Nov. 17th

The Modified Julian Date

Nov. 17, 1868

The Smithsonian Astrophysical Observatory (SAO) started tracking satellites in 1957 soon after Sputnik was launched [Oct 4], and stored the data on a 36-bit IBM 704 [May 7].

This information naturally included the Julian Day (JD) which is measured in days since Jan. 1, 4713 B.C.. However, this meant that Jan. 1, 1957 would be encoded as 2,435,839, which was too big to fit into an 18-bit field on the machine. Memory was expensive back then, and so rather than be wasteful and utilize a 36-bit word, the astronomers came up with the Modified Julian Day (MJD), which was calculated like so:

```
MJD = JD - 2,400,000.5
```

It just so happens that Nov. 17, 1858 is the Julian Day (JD) 2,400,000, and predated the oldest star catalog in use at the SAO, thereby avoiding having to use negative MJD values in any satellite tracking calculations.

The 0.5 was included so that an MJD day starts at noon so that nighttime observation times (as preferred by astronomers) fall in the middle of a 24 hour period.

An MJD starting from Nov. 17, 1858, stored in an 18-bit word, would supply enough space for seven centuries. Even better, dates could still cover 3 centuries in only 17-bits, with the other bit used to represent negatives.

MJD is still employed in OpenVMS [Oct 25], but with 100 nanosecond granularity, and stored in 63-bits. This means that OpenVMS should have no trouble with dates until:

```
July 31, 31086 02:48:05.47
```

At that moment, time will overflow, and become negative. Actually, this calamity will be preceded much sooner by another, occuring at the end of the year 9999, when the 4-digit year field using by OpenVMS will max out.

For links to more date/time related problems, see [Jan 1].

Gödel Completes Incompleteness

Nov. 17, 1930

Kurt Gödel [April 28] completed his paper, “Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I” (“On Formally Undecidable Propositions of Principia Mathematica and Related Systems I”).

The paper sets out Gödel 's incompleteness theorems, which answer the first two parts of David Hilbert’s three-part "second problem" [Sept 3]: is mathematics complete, is it consistent, and is it decidable?

No and no. In other words, any system powerful enough to describe arithmetic must contain statements which can neither be proved true nor false (i.e. the system is "incomplete"). In essence, Gödel had showed that any reasonably powerful system of maths has limits.

This left the decidability question, often known by its catchy Germany name, the Entscheidungsproblem (Decision Problem). Working independently, Alonzo Church [June 14], Alan Turing [June 23], and Emil Post [Feb 11] published answers in 1936. (All of them amounting to "no".) Also, Turing by framing his approach in terms of a 'machine' showed that Gödel 's results impose similar limitations on computer algorithms.

Electronic Cupid

Nov. 17, 1956

On "People Are Funny", an American TV game show, host Art Linkletter reported on how he had asked Dr. Paul Popenoe of Los Angeles' American Institute of Family Relations to help him create a computerized way to successfully match men and women.

The pair drew up a questionnaire of 32 items that affect marital relations (sex, race, religion, politics, weight, height, pets, drinking, preferences for double or twin beds, etc.). Linkletter put ads in local papers asking people over 21 who were seeking companionship to get in touch. To the more than 4,000 who replied, he dispatched the questionnaires.

Then Remington Rand's UNIVAC [March 31] stepped in, sifted and sorted the answers supplied by both sexes, bringing forth its matches: John Caran, 28, a Los Angeles adman, and Barbara Smith, 23, a receptionist.

In September the couple saw each other for the first time, in front of the "People Are Funny" cameras. On tonight's show, Barbara reported: "UNIVAC is a pretty good deal."

The most detailed report says that a UNIVAC No. 21 was used, although no such product was ever released. There was a UNIVAC 121 during that period, a punched card calculator rather than a computer.

A slightly better documented computer dating service debuted on [Sept 25] 1959.

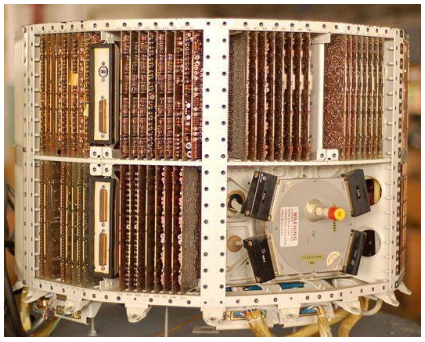
Guiding a Minuteman I

Nov. 17, 1961

This day saw the first successful launch from a silo of the Minuteman I ICBM, which US President John F. Kennedy referred to as his “ace in the

hole" during the Cuban Missile Crisis (Oct. 1962).

The Minuteman's inertial guidance system used the completely solid-state Autonetics D-17B computer. It contained 1,500 transistors, and could execute almost 13,000 additions per second. Each D-17B was cylindrical (to fit inside a missile), about the size of a fifty-five-gallon drum, and weighed around 62 pounds.



An Autonetics D-17B guidance computer from a Minuteman I missile. Photo by Jnanna. CC BY-SA 3.0.

The Air Force spent millions improving the reliability of the D-17B's transistors, which greatly reduced the failure rate of all transistor production lines, and lowered costs. In turn, this encouraged the uptake of transistors by the general electronics industry.

Even after the Air Force decommissioned a 1,000 Minuteman l missiles in the early 1970's, their D-17B's still proved to be useful. For just $100 shipping, and a qualifying letter from the National Science Foundation, colleges and universities could receive one. Each D-17B came with thirty pounds of manuals, but no software or peripherals.

The next-generation Minuteman II [Aug 5] also had a massive effect on the electronics industry, but in the area of IC design.

Second E-book

Nov. 17, 1982

The second electronically published novel, "Blind Pharaoh" was made available chapter-by-chapter to subscribers of "The Source", an early online service [Dec 3]. It was written by Canadian Burke Campbell on an Apple III [May 19] during a single massive 61.5 hour writing session (with brief toilet breaks).

The three-day writing spree was a media event held at a Toronto art gallery to coincide with a local computer show. Campbell later recalled, "I arrived in a black chauffeur-driven limousine in a sweat suit made out of black sequins and I wore black cowboy boots. I mounted the black vinyl stage and there was the microcomputer."

"Blind Pharaoh" is a thriller about a mysterious man who travels around North America in his limousine manipulating the lives of others.

The first electronic novel was "Mylar's Warp", a science fiction work by Floyd Flanagan, released in 1981, also on 'The Source". Its story involves cryogenic preservation, electronic world domination, and Johnny Mylar, a modern-day everyman.

Transputer Announced

Nov. 17, 1983

The transputer (a name derived from "transistor" and "computer") was the first general purpose microprocessor intended for parallel computing systems. It was developed at Inmos, a semiconductor company in Bristol, UK, with early designs created by David May and Robert Milne.

Each transputer included a built-in simple OS for running processes in parallel, its own memory, and four high speed (20 Mbit/s full duplex) bi-directional serial links to talk to other transputers.

The plan was to program transputers using the high-level Occam language which supported concurrency and channel-based communication, and was based on Tony Hoare's [Jan 11] CSP process calculus.

An Immos T414 transputer chip. Photo by Letdorf. CC BY 2.5.

Although a great idea, transputers were expensive and relatively slow for their price. As a result, few transputer-based machine were ever built; the most notable probably being the Atari [June 27] Transputer Workstation (1988), which was canceled after only a few hundred had been produced.

PHRACK Starts

Nov. 17, 1985

PHRACK was an "e-zine" (electronic magazine) covering a wide range of topics including computer and physical security, hacking, cryptography, and the counter culture. It took its name from the words "phreak" and "hack".

Craig Neidorf (aka "Knight Lightning" [July 23]) and Randy Tischler (aka "Taran King") edited the first 30 issues, which were uploaded to Tischler's "Metal Shop" BBS. Its best known articles include:

- "The Hacker Manifesto" [Jan 8] by "The Mentor", published in the seventh issue.
- "Smashing The Stack For Fun And Profit" by "Aleph One", published in issue 49. It explained the joys of causing stack buffer overflows.

- "The Art of Scanning" by Fyodor, in issue 51, which introduced the nmap network scanning tool.

Mavis Beacon
Nov. 17, 1987

After *The New York Times* ran a glowing review by Peter Lewis of "Mavis Beacon Teaches Typing", sales of the touch typing software took off.

Mavis Beacon was groundbreaking for being one of the first female African-American embodiments of software. Throughout the 1990's, Mavis Beacon served as the virtual typing instructor at numerous US schools, and has been called "the Betty Crocker of cyberspace" [March 19].

Sadly the fact that Mavis Beacon was a black woman meant that some retailers were reluctant to display the product. However, once the popularity of the program became evident, spurred on by the NYT review, many of them reversed their decision.

The program was released by "The Software Toolworks" for MS-DOS, and written by Norm Worthington, Walt Bilofsky, and Mike Duffy. They worked from Bilofsky's home, taking just six months to develop the program although Duffy later recalled often having to work more than 140 hours per week.

The team aimed at making the application fun—it included a number of typing games, and a certificate of achievement could be printed at the end of the tests. But, most surprisingly, there was no real life Mavis Beacon.

The model chosen to be the face of Mavis was Haitian-born Renée L'Espérance, who was discovered working behind the perfume counter at Saks Fifth Avenue Beverly Hills by former talk-show host and partner at "The Software Toolworks" Les Crane.

Mavis's name comes from a combination of Mavis Staples (one of the software developer's favorite singers) and the word beacon (i.e. as a guide to typing).

Veronica
Nov. 17, 1992

Steven Foster and Fred Barrie at the University of Nevada released Veronica ("Very Easy Rodent-Oriented Net-wide Index to Computer Archives"), one of the earliest search engines for the Gopher protocol [Feb 7]. It maintained a database of nearly every menu item on nearly every active Gopher server.

Its name was chosen to match the still-popular Archie FTP search service [Sept 10] in reference to the Archie Andrews and Veronica Lodge characters in *Archie Comics*.

Veronica was followed by Jughead in 1993, an alternative search engine system for Gopher (Jughead Jones is Archie Andrews' pal). It was developed by Rhett Jones (no relation to Jughead) at the University of Utah. A backronym was suggested later: "Jonzy's Universal Gopher Hierarchy Excavation And Display."

Classmates
Nov. 17, 1995

Randy Conrads' Classmates.com was probably the first social networking website. Originally launched as a list of school affiliations, it later incorporated features like member profiles and friends lists. It also maintained an online archive of over 300,000 yearbooks, the world's largest digital yearbook collection. The oldest was the 1885 yearbook from Central High School in Manchester, New Hampshire.

Other possibilities for "first social network site" are SixDegrees.com [Dec 00] and SocialNet.com [Aug 5].

Geometry Wars
Nov. 17, 2003

"Geometry Wars" was a 2D arcade style shooter created by Stephen Cakebread at Bizarre Creations. It began as a mini-game inside the Xbox [Nov 15] game "Project Gotham Racing 2", but was such a big hit that it was released standalone through the Xbox Live Marketplace.

Despite never being a boxed game sold on store shelves, it proved to be extremely popular, and demonstrated the viability of moving away from physical game discs towards downloads.

CrackStation
Nov. 17-18, 2007

Security consultant Nick Breese described his "CrackStation" project at the Kiwicon hacker conference in New Zealand.

The CrackStation's password cracking software employed six of the PlayStation 3's [Nov 11] processors (out of 8) to perform 1.4 billion calculations per second to generate MD5 cryptographic hash functions [May 6]. This was a dramatic increase in speed over similar software running on Intel architectures, which could only manage a meager 10 - 15 million calculations per second.

His announcement raised serious concerns over the safety of MD5 for encryption. In 2010, the CMU Software Engineering Institute stated that MD5 was "cryptographically broken and unsuitable for further use". Most US government applications now require the SHA-2 family of hash functions.