Bubble City: Chapter 9

November 19, 2007

Original link

Derren, head of sensitive public relations operations for Google, had to figure out what to do about Jason. Normally Google prided itself on being very "flat" — few people were in charge, most people worked in teams. But the bosses had decided that public relations had to be special, which meant that all these tough choices fell on Derren's shoulders alone.

But Derren knew better than that. He'd previously had a similar position at Yahoo, where the Chinese government made him give up the names of bloggers to their secret police. The guilt wouldn't go away for weeks. Derren was sick of that kind of stress.

Google was a company of hackers, so when he moved there he got there he had the programmers whip up a technical solution to his social problem. Now when he faced a tough decision like this, he punched the key facts into the computer and had his team vote on the solution. That way it wasn't his decision — it was simply the "wisdom of crowds," the aggregated knowledge of Google's crack team of spooks.

Describing Jason's case would be simple:

> Fresh MIT grad discovers backdoor in key public algorithm. Works at related SF startup. Doesn't yet have enough details to go public.
>
> Should we:
>
> - Nab him and begin the coverup.
> - Infiltrate his office and friends and follow his progress.
> - Do nothing.

He always left that last one in there just to make sure his ass was covered. But it almost never got any votes.

He sent out the questionnaire and watched the results pour in. There was the support from the kidnapping crowd for immediately seizing the kid and figuring out the questions later, but most of the team supported the more cautious position. Fair enough.

He looked to see what staff he had available and dispatched one woman to get more details from the kids boss, just to make sure he was oblivious and dispatched a guy to get to know the kid's girlfriend. Finally, he assigned an office drone to monitor the kid and keep tabs on his progress. The guy who'd done the original work-up was still available, so he pushed the task back to him.

Boy, this job sure was easier without the guilt.

Jason started noticing them at the gym. Guys that geeky didn't work out. And certainly not with those dorky glasses still on. And whenever he biked anywhere he was followed by an unusually large number of white Priuses. At first he ascribed things to paranoia — he'd been having weird dreams ever since his visit to Miller == but when he got to the office he ran some numbers and calculated the probability of seeing that many white Priuses in San Francisco and realized something was up.

Dorks. Priuses. His work on NNA. What did it all add up to? Did the media industry have some secret San Francisco team working on the NNA backdoor? No, that couldn't be — anyone the media industry hired would be way more attractive. And then it hit him — the only organization that fit the combination of stealthiness, geekiness, and obsessive control: Google.

Shit, he thought.

He looked around to see how they were tracking on him. Open on his screen was a Google query for white priuses in San Francisco. *Fuck*, he thought, quickly closing it. They knew he was on to them; they were sure to close in on him now. He quickly set up a rule in his firewall to block all outgoing connections to Google servers. He watched his other search queries, his email, his calendar, and his chats all go dead. Soon his desktop search thing fizzled out too.

He tried to think of other Google products, but his officemate was laughing at some stupid YouTube video. Oh, damn, YouTube. He blocked that too, along with Blogger. In fact, he blocked the whole Google IP space. There was time to figure out how to circumvent this stuff later.

He looked around for other Google products. Surely they couldn't track him with his Google tshirts. But his phone! It not only ran Google apps, but a Google OS. He had to toss it. He removed the battery, ran a magnet over the case, and tossed the result in the trash. In fact, maybe it'd just be safer to toss his whole computer as well. At the very least, he changed the password on his hard drive encryption and removed the battery and power cord and stuffed it in his bag.

Shit, the dorks were at the receptionist. He had to get out. He ducked under his desk so he could think. Soon they'd be at his desk. He couldn't be here. He vaguely recalled seeing some back door over by the bathrooms, so he crawled that way. Luckily, most of the office was too enthralled by their monitors to notice.

He snuck out the door and jogged to the BART station. He bought a new ticket, with cash (just to be on the safe side — hadn't he heard something about Google beta-testing a new public transit program?) He rode the train all the way to Bay Point, on the theory that getting as far away from Google as possible would be a good idea right now.

He spent the whole train ride shifty and nervously looking at the other passengers, seeing if any of them were suspiciously geeky. But few people seemed to last the whole ride from San Francisco to Bay Point; mostly they got rotated. So eventually he calmed down and tried to plot his next move.

When he got off he began looking for a library where he might be able to get an Internet connection. He was obviously a bit wary of using Google, even though it'd be pretty impressive for them to track him from a random library computer, so he went to scroogle.org, a site that let you do Google searches while hiding your IP address. Instead of visiting Google directly, you sent your query to Scroogle, which passed the query on to Google and then back to you, after stripping out all the Google tracking cookies and the ads.

For other Google products there was Tor, a clever little app that encrypted your Internet usage and bounced it through three machines around the world before sending it on to its intended destination. At every step, your traffic gets encrypted a different way and delayed a small amount, so that even an observer listening to every single bit of Internet traffic can't keep track of which was yours.

Think of it this way: Imagine you want to get across town without being followed by a spy satellite that can see everything from overhead. Well, first you leave your house — the spy satellite can see that, of course — and you head to a department store. Inside the department store, you toss your clothes and buy all new ones. Then, when you come out, you look like a completely different person — the guy using the spy satellite can't tell which person leaving the store is you. Then, just in case the guy using the spy satellite cut a deal with the department store's security cameras, you do this a couple more times with different department stores. Finally, pretty confident you've lost the spy, you head to your final destination.

Tor works the same way, only instead of you there's your message and instead of new clothes there's encryption. You first pick out three Tor servers (the equivalent of the department store) that you want to route your message to. First you write out a note saying "please send the following message to www.google.com" with the message and encrypt it so that only the third computer on your list can read it. Then you write out "please send this to [the third Tor server]" and the previous encrypted message and encrypt that. And then you write out "please send this to [the second Tor server]" and the previous encrypted message. Then you encrypt that and send it to the first computer on your list. It decrypts it, follows the instructions, and all the other servers do the same.

Of course all of this was for nothing if you ever logged into a Google product or even accepted a Google cookie — a special tracking number that Google send out with every web page they serve. Most browsers automatically save the tracking number and send it back every time you visit something on google.com. Cookies were designed so that when you logged into something like your email, you would stay logged in. The first time you typed your email and password, you'd get back a cookie proving you'd logged in. Then, every other time you visited the site, your browser would send back the cookie and the site would know you were logged in.

But pretty quickly, sites started using this to track all their visitors. Instead of sending cookies only when you logged in, they sent them to every user, allowing them to keep track of people even when they took their laptop to a new place or disguised their connections through something like Tor. Google, of course, does the same, giving every Google visitor a tracking number that identifies their computer forever.

Thus, to be sure Google can't track you, you need to do at least three things: never long in, never accept tracking cookies, and use some kind of anonymization of your IP address (like Scroogle or Tor). And that's just for the Web.

God, this was going to be hard.

Tomorrow: Chapter Ten