Dec. 23rd

Analytical Engine

Dec. 23, 1834

Charles Babbage [Dec 26] announced a new machine with far greater capabilities than the Difference Engine [June 14] in a letter to the Duke of Wellington (which was mainly about the government's bedeviling lack of funding for the Difference Engine).

Henry Babbage's Analytical Engine Mill (1910). Photo by Marcin Wichary. CC BY 2.0.

The first notes on the machine appeared in mid-1834, the first design drawing is dated Sept. 1834, and a workable design had evolved by mid-1836, but underwent a major revision in late 1837. For the next decade, work on the Analytical Engine consisted largely of refining that basic design, with no attempt made to construct it. Over two hundred detailed engineering drawings were created.

The Analytical Engine would be able to store a 1,000 fifty-digit numbers, and calculate using base-10 fixed-point arithmetic. Programs and data were to be provided on punched cards, a method inspired by its successful use in Jacquard looms [July 7]. When the machine needed any additional input, it would alert its operator by ringing a bell. For output, the engine would include a printer and a curve plotter, and also be able to punch numbers onto cards for later use. The machine would be powered by steam.

Sadly, the engine was never constructed during Babbage's lifetime, but Babbage's son, Henry, did build the mill portion (what we would call the ALU) working from his father's drawings [Jan 21].

Perhaps more importantly for future inventors, Henry also published his father's plans and notebooks, along with Ada Lovelace's [Dec 10] "Sketch of the Analytical Engine Invented by Charles Babbage . . . with Notes by the Translator" [July 10].

In 1878 (after Babbage's death), the British Association for the Advancement of Science described the engine as "a marvel of mechanical ingenuity", but decided against making one.

John Hamilton Curtiss

Born: Dec. 23, 1909;

USA
Died: Aug. 13, 1977

Curtiss played a key role in persuading US government to utilize computers more widely after WWII. This began after Edward U. Condon, the director of the National Bureau of Standards (NBS), assigned Curtis to survey the federal needs for computers and for a national computing center.

Curtiss had the opportunity to put his ideas into practice after becoming the head of the National Applied Mathematics Labs in 1947. He undertook a massive recruitment program, with the aim of accelerating the construction of computers and their use for scientific computations.

He was also involved in the organization of the Eastern Association of Computing Machinery (ACM), which dropped the "Eastern" adjective in 1948; he was its first president in 1947.

While no one could ever recall seeing Curtiss sat at a computer console, he always argued that, "I was involved in the salt mines of computing."

Robert Elliot Kahn

Born: Dec. 23, 1938;

Brooklyn, New York

Kahn is one of the "fathers of the Internet"; other parents include Vint Cerf [June 23]. Jon Postel [Aug 6] and Larry Roberts [Dec 21].

In early 1969, Kahn helped build the Interface Message Processors (IMPs [Aug 30]) at BBN [Oct 15] which acted as the system independent interfaces between host computers and the ARPANET [July 29]. He also gave the first public demo of the network at a conference in Oct. 1972 by connecting twenty computers together (some reports say 40). He remarked later that this was "the watershed event that made people suddenly realize that packet switching was a real technology."

In 1973-74, Cerf and Kahn co-invented the Transmission Control Protocol (TCP) by doodling on napkins [Sept 9], although they later published a learned paper about it [May 5]. Subsequently the protocol was split into more modular pieces, consisting of TCP and the User Datagram Protocol (UDP) at the transport layer [Jan 31], and the Internet Protocol (IP [Sept 1]) at the network layer; this became known as TCP/IP [Sept 9].

On [Jan 1] 1983, TCP/IP was adapted as the communication protocol at the heart of the "Internet", a term Cerf and Kahn had invented in 1973 as an abbreviation for "inter-networking of networks."

Butler W. Lampson

Born: Dec. 23, 1943;

Washington, DC

Lampson was part of Project GENIE [Nov 30] at UC Berkeley, which helped develop the Berkeley Timesharing System for Scientific Data Systems' SDS 940 [July 24]. The goal was to show that a time-sharing OS could be fast, small, and economically feasible – features that were somewhat lacking in MIT's mammoth time-sharing project, Multics [Nov 30].

Butler Lampson (2018). Photo by Duncan.Hull. CC BY-SA 4.0.

Lampson is also a developer of programming languages, notably Cal, an interactive language for numerical computation derived from J. Clifford Shaw's JOSS [June 17].

Lampson and L. Peter Deutsch [Aug 7] co-developed the QSPL system programming language, and also QED [March 26], a line-oriented computer text editor. QED was a strong influence on later UNIX text editors, such as ed and sed.

Lampson was a founding member of Xerox PARC [July 1] where he contributed to many projects, including the Xerox Alto [March 1] and Dorado [May 6], the laser printer [Jan 21]; two-phase commit protocols; Bravo [Oct 00] with Charles Simonyi [Sept 10]; Ethernet [May 22]; and several languages such as Euclid (the first one specifically designed to support program verification).

In the Jargon File [Oct 2], his name is associated with the milliLampson, a unit of talking speed, abbreviated as mL. Most people talk at around 200 mLs, but Lampson supposedly speaks at 1,000 mLs.

Transistor Demo

Dec. 23, 1947

Prev: [Dec 16] Next: [June 23]

The point-contact transistor was demonstrated by William Shockley [Feb 13], Walter Brattain [Feb 10], and John Bardeen [May 23] to senior management at Bell Labs.

To illustrate its use as a current amplifier, they connected a microphone and loudspeaker (or perhaps a pair of headphones) to the transistor. The story goes that one by one the managers picked up the microphone and whispered, "Hello." The loudspeaker at the other end of the circuit shouted, "HELLO!". However, Brattain's notes from that day only mention that the amplification suffered "no noticeable change in quality". Shockley later wrote that hearing speech amplified by the transistor was a moment similar to Alexander Graham Bell's "Mr. Watson, come here, I want you" [March 10].

This day is usually included in the transistor's "Miracle Month," which started on Nov. 17 when Bardeen and Brattain had begun their experiments.

The "transistor" name is due to Bardeen and Brattain's immediate supervisor, John R. Pierce [March 27], who recalled:

"The way I provided the name, was to think of what the device did. And at that time, it was supposed to be the dual of the vacuum tube. The vacuum tube had transconductance, so the transistor would have 'transresistance.' And the name should fit in with the names of other devices, such as varistor and thermistor. And. . . I suggested the name 'transistor.'"

The MH-1 Mechanical Hand

Dec. 23, 1961

Heinrich Arnold Ernst completed his D.Sc. thesis at MIT on the MH-1 mechanical hand. It was unique [March 13; Dec 10] in being equipped with binary touch sensors placed in different parts of the gripper, and with pressure sensors inside the gripper. The touch sensors were used to detect contact between the gripper and any obstacles in the environment, and between the gripper and the object being grasped; the pressure sensors supplied data on the size of the object.

The control system executed on the TX-0 [Nov 20], and used its sensory feedback to determine a reasonable course of action after a goal has been specified for the hand. The idea was to replace traditional controls based on numerical operations by pattern recognition and simulation of higher cognitive processes such as awareness and understanding.

The concept had originated with Claude Shannon [April 30] (Ernst's supervisor) and Marvin Minsky [Aug 9] in 1958.

For more handy robots, see [Feb 20; Sept 9; Nov 29; Nov 30].

DNSSEC Sourced

Dec. 23, 1997

John Gilmore [Aug 00], co-founder of the EFF [July 6], published the source code for DNSSEC (the Domain Name System Security Extensions), and thereby probably broke the law that restricted the 'export' of cryptographic software.

Since DNS [June 23] is the Internet's phone book, there's a strong incentive to keep it secure, and DNSSEC is

considered a major part of that effort. DNSSEC uses public key encryption and digital signatures to certify every address that's resolved by DNS [Feb 13].

However, over time it's gradually become clear that DNSSEC has a few security problems of its own, adds significant load to DNS servers, and cannot easily be scaled up to cover the full Internet.

OpenSSL Begins

Dec. 23, 1998

OpenSSL protects network communication against eavesdropping, and hides the identity of the user at the other end of the link. The library includes open-source implementations of the SSL and TLS internet protocols, basic cryptographic functions, and various utilities.

OpenSSL began life as a fork of SSLeay by Eric Andrew Young and Tim Hudson, which had ceased development the week before.

As OpenSSL's importance has grown, the development team has also grown, but still only consists of around 20 developers, and, despite its importance, relies mostly on donations to keep going.

In 2013, WikiLeaks [Oct 4] published documents obtained by Edward Snowden [June 21], which revealed that the NSA [Oct 24] had broken early versions of SSL by exploiting vulnerabilities such as the HeartBleed [April 1] bug.

Royal YouTube Channel

Dec. 23, 2007

The UK Royal Household launched a Royal Channel on YouTube to showcase exciting videos of Queen Elizabeth II and other members of the family in action.

At its launch, the channel included the first televised Christmas broadcast by the Queen from 1957, and gradually added all the others. Other material included royal speeches, royal interviews, royal visits, and, of course, royal weddings.

The previous year, the Queen's Christmas message had been released as a podcast.

For more royal online activities, see [March 6], [March 26]

The End of VHS

Dec. 23, 2008

The last major US supplier of pre-recorded VHS tapes, Distribution Video Audio, Inc., based in Palm Harbor, Florida shipped its final truckload of tapes. And so the VHS format died.

The first film released on VHS was the 1976 South Korean drama, "The Young Teacher". The first three US movies were: "The Sound of Music", "Patton", and "M*A*S*H", at $50-$70 each.

The last major Hollywood movie released in the format was "A History Of Violence" in 2006.

Ukraine Power Grid Cyberattack

Dec. 23, 2015

The first known successful cyberattack on a power grid occurred on this day at 3:30pm. Hackers successfully compromised information systems of three energy distribution companies in the Ukraine and temporarily disrupted the country's electricity supply.

One worker reported seeing the cursor on his screen moving by itself, and clicking on buttons to take substations offline. The machine then logged him out, and changed his password.

Thirty substations were switched off, and about 230,000 people were left without electricity for up to six hours during winter.

According to the companies, the attacks came from computers with IP addresses located in the Russian Federation.

The offensive seems to have started in the previous spring when emails were sent to workers containing an infected Word document [March 26].

For another Ukrainian cyberattack, see [June 27].