Security Workshop

Dr. Carl Pulley
c.j.pulley@hud.ac.uk

Wednesday, 29 September 2010

Reference: Chapter 1 of Security Power Tools (see reading list).
UK Statute Law is available online at http://www.statutelaw.gov.uk.
Judgments from the Civil and Criminal Divisions of the Court of Appeal, and from the Administrative Court are available online at http://www.bailii.org (not all high court judgements are available online).

Computer Access

- Law has an expansive view of computer access
  - based on the physical exchange of electrons and the uses of CPU cycles
  - **all** networked computer use is access
- Dividing line is between legal/illegal access
  - does the user have permission or authorisation?

Adequate Authorisation

- Access without permission is improper and so should be illegal
- Law attempts to distinguish between
  - situations where user can assume permissions
  - situations where otherwise accessible files should remain off limits

Example: Active Defence

- Network being hit by an army of zombie machines infected with Code-red
- You have software to stop the attack
  - infiltrate infected machines and patch them to stop the attack
- Is this type of *active defence* legal?

Example: Active Defence

- You would intentionally be using the active defence software against zombie machines
- Code placed without owners permission
- When system is altered, its integrity is implicated (and so damage may occur)
- Basis of legal case against you!
- Is your behaviour ethical?

Example: Poor Ethics

- ISP website is tested for a path navigation vulnerability
- Website allows you to access the encrypted password file
- Technically, the crime has now occurred!
  - good chance though that they'll be no forthcoming prosecution

Example: Poor Ethics

- What if you now crack the passwords?
  - this act itself is not illegal
- What if you now distribute your findings publicly?
  - again, not illegal
- Highly probable that ISP and legal authorities would not like these acts
  - you would be judged as out to harm ISP

Example: Good Ethics

- A law court has a wireless network
- You demonstrate to the court clerk that it is readily accessible to hackers
- No demonstrable intention to cause damage
  - intention to improve court's wireless security

The Lesson

- Perceived *ethics* of the individual affect whether they will be charged and convicted
- Do **not** act to *intentionally* harm the *interests* of the system owner, no matter how *insecure* the machine may be

Bottom Line

- Get permission first!
- Do research on your own machine
- Don't cause harm to a victim
- Report findings directly to system administrator or vendor
- Don't ask for money for your findings
- Don't report to people likely to misuse your findings!

Reverse Engineering

- Reading about a program
- Observing the program in operation by using it on a computer
- Performing a static examination of the individual instructions within the program
- Performing a dynamic examination of the individual instructions within the program

Software Copyright

- Copyright owner has *exclusive* rights to work
  - even when its sold or given away
  - right to reproduce and prepare derivatives
  - right to distribute copies
  - right to perform and display work publicly
- Reverse engineering *will* create infringing copies of a software program

Copyright Defences

- Owner of a copy is allowed to reproduce or adapt program if this is necessary for the program to be used in conjunction with a machine
  - only applies to owner seeking to adapt their copy

Copyright Defences

- Legitimate owner of program is allowed to make *fair use* of the program
- Reverse Engineering *can* be fair use
  - copies should be used for working out how program works and accessing ideas, facts and functional concepts within software
  - copies should be *intermediate* - can **not** use copyrighted code in your final product
  - need to own a *legitimate* copy of work

Trade Secrets

- Protection against theft or misuse of certain kinds of information
  - once public legitimately learns information, it can not be a trade secret!
- Generally, reverse engineering doesn't violate trade secret law
  - it is a fair and honest means of learning information

EULA and NDA

- Legal instruments that could be used to explicitly prohibit reverse engineering
  - could a fair use defence still be used by a reverse engineer?
  - are the terms: enforceable; breeched; copyright infringed; trade secrets misappropriated?

Example

- M.Lynn due to speak at Black Hat 2005 about vulnerabilities in Cisco routers
  - attacker could fully compromise routers
- Cisco didn't want presentation to go ahead
- Lynn's employee agreed to alter talk
- Night before speech, Lynn's material seized

Example

- Lynn quit his job and gave the talk anyway
  - the flaws so serious that he believed it was important to inform system administrators
  - simple software upgrade fixed issue
- Alleged copyright infringement, trade secret disclosure and breech of employer contract
- Lynn disclosed enough data to show flaw existence but not how to exploit it
  - ie. ethical behaviour