Internet Security – engineering solutions to societal needs

Remarks by Dr Richard Clayton, House of Lords, 30 March 2008

Long ago, and you can tell that it was long ago because of the currency, I was taught that an engineer is someone who can make something for sixpence, what any fool could make for a shilling.

We can see the truth of this when we look at the Internet. In computing and in cyberspace the engineers have given us processing power, memory, storage, and bandwidth that is cheaper and bigger and faster every year. Hard discs already cost sixpence a gigabyte, and connectivity to the far side of the world is only five shillings a gigabyte for consumers and a lot less if you buy it in bulk.

But there's a dark side to the Internet as the Science & Technology Committee report made clear: the kids in bedrooms who used to be content with hacking into websites to impress their girlfriends, are now doing it for money. That's leading them into the arms of organised crime, and suddenly cyberspace isn't the safe place that we'd all like it to be.

It's very common to try and understand the Internet by means of analogies, and they always seem to involve roads and cars. But please bear in mind that analogy is an imperfect tool and you have to be careful not to be too carried away: the Cadillac I was told once, is the Rolls Royce of motor cars!

We make people safe on the roads not just by having driving tests and speed limits, but by engineering the roads to be tolerant of driving mistakes. We put crash barriers down the middle of motorways to prevent head-on collisions, we smooth out curves and redesign junctions, we fit air-bags into cars and we make people wear their seat-belts. Lots of engineering, lots of sixpences, and less people die on the roads than they used to.

So maybe engineering is going to fix cyberspace as well? Well yes, it eventually I think it will, but all the experts, and I count myself among them, think it's going to get worse before it gets better.

Analogies with roads have their limitations, because the Internet isn't quite like anything else that humanity has ever constructed before. So don't rush in quite yet, waving your slide rules (or do you still use log tables?), fitting air bags into keyboards and looking for people spending inappropriate shillings. On the Internet, we have to make things safer and more secure for extremely fallible humans, and you will need more than just engineering skills to do that.

There's been a lot of concern about phishing (with a PH) – fake websites that pretend to be online banking, so that the bad guys can capture your login passwords and run off with your money. These phishing sites are rapidly identified, and you can get attachments for your browser that flash lights, or show red address bars, or sound sirens, just to say that this is a bad site. Guess what? They don't actually work – when you evaluate them carefully you find that the humans are more interested in getting their task done ("I have to login quickly or my account will be suspended") than in taking any notice of safety warnings. All the fancy engineering is a waste of time. So you can't just be an engineer, you have to be a psychologist as well.

There are other skills you need too, and there's time to mention just one. You need to learn some economics, and in particular about incentives.

When you log in to a remote machine across the Internet, long ago you used a protocol called telnet which sent all the data in the clear. This was a security risk and so some engineers knocked up a new protocol called SSH which encrypts the data. They were engineers, practical people, so they didn't try and check the identity of the remote machine – because that's a very complicated problem and requires a complex infrastructure. Instead they just checked if the machine was the same as last time, which was easy and cheap and effective. SSH is now almost universally used, because you can swap over to it at any time, and you're immediately more secure.

Unfortunately, the Internet's foundations are horribly insecure. The routing protocols that arrange for packets to go to the right place have no security to speak off. That's why a small error in Pakistan a few weeks ago made YouTube disappear from the Internet for a few hours. There are some plausible engineering solutions to fix this – but you don't get very much benefit at all until almost everyone adopts them, and since customers are remarkably tolerant of YouTube disappearing once in a while, this means that there's no economic pressure on ISPs to fix the problems. Why should they spend lots of money on new systems when no-one cares either way?

Eventually some engineers will come up with a cheap way of creating routing security, they'll have learnt some psychology so their solution will not be simply ignored, and they'll have got the economic incentives right, so that ISPs can see the good sense, and profits, in deploying their system.

Apply this type of good engineering across all of the Internet's security problems, and we can change my definition. An engineer will be someone who helps you spend only sixpence, so that all the fools can keep their shillings safe!