of exciting workshops around security, covering all sorts of awesome security/hacking content; as well as running our own competitions, and competing in, and winning, national and international CTFs.

Last year we took out the top 3 places in CySCA, a Telstra/DoD-run competition for Australian uni students. We also sent a team to DEFCON, effectively the biggest, hardest, and most important CTF, where we placed ninth in the world. So if this sounds like something you might be interested in, definitely come and say hi.

http://facebook.com/groups/dotsoc

unswsecurity.com

execs@unswsecurity.com

`\x68\x73\x2F\x6E\x69\x62\x2F\x00\unswsecurity.com\x6A\x6F\x69\x6E\x75\x73\x00`

Robogals UNSW

Robogals runs engineering-related workshops for high-school students, covering an ever-expanding variety of topics ranging from programming in Python to robotics with LEGO Mindstorms.

Robogals is passionate about promoting engineering to young women, especially because of the gender gap that currently exists. It's a great cause, it's fun, and you'll get to meet lots of people both within and outside your degree.

Check out `facebook.com/robogalsunsw` or sign up at `my.robogals.org/join/sydney`