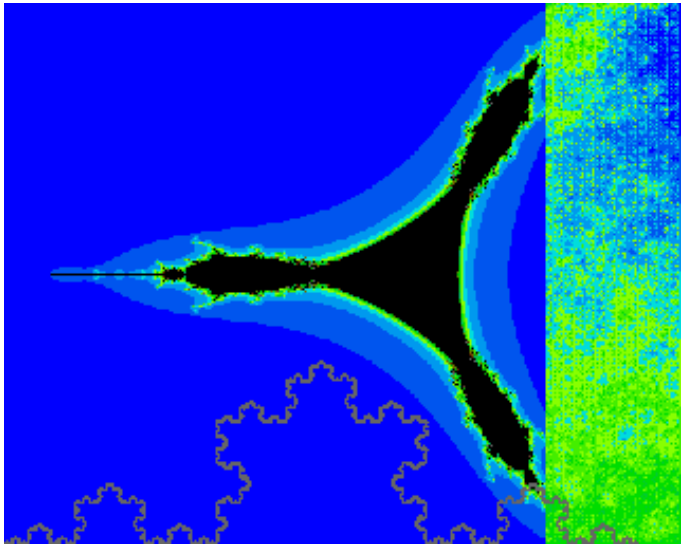
My Experience of Open Source and Academia

David Malone
Hamilton Institute / Department of Maths & Stats
Maynooth University

2021-05-10

Sharing Software

Got interested in sharing of software in secondary school.



Was sharing my code software for drawing fractals.

At College

- Studied maths as undergrad/postgrad,
- Shared departmental Unix system — encouraged to play,
- Computer system was maintained by students,
- Began sysadmining while in second year (1994).
- System largely ran from open source software:
  e-mail, usenet news, web, programming languages, document formatting, plotting tools, ...
- A few exceptions: operating system, Mathematica, maple.

Still at College

Worked at IEUnet (early Irish ISP), also run of open source software and replaced some OS with FreeBSD.

Started using both FreeBSD and Linux in college after that too. Even built a network switch with Ian Dowse.

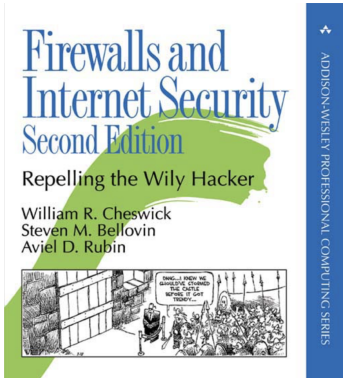
Towards the end of my PhD, got involved with FreeBSD project.

Research...

Started working on an SFI project in 2001.

- Network performance
  WiFi open source drivers, TCP performance.
- Internet Measurement
  Infrastructure: DNS, IPv6, ICMP, NTP, ...
  Tools: tcdpump, pcap, wireshark, ...
  Sometimes the software can be the subject of study.

Also been able to help IT services with problems.



6.6.1 Back Doors

Once *root* access is gained, attackers usually install new, more reliable access holes to the host. They may even fix the security hole that they first used, to deny access by other hackers.

These holes are many and varied. *Inetd,* which runs as *root,* may suddenly offer a new TCP service. *Telnetd* may skip the login and password checks if the TERM environment variable is set to some special, innocuous string. This string might be unexceptional when listed by the *strings* command, such as

```
SFreeBSD: src/usr.sbin/inetd/inetd.c, v 1.80.2.5 2001/07/17 10:45:03 dwmalone
```

which was required in the incoming TERM environment variable for a Trojan-horsed version of *telnetd.* We've also seen a *telnetd* daemon that is activated when a certain UDP packet is received. This could use public key cryptography to validate the UDP packet! The *ps* command may omit certain processes in a process list. A rogue network daemon may show the name "[zombie]" in a *ps* listing, looking like a program that is going away,

. . . More Research

- Network security
  Can directly improve security (e.g. better firewall),
  Also gave some useful reference points (e.g. electronic voting)
- Passwords
  Not so much open software, but open(?) data.
- Maths and other STEM subjects at the leaving cert.
  Not so much open source software.

Industrial Collaborations

- Testing network software (Dummynet),
- Software switching (Open vSwitch),
- Analysis of social/network/log data (R, NetworkX),
- Security/authentication/incident analysis.

To Finish

Many of the open-source gaps have now been filled (R, octave, SageMath, . . .)

Open source now seems more common than ever (iOS, Android, Chrome, Firefox, . . .)

Still teaching, researching and providing services.
Not contributing as much as I'd like.