Security and Free Software : Friends ?

hack.lu 2006 - a perspective about free software and security

Alexandre Dulaunoy

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

25th October 2006

Security in Software Engineering

- Security is not a default feature in software...
  - unsecure is often the default behavior
  - crappy is often the default feature
  - unstable is often the default state
- We are all writing unsecure, crappy & unstable software
  - Proprietary software (no 4 freedoms)
  - and Free software (4 freedoms)
- So what ?

Free Software - Advantages for Security ?

- Free software is **not** more secure because it's free software
- but free software is providing some advantages to make it more secure (and sometimes less crappy)
  - The freedom to run the program, for any purpose (freedom 0)
  - The freedom to study how the program works, and adapt it to your needs (freedom 1). access to source code...
  - The freedom to redistribute copies (freedom 2)
  - The freedom to improve the program, and release the improvements to the public (freedom 3)

Notorious Example

- Unsecure and crappy software engineering
  - wu-ftpd
  - sendmail
  - ircII
- Good security engineering
  - Postfix
  - OpenBGPD
- a lot of free software between the two extreme groups

hack.lu - Netflow and Free Software

- Netflow is Cisco proprietary (but open) protocol to export network flows from routers
- A lot of Netflow collectors are free software (based on the available specification from Cisco)
- During hack.lu 2006, Nfsen/Nfdump (a free software developed by SWITCH) was demonstrated
- Various possible enhancement were discussed during the conference including extension of the protocol by Cisco
- **Free software as reference software implementation of a standard**

hack.lu - Wireless Security

- Wireless standard (802.11) is used everywhere
- Around 3 presentations about Wireless Security at hack.lu 2006
  - 802.11 Security (some nice example on how to gain access in a hotspot environment)
  - WiFi Advanced Stealh (how to implement a "proprietary" protocol over 802.11 bands)
- **Free software is used as toolbox** to discover/use (and fix) the security vulnerabilities in 802.11
- The madwifi-ng (free software) driver is giving new ways to use 802.11

hack.lu - Software Engineering and Security

- The topic of "writing/exploiting" vulnerabilities was well covered
- ... of course, **to better understand how the attackers are abusing** "our" crappy software
- Metasploit framework is a free software for developing, testing and using exploit code (a workshop took place)
- A nice library for crafting network packet was described and using some strategies to avoid most bug
  - The design was based on some other existing free software (sapy, Click router, conduit+)

hack.lu - Software Engineering Good Practices

- Wietse Venema made a presentation about Secure Programming Traps and Pitfalls
  - A simple software (a file shredder) was shown in order to demonstrate the difficulty of building secure sofware
- Postfix is one of the example in **software engineering for showing good practices**
- OpenBGP (a free software implementation of BGP (the protocol routing Internet)) was shown with a strong emphasis on its secure design
- Security is not very sexy... but the simplicity plays an important role in the security of a software

Conclusion ?

- Free software adds some advantages over proprietary software on the security side
- But only a small subset of free software is using the advantages...
- Free software is a nice playground for security engineer, hackers, ...
- A role of leader for showing the security engineering principle
- Triggering proprietary software to better follow good practises (e.g. standards)
- Free software is an important learning tool (and not only security)

Q and A

- Thanks for listening.
- http://www.csrrt.org/ - http://www.hack.lu/
- http://www.hack.lu/index.php/Archive - for all the presentations, papers and alike
- adulau@foo.be