Protecting Yourself Online

Adam Bolte

abolte@systemsaviour.com

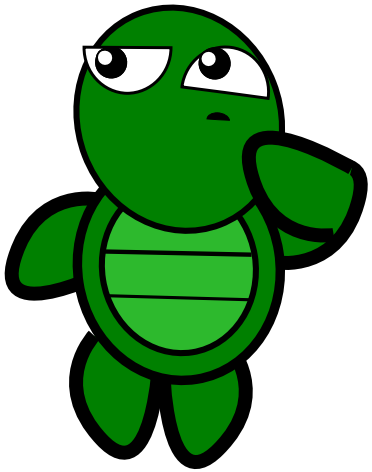
GnuPG:
1C2D 178E EBBE BE08 0A5D EBE2 4D8C FD39 34A6 2048

Slides online here:

https://systemsaviour.com/downloads/

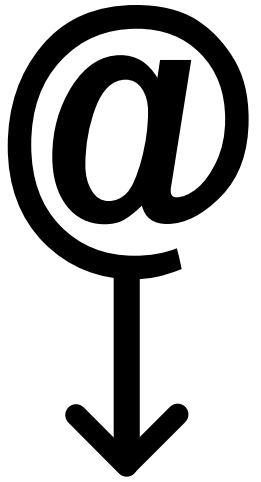
Privacy

- To have privacy, you must first trust that your computer is under your control.
  - Free software
  - no untrusted binaries
- Confidence that I'm not being tracked or monitored.
- Ability to exchange confidential information securely with the correct person.
- Privacy from whom? Does it matter?



Why does it matter if people know what I'm up to?

- Does anyone here think that they've "*got nothing to hide*"?
- Do the people spying on you have nothing to hide as well? Do they let you spy on them?
- It seems that most people don't realise how valuable it can be until it's too late!
- Privacy is not about hiding a wrong.



Fraud

- Phishing, social engineering
- Pharming
- E-mail scams, spoofing (fake return address)
- Identity theft
- PayPal Fraud
  - Selling bitcoin
  - eBay “collection in person” scam
- For a comprehensive list: https://en.wikipedia.org/wiki/Internet_fraud

Keeping safe online

- E-mail
- World Wide Web
  - SaaS
  - Social Networks
  - Browsers
- Instant messaging
- Online transactions
- Installed software

E-mail: Insecure by default

- E-mails are often transmitted and stored in plain text
- Trivial for a mail server sysadmin to peek...

```
# postconf -e master_service_disable=qmgr.fifo in_flow_delay=0s
# invoke-rc.d postfix reload
<wait for mails>
$ mailq
# postcat -q <dueue id> >interesting-save_for_later.txt
# postconf -e master_service_disable= in_flow_delay=1s
# invoke-rc.d postfix reload
```

- … or just silently send a second copy of all e-mail to another address.

E-mail (cont.)

- Companies such as GMail make money by spying on your e-mails, so they can better target you with adverts!
- If you don't use Gmail (and expect Google and the NSA won't be able to spy), does it make a difference when other people you are communicating with use Gmail or other USA-based providers? What to do?

Email: Enter asymmetric encryption technologies

- Pretty Good Privacy (PGP Corporation acquired by Symantec)
- GnuPG (free software, http://www.gnupg.org/)
- S/MIME (no-cost CAs likely won't perform strong validation, so is not common outside of corporate environments)

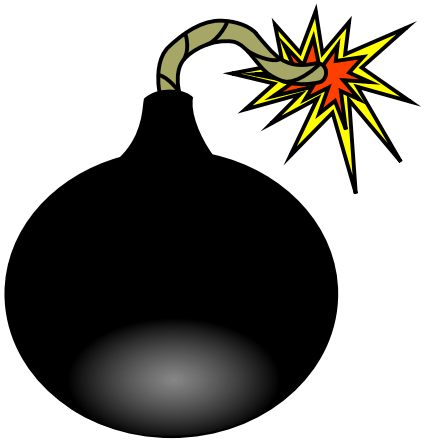
GnuPG

- Web of Trust
  - Key-signing parties
- Inline Vs PGP/MIME signatures
- Web-mail issues

Software as a Service

Involves doing your computing on a server probably owned and managed by somebody else. Examples include:

- GMail (and Google Apps)
- Microsoft Office 365
- Accounting software
- Dropbox
  - But would it be okay if they encrypted our data?



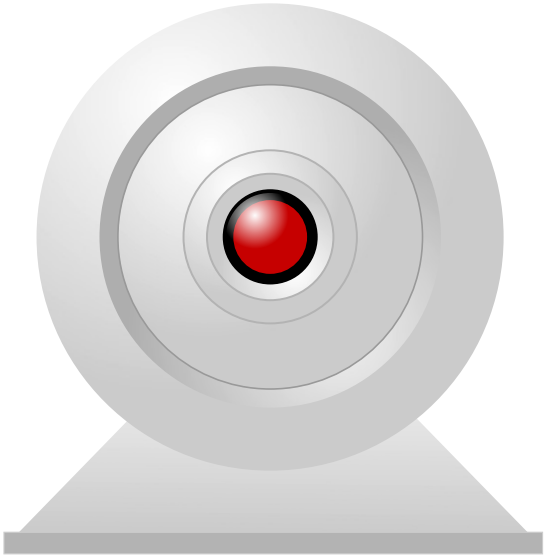
SaaS Alternatives

- ~~Dropbox, Google Calendar~~ ownCloud
- ~~Google Docs~~ MediaWiki or EtherPad
- ~~Gmail/Google Mail~~ RoundCube
- ~~GitHub~~ Gitweb

Centralised Social Networks

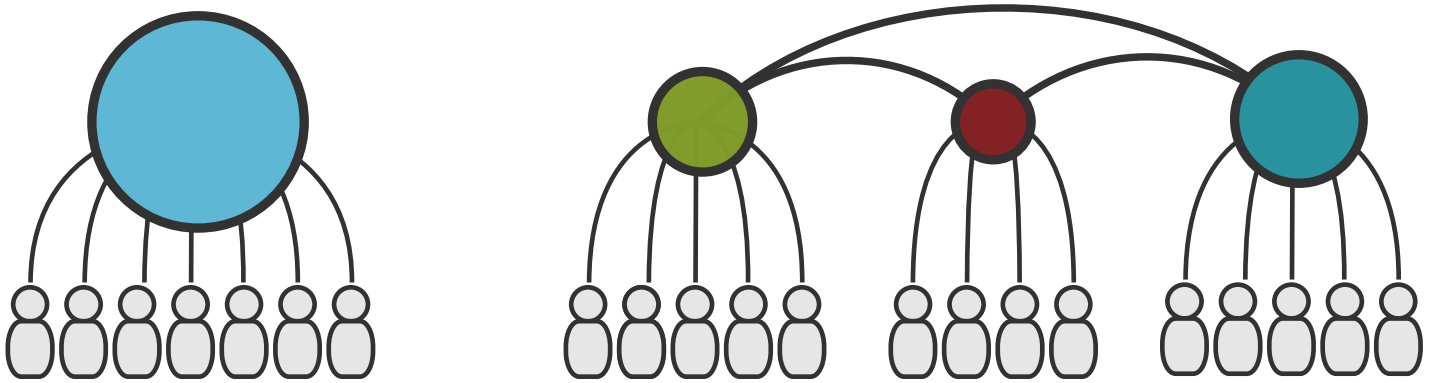
- Facebook
- Google+
- Twitter
- tumblr
- LinkedIn

...and hundreds more!



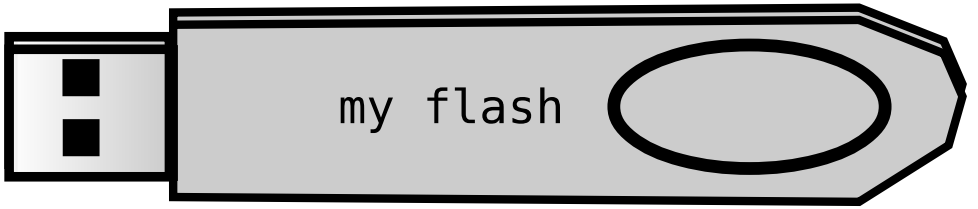
Distributed Social Networks
(the way the web was supposed to work)

- GNU Social (formally StatusNet, Laconica)
- Pump.io, http://pump.io/
- Friendica, http://friendica.com/
- DIASPORA*, https://diasporafoundation.org/
- MediaGoblin, http://mediagoblin.org/
- WordPress, http://wordpress.org/



Browsers and browsing habits

- Firefox, Konqueror, Midori, Elinks
- Do Not Track enabled (but does it help?) and disable the attack sites and web forgeries look-up options
- DuckDuckGo / Ixquick / StartPage
- Verify PGP/GPG signatures and/or checksums of downloads
- Don't reuse passwords, and use a password manager
- Refuse the temptation to install things that you weren't looking for.
- If using the Firefox built-in password manager, use a Master Password.



Browser Extensions

- Request Policy, white-list cross-site requests
- NoScript, white-list for JavaScript, some plugins, activates DoNotTrack, and prevents certain kinds of attacks.
- Cookie Monster, white-list cookies
- HTTPS Everywhere, black-list of sites for HTTPS-only traffic
- BetterPrivacy, zap Super-Cookies
- User Agent Switcher
- Greasemonkey, customise website functionality

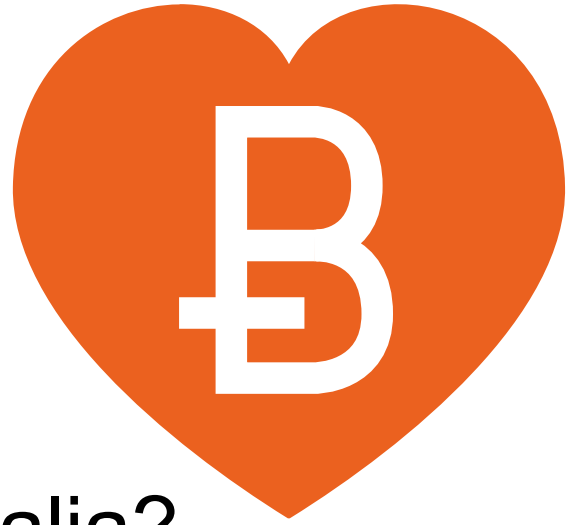
Tor

- Quite usable. Speed is slower, but generally acceptable.
- Designed to protect the U.S. Navy's communications
- TCP streams only
- Tor Browser Bundle, Tails (read-only VM)
- Picks random hops until the destination. No individual server ever knows the complete path.
- Onion addresses
- US Government have been attacking Tor, so they must be worried about it!
- Grab it here: https://www.torproject.org/

IM and video conferencing

- Proprietary voice and chat protocols like Skype are guaranteed to be insecure.
- **Microsoft Reads Your Skype Chat Messages**, 2013-05-15, http://yro.slashdot.org/story/13/05/14/1516247/microsoft-reads-your-skype-chat-messages
- XMPP / Jingle (eg. Pidgin)
- Jitsi, https://jitsi.org/
- Off-the-Record (OTR) for deniability

Bitcoin



- Why is it important?
- Bitcoin ATMs coming soon to Australia?
- Getting easier and more popular all the time.
- Closest thing to digital cash, although not necessarily anonymous (but still the best we have).
- Can take a few minutes for transactions to be confirmed.

Local software security

- Run a browser in a separate account
- Check your browser plug-ins
  - Flash?
  - Java?
- Use HDD encryption
  - dm-crypt + LUKS (block-level, full disk encryption)
  - eCryptfs (filesystem-level)
- Screen-saver lock short-cut – don't rely on a timeout
- 100% Free Software distribution
- AIDE (Advanced Intrusion Detection Environment)
  http://aide.sourceforge.net/
- ClamAV
  http://www.clamav.net/

DRM and Adware

Programs may be reporting behind your back:

- Steam, knows when you are online, what programs you have installed, what you are running, who your friends are, your interests, your game buying habits and wish list, credit card?, etc. Compare to Humble Bundle.
- Apple iTunes/Store, just as bad as Steam.
- Even Ubuntu GNU/Linux, knows when you are online, what your interests are (Unity shopping lens).


THEY ARE WACHING YOU

Further Reading (the bad)

- **Privacy is Dead. The NSA Killed it. Now What?**, PCMag, 2013-09-10, Neil J. Rubenking

  http://securitywatch.pcmag.com/hacking/315668-privacy-is-dead-the-nsa-killed-it-now-what
- **Microsoft handed the NSA access to encrypted messages**, The Guardian, 2013-07-12, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
- **Aussie Telco Telstra Agreed To Spy For America**, Slashdot, 2013-07-12

  http://yro.slashdot.org/story/13/07/12/1225211/aussie-telco-telstra-agreed-to-spy-for-america
- **GCHQ intercepted foreign politicians' communications at G20 summits**, The Guardian, 2013-06-17

  “phones were monitored and fake internet cafes set up to gather information from allies in London in 2009”

  http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits
- **FBI Admits It Controlled Tor Servers Behind Mass Malware Attack**, 2013-09-13, Kevin Poulsen

  http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

Further Reading (the good)

- **Prism Break**

  http://prism-break.org/

  Why Privacy Matters Even if You Have 'Nothing to Hide', The Chronicle of Higher Education, 2011-05-15, Daniel J. Solove

  https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

The end