Trends in Licensing of Security Tools

Chuck Willis
chuck@securityfoundry.com

DefCon 13
July 2005

Most recent slides available at:
http://www.securityfoundry.com/

Purpose

- Discuss license trends and how they affect the security community
- Discuss how licensing can be improved (if necessary)
- Educate security tool users about license requirements to avoid infringements

*** This session should be interactive ***

Disclaimers

- I will mention specific tools later that have various license restrictions
  - This is not meant to be a critique of that tool or its author(s)
  - I believe that all of the authors of the security tools mentioned have done a service to the community by releasing the tools
- This session is not a substitute for reading tool license agreements

About Me

- I do not work for a commercial consulting or software company
- I am not a Free Software zealot
- I am not a lawyer, this is not legal advice

About Me

- I think I am a typical security tool user:
  - I use Linux and Windows primarily, occasionally other Unix variants
  - I am not an expert programmer or developer
  - I compile tools (on Unix and Windows)
  - I debug compilation issues, including issues in porting to a different platform
  - I build small tools and scripts to automate tasks
  - I modify tools to better suit my needs
  - I share tools and tool modifications with others

Motivation

- I use a lot of security tools
- I read the licenses
- I have been surprised by some of the licenses
- Over the years, I have noticed some trends in the licenses of tools

Example

License for Wikto:
http://www.sensepost.com/research/wikto/

```
Copyright (C) 2004,2005 SensePost Research

This program is free software; you can
redistribute it and/or modify it under the terms
of the GNU General Public License

(...)

Additionally, should you find this software
useful you should buy a drink of their choice to
the contributors, if you bump into them at a
conference, but of course…nobody ever reads this
fine print.
```

Scope

- This session will cover tools that can be obtained and used without cost for at least some purposes, but:
    - Not strictly commercial tools
    - Not Open Source tools (OSI Certified license)
- This session will consider running and redistributing the (perhaps modified) tool
- This session does not consider selling someone else's tool or a derived work (most licenses restrict this)

Open Source Tools

- There are a lot of great security tools released under an OSI Certified license:
  - NMap: http://www.insecure.org/
  - Ethereal: http://www.ethereal.com/
  - Metasploit Framework: http://www.metasploit.com/
  - Sleuthkit and Autopsy: http://www.sleuthkit.org/
  - WebScarab: http://www.owasp.org/software/webscarab.html
  - Paros Web Proxy: http://www.parosproxy.org/
  - Kismet: http://www.kismetwireless.net/
  - Hping: http://www.hping.org/
  - Nikto: http://www.cirt.net/code/nikto.shtml
  - Many, many others

Licensing Trends I Have Noticed

(feel free to disagree)

More tools require payment or permission for some uses

- Some are free of cost for some uses, but do not indicate price or payment method for other uses
- Examples:
  - THC-RUT: http://www.thc.org/thc-rut/
  - Foundstone Tools: http://www.foundstone.com/resources/freetools.htm
  - Registered plugins for Nessus: http://www.nessus.org/plugins/
  - VRT Certified Rules for Snort: http://www.snort.org/rules/
  - HTTPrint: http://net-square.com/httprint/

More tools restrict redistribution

- Users can only get the tool from the author
- What if author is no longer available?
- Examples:
  - Sysinternals Tools: http://www.sysinternals.com/
  - Netstumbler: http://www.netstumbler.com/
  - Foundstone Tools
  - Registered plugins for Nessus
  - VRT Certified rules for Snort

More tools prohibit modification and reverse engineering

- Denies users the ability to customize tool and fix bugs themselves
- Examples:
  - Cain and Abel: http://www.oxid.it/cain.html
  - Foundstone Tools
  - Registered plugins for Nessus
  - Netstumbler

More tools are distributed without source code

- Not a license issue, strictly speaking, but lack of source code prevents easy modifications, improvements, and bug fixes by users
- Source code is valuable for users and others to look at and learn from
- Source code is necessary if users wish to port tool to another platform
- Tools that do not include source code often run on Windows only

More tools are distributed without source code

- Examples:
  - Achilles: http://www.mavensecurity.com/achilles
  - Brutus: http://www.hoobie.net/brutus/
  - Sam Spade for Windows: http://www.samspade.org/ssw/
  - Odysseus: http://www.wastelands.gen.nz/odysseus/
  - Netstumbler
  - Cain and Abel
  - Foundstone Tools

Some tools require credit in consulting reports

- Examples:
  - THC-Hydra: http://thc.org/thc-hydra/
  - THC-Amap: http://thc.org/thc-amap/

From THC-Amap's License:

```
... 4. If this tool is used while providing a
commercial service (e.g. as part of a penetration
test) the report has to state the tools name and
version, and additionally the author (van Hauser
and Dj RevMoon) and the distribution homepage
(http://www.thc.org) ...
```

Some tools and authors are inconsistent in their license

- Sometimes the license on the tool’s Web site is different from the license that comes with the tool
- Example: THC-Hydra and THC-Amap both ship with slightly different licenses from what is on their web sites

Some tools and authors are inconsistent in their license

- Sometimes the author contradicts a tool's license
- Examples:
  - Foundstone's HacmeBooks and HacmeBank
    - License states they are for “personal and non-commercial use”
    - Emails with authors indicate commercial use on an internal lab is acceptable
  - Registered plugins for Nessus
    - License prevents reverse engineering or modifying plugins
    - Mailing list posts state that modifying the plugins and posting changes to the mailing list is acceptable

Many tools lack a clearly defined license

- The license may be in the tool distribution, just hard to find
- The license may not be present at all
- The license may be incomplete, it may not address some issues and uses
- The tool may be a small exploit, script, or patch that is posted in an online forum without a license specified

Many tools lack a clearly defined license

- Examples:
  - enum: http://www.bindview.com/Services/RAZOR/Utilities/Windows/enum_readme.cfm
  - Hobbit's original netcat: http://packetstormsecurity.org/UNIX/utilities/nc110.tgz
  - John the Ripper: http://www.openwall.com/john/
    - Solar Designer is aware of the issue with version 1.6
    - Version 1.7 will be released under the GPL
  - SQLSecurity.com Free Tools: http://sqlsecurity.com/DesktopDefault.aspx?tabid=26

Many tools lack a clearly defined license

- More Examples:
  - Brutus
  - Odysseus
  - Achilles
  - Almost all mailing list, bulletin board, and newsgroup postings
  - Almost all exploits
  - Many more...

Discussion:

Do you agree that these trends exist?

Discussion:

Overall, is the current state of security tool licensing good or bad?

Discussion:

What would you do to improve it?

My Suggestions

(feel free to disagree)

Tool Users

- Read and follow tool licenses
- Don't use the tool if you don't like or cannot follow the license
- Politely work with tool writers to clarify any ambiguous or lacking licenses
- Don't use legal trickery to follow the letter of the license and violate the spirit of the license

Tool Writers

- Follow the license for any other software that you incorporate into your tool
- Choose a license or licenses and include them with every tool
- Remember: you are the copyright holder, you can add an additional license to the same tool or a derivative work at any time

Tool Writers

- Avoid over-licensing. Do not use an overly restrictive license for a relatively simple tool.
- Say what you mean in the license and mean what you say. Do not restrict something in the license and then tell people in other ways that it is acceptable.
- If the tool is meant to be “Open Source”, use a standard, OSI Certified license instead of making up your own (http://opensource.org/)

Tool Writers

- If payment is required for selected uses:
  - Make the cost reasonable and easy to find
  - Make finding and following purchasing instructions easy for the users
  - Specify what upgrades (if any) are included in purchase price
  - Specify what support (if any) is included in the purchase price
  - Consider offering bundles of programs (possibly from other authors) in one purchase to ease administrative burden on users

Tool Writers

- If payment is required for selected uses:
  - Clearly define those uses, considering:
    - Commercial Users
      - Testing and development use
      - Internal company use
      - External and consulting use
    - Educational Institutions (K-12, College, Universities; Private and Public)
    - Government Entities (Local, State, National)
    - Charitable Organizations
    - Other Non-Profit Entities
    - Home Users

Tool Writers

- If you wish to restrict redistribution of the tool, I recommend against disallowing it entirely:
  - Allow users to redistribute directly to other users or potential users
  - Allow anyone to distribute the tool widely in the event that the tool is no longer available from the original source

Tool Writers

- Make source code available and allow:
  - Modification for internal use so users can easily and legally address simple bugs, porting issues, and tool improvements themselves
  - Users to distribute modifications to one another
- Ensure that the source code is complete, including build files and any modified libraries
- Include at least a short description of how to build the tool

Tool Writers

- Make tool license clear and consistent:
  - Post license on the Web site, accessible before downloading the tool
  - Including a summary of the license on any release notices or news items
  - Include the license in the tool distribution, in a file named “COPYING”, “LICENSE”, or similar
  - Include the license or a summary of the license in the tool's online help
  - Summarize the license when presenting the tool at conferences and similar events

Conference and Training Organizers

- Consider requiring that tools presented be made available to conference attendees free of cost for all purposes
- Ensure that presenters make license clear for tools presented
- Ensure licenses are clearly indicated for tools provided to attendees
- Ensure that tool licenses are not violated if tools are included with conference materials

Online Forum Administrators

- Decide on a “default” license for scripts and code posted
- I recommend making postings fall under the MIT license or a BSD-style license
- Patches to existing tools should be by default, dual-licensed under:
  - Forum's default license
  - Existing tool's license

Online Forum Administrators

- Decide if posting under a different license will be allowed. In particular, postings under a license that restricts redistribution may cause problems with mailing list archives.
- Make clear to current members and to new members the forum's license policy. Include such information in any FAQ or Web site for the forum.

Conclusions, Comments, and Questions

Trends in Licensing of Security Tools

Chuck Willis
chuck@securityfoundry.com

DefCon 13
July 2005

Most recent slides available at:
http://www.securityfoundry.com/