βeta

— news from computer science and engineering —

the network is **hostile**

what have we learned this year in NSA leaks?

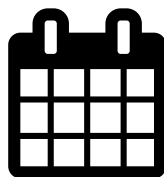# alternatives to your **tech career**

for when it all gets too much

and...

catch up on
technology news

find out
what's on

review
tigersapp

brain-bending
puzzles

βeta

CSESoc βeta, issue 110

In This Issue

The News

Windows collateral. Several serious complaints about Windows 10 have sprung up, despite the product's strong launch this month. Electronic Frontiers Australia were forced to speak up on behalf of Cook Islands residents, after frequent and mandatory software updates caused massive data bills. Meanwhile, the OS seems to send daily dossiers of internet and app usage to parents by default, potentially outing the world's youth without their knowledge or consent. In Russia, a prominent politician is calling for Windows 10 to be banned from government use, concerned about ambiguous data collection and black-box updates. Sources suggest Redmond's 'intentions' were 'good,' or something.

Dallas DVD Buyers Club. Things seemed dire in April, when the Federal Court ordered ISPs to hand torrenting customer details over to Dallas Buyers Club LLC. A subsequent ruling from Justice Nye Perram this week allows the troll gang to collect only the cost of a copy of the film, plus a small share of court expenses. The Court sought a $600,000 bond to enforce these terms, protecting users from speculative invoicing. Some are concerned that the ruling will be cited down the track, in the application of Australia's new site-blocking laws.

Twitter cuts off transparency orgs. Organisations like Sunlight Foundation and the Open State Foundation, who specialise in archiving the deleted tweets of the world's politicians, have had their access to Twitter's firehose APIs cut off. Twitter, who still grant advertising partners access to the deleted tweets of all users, told the OSF that "deleting a tweet is an expression of the user's voice."

The right to be repeatedly forgotten. The EU's "right to be forgotten" judgement is proving difficult for Google. A ruling in 2014 ordered the removal of listings containing personal data when an affected individual so demands. This week, the Information Commissioner's Office in the UK has ordered the delisting of articles reporting on the original verdict, since they mention the complainant. This may devolve into a bottomless pit of manual curation.

Ashley Madison breach aftermath. In your fortnightly reminder not to trust computers or people who like computers with anything at all, hackers have released the full databases of seedy online dating destination Ashley Madison. Thus far, the release has led to class action lawsuits, large-scale cybercriminal cyberhunting, automated extortion scams, and reports of casualties. The motives behind the release are not entirely clear, with no ransom demanded.

DirectX 12 ends NVidia supremacy. Early benchmarks using DirectX 12 seem to show older AMD cards keeping pace with NVidia's most expensive offerings. This is very good news for GPU consumers.

NBN cost blowout. The Coalition's mangled idea of a National Broadband Network is proving much more expensive than they had intended. It will still deliver minimal service improvement.

■ *Timothy Humphries*

Because we're running low on content, as usual,
enjoy some assorted detritus.

YOUR ARTICLE HERE!

beta@cse.unsw.edu.au

We received a great message from Alex North
who was instrumental in starting Beta
ith Adam Brimo and Sam Gentle,
congratulating us on keeping it going.

Thanks to everyone who's contributed over the years!
We couldn't have done it without you.

Don't forget to check out the Beta website,
where we've also found some archived issues.

(If you have PDFs of Beta from 2012 or before,
we'd love to have them for completeness.
Send them in to csesoc.beta.head@csesoc.unsw.edu.au.
We may be able to get you a prize.)

and now, on with the show...

The Network is Hostile

2013 was a pretty integral year from a cyber-security perspective, with the release of large quantities of files from the NSA which confirmed that the American government was actively spying on ……………………… This included gems such as tapping the fiber connection supporting the UN, as well as many others.

Since then, there have been a series of further leaks and revelations on this topic, and a lot of arguing about whether this is actually news from people in tech [0]. As with all these things, the answer is a combination of yes and no, though I suspect that a majority of people are starting to suffer from revelation fatigue. I know I am.

But this article isn't about the latest revelation that, in fact, the NSA is further into our networks than we ever thought before. Rather, this is about what the leaks have taught us, from beginning to end, and, perhaps more importantly, what these revelations mean for how we should be thinking and acting on the Internet.

One of the first rules of Internet security is that there is no Internet security. This assumption is based on the design of the Internet, where unknown third parties are responsible for handling and routing your data. No matter whether you're using Tor or a VPN or any "safe" router you like, there is no way to ensure your packets will be routed as you want them, and absolutely no way to ensure that they won't be looked at.

With the way things are, it's easy to think that this is a new problem. However, nothing could be further from the truth. As far back as the ARPANET it was known that connecting from *A* to *B* meant passing through a variety of untrusted machines. At that time, the only thing protecting your data was a gentlemen's agreement not to look. Somehow, we haven't progressed much from this stage since.

From the reaction to the leaks, we can see that even though it was "obvious" that anyone could be spying on our data, we were only aware of it intellectually. Even knowing that the worst was possible, we still chose to believe that leased lines from reputable providers would make us safe. If nothing else, these recent leaks have thoroughly refuted this assumption.

A surprising lesson has been that over 20 years since development of SSL encryption, we still send enormous amounts of valuable data as plaintext.

Even in 2014, things like Yahoo Mail were routinely routed in cleartext. Good job, guys [1]. This doesn't just make it vulnerable to people like the NSA, but also to everyone— *everyone*—on your local network. And it gets better: even if you managed to get all your data sent encrypted across the wider network, companies would transmit the same, unencrypted, data naively through inter-datacenter connections. And guess who was sitting on those lines (hint: it was the NSA) [2].

img

It's easy to think that were doing much better now than we were in 2013, and perhaps in some ways we are. But as long as were sending and tolerating unencrypted packets, we have a long way to go.

But even if we miraculously manage to achieve 100% encryption, we still haven't solved the whole problem. Session metadata in today's protocols leak an enormous amount of data, and we have no way to defend against it.

Some examples of metadata: protocol type, port number, routing information, session duration, source and destination address and communication bandwidth. Unsurprisingly, traffic analysis remains a particular problem as this can leak vast amounts of information about a user's browsing habits. None of this is news to us in Australia, after our metadata laws of yesteryear. The problem is that there's so little we can do about it. Networks like Tor protect the identity of connection endpoints, but with huge cost in bandwidth and latency, plus they only offer limited protection when faced with a motivated global adversary [3]. IP tunnels only pass the problem to a different set of trusted components, and these too can be subverted.

An eye opening fact of the intelligence leaks has been the sheer volume of data that agencies have been willing to collect. Famously exemplified with the US data collection policies, it's more worrying cousin is "full take" devices like TEMPORA [4], which sits atop the backbone of the Internet and reads it all.

If we just look at the collection of this data, rather than how it's accessed, it looks like the limiting factors are purely technical. In other words, data collection is a function of processing power, bandwidth and storage. Does that sound reassuring? Because it shouldn't.

This is because while human communication bandwidth is increasing, storage and processing power is increasing faster. With some basic filtration (lists of keywords, anyone?) and no encryption, this form of data collection is increasingly headed towards being the norm rather than the exception.

Even if you're not inclined to see the NSA as the bad guy (and I know some people who don't), they're hardly the only agency able to subvert a global network. I've already mentioned the UK, but other nations such as China and Russia (apologies for bringing up Cold War boogeymen) are also laying cable, and are thus increasingly able to lay their own back-doors within them. It's important to realise that, someday, traffic will be flowing through networks controlled by governments that are not your friends and want to see you come to harm. And with the current state of our networks, you're giving them the power to do just that.

If you're concerned about the future, then the answer is to finally, truly believe our propaganda about network trust. We need to learn to build systems today that can survive in such a hostile environment. Failing that, we need to adjust to a very different world.

References

[0]: news.ycombinator.com/item?id=10066014
[1]: grahamcluley.com/2013/10/yahoo-ssl-https
[2]: tinyurl.com/ofcfkj8
[3]: www.spiegel.de/media/media-35541.pdf
[4]: en.wikipedia.org/wiki/Tempora

■ *Emily Saunders Walmsley*

Alternatives to your Tech Career

Nobody ever said you HAD to use computers. Computers ruin lives, and let hackers into your home. Had you even heard of hackers before you started to use computers? Didn't think so. It's no coincidence. It's not too late. Your past does not define your future. Many folks graduate from degrees in computing and go on to live productive, computer-free lives. Some of them paint, and some of them surf, for instance.

This βeta listicle is all about options. Your options. You have a lot of options, and you need to think carefully before walking headlong into the quicksort hellworld that is a career in tech.

Goat life

We're not kidding.

Maybe you read a little about Thomas Thwaites, a British designer who, for a time in 2015, ran among the goats. He gave himself wonderful little prosthetic goat legs and hung out in the hills eating grass and balancing on awkward slopes. Goat life could be for you. Goats live on a diet of grass and rock mountain garbage, and there's no shortage of the stuff. Goat life will take you places, including up rocky mountains in search of moss and natural fungus, and if you move well among them they may let you into the top-secret Goat Tower. The only graphs in goat life are the powerful bonds of herd kinship, and the only ISAs are Independent Strong Animals. You might think that computers would help with goat matters, like figuring out where the grass grows best, or where the coolest mountains are, but you'd be wrong.

Bat life

If you like to sit in the dark and screech a lot, consider the bat life. Bats love to hang out, all the time, often upside down, which may be of interest to you. Your command line skills may translate well to bat life, as a good bat can command a powerline without dying sometimes. Bats can mess with stuff that skywriters write in the sky, if they want to. Hollywood wants you to believe that dressing up like a bat is for angry billionaires acting out male power fantasies. This is because they want the bat life all for themselves. You could also live in a tree or whatever. If you played Pokémon, you probably knocked out a heck of a lot of Zubats, so you are kind of obliged to do this.

Shark life

It is often said that computers belong on the bottom of the ocean. However, have you even tried putting a computer into the ocean? It just sinks, and then gets to hang out under the sea. Many fun characters live under the sea, such as Mr Sparkle and Patrick Star. The computers will have fun down there. This cannot happen. You can only imagine the partying that will go on when we put the rest of the industry down there. Software will eat the world, probably, but you could eat the bro-CEOs destroying the earth. Sharks answer to no-one. All fin, no ack. This is also the only career path that involves eating famed Soylent creator Rob Rhinehart. Consider shark life.

Carmack life

You don't have to create DOOM, or be John Carmack, to become John Carmack. Anyone can be John Carmack with the right Carmack aesthetic and related accessories. Though John Carmack may choose to compute, you, as a Carmack, will not have to do anything you do not want to do. No more Unix, no more shell scripts. Nothing but you time. Carmack

■ *Timothy "John Carmack" Humphries*
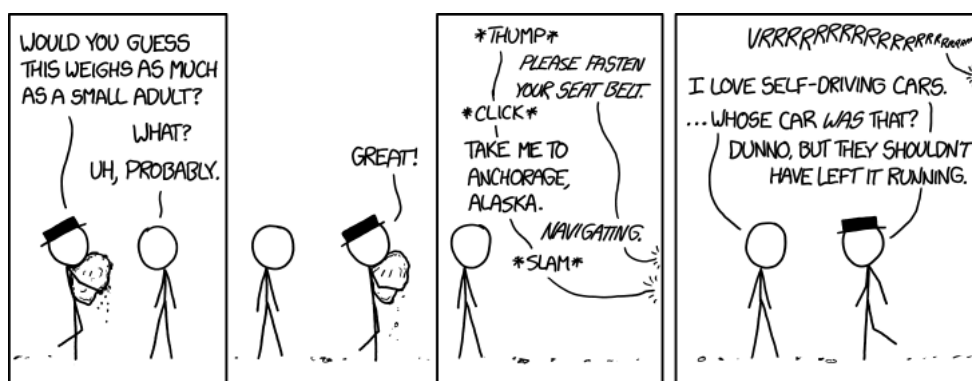
Sadly, it probably won't even have enough gas to make it to the first border crossing.

xkcd 1559 // Randall Munroe // CC-BY-NC 2.5

Upcoming Events

every Wednesday CSESoc's Weekly Barbecue `social`
1–2p, John Lions Garden

Come on down to the John Lions Garden for your weekly dose of free barbecue, on a brand new day in an old favourite spot! Don't forget to pick up your copy of CSESoc βeta, and make some new friends!

3 September CSESoc & SUITS go Rock Climbing `social`
6:15p, Sydney Indoor Climbing Gym

CSESoc and SUITS have banded together once again to reach higher places! This is what all those years of typing and coding has prepared you for. Those fine metacarpals have been trained, refined and crafted for this peak in humanity's existence. Come Rock Climbing with CSESoc and SUITS to test yourself against your peers, ones who gets the highest fastest win a small few seconds of pride and fame!

For more details, head to
`csesoc.unsw.edu.au/blog/`
`        csesoc-suits-go-rock-climbing`

5 September UNSW Open Day!

9 September The 2015 Utzon Lectures: Mario Carpo
6:30p, Law Theatre

"The second digital turn in architecture: computation, simulation, optimization, and the style of big data"

For more details, head to
`be.unsw.edu.au/Utzon2015`

15 September Git Talkshop `tech`
11a, K17 Seminar Room

Come along to the CSESoc Git Talkshop to learn about how you can use Git as a development tool, rather than a development enemy in your projects.

For more details, head to
`csesoc.unsw.edu.au/blog/`
`        git-talkshop-with-nick-whyte`

24/25 September PwC STEM Academy `careers`

Are you studying Science, Technology, Engineering or Maths? Apply to PwC's STEM Academy to be immersed in an interactive two days of professional development and a look inside your career options as a STEM student.

For more details, head to
`csesoc.unsw.edu.au/blog/`
`        pwc-stem-academy`

Review: 'Tigersapp'

Enough has been written about the story of Szymon Borzestowski, genius young Australian musician, in the wake of the posthumous release of *Tigersapp*. But very little has been written about the music itself: it's implied to be good, but only based on the wonderment of a record producer. What about mere mortals who listen to music?

Well, it's *good*. It's every bit as good as people rave about.

'Golden' kicks off *Tigersapp* with a superbly-balanced blend of delicately plucked guitars, a silvery synthesizer picking out a fine, intricate melody, and ethereal vocals, which gains a drum/bass line and delightfully memorable hook into its chorus.

And the vocals! Szymon's truly delightful, multi-layered, exceptionally talented voice blends in as gentle counterpoint, not, as is so often the case in modern "popular" music, a harsh collision of grating sounds.

'Locks' follows, its minor key juxtaposed with intricately-interwoven sounds of a deeply complex instrumentation, while 'Medusa' has a surprisingly different sound, evocative of surf rock with its twanging, gritty guitar line.

'Roma' opens with another superbly picked-out melody, balanced against a clarinet counterpoint, and brilliantly subverting conventional notions of common rhythm. 'Katyusha' follows, opening with what could be a sample of Vangelis, but tinged with the flavours of Flume, and all evoking the soundscape of a less dystopic Los Angeles, 2019.

'Runaway' twangs out a juicy bassline, then lays down a pumping trip-hop groove, with definite flavours of Emancipator. A significant improvement on the current popular fare sharing many of its lyrics. 'Saigon' follows the formula: a delicate introduction (on piano), evocative sounds (a very Massive Attack feel), and a mellow, makes-you-move groove, lightly tinted with unexpected, but spot-on, woodwinds.

'Brokenworld' follows the lyrical trope of a sad resignation to reality, with the precision mingling of woodwinds, this time saxophone and clarinet, rounding out. Following, but much more instrumental, 'Zoo Story' is almost the exact reverse: an infectious up-beat groove.

'Trojan Stalks' is a delicate, more folk-style piece, different again, but in keeping with the eclectic compendium of sounds in the album. It's followed up with 'Floods', which is a superb twinkling song, and is truly great.

Rounding out the album, 'Polen', a quiet and gentle homage to Szymon's homeland, Poland, humming with different layers and sounds, and demonstrating again the artist's skill at balancing parts.

This is music as artistry, the likes of which is so, so rarely heard. I keep saying balance when I talk about this album, and truly, that is the ultimate feature of this album: genius filling and balancing of pure instrumental sounds, in equal parts joyous and firmly focussed in its execution.

■ *Jashank Jeremy*

Puzzles

Crossword
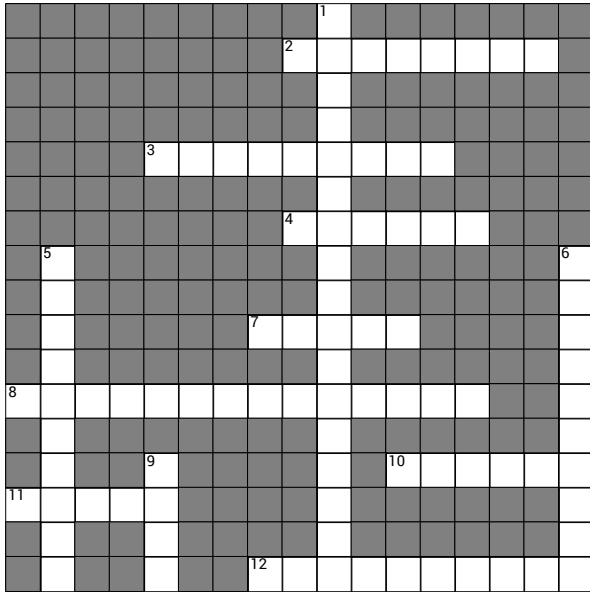
Across. 2 Cory ____, scifi writer and journalist **3** One of the medical devices open to takeover **4** Annual hacker conference in America **7** Tor's mascot **8** How hard can you hack, in competition form **10** Australian version of 4 **11** Electric cars, and timely security patches **12** _____'s always watching

Down. 1 Women won this for the third year running at this year's DEFCON **5** Hackers, but wetter **6** 4s theme this year **9** Security-oriented Linux distro

Takuzu

	1			O		O			
			1				1		O
O			1				1		
	O							O	
	1	1		1	1			O	O
					1				O
	1			1					
		O			O		1	1	
	1				O				1
	O	O		O	O			1	1

Brain Teasers

A. PU. FDHVDULDQ ZLOO EH RXW QHAW ZHHN. PU. DWEDVK ZLOO VXEVWLWXWH.

B. KFYVIGB RH GSV TIVZGVHG NBHGVIB LU ZOO, ZOHL: TL LFGHRWV ZMW NZPV UIRVMWH.

C. 84 82 65 80 80 69 68 32 73 78 32 66 69 84 65 32 83 69 78 68 32 72 69 76 80

Issue 109 Solutions

Brain Teasers

A. Fill the 3L and put it into the 5L jug. Fill the 3L jug again, then pour as much as will fit into the 5L jug. The remainder in the 3L jug will be 1L.

B. As above to measure 1L; place this in the 5L jug. Then fill the 3L jug and add this to the 1L.

C. ℅ Remember that not on the scale is a valid option.

Takuzu

O	1	1	O	O	1	1	O	O	1
O	1	1	O	1	O	O	1	1	O
1	O	O	1	O	1	1	O	1	O
1	O	O	1	1	O	O	1	O	1
O	1	1	O	O	1	O	1	1	O
1	O	O	1	1	O	1	O	O	1
O	1	O	O	1	O	1	O	1	1
1	O	1	1	O	1	O	1	O	O
1	1	O	O	1	O	1	O	O	1
O	O	1	1	O	1	O	1	1	O

Crossword

■ *Emily Saunders Walmsley*

This Edition of βeta Sponsored By...

The Last Word

Well, here we are: the end of another week's Beta. I hope you enjoyed it, and hey, we did too.

Last week, I was on a training course to learn about an application that will form a key part of the business flow with the company I work for. The first time I came across it, I was less than impressed: it's closed-source, it only runs on Windows, it's got a lumbering, painful workflow, it *requires* you use Outlook, its management console only works with ancient versions of IE, its "web console" uses Silverlight... you know the sort of thing I'm talking about.

But now, after spending a week properly learning to use the software, and learning what it's capable of in more detail, I'm really excited to use it for stuff, and one of my coworkers (a UNSW Engineering alumnus) who came along for the course was *really* quite excited about the software too.

And that's weird. Because the course itself was quite peculiarly structured—the introductory task, for example, was essentially, "here's how you make it connect to SQL Server"—and the 'lectures' (and I use the term loosely) were just a guy reading off the projected screen.

I know I wasn't alone in nodding off at least once... but somehow, I'm excited about this hunk of ugly and misshapen goo. It does one thing, and it does it surprisingly well. It fits into a perfect gap in our business workflow, and it's easy to make it do exactly what we want.

I still don't understand much of the how, though. Perhaps that's why it's enjoyable: a tool that does what you expect within the black box of idealism.

Anyhow, that's enough of me rambling on. If you've stumbled across anything interesting, or you're keen to get involved, join the team via the CSESoc website, or send in an article: `beta@cse.unsw.edu.au`. We'd love to hear from you, and hey, your article will very likely end up in print.

Catch you next week!

■ *Jashank Jeremy*