βeta

– news from computer science and engineering –

<meta name=“data” content=“**You**” />

an open letter on **data retention**

Emacs Cheat-Sheet

come to the **Emacs Workshop** to learn more

and...

issue 106 — 11 May 2015 — 15s1 week 10

βeta

About CSESoc βeta

CSESoc **βeta** is published fortnightly
by UNSW CSESoc, Beta team.

Find us online at
www.csesoc.unsw.edu.au
Got some good content? Email us!
beta@cse.unsw.edu.au

2015 issue 106

βeta Head
Jashank Jeremy

Contributors
Jake Bloom   Andrew Bennett   David Sison
Octavia Soegyono   John Wiseheart

Puzzle Wrangler
Emily Saunders Walmsley

News Chaser
Timothy Humphries

Editorial

Hello, hello, and welcome to this edition of CSESoc **βeta**.

You may have noticed a bit of a gap in the chronology. Our last scheduled issue, two weeks ago, didn't have enough content to go to print, and we couldn't scavenge enough up in time.

Thankfully, we don't have a single, full-page pun, telling you that we need content in this issue. Thankfully. Even so, we really, really do: it's been an awfully light week, and much of the content you see here was stitched together in a great hurry.

It's actually surprisingly difficult to fill an issue, and we rely on the work of many.

As ever, if you've stumbled on 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!

We hope you enjoy this issue, and I hope to see many of you at the Emacs workshop!

■ *Jashank Jeremy*

In This Issue

StuRep Report 15s1

The StuRep report for session 1, 2015 is out now. Head to the StuRep website to pick it up.

cse.unsw.edu.au/stureps

On Data Retention

In which we indefinitely retain Jake's frustrations about new data retention legislation.

Dear Mr. Turnbull,

My name is Jake Bloom and I am a 19 year old University Student at UNSW and Software Developer from Rose Bay. I intend to vote for you in the 2016 Federal Election and also for your colleague Gabrielle Upton in the coming NSW State Election. I am not involved in any political clubs or societies at uni, and I cast my vote as such because I believe that yourself and Ms Upton are the best candidates to represent my local electorate.

I don't typically get involved in politics, however the current debate about mandatory data retention laws, and Labor's new position on the laws have me very concerned about my future, and what kind of society I will be raising my children in.

I believe that these laws are a "knee-jerk" reaction to the increase in global terrorist activity and Australian terrorist activity seen in 2014, and while action is needed to ensure we can live happily in a safe and peaceful society, the metadata laws seem as though they will be ineffectual, and even worse, their full impacts are poorly understood by members of government who did not have the opportunity to learn about the framework of the Internet during the years they were studying, as the Internet was still in it's infancy in those days.

Firstly, I believe that these laws will be ineffective as those who will be using the Internet to conduct terrorist activities will be using a Virtual Private Network (VPN). A VPN works by encrypting a request made by a computer, so that Internet Service Providers (ISPs) are unable to detect and alter these requests on their way to their destination. VPNs are widely used by large corporations, such as banks, to enable employees to work from home without fear of confidential information being intercepted by malicious attackers. It is also how travellers to countries such as China and Iran are able to access social media websites that are censored in those countries. VPNs require little to no technical knowledge to set up and implement, and the most basic of Google searches will give instructions on how to set one up, allowing any user to circumnavigate these laws.

Additionally, the vast majority of online criminal and terrorist activity takes place on what is called the "dark web". The dark web is accessed by using a privacy tool called Tor, which sends an Internet request from a client to a server via a long and convoluted route, encapsulating requests within requests until it becomes very difficult to track. Tor originally was, and still is, funded by the US government as a way to mask their military communications.

The University of Arizona's Artificial Intelligence Lab has spent eight years researching terrorist activity on the deep web, and has been published in a number of articles on topics such as bioterrorism and identifying anonymous users. However, even the briefest of glances reveals how much data retention and analysis takes place in order to make small progress in these areas, and this is retention and analysis that ISPs will be reluctant to undertake.

Which brings me to the second half of my argument, which involves the ISPs themselves. Under the proposed laws, ISPs will be required to store extra data—they already store lots of data, of course, that assists them with billing, service provision and also, perhaps, some data that will help them identify trends in their business. However it's most likely that they do not already store as much data as the laws stipulate they must.

This means that ISPs will have to buy more servers, install them, pay for their maintenance and design a way to intercept requests coming from their customers and store them in these databases. Obviously, this will cost a large amount of money, which will be passed onto the consumers, who are already paying high costs for one of the slowest connection speeds in the developed world.

In five to ten years time, the infrastructure of the Internet in Australia will become just as important as our road and rail infrastructure, and these laws will raise the cost of a person's access to this infrastructure and weaken the network itself.

The final point I wanted to make is about the security of Australian's metadata. It's well known in cyber security circles that Telstra stored their password database unencrypted until a few years ago. This meant that any breach of security at Telstra would put every Australian's data at risk, as many people will reuse that password for things like their bank accounts, Facebook accounts and more.

What these proposed laws will do is announce that ISPs are carrying plenty of personal data about many Australians. While my friends in the cyber security community and I act in good faith and would never attempt to compromise this information, somebody, whether in Australia or overseas, will take this data retention as as a challenge of sorts. It would not at all be surprising if an ISP's server was attacked, and everyday Australians have their personal information leaked for anyone to see.

I hope that I've raised a few points that you will consider when you next consider these laws and which way you will vote on them. However failing that, by publishing this article in Beta, I hope that I become considered a journalist, so you'll need a warrant to find me.

Kind Regards,

■ *Jake Bloom*

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.

We've already run a workshop on using a framework called Metasploit to exploit vulnerabilities in practice servers we set up, as well as one on lockpicking; we're planning to run another one on Thursday next week on hacking WiFi networks.

If this sounds like fun, then come along and check us out.

http://facebook.com/groups/dotsoc
unswsecurity.com
execs@unswsecurity.com

From The Trenches

or, The Adventures of Edward Gough Webapp, in which Jashank grumbles about his job.

First, a précis: I got made an offer to take a year off uni and write code. I compromised, and I'm taking a year doing full-time work and part-time uni, which means I still get to bring you Beta each week. But I also have some fun stories to share, so each issue, I hope to bring you a few of them.

Database design is tricky.

And, no, I didn't just spoil COMP3311; it gets better. But for now, just sit down, and try to work out how to store data correctly.

You'll find many textbooks cover this in a disturbing degree of detail, usually by example, and typically with an otherwise completely meaningless example that, while you'd be familiar with at a distance, you have no practical use for, and that leaves out all sorts of useful things.

My preferred approach is to get a nice clear desk space, several pads of sticky notes, a good pen, some blutak, string, and scissors. How much string? More than you think you'll need.

Write down what it is you're storing data about—one entity per sticky note—and list some basic properties. It's definitely worthwhile leaving room to add more, because you'll need it.

This is around the point where your coworkers start to ask why your desk is covered with sticky notes, and the correct answer is, "all your data will be stored on sticky notes."

For example, if you have a client, you'll need to store their name, some information about them, and maybe a contact—which is a separate entity, so we put that on a separate sticky note, put them a reasonable distance apart, and blutak a piece of string between them.

Maybe a clients can have multiple contacts—in which case, you put a sticky between the two, linking client and contacts. That's optional, if you can hold all that data in your head, or mark it on your sticky notes.

Voila, database design.

I opted for this approach, because Oracle MySQL Workbench keeps screaming that my version of "Oracle MySQL" reported itself as "MariaDB 10.0.17", and every other piece of database design software I've found requires one to pay an exorbitant amount of money, and probably locks you into some broken database system anyway.

I then turn each entity into a description—the first point at which code actually happens—and build a set of database migrations and ORM classes and fudges. I use Ruby's ActiveRecord, which is, in my view, a pretty good ORM, which has pretty good migrations.

And, of course, because I'm also completely neurotic, I have MongoDB in there too. Big-data ready, I guess.

■ *Jashank Jeremy*

An Emacs Cheat-Sheet

— for the CSESoc Emacs Workshop —

K17 Seminar Room, 2pm

Jashank Jeremy
⟨jashankj@cse.unsw.edu.au⟩
⟨csesoc.beta.head@cse.unsw.edu.au⟩

Coming Up

Emacs Conventions	how + why
Line Editing	basic editing everywhere
Buffers and Modes	files + more editing
Programmable	extensible, macros, Lisp

The Keyboard

C-h → Ctrl + H   M-h → Alt + H

Common Interactions

C-x C-s	`save-buffer`
C-x C-c	`save-buffers-kill-emacs`
M-x	`execute-extended-command`
C-g	`keyboard-quit`

Inserting, Navigating

<right>	`right-char`
<left>	`left-char`
C-f	`forward-char`
C-b	`backward-char`
C-p	`previous-line`
<up>	`previous-line`
C-n	`next-line`
<down>	`next-line`

Characters, Words, Screens

M-f	`forward-word`
M-b	`backward-word`
M-v	`scroll-up-command`
<prior>	`scroll-up-command`
C-v	`scroll-down-command`
<next>	`scroll-down-command`

Line Editing

C-a	`beginning-of-line`
C-e	`end-of-line`
C-t	`transpose-chars`
C-l	`recenter-top-bottom`

Deleting

<backspace>	`delete-backward-char`
<delete>	`delete-forward-char`
C-d	`delete-char`
C-k	`kill-line`
M-d	`kill-word`
M-<delete>	`backward-kill-word`

Buffers

C-x C-f	`find-file`
C-x b	`switch-to-buffer`
C-x C-b	`list-buffers`
C-x k	`kill-buffer`

Mark and Point

C-SPC	`set-mark-command`
C-x C-x	`exchange-point-and-mark`

Save, Kill, Yank

C-w	`kill-region`
M-w	`kill-ring-save`
C-y	`yank`

Text

M-l	`downcase-word`
M-u	`upcase-word`
M-c	`capitalize-word`
M-q	`fill-paragraph`
C-x f	`set-fill-column`

Find and Replace

C-s	`isearch-forward`
C-r	`isearch-backward`
M-%	`query-replace`
C-M-s	`isearch-forward-regexp`
C-M-%	`query-replace-regexp`

Frames and Windows

C-x o	`other-window`
C-x 2	`split-window-below`
C-x 3	`split-window-right`
C-x 1	`delete-other-windows`
C-x 0	`delete-window`
C-x 5 2	`make-frame-command`
C-x 5 0	`delete-frame`

Macros

C-x (	`kmacro-start-macro`
C-x)	`kmacro-end-macro`
C-x e	`kmacro-end-and-call-macro`

Lisp

M-:	`eval-expression`
C-x C-e	`eval-last-sexp`

Self-Help

C-h c	`describe-key-briefly`
C-h k	`describe-key`
C-h f	`describe-function`

Upcoming Events

every Monday CSESoc's Weekly Barbecue social

1–2p, Physics Lawn

Come on down to the Physics Lawn for your weekly dose of free barbecue! Don't forget to pick up your copy of CSESoc **βeta**, and make some new friends!

11 May Emacs Workshop tech

2p, K17 Seminar Room

If you want an editor that's extensible, flexible, graphical, and helpful, why not try Emacs?

This workshop introduces Emacs as a day-to-day tool to write and edit text and code, and shows some sweet shortcuts to make your life easier. Like other editors, it's got a lots of power tucked away under the hood, and it can even help you scale its learning curve.

For more details, head to
`csesoc.unsw.edu.au/blog/emacs-workshop`

15 May Optiver Site Visit careers

1–3p, Optiver Sydney

Optiver, voted #1 in Australia's Best Place to Work List in 2013 and #2 in 2014 is opening its doors!

Come find out about the graduate and internship roles available in both IT (Software Development, Trading Systems Engineering) and Trading and chat to recent grads. This is an excellent opportunity to gain insight into the way IT and Trading work as the right and left hand arms of the business to solve complex problems together and stay at the top of the financial markets.

Places are limited. For more details, head to
`csesoc.unsw.edu.au/blog/optiver-site-visit`

15 May Applications Close: careers

Google Anita Borg Memorial Scholarship 2015

Dr. Anita Borg (1949–2003) devoted her life to revolutionizing the way we think about technology and dismantling the barriers that keep minorities and women from entering the computing and technology fields.

As part of Google's ongoing commitment to furthering Anita's vision, the Google Anita Borg Memorial Scholarship 2015: Asia-Pacific (APAC) has been announced; its aim is to encourage women to excel in computing and technology, and become active role models and leaders.

For more details, head to
`csesoc.unsw.edu.au/blog/google-anita-borg-scholarship`

18 May Security Talk tech

2p, K17 Seminar Room

Ever wondered, "why does security even matter?" Come to the Seminar Room on May 18th at 2pm to have your mind changed!

Held by the president of the Security Society of UNSW, Andrew Bennett, this talk will cover the idea of the "hacker mindset", why security is both important and fun, and some mistakes that developers have made in the past—both within CSE and on a global scale.

For more details, head to
`csesoc.unsw.edu.au/blog/security-talk`

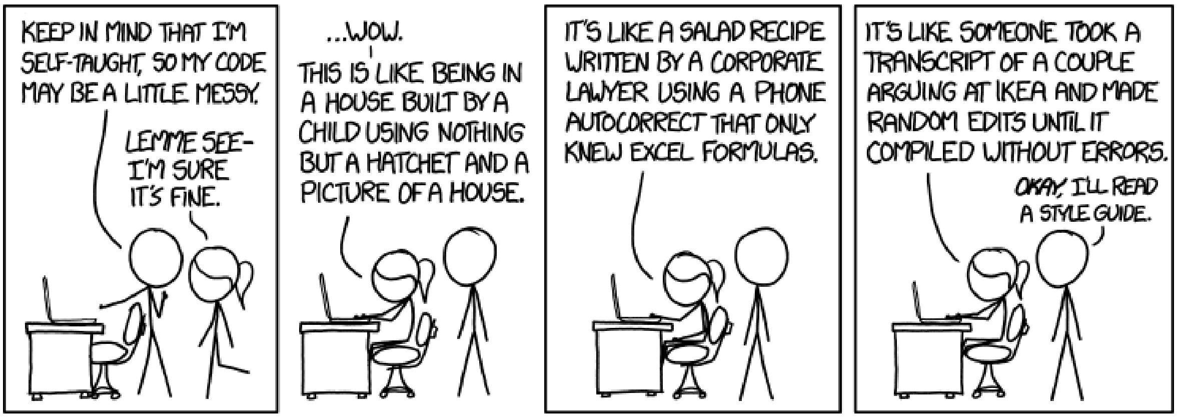
20 May Ice-skating social

8–10p, Macquarie Ice Rink

You know what life needs more of? Ice. Lots and lots of nice, powdery ice. CSESoc and Macquarie Ice Skating has you covered!

The CSESoc Choo-Choo-Chugga-Chugga Express will leave from Central Platform 16 at 6:50pm, to Macquarie University Station. To get back to Central, trains leave every 30 minutes after 10:15pm, last one departing at 11:45pm.

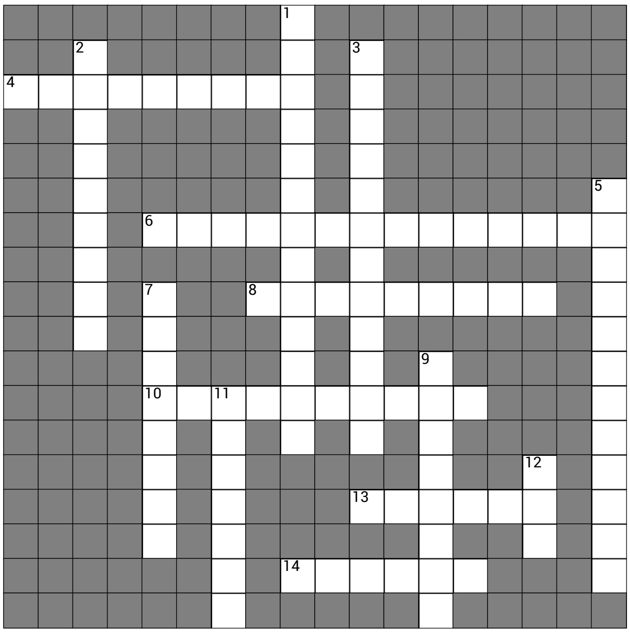
For more details, head to
`csesoc.unsw.edu.au/blog/iceskating`


KEEP IN MIND THAT I'M SELF-TAUGHT, SO MY CODE MAY BE A LITTLE MESSY.
LEMME SEE– I'M SURE IT'S FINE.
...WOW.
THIS IS LIKE BEING IN A HOUSE BUILT BY A CHILD USING NOTHING BUT A HATCHET AND A PICTURE OF A HOUSE.
IT'S LIKE A SALAD RECIPE WRITTEN BY A CORPORATE LAWYER USING A PHONE AUTOCORRECT THAT ONLY KNEW EXCEL FORMULAS.
IT'S LIKE SOMEONE TOOK A TRANSCRIPT OF A COUPLE ARGUING AT IKEA AND MADE RANDOM EDITS UNTIL IT COMPILED WITHOUT ERRORS.
OKAY, I'LL READ A STYLE GUIDE.

I honestly didn't think you could even USE emoji in variable names. Or that there were so many different crying ones.

Puzzles

Crossword



Across. **4** How often letters occur **6** Multiples of [caesarciphers], in a row. **8** Pre-encrypted text, much less exciting **10** Unbreakable if things are really random **13** 160-bit hash function **14** Replaces one with another

Down. **1** Deciphering codes (not necessarily Perl) **2** Key, not algorithm, secrecy **3** rot13 **5** Hidden writing, but in Greek **7** Cracked the Lorenz cipher **9** 128-bit theoretical limit, but people **11** Shannon measure of coding efficiency **12** Public and private

Takuzu

1			0		1	0		0	
							1		
	0		1						
					1			0	
1		0				0			
				1					1
	1				1			1	
0	1			0		1			1
			0					1	1
0			0		0			0	

Brain Teasers

A. Guvf vf gur bayl Pnrfne Pvcure gung vf vgf bja vairefr. Juvpu bar vf vg?

B. Most books have an ISBN number. The ISBN number of "Applied Cryptography" is 0471117099. Let's multiply these digits by the numbers ten to one: 100+94+87+71+61+51+47+30+29+19 = 165 = 15*11. As you can see, the sum is divisible by 11. In fact, this property holds true for all ISBNs.

The number 0100000001 cannot be an ISBN. If we know that one digit is wrong, how many possible ISBNs could it have originally been?

C. In this puzzle, each letter stands for unique digit that makes the arithmetic equation true. What are the values of the letters in: *SEVEN + SEVEN + SIX = TWENTY*

Issue 105 Solutions

Brain Teasers

A. 6 steps: work, pork, perk, peak, peat, plat, play.

B. The king assigns each servant a number from 1-10. The king assigns each bottle a number from 0-999. When he labels them, though, he writes the number on the bottle in binary with ten digits, like this: 0: 000000000 1: 000000001 2: 000000010 3: 000000011 4: 000000100 5: 000000101 … 999: 1111100111 and so on.

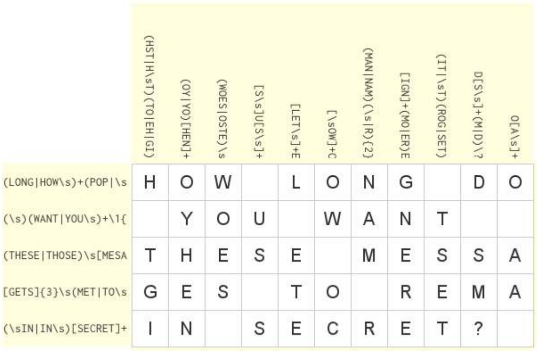
Now, each servant takes a small sip from every bottle where the servant's number equals 1 in the binary number on the bottle. So, the 1st servant drinks from every other bottle. The second servant drinks from bottles 2, 3, 6, 7, 10, 11, etc.

Then based on the combination of servants that die, he can identify the poisoned bottle. For example, if none of them die, the 0th bottle was poisoned because none of them drank from it. If only servant 1 dies, then bottle 1 was poisoned, because he's the only person who drank from it. Finally, if servants 1, 2, 3, 6, 7, 8, 9, and 10 die, then the 999th bottle was poisoned.

Takuzu

1	1	0	0	1	0	1	1	0	0
0	1	1	0	0	1	0	0	1	1
1	0	1	1	0	0	1	1	0	0
0	1	0	0	1	1	0	0	1	1
1	0	0	1	0	1	1	0	1	0
1	0	1	0	1	0	0	1	0	1
0	1	0	1	0	1	1	0	1	0
0	0	1	1	0	1	0	1	0	1
1	0	1	0	1	0	0	1	1	0
0	1	0	1	1	0	1	0	0	1

Regular Expression Crossword



<table>
<tr><th></th><th>(HST|H\sT)(TO|EH|GI)</th><th>(OY|YO)[HEN]+</th><th>(WOES|OSTE)\s</th><th>[S\s]U[S\s]+</th><th>[LET\s]+E</th><th>[\sOW]+C</th><th>(MAN|NAM)(\s|R){2}</th><th>[IGN]+(MO|ER)E</th><th>(IT|\sT)(ROG|SET)</th><th>D[S\s]+(M|D)\?</th><th>O[A\s]+</th></tr>
<tr><td>(LONG|HOW\s)+(POP|\s</td><td>H</td><td>O</td><td>W</td><td></td><td>L</td><td>O</td><td>N</td><td>G</td><td></td><td>D</td><td>O</td></tr>
<tr><td>(\s)(WANT|YOU\s)+\1{</td><td></td><td>Y</td><td>O</td><td>U</td><td></td><td>W</td><td>A</td><td>N</td><td>T</td><td></td><td></td></tr>
<tr><td>(THESE|THOSE)\s[MESA</td><td>T</td><td>H</td><td>E</td><td>S</td><td>E</td><td></td><td>M</td><td>E</td><td>S</td><td>S</td><td>A</td></tr>
<tr><td>[GETS]{3}\s(MET|TO\s</td><td>G</td><td>E</td><td>S</td><td></td><td>T</td><td>O</td><td></td><td>R</td><td>E</td><td>M</td><td>A</td></tr>
<tr><td>(\sIN|IN\s)[SECRET]+</td><td>I</td><td>N</td><td></td><td>S</td><td>E</td><td>C</td><td>R</td><td>E</td><td>T</td><td>?</td><td></td></tr>
</table>

■ *Emily Saunders Walmsley*

The News

or, "nothing happened this week tbh"

Optus doesn't see the appeal of net neutrality. Optus CEO Allan Lew has publicly suggested high bandwidth players such as Netflix pay ISPs to maintain quality of service. Speaking at industry event CommsDay, he seems to have suggested this would improve end user experience, and not just the bottom line at Optus. Netflix has publicly retreated from its unmetered sweetheart deal with iiNet in the weeks since launch, claiming it went against the neutrality ethos.

NBN becomes a cocompany. NBN Co has spent an absurd sum rebranding itself as *nbn*™, without the Co. Along with the "new" "name", the company bought itself a new logo that vaguely resembles its modus operandi—a large fibre dot that quickly trickles down into tiny dial-up dots the further you get from a wealthy urban centre. For some reason, the fibre dot is located at Pine Gap.

nbn™

Google, Facebook earthquake relief. Both Google and Facebook have rolled out their disaster relief programs to improve the response to a magnitude 6.7 earthquake in Nepal. Google Person Finder maintains a separate database allowing one to request or provide information about a missing person, used by those on the ground. Facebook's Safety Check allows those in the affected area to broadcast a sign of life to their Facebook friends. Facebook users received a list of their contacts in the area shortly after the incident.

`wpa_supplicant` **vulnerability.** Vulnerability CVE-2015-1863, discovered by Alibaba, affects popular WPA2 implementation wpa_supplicant. In peer-to-peer mode, the code responsible for parsing the management frame's SSID field was not correctly verifying payload length, leading to a possible 223-byte buffer overflow. Patches are available and will be included in version 2.5.

iOS SSL certificate parser vuln. Security researchers Skycure have demonstrated a bug in the iOS SSL certificate parser at the RSA conference, though details will not be released until Apple releases a fix. The attack causes iOS apps to crash, and repeated attacks eventually knock over the OS itself, bricking the device while it is in range of their malicious Wi-Fi network.

API flaw creates 25,000 vulns. SourceDNA researchers have noticed an API flaw in Apple's `AFNetworking` framework that has led to the publication of 25,000 vulnerable apps. The TLS implementation does not check domain names when validating certificates unless it is told to—behaviour that developers clearly did not expect. Any valid SSL certificate could thus be used to masquerade as the intended host. Versions 2.5.3 and above contain a fix.

New ARM core. ARM have announced their latest CPU. The Cortex A72 features speed, efficiency and size improvements that render it comparable to Intel's Broadwell line when power supply is constrained. ARM also touted the A72's improved branch prediction, and an overall instructions-per-clock increase over predecessor A57 of 20%-60%.

Pebble vengeance. In the days after the release of the Watch, Apple had been selectively rejecting apps that mention support for rival Pebble in their description. It is now claimed to have been a mistake at the App Store reviewer level, though it disrupted multiple app publishers first.

■ *Timothy Humphries*

This Edition of βeta Sponsored By...