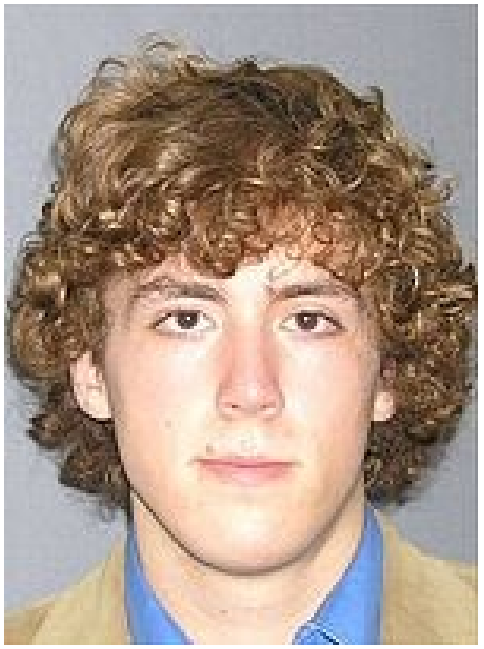
Security

It’s for everyone, not just the paranoid.

Networked Interactivity -SP2020

Passwords



In 2008, David Kernel obtained access to Palin's account by looking up biographical details such as her high school and birthdate and using Yahoo!'s account recovery for forgotten passwords.

In November 2010 Kernell was sentenced to a year and a day of prison, preferably to be served in a halfway house, plus three years of probation.

Pick
a
P4ssw0rd?

These are all pretty much useless:

Kissme

Harvey

1L0vey0u

Daff0dil

B4byd0ll

(From a phrase you can remember…)

“If you liked it then you shoulda put a ring on it”

=

lylitysparoi

or maybe:

1yl1tyspar01

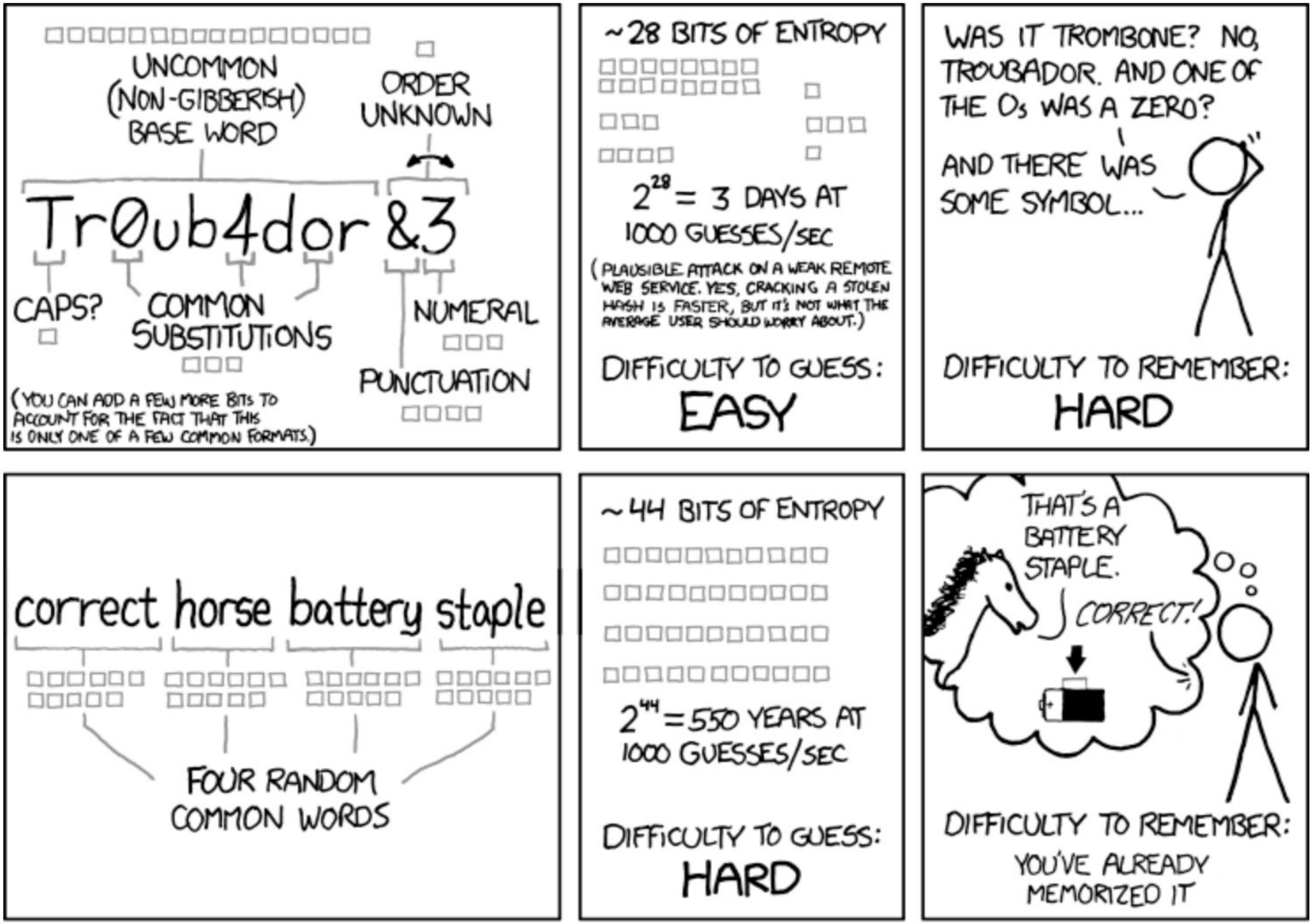
It can be customized in order to not use the same password for everything:

=

1yl1tyspar01m4$$4rt

1yl1tyspar011nst4gr4m?

(XKCD comic)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Phishing and “Spear Phishing”

John Podesta, chairman of Hillary Clinton’s presidential campaign, had his email hacked as a result of spear phishing.

Subject: *SOmeOne has your passwOrd*

Hi John.

Someone just used your password to try to sign in to your Google Account:
john.podesta@gmail.com.

Details: Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt.
You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team

Charles Delava's reply (with typo, missing "not")

"Is This Something That's Going to Haunt Me the Rest of My Life?"

Sara,

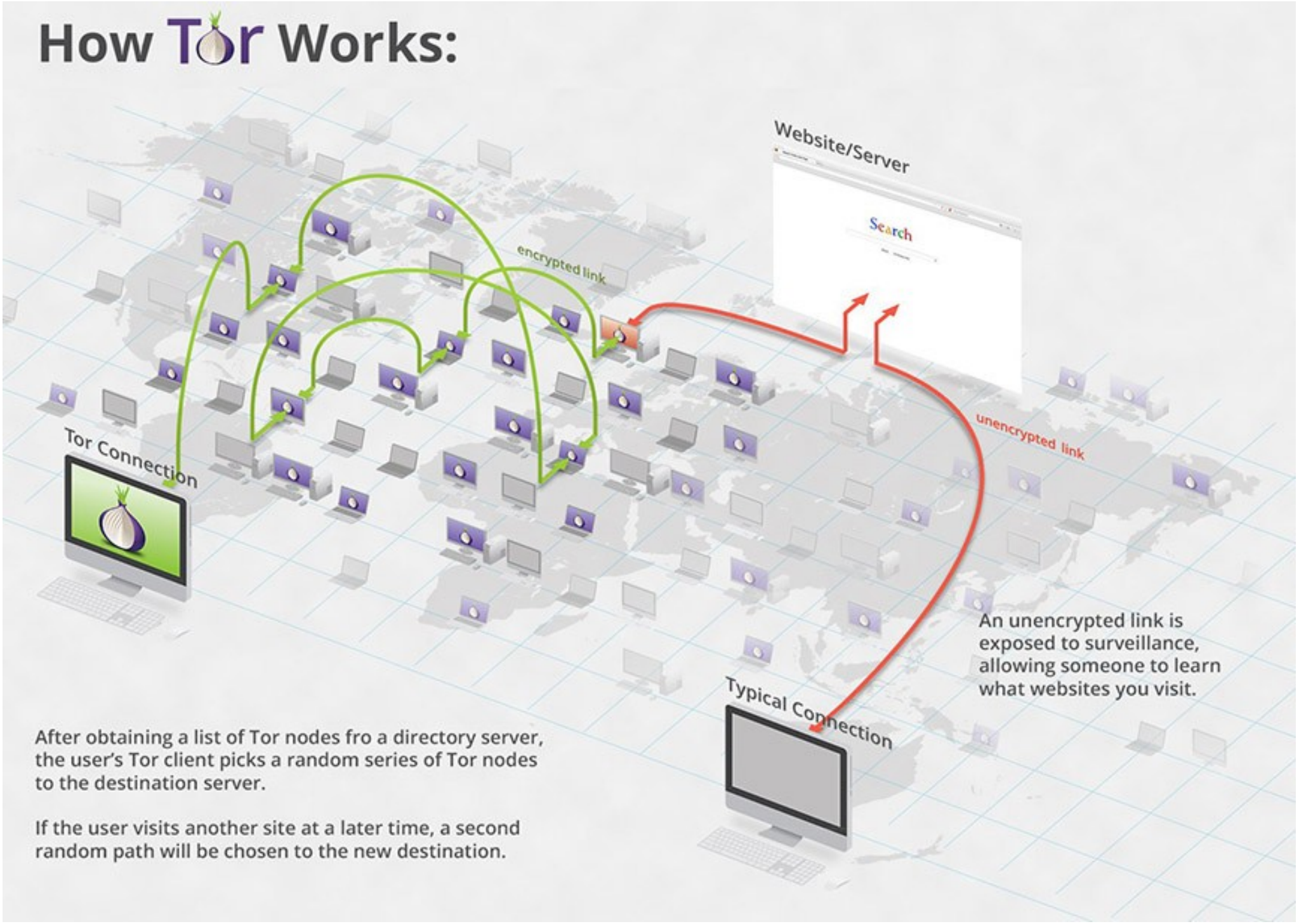
This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security

to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at [redacted]

How Tor Works:



After obtaining a list of Tor nodes fro a directory server, the user's Tor client picks a random series of Tor nodes to the destination server.

If the user visits another site at a later time, a second random path will be chosen to the new destination.

Some Notes on the Pi and Free/Open Source Movement

1952: Polio Vaccine

Jonas Salk led the team of medical researchers who developed a vaccine to prevent the transmission of a deadly paralyzing virus.

When asked by an interviewer, “Who owns the patent on this?” He replied, ”I would say, ...the people. There is no patent. Could you patent the sun?”

2015: Martin Shkreli

Shkreli, 32, a former hedge fund manager, purchased the rights to Daraprim, a 62-year-old life-saving drug used for treating AIDS patients.

He then raised the price overnight from $13.50 per tablet to $750.

In 2018 was sentenced to seven years in federal prison for securities fraud.

Free Software Movement

In the 1950s into the 1960s almost all software was produced by computer science academics and corporate researchers working in collaboration.

The philosophy of the movement is that the use of computers should not lead to people being prevented from cooperating with each other. In practice, this means rejecting "proprietary software" (which imposes such restrictions), and promoting free software.

In 1983, Richard Stallman published the GNU Manifesto and launched the GNU Project. It's goal was to create from scratch a free version of the Unix Operating System. The “free software definition” was published in February 1986.

Free Software Movement

The Four Freedoms:

Freedom 0: The freedom to run the program for any purpose.

Freedom 1: The freedom to study how the program works, and change it to make it do what you wish.

Freedom 2: The freedom to redistribute copies so you can help your neighbor.

Freedom 3: The freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits.

Freedoms 1 and 3 require source code to be available because studying and modifying software without its source code is highly impractical.

Linux (GNU/Linux)

In 1991 a computer student from Helsinki, Finland named Linus Torvalds posted to a newsgroup on operating systems:
"I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones."

Linus Torvalds

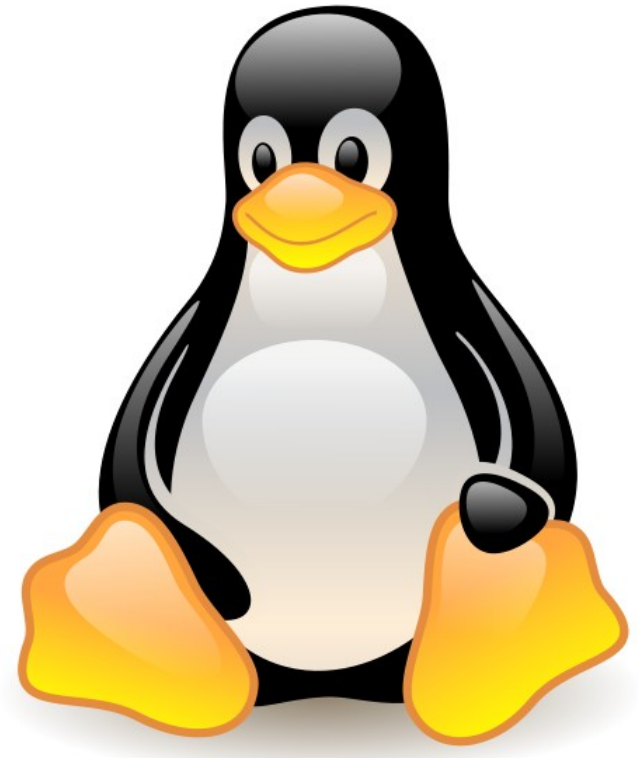
Linux (GNU/Linux)

In 2015:
Of the top 500 super computers in the world, 498 run Linux.

In 2020, it’s 500 out of 500.

Linux (GNU/Linux)

Software developed over the Internet.



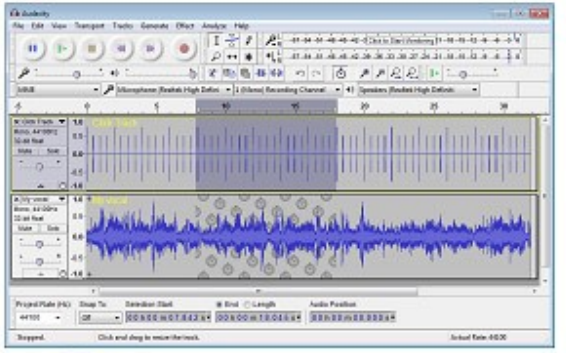
First Large-Scale example of an Internet-based, distributed development model (with prominent success stories like Apache web-server.)

Some major Free Software projects:

LibreOffice
The Document Foundation
5

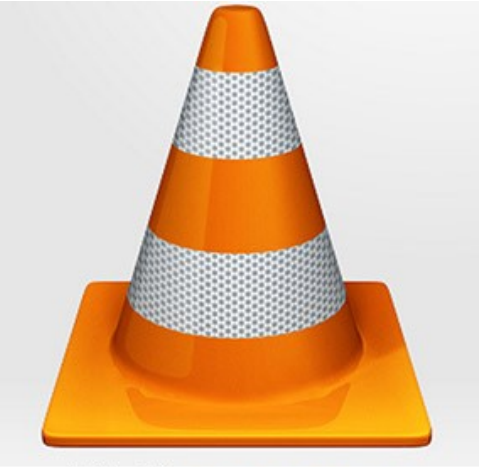
(Office Suite)
OpenOffice / LibreOffice

blender™
3D Rendering &
Animation



Audacity
Audio Editor

Apache
HTTP SERVER PROJECT



VLC Media Player

mozilla

Web Browser, plugins, Email

Coining the term “Open Source”

The “open source” label was created at a strategy session held on February 3rd, 1998 in Palo Alto, California, shortly after the announcement of the release of the Netscape source code.

The conferees believed that it would be useful to have a single label that identified this approach and distinguished it from the philosophically- and politically-focused label "free software." Brainstorming for this new label eventually converged on the term "open source", originally suggested by Christine Peterson.

Threats and Reasons to Care About Free

- Patents
- Perversion of Copyright
- DRM
- Trade Agreements

Apple filed for *and received* a design patent on rectangles with rounded corners on mobile devices

Apple owns patent D670,286, which is design patent for the rounded edges of the rectangular screen and icons of the iPhone and iPad. They sued Samsung for allegedly copying the iOS look-and-feel in its line of Galaxy smartphones and tablets in a famous lawsuit that dragged on for years.

Protecting Consumers Health and Safety

Karen Sandler has an amazing Ted Talk about “Being a Cyborg. A Free Software advocate with proprietary software in her heart”

https://www.youtube.com/watch?v=GcWID2Y6HNM

Karen Sandler

Protecting Consumers Health and Safety

Alison Chaiken is a Free Software advocate for software that is running in automobiles.

Alison Chaiken

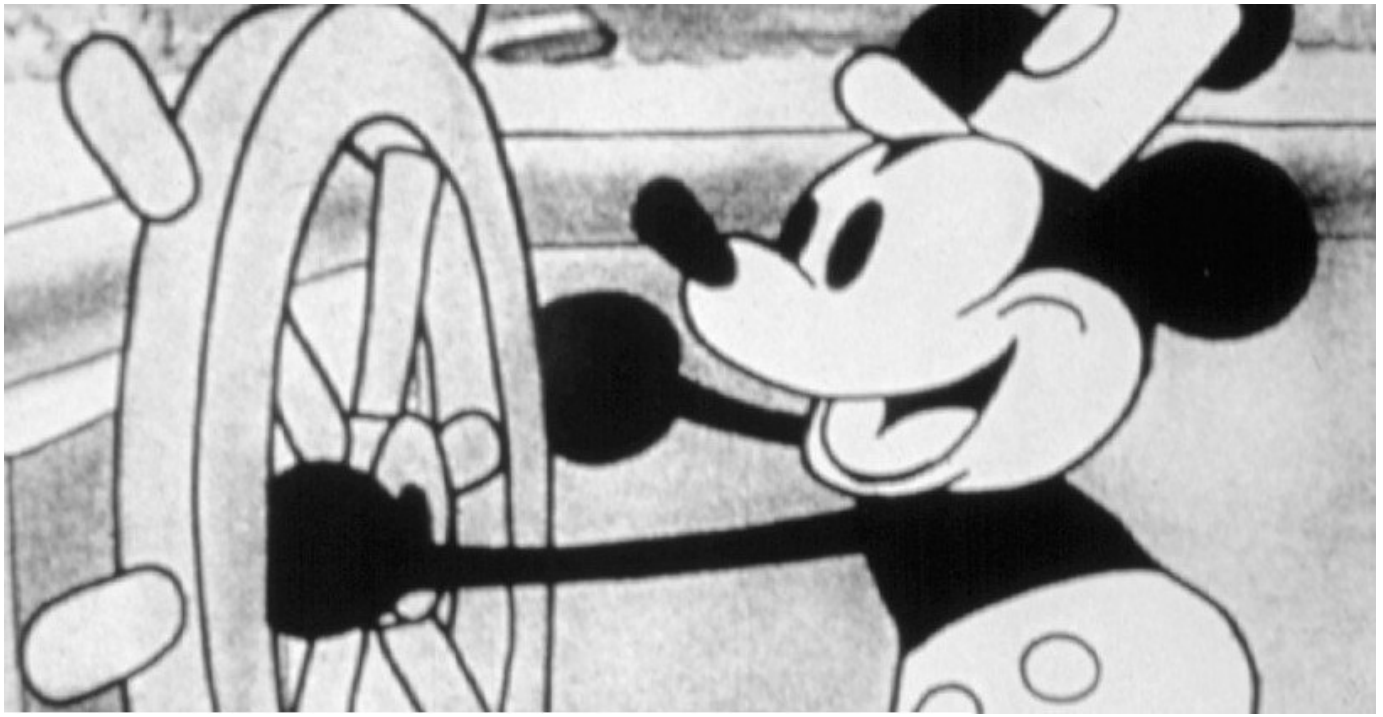
https://www.youtube.com/watch?v=dfQYIJsiSG0

Voting Machines

The **Diebold Corporation** was embarrassed when some of the source code from their voting machines was released in 2003. Avi Rubin, Professor of Computer Science at Johns Hopkins University and Technical Director of the Information Security Institute analyzed the source code used in these voting machines in 2004 and reports:

"this voting system is far below even the most minimal security standards applicable in other contexts."
Following the publication of this paper, the State of Maryland hired Science Applications International Corporation (SAIC) to perform another analysis of the Diebold voting machines. SAIC concluded "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise."

Mickey Mouse and US copyright law



When first introduced, US copyright was for 14 years.
Now it can last over a century thanks to special interest legislation from Corporate lobbyists. Corporate lobbyists have procured legislation that has pushed this to over 120 years.

The Massachusetts Open File Format Decision

In early 2005, Eric Kriss, Secretary of Administration and Finance in Massachusetts, was the first government official in the United States to publicly connect open formats to a public policy purpose:

"It is an overriding imperative of the American democratic system that we cannot have our public documents locked up in some kind of proprietary format, perhaps unreadable in the future, or subject to a proprietary system license that restricts access."

This caused a fire storm of controversy as other states and nations around the world followed suit, ditching Microsoft Office as a result.

It prompted Microsoft to develop it's own file format ".docx" with they maintain is an open standard for storing data.

The Privatization of Water - Bolivia 2000

The International Monetary Fund (IMF) approved a $138 million loan for Bolivia to “help the country control inflation and bolster economic growth.” In compliance with IMF-drafted "structural reforms", Bolivia agrees to sell off "all remaining public enterprises," including privatizing water supplies.

Water costs increased.

Riots and strikes ensued in the country's 3rd largest city, Cochabamba. The residents claimed that “access to clean water was a human right.” As a result, the government backed down. The public's ownership of water was restored.

Criminalizing Farmers Saving Seeds - Monsanto

For as long as humans have been growing food, farmers have saved seeds from their harvest to sow the following year. But Monsanto and other big seed companies have successfully argued that since they spend millions of dollars developing new crop varieties and that these products should be treated as proprietary inventions with full patent protection.

Just as one can't legally reproduce a CD or DVD, farmers are now prohibited from copying the GM seeds that they purchase from companies like Monsanto, Bayer, Dow and Syngenta.

“Corporate Personhood”

The **Bill of Rights** in the United States Constitution was written to protect the citizens from oppressive forces, private or governmental.

Corporate lawyers (acting as both attorneys and judges) subverted our Bill of Rights in the late 1800’s by establishing the doctrine of “corporate personhood” — the claim that corporations were intended to fully enjoy the legal status and protections created for human beings.

“Citizen's United”

What is it?

In the 2008 election season, Citizens United the PAC (heavily funded by the Koch Brothers) sought to broadcast TV ads for a video-on-demand film criticizing presidential candidate Hilary Rodham Clinton. The Federal Election Commission ruled that they could not based on long standing legal protection from wealthy interests “buying” elections.

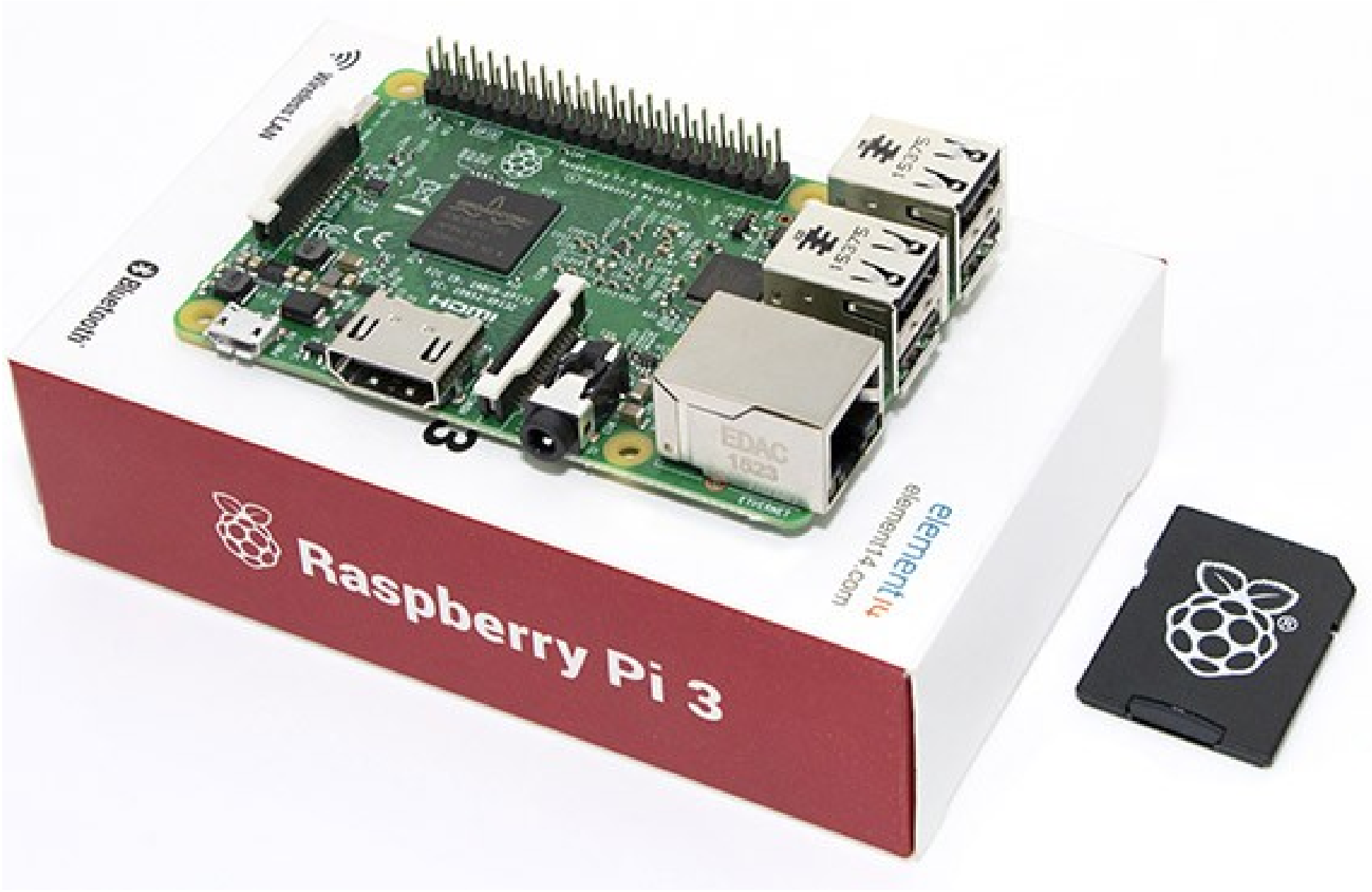
In 2010 the Supreme Court, in a controversial decision, found that preventing corporate campaign contributions interfered with corporations' First Amendment Right to Freedom of Speech.

Jim Kent

While working on his PhD in Biology at the University of California, Santa Cruz, Kent in May 2000, wrote a program that allowed the publicly funded Human Genome Project to assemble and publish the human genome sequence. His efforts were motivated by the research needs of himself and his colleagues, but also out of concern that the data might be made proprietary via patents by Celera Genomics.

In his close race with Celera, Kent and the UCSC Professor David Haussler quickly built a modest cluster of 50 commodity Personal Computers running the Linux operating system to run the software. In contrast Celera was using what was thought of then as one of the most powerful civilian supercomputers in the world. His first assembly on the human genome was released on June 22. Celera finished its assembly on June 25, and the dual results were announced at the White House on June 26. On July 7, the Santa Cruz data was made publicly available on the Web Wide Web.

The Raspberry Pi



Eben Upton, Executive Director, Paspberry Pi Foundation

What Operating system does this computer run?

– ***Raspbian***, based on Debian Linux is recommended for newcomers.

-But there are many Linux distributions including: Arch, Android, Fedora, Gentoo, RISC OS, and Occidentalis (by Lady Ada)

Many people choose to run “headless” via SSH, but it also supports a full-fledged desktop.

Raspberry Pi 3 Specs:

- A 1.2GHz 64-bit quad-core ARMv8 CPU
- 802.11n Wireless LAN
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
-

-And like the Raspberry Pi 2:

-

- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port
- Combined 3.5mm audio jack and composite video
- Camera interface (CSI)
- Display interface (DSI)
- Micro SD card slot (now push-pull rather than push-push)
- VideoCore IV 3D graphics core

Install LAMP stack:

```
$ sudo apt-get install apache2

$ sudo apt-get install php5 libapache2-mod-php5

$ sudo apt-get install mysql-server

$ sudo apt-get install libapache2-mod-auth-mysql

      php5-mysql
```

Install Python for GPIO:

```
$sudo apt-get install python-dev

$sudo apt-get install python-rpi.gpio
```

Raspberry Pinout