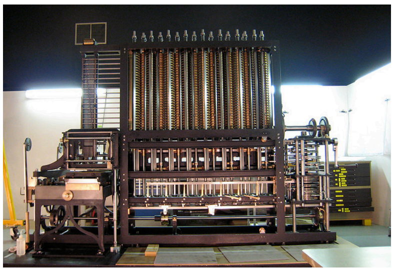
NEWS FROM COMPUTER SCIENCE AND ENGINEERING

Written by the Beta Team of CSESoc
Produced by Angelo TAMAYO
Edited by CSESoc Beta Team

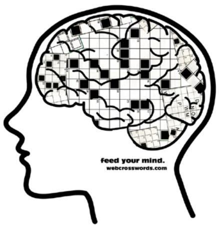
βETA

Free as in speech and our awesome BBQs.

Beta Issue #98b
Open Day Edition
Week 7 Session 2, 2014



SPECIAL OPEN DAY EDITION



Announcement

What is βeta?

Greetings weary traveller, what you hold in your hands now is an ancient grimoire of CSESoc. Beta is a student-run newsletter by CSESoc, containing articles ranging from reviews and guides, to opinions and poems. It also includes a calendar for upcoming events, an entertainment section with crosswords and riddles, and a dose of the daily weird happenings in the world, tech-related or not. This edition of Beta was assembled to give you a taste of what Beta is like. Enjoy!

Angelo Tamayo

CSE Societies and Events

CSESoc - Where all the *cool* nerds are!

CSESoc is the principal representative body for computing students on campus - all CSE Students are automatically members. We're here to grow the school community and provide opportunities for all computing students to have fun and meet other students outside of your studies. To this end, we run weekly social and technical events throughout the year (and nearly all are free to attend!).

Our social events are an opportunity for you to meet other CSE students and take a break from studying. In the past we've run:

- Our famous free weekly BBQ
- Trivia Nights
- Poker Nights
- Movie Nights
- LAN Parties
- Cocktail Parties

Tech events allow you to learn about, practise and explore any technical interests outside of your studies with others who share them. These take the form of:

- Tech Talks (on anything from Google Maps to a Security Workshop from Deloitte)
- Android and iPhone Workshops
- Project teams (anyone can contribute to something CSESoc is working on)

We announce these events by email, so make sure you sign up to the 'soc-announce' mailing list during Lab 0 to receive them! Our events are open to all students, although if you're not a CSE student (enrolled in a CSE degree or course) and want the full benefits of membership, ask the executives about becoming an associate member.

There are plenty of opportunities to get involved with running events and activities; we're always looking for volunteers, and it's a great way to develop your leadership and teamwork skills.

There are a number of teams that you can volunteer for:

- Beta - Writes the publication you're reading now
- Publicity - Promotes our events by creating posters and running our social media
- Dev - Runs projects and code jams and maintains CSESoc's website/server
- Social - Organises and runs all of our social events
- Tech - Organises and runs the society's technical talks and workshops
- High School Comp Club - Provides a head start for high school students to explore computing and eat pizza.

Most of all, we're here to help you settle in and have a great time at UNSW - we look forward to meeting all of you and helping you get the most out of this year!

CSESoc Beta Head

News

Heartbleed

11/10 on the security vulnerability scale

OpenSSL is an open source cryptography software used by websites such as Google, Facebook, and Instagram to keep data safe by implementing HTTPS encryption. An estimated two-thirds of the Internet's Web servers use OpenSSL. The Heartbleed bug is a vulnerability in OpenSSL, that allowed attackers to get passwords, encryption keys and other sensitive data. The bug is in the OpenSSL's implementation of the Transport Layer Security (TLS) Heartbeat Extension. The heartbeat protocol ensures that communications between user and the site are kept alive even when the line goes quiet. When it is exploited, the attacker can read the memory contents of the SSL server without leaving any trace. Not all websites using OpenSSL were affected, as some were using older versions and others had not enabled the "heartbeat" feature.

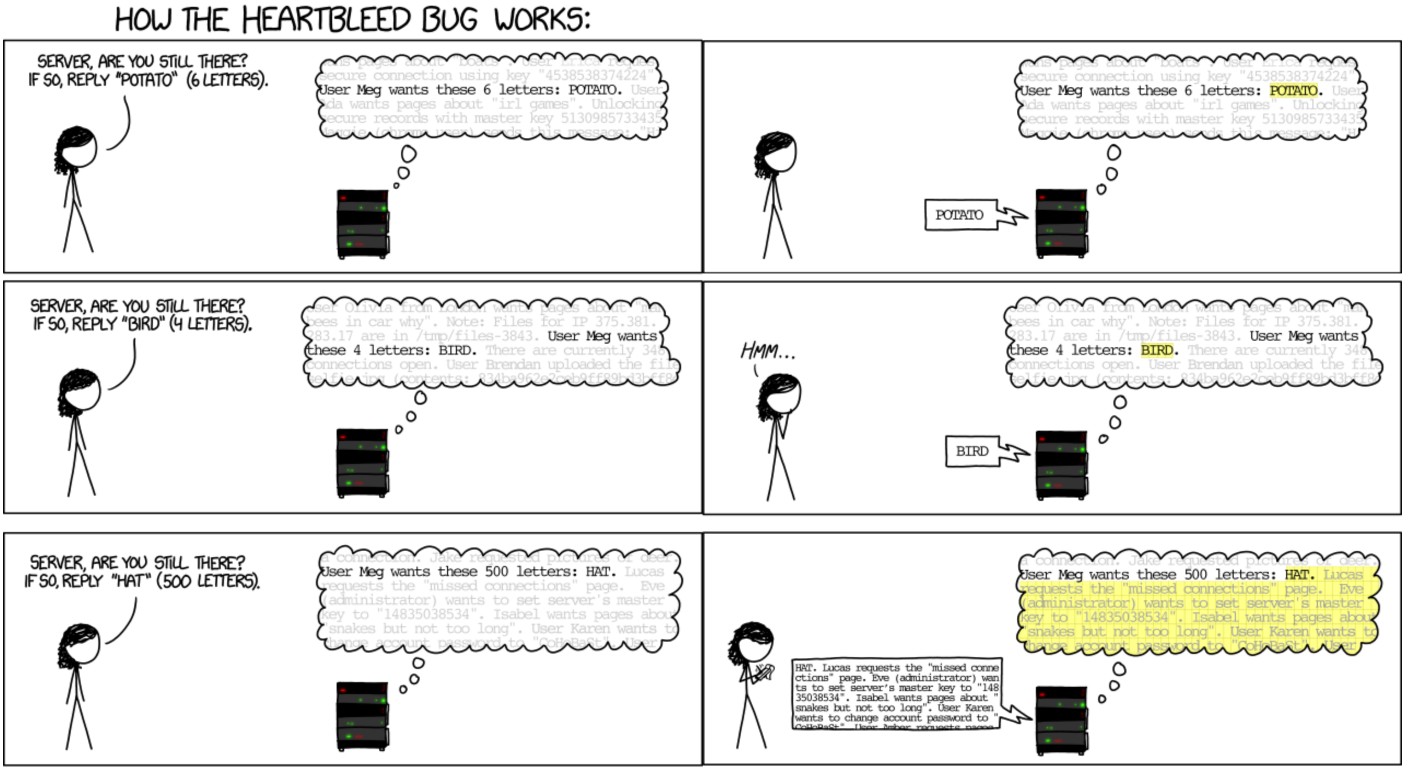
This is one of the most serious security flaws discovered recently. Codenomicon and Google researcher Neel Mehta both found the bug independently from each other, but on the same day. We don't know if it was exploited but it is possible that your data could have been captured by criminals or intelligence agencies, such as the NSA. As a consumer, you should check if the websites you use have patched their code and then change your passwords. As a developer, you should update your version of OpenSSL. A new fixed version has been released. OpenSSL 1.0.1g, released on 7th of April 2014, fixes the bug. You should reissue and reinstall SSL certificates and ask customers to change their passwords.

Companies have been rushing to patch vulnerable code. cnet.com is tracking which of the top 100 US sites have patched the Heartbleed bug. Microsoft confirmed that Microsoft and MSN were not vulnerable, as they were not running OpenSSL. Google, and Facebook have patched the vulnerability.

The bug was introduced to OpenSSL in December 2011 and was in the OpenSSL release 1.0.1 on 14th of March 2012. The error was unfortunately introduced by Dr Seggelmann, of Münster in Germany but the error wasn't detected by him or by the reviewer. He missed validating a variable containing a length. The payload length is never actually checked against the size of the payload. Therefore, it reads arbitrary data beyond the storage location of the request if you send a payload length (up to 64K) and an undersized payload.

He claims that it was not inserted maliciously. "It was a simple programming error in a new feature, which unfortunately occurred in a security relevant area", he said. The main reason this wasn't discovered earlier is that OpenSSL is an open source project which only a few people contribute to. Large companies use it without doing anything to contribute to the project. If the users of OpenSSL contributed to checking the code, then this problem could have been detected much earlier.

Savinka Wijeyratne


HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
secure connection using key "4538538374224" User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file
HMM...
BIRD
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

History

Weird Computing I: Like Clockwork

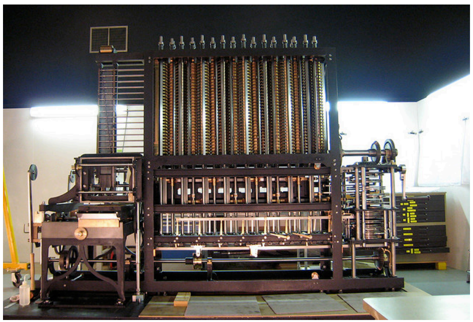
One of the most important and powerful facts about computing is that the top level doesn't need to know what the bottom level is doing. It is this single idea that allows computer scientists to design algorithms and not care how they're used, allows software engineers to write programs and not care how they're run, allows computer engineers to design processors and not care how they work, and finally, allows the physics nerds in OMB to design transistors without needing to be friends with anyone in K17. In fact, this very same boon is what allows my mum to work her iMac without having the vaguest idea what the magical box is actually doing.

That being said, it is a lack of understanding how computers work on a basic level that leads to the 'magical smoke' problem – computers work on magic smoke, and if it gets out of the box, you're screwed. Neither the average person, nor the average computer science student, has a strong handle on what computing is at the bottom level.

In this series of articles, I plan on shining the bright light of Learning into the murky depths of the actual implementations of computers, especially the ones that aren't common (while mixing in a brief guide to good speculative fiction, because everybody needs a hobby). In this opening foray into the unknown, I decided to cover a bit of history and have a look at the very first Computer ever designed, (and maybe a little bit of steampunk). In the future, we can look forward to non-deterministic molecular computers, mind bending quantum computers and gooey brain computers. But first we really need a bit of background. So let's get started.

A Computer is defined as a device which can be programmed to carry out logical operations. In particular, I'd like to take note of the 'programmable' requirement – this means you have to be able to given the computer not only a set of inputs, but also be able to tell it what to do with those inputs. This is the bit that lets us do whatever we want with the thing, so really it's quite important. It's also pretty difficult to manage. So how did they go about managing it?

Well, up until 1800, the best things anyone ever used were computational aids or Calculators. These are things like abacuses and slide rules – they are distinctly non programmable, but allowed people to do complicated operations much more quickly. Everyone from University students to great physicists hated doing maths back then as much as we all do today, and so there was much interest in figuring out ways to make something else do it for you. To this end, a bright bean named Charles Babbage was designing a mechanical calculator called the Difference Engine, which was capable of calculating polynomial functions, thereby approximating the logarithmic and trigonometric functions that nobody really likes. (What is the ln(148.42) to 4 decimal places? No? It's 5.) Babbage finished his very expensive hand cranked monstrosity, and thought to himself 'Hang on a minute, why stop at polynomials?'. So Charles designed the Analytical Engine, the first Real and Actual Computer, and promptly died.



Replica of Babbage's Difference Engine

It took about another century before someone else tried the same trick, and I think we all have a pretty good handle on what followed. (Hint: Computers.) But what if Babbage has actually managed to build an Analytical Engine before he kicked the bucket? And why did it count as a Real Computer? About 60 years after Babbage sodded off, a totally different smart bean called Alan Turing was working at Cambridge on what 'computable' actually meant. Turing developed the idea of the Universal Turing machine here, a dirt simple device which could be proved to be able to compute anything that was theoretically computable. This theoretical machine and all other machines with the same characteristics are called Turing Complete, or Universal.

Despite the obvious handicap of dying before Turing's father was born, Babbage's Analytical Engine was also Turing Complete. Babbage exclusively used mechanical gears in his design: he stored numbers in registers by rotating gears into various positions. It took inputs on punched cards, which were stacked in an input track and sucked in by the machine one by one. The real kicker in Babbage's design is that he included the ability to execute commands out of order – he had a Program Counter and a conditional branch (which, by the way, worked by mechanically preventing the jump unless a certain gear was in the 0 position). This allowed the creation of loops, by jumping back to an earlier punch card command and continuing to execute, along with all the other programming structures available to Turing complete systems. If you have done Microprocessors (2121) or Computer Architecture (3222), looking at Babbage's design is a real hoot.

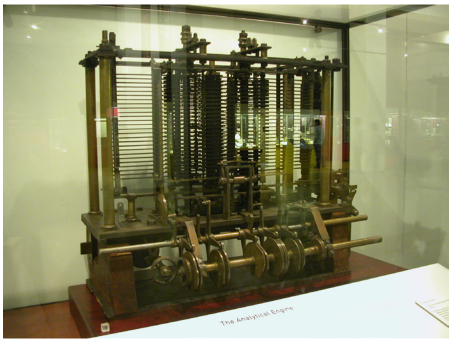
The Engine was divided into 'chunks', the most important of which was the Mill, or 'CPU'. The entire engine used decimal encoding exclusively, and the mill was no exception. In order to implement addition, subtraction, multiplication and division, it sported 2 Ingress Axes, which were stacks of 50 gears each representing a digit (along with a switch representing the sign). The First Ingress Axis also featured a Primed Axis of another 50 digits for use in division. It also possessed an Egress Axis of 50 Digits for output, accompanied by another Primed Axis for the most significant bits in multiplication, and the remainder in division. It was also quite capable of handling fixed point arithmetic for fractions, and the engine was capable of converting between different floating points. The Mill also possesses a 'Run-Up lever' which would be flipped on arithmetic overflow, or if the divisor was 0, and which could influence the subsequent execution of the program. The Engine also possessed a bell to alert the attendant to its halting, and a printing machine to punch out its results, and a bank of a thousand 50 digit registers (which Babbage called Store 000 to 999). It was capable of drawing graphs of its results, ignoring 'comment' cards, and, get this, had specific cards for debugging.

Just checking that you didn't miss any of that – the Analytical engine natively computed on signed 50 digit numbers, had flow control and flags, could handle floating points, has 1000 registers, could print numbers and graphs, and had Victorian era GDB.

Exclusively using gears and rods.

I hope this has sufficiently blown your mind. Incidentally, a very nice repository of information about it is held on the website of John Walker, the inventor of AutoCAD, and can be found at http://www.fourmilab.ch/babbage/

So what would the world have been like if Babbage had been trusted with more money and a longer life? For starters, Bugs would probably be called Wrenches – gears have a tendency to be much less merciful to moths than electromechanical valves. Other than that, society could have gotten their hands on computability and mass data about a century earlier than it actually did. That looks like fertile ground for speculative fiction. In 1990, the Cyberpunk genre was finishing up its golden age, and SF authors were looking for new ideas to play with. Bruce Sterling and William Gibson, two of the giants of the Cyberpunk movement, sat down at their respective computers and started collaborating on a new kind of punk. The resulting book, The Difference Engine, was set in 1855, in an alternate history where Babbage got his chance. It proceeded to win a serious number of very important SF awards and is widely considered the first book in the new genre of Steampunk. Steampunk is characterized by its anachronistic treatment of history, providing Victorian-era societies with far more tech than it ever knew what to do with. The results are intercontinental blimp flights, moving cities, the omnipresence of mechanical computers, and fantastic fiction.



Analytical Engine

So hopefully this article has given you a little bit of the 'truth is stranger than fiction' feeling with regards to Mister Babbage and his Analytical Engine. If you're ever in London (don't question it), I highly recommend visiting the Science Museum, where you can see a testing model of a small bit of the Analytical engine, along with modern replicas of his Difference engine and a whole bunch of other weird computing artifacts. Unfortunately, there still does not exist an actual replica of the whole machine, but there are a bunch of cool people trying to build one (In time for Babbages 150th birthday in 2021). They live at plan28.org, check them out.

Tune in to the next Beta for some fun with molecular computers and non-deterministic machines (and possibly a crash course in post-cyberpunk science fiction).

Matthew McEwen

Poetry

A Dingo ate my Laptop

Bright sunny morning, a new semester calls,
With great adventures waiting to befall.
Humming and happy, I skip through the park,
Until I'm startled by a horrific bark.

Tearing from the bushes it agiley dives,
The bane of all of mankinds' lives.
A dingo most queer indeed,
Which for our flesh it longs to feed.

Orange fur, and canine teeth,
With long lithe legs left underneath.
Its beadlike eyes seek yet more prey,
To sate its longing for the fray.

Sniffing the air to catch a scent,
Its ears prick upward to my lament.
"I'm next"! I panic, yet freeze with fear,
As its gaze locks upon me with a mesmorising leer.

One foot placed forward, and then the next,
But then it pauses, with hind legs flexed.
A moan escapes me, but I still can't budge,
Alas - am I soon.... to meet my judge?

It bounds the distance with powerful strides,
And with graceful splendour it pounces and glides.
But breaking free from its enthralling spell,
Its burning hunger, I refuse to quell.

I raise my arm to guard the blows,
Caution to the wind, my bloodlust grows.
Swinging my bag like a flat-head mace,
The dingo meets it with a willing face.

Its teeth sink in and there's a splitting crack
as my bag is wrenched away, I'm taken aback.
It gnaws at my laptop, its wires torn free.
Like eating the intestines of my 15.6" baby.

And that sir, is why I was late to class,
With no code for your dryruns, that adequately pass.
So always remember to keep a backup,
Cos' a dingo may just eat your laptop.

Angelo Tamayo

NEWS

News in Brief

Barley a Difference
CenturyLink Arena in Idaho is being sued by fans for $10,000 for being ripped off into believing that the $7 large beer gives the same amount of beer as the $3 small beer. The large cups are tall and narrow, whereas the small cups are shorter, yet wider, but ultimately, they serve the exact same amount.

Wanted: Giant Mango Thief
A 10 metre high fibreglass replica of a mango has gone missing in Bowen, Queensland. Security footage shows that a crane was driving in the direction of the mango at 2am, and the following morning, the giant mango had disappeared. I wonder how much a giant mango goes for in the black market?

Kettle Chips: A surprising new flavour
After finishing half a pack of kettle chips, a couple was shocked to find a dead shrew inside. Taking the case to Kettle, and after much investigation, it is clear that the shrew did not enter the bag at Kettle foods, nor did it enter during distribution. Further, the shrew had been dead for quite a short time, puzzling everybody how it got there at all. Although the most puzzling thing to me is why the couple was so shocked. They must have been vegetarians.

Lock out Laws
For those of you unaware, the legislation enforces 1:30am lockouts and refusing the service of alcohol at 3am in the CBD and Kings Cross areas. Further, alcohol shops will be forced to close at 10pm. This will change the late-night party culture that is prominent in the youth of Sydney today, especially uni students.

Man Kicked Off Flight For Tweeting About Bad Service
Duff Watson complained on Twitter when his two young daughters were refused boarding with him in the priority queue when travelling from Denver to Washington. Southwest Airlines then removed him and his family from the flight until he deleted the tweet.

"I thought she was very rude and wanted to complain to customer service, so I asked her: 'Can I get your last name?'" Watson told ABC News.

"She told me: 'You don't need my last name for anything'. I tweeted something like, 'Wow, rudest agent in Denver. Kimberly S, gate C39, not happy @SWA.'"

After Watson boarded the plane, his name was announced over the tannoy and he was told to "exit the flight immediately". At the gate, the attendant Watson told him he was a "safety threat" and threatened to call the police unless he deleted his tweet.

"I was shocked. There was no use of profanity, there were no threats made. How was I a safety threat?" Watson told ABC News. "She [the attendant] watched me as I deleted the tweet. I was taken aback by the situation. My two kids were crying."

Since the incident, Southwest Airlines has apologised to Duff Watson via email, and offered him a $50 voucher. Watson, formerly an A-list member of the airline, doesn't feel this makes up for the poor service he received – and plans to donate the voucher to charity.

Man Squeezes 10 People Into Sedan, Kills 4
Mohad Azuwan crammed 10 illegal immigrants, aged from 20 to 30, from Myanmar into a five seater sedan. He was transporting them from Rantau Panjang, Kelantan to Kuala Lumpur on June 16, when he crashed his car at 4am on the East Coast Expressway. Four of the illegal immigrants died. The immigrants are typically sold to businesses, and work for months with no wages to pay off their debt. Mohad Azuwan was charged this month for transporting six illegal immigrants.

CSESoc Beta Team

ENTERTAINMENT

Puzzles!

1. Mary's father has 5 daughters – Nana, Nene, Nini, Nono. What is the fifth daughters name?

2. Take away my first letter, and I still sound the same. Take away my last letter, I still sound the same. Even take away my letter in the middle, I will still sound the same. I am a five letter word. What am I?

3. A carpenter was in a terrible hurry. He had to work as quickly as possible to cut a very heavy 10 foot plank into 10 equal sections. If it takes 1 minute per cut, how long will it take him to get the 10 equal pieces?

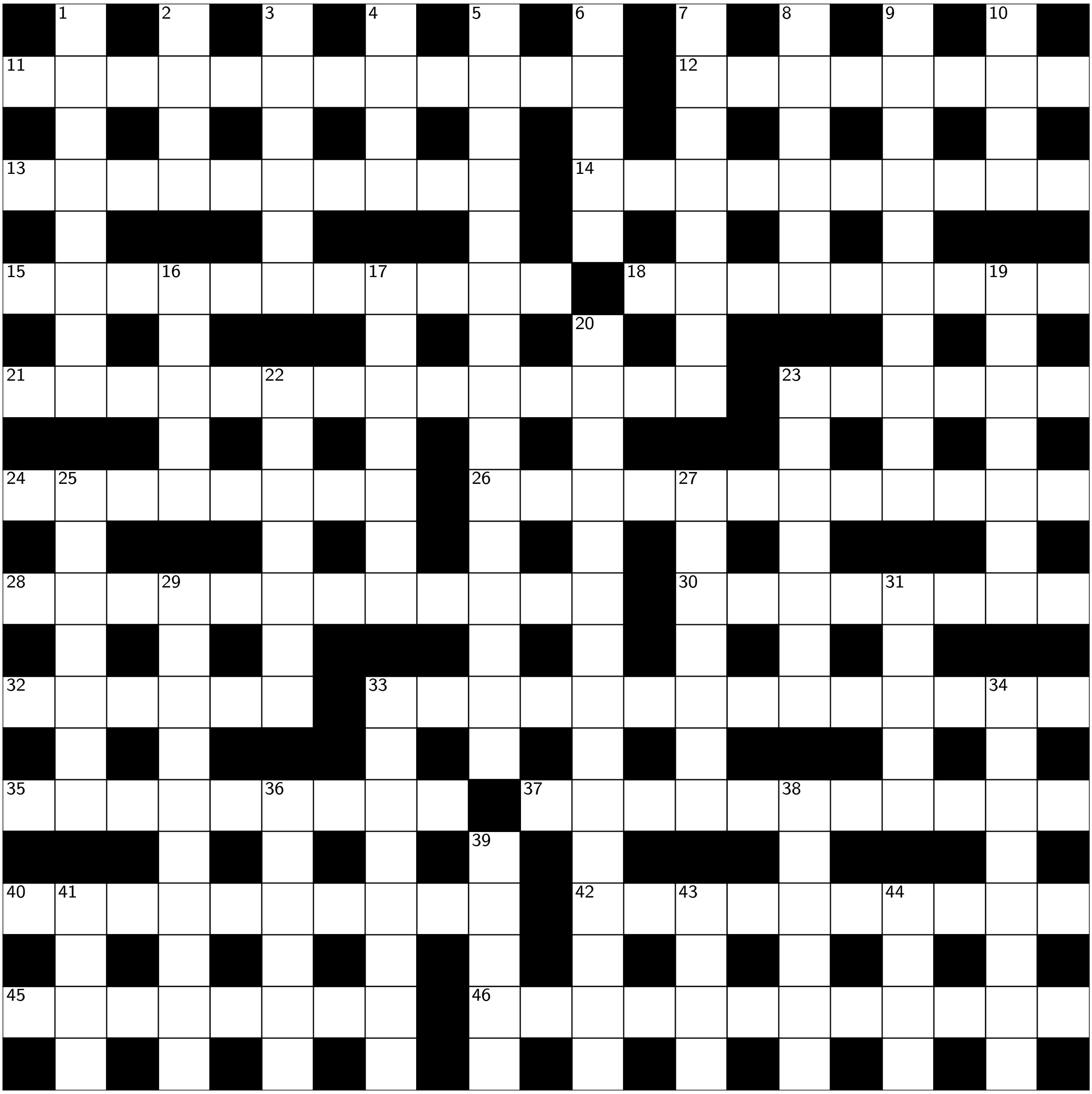
4. A woman goes into a hardware store to buy something for her house. When asked the price, the clerk replies, "the price of one is twelve cents, the price of forty-four is twenty-four cents, and the price a hundred and forty-four is thirty-six cents. What does the woman want to buy?

5. Divide 110 into two parts so that one will be 150 percent of the other. What are the 2 numbers?

6. At a sports banquet there are one hundred athletes. Each one is either a football or basketball player. At least one is a football player. Given any two of the athletes, at least one is a basketball player. How many of the athletes are football players?

CSESoc Beta Team

Super-Mega-Awesome-Jumbo Crossword



Across

11. A sailing ship with a fore-and-aft rig. (4,3,5)

13. A value that represents a point on a continuous number line (4,6)

14. An area to have a picnic (6,4)

15. Candle holders with multiple arms

18. Branch of mathematics that studies sets (3,6)

21. Communication through letters

23. Airships

24. One of the points which divide a statistical sample in four

26. Scientific inventions

28. A change in gradient

30. Oak container used in fermentation (4,4)

32. Cosmetics

33. Full scale preparation for a performance (5,9)

35. A symbolic meaning or representation

37. One's natural tendency

40. A dress shirt (6,4)

42. To make impervious to water

45. Warn in advance

46. Inflammation of the brain

Down

1. Music: moderate tempo

2. Cut down

3. Yearly

4. Sheep meat

5. USA Flag (5,3,7)

6. Set of vertices and edges

7. Individually distinct, rather than continuous

8. Stern, uncompromising

9. Becoming larger in width

10. The number of digits used to represent numbers

16. More dire

17. True or false value

19. Slender swords

20. Proverbial punch to the mouth (7,8)

22. Part of saddle for feet

23. Even distribution of weight

25. Relating to units

27. Programs in response to the Great Depression in the USA (3,4)

29. Infested with fleas (4,6)

31. Measure of mass, generally for gemstones

33. Having no elements in common

34. Formal written defence

36. In a straight line

38. Perpendicular

39. Numerical reference to an element

41. Unidentified flying objects

43. Narrow strip of adhesive material

44. Disrepair, decay

Oswyn Brent

This Edition of Beta is Sponsored By...