PHYS.ORG

The structural insecurities underlying the internet

March 13 2014, by Alan Woodward

After 25 years, it's getting a bit dusty in there. Credit: Arrqh, CC BY-SA

Most people would agree with the principle that good foundations are essential to any structure that is intended to last. But what if when you started building, you didn't envisage how large, complex or essential your structure would become? As we celebrate 25 years of the world wide web, the extraordinarily accurate science of hindsight brings to light just such a situation.

We have all become dependent on a network that was never intended to be as large or secure as it is now required to be. The big question is, do we go back and start again or do we simply accept history and ensure that our structure somehow compensates for its weaknesses?

Shaky foundations

To decide, we have to distinguish between two quite distinct entities: the internet, and the world wide web, which sits on top of it. It is the internet, in the form of its underlying network protocol known as IPv4, that provides the weak link being broken by some of the latest high profile cyber attacks.

When the first few computer networks were connected, it was to share resources. Spreading the load between machines meant that those with spare capacity could help out those that needed more.

By the time Tim Berners-Lee and his colleagues at CERN came to think about networking, academics around the world were already using precursors of the internet to share data, from JANET, which still thrives today, to the stranger, more esoteric applications running on the internet such as the long forgotten GOPHER.

The brilliance of what Berners-Lee did was to come up with an extensible mark-up language known as Hypertext Mark-up Language, or HTML. This allowed us all to write pages that could be universally accessed. Crucially, HTML was made freely available so people started writing browsers that would enable you to read HTML based web pages.

And that, with the benefit of hindsight, was where the problem inherent in the internet was compounded. Neither IPv4 nor HTML were built with security in mind. The entire purpose of the web was to allow academics and other researchers to freely share their work. Indeed, the more people that accessed it and read your work the happier you would be.

It never entered anyone's head that we might wish to restrict access or that we might one day pay for things online or use it to communicate our most intimate thoughts. The web was a victim of its own success. HTML unlocked the potential of connecting people, and since humans just love to share and chat, we all got hooked.

By the mid-1990s, businesses finally found the web and that's when the floodgates opened. It was when money became involved that people really began to realise that security was an issue. Secure HTML emerged alongside other secure extensions to the original protocols which made it possible for us to interact over a public network in a secure manner.

Enter the baddies

For a while, these extra layers of security added on top of the web seemed to work well but the shaky foundations on which they were built soon began to cause problems.

As more and more commerce went on over the web, the criminally minded, who should never be underestimated for their ingenuity, began to look at how they could subvert the system. And as criminals always do, they went straight for the weakest link. In this case, that was the basic technology underpinning the web.

They began to impersonate users sometimes using IP "spoofing" to trick others into giving up information, and to mount distributed denial of service (DDOS) attacks. Initially these DDOS attacks were simplistic. Hacktivists would harness an army of supporters to all send simultaneous requests for the same web page at the same time. The site would be unable to cope with the number of requests and would become unavailable to valid users.

But then criminals, who had always had an eye on those ageing underlying technologies, realised that because IPv4 allowed you to spoof your address, you could ask a question but have the answer sent to someone else. Worse still, they realised that the domain name server (DNS) – the essential component that enables web addresses to be converted to internet addresses, meaning data can actually be routed around networks – could be used to amplify the data being directed at a victim.

Since using DNS in DDOS attacks, the internet's other older protocols have been co-opted to mount similar DDOS attacks employing ever greater volumes of data, and increasingly by people with criminal intent rather than hacktivists. All of this is possible because of the technological foundations upon which the Web is built.

The next 25 years

There are those who suggest we should effectively start again but this is probably not practical. The web doesn't run on some ethereal cloud but on real physical networks which have taken considerable investment to produce.

Others suggest that IPv4 should be abandoned and we should move onto the IPv6 – the most recent version of the internet protocol, which has the potential to be more secure because it has the potential to prevent spoofing of IP addresses and to guarantee the sender is who they cliam to be. IPv6 has added advantages such as the fact that IPv4 long since exhausted its addresses whereas IPv6 has no such limitation – yet another indication of how people drastically underestimated how much would eventually be attached to the web and would thus require an address. Despite this, network providers seem in no hurry to replace

IPv4 as the de facto standard.

It's not all doom and gloom though. The days of the web are not necessarily numbered. It has a way of evolving, almost organically, as threats emerge. We have solutions to many of the problems that threaten our safety online, particularly those that relate to spoofing IP addresses, and miusing tyhe older protocols, and will probably continue to produce more.

The irony is that in such a hyper-connected world we struggle to get the word out about these solutions. People can access the information they need to stay safe online but are not doing so. It is almost as if there is so much communication that important messages are being lost in what is perceived as background noise.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: The structural insecurities underlying the internet (2014, March 13) retrieved 24 April 2024 from https://phys.org/news/2014-03-insecurities-underlying-internet.html