Criminalising Hacking Tools

Peter Sommer

Summary

Making the sale, possession and distribution of the tools of hacking a criminal offence has obvious attractions. But many such tools are dual use and new laws run the risk of significantly inhibiting the activities of investigators, incident responders, penetration testers and academics. Recent UK attempts at framing such a law are discussed in order to show the broader problems of policy and wording.

It is one of the most frequently reproduced graphs in information system security. The horizontal axis is a time line; the vertical axis is marked from "low" to "high". There are two trawls. The first, starting "low" in the 1980s and increasing to "high" as we move forward in time is marked "Sophistication of Attacker Tools". the second starts "high" and decreases to "low" over time and is marked "Required Knowledge of Attackers".

The graph first appeared (I think) in a GAO Report in May 1996[1] and took the story in terms of hacking tools as far as sniffers, packet spoofing and tools with GUIs. Today the tools would include virus generators, DNS polluters, botnet control tools as well as versions of older tools which are now much more sophisticated.

It is not surprising that there should have been demands to criminalize hacking tools – production, sale, even possession.

These demands were reflected in the 2001 Council of Europe Cybercrime Treaty[2]

The difficulty is that many hacking tools are indistinguishable from utilities that are essential for the maintenance and security of computers and networks. Eleven years ago, in April 1995, Dan Farmer and Wietze Venema released a program called *Security Administrator Tool for Analyzing Networks,* which resolves for better or worse to the acronym SATAN. It was designed to automate the process of testing systems for security vulnerabilities. Written largely in perl it adopted the then relatively novel technique of using a web browser as an interface. In essence it was a rule-based engine backed by a database of vulnerabilities. As well as reporting the presence of vulnerabilities, SATAN also gathered large amounts of general network information, such as which hosts are connected to subnets, what types of machines they are and which services they offer.

As soon as it was announced, critics rushed in to complain that although not intended as such, it was in essence a series of gifts to hackers. Farmer and Venema went on to write the Coroner's Toolkit, a series of Unix-based forensics utilities. They are also

[1] GAO/AIMD-96-84 Defense Information Security

[2] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm Despite its name has been signed up to by such countries as the USA, Canada, South Africa and Japan. As of March 2006 twelve signatories had ratified but there are a further 30 nations who has signed the convention but not ratified

the authors of the book *Forensic Discovery.* [3] SATAN and another similar automated testing tool, ISS (which for some reason never attracted the same level of ire from security professionals) , soon started to turn up on the hacker bulletin boards, IRC channels and indeed on the hard-disks of hackers who had been raided by the authorities. ISS in an early form, for example, was used by the UK hacker "DataStream Cowboy" in his attacks on sensitive US military sites in March 1994.[4]

If we look at the range of security and hacking tools available at the moment we can see the extent of the problem of "dual use":

Class of Tool	**Legitimate and Illegitimate Uses**
Automated Penetration Testing	Modern ICT systems are too complex and too subjected to constant change for the traditional "specify and verify" approach to the selection of security measures. Regular penetration testing is an essential additional element in providing security. Having reached that decision it makes sense to create automated tools. The typical penetration testing tool consists in the first instance of a series of probes to get an operating system or application to disclose information about themselves. The tool also has a database of weaknesses, so that subsequent probes are designed to establish whether the weaknesses have been patched. In the hands of a penetration tester, the outcome is simply a technical report with recommendations. The identical tool used by a malicious hacker identifies routes to unauthorised access.
Website Load Capacity Testing	The owners of large websites need server resources sufficient to meet given levels of customer demand – or run the risk of complaints. They use tools to assist them. The same tool can be used to cause a Denial of Service
Password Cracking; Decryption Tools	Many modern password-based access control systems are designed so that the system administrator does not have direct access to the list of passwords for his users. Many individuals use stand-alone encryption to protect their sensitive files. In those circumstances there is a legitimate requirement for tools that can crack passwords. The same tools can be used to gain unauthorised access to a computer or to

[3] Addison-Wesley, 2004, ISBN 0-201-63497-X

[4] The matter came to trial in the UK in 1997; the author was the expert witness hired by DataStream Cowboy's lawyers to help them understand the evidence.

Class of Tool	Legitimate and Illegitimate Uses
	protected files
Remote Administration	Organisations have “help” desks run by IT specialists to help other staff with their computer problems; in some organisations one individual may be running a number of separate computer systems. In both of these situations software which allows an operator to “run” a computer remotely, to the point of having an exact replica of the screen of the remote machine on his local computer, is extremely helpful. Yet in essence such software is little different from classic Trojan software, the only distinguishing feature being that the existence of the Trojan is kept hidden. Trojan software enables a hacker to carry out actions in the name of remote 3rd party
Network Monitoring / IP Filtering	These tools are legitimately used to check quality of service / locate faults in networks. They can be an important legitimate tool in identifying and locating abuse. But they can also be used, unaltered, for unauthorised eavesdropping on networks, including the acquisition of usernames and passwords
Code Disassemblers	The role of a code disassembler is to convert machine code into a form in which it can be read by an analyst or programmer. Machine code is programming instructions as best understood by a computer but is of itself usually impossible for a human to read. Code disassemblers are important in legitimate reverse engineering and in fault-finding. But reverse engineering can also be used to break intellectual property rights and to subvert the original intentions of a device designer
Rootkits / Rootkit Revealers	A rootkit is a set of tools which are intended to conceal processes running on a computer. Rootkits are frequently used to provide covert remote control of a computer. They can also be used to support Digital Rights Management, famously in the case of Sony’s attempt to prevent copying of audio CDs. [5] Rootkit revealers are essential tools to detect hidden malicious activity on computer systems
Hardware: PIC	PICs are a class of devices which are

[5] http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

Class of Tool	Legitimate and Illegitimate Uses
Programmers	essentially miniature computers, program instructions and limited memory, all on one chip. They are used for process control, as in many sophisticated domestic devices, machine tools, security systems, lifts etc. Systems designers need to be able to create new programs and do so using external computer programs (on a PC) and a burner which imprints the instructions on a chip which can then be installed on a printer circuit board. But PICs are also used to subvert legitimate devices such as cable tv decoders, dvd players, games machines

There are of course a number of hacking tools which are non dual-use and these might include:

- virus creation kits
- phishing kits
- DDOS kits
- email bombers
- Botnet management tools

Sometimes the intentions of a "remote administrator" tool may be inferred from its name, graphic appearance and the facilities actually offered. What is one to conclude about Hack 'a'Tack [6], for example? Here are its advertised features:

FTP
Transmit IP:
IP-Scanner
General Information i.e. Current User, Country, Time, OS and CPU.
Send Messages:
Open/Close the CDROM
Hide/Show the taskbar
Disable/enable the monitor
Disable keys
Swap and click mouse buttons
Set/freeze the cursor at a position you can adjust by coordinates.
Window Events allowing you to kill, focus, hide, show and rename a process.
You can also see what the remote computer has in its clipboard and send text to the actually focused window. (also in intervals)
Boot Operations i.e. shut down, reboot, poweroff and logoff the remote computer here.
Get Passwords
Keyspy
Filemanager
Make Screenshot

[6] http://www.xploiter.com/security/hackattack.html

Hack 'a'Tack, it must be said, doesn’t normally show an obvious presence, in the form of an icon or tray item, on a target computer but operates stealthily.

The problem in designing an appropriate law is to separate the sincere from the insincere. Criminal law requires clarity, not generalised ambitions; a court – a judge or a jury – needs to know what tests to apply; investigators need to know what evidence to assemble.

This is how clause 6 of the EU CyberCrime Treaty tackles the matter:

> 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
>
> > a the production, sale, procurement for use, import, distribution or otherwise making available of:
> >
> > > i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
> > >
> > > ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
> >
> > b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
>
> 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
>
> 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Articles 2 through 5 of the Convention deal with, respectively: illegal access, illegal interception, data interference and system interference. The Convention requires signatories to ensure that their local laws cover these aims, albeit within the framework of the local criminal justice system. Where individual countries do not already have adequate legislation they are expected to create new laws.

The trouble with this wording, it might be argued, is that it provides too wide a set of loopholes. A prosecutor would need to be able to show that a tool was “designed or adapted **primarily** for the purpose of committing any of the offences…” This might include Hack 'a'Tack, the graphic interface of which is much more “informal and jokey” than is usual for professional utilities. Possession would only be an offence "with intent that it be used for the purpose of committing any of the offences", again a high threshold for a prosecutor to have to achieve. The many websites which host hacking tools but which announce, tongue-in-cheek, that the aim was "for educational purposes" only, would probably be able to continue distribution without much fear.

Contrast this with how the UK has been trying to implement the legislation. It appears as proposed section 35 of the Police and Justice Bill 2006[7]. The Bill itself covers a wide range of "criminal justice" matters. Section 33 increases the penalties for offences under the Computer Misuse Act 1990, while section 34 is an uncontroversial implementation of Article 5 of the CyberCrime Treaty; "data interference". The main effect is to make an explicit offence of denial of service attacks – "unauthorised acts with intent to impair operation of computer".

But section 35 shows the difficulties. In its original form it read like this:

> 35 **Making, supplying or obtaining articles for use in computer misuse offences**
>
> After section 3 of the 1990 Act insert—
>
> 3A
>
> (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—
>
> > (a) knowing that it is designed or adapted for use in the course of or in connection with an offence under section 1 or 3; or
> >
> > (b) intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
>
> (2) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
>
> (3) In this section "article" includes any program or data held in electronic form.
>
> (4) A person guilty of an offence under this section shall be liable—
>
> > (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
> >
> > (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;
> >
> > (c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

There is no explicit defence of "legitimate use" and no unambiguous protection for system administrators and penetration testers. In the furore that followed, some critics pointed out that even those who offered popular Linux distributions were at risk of criminal charge because most of these contain utilities such as *tcpdump* and

[7] http://www.publications.parliament.uk/pa/cm200506/cmbills/119/06119.i-iv.html

*etherea*l, which can be used to monitor network traffic and, in that process capture passwords and other sensitive data which could be a precursor to a system compromise. This first draft of UK legislation had simply forgotten about the safeguards within the CyberCrime Convention.

The Liberal Party proposed an amendment[8]:

> 3A Making, supplying or obtaining articles for use in offence under section 1 or 3
>
> (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—
>
> (a) knowing that it is designed or adapted for use in the course of or in connection with an offence under section 1 or 3; **or**
>
> (b) intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

But this was felt to provide too high a test of knowledge or intent for a prosecutor to have to prove.

The governing Labour Party then offered:

> (b) believing that it is likely to be so used.

This wording is slightly better than the original but still potentially leaves tool writers and distributors exposed. What happens, for example, if you prepare a tool for the sincere purpose of testing system security but you become aware that it is being used by hackers? Do you then need to stop distribution? Or do you need to interrogate each customer (that is, if you actually charge for the item as opposed to making it available via open source?) Is the position different if you only sell to those whom you have vetted but you become aware that pirated or "cracked" versions have become available – do you have to increase the security on later versions, for example?

There is perhaps some comfort to be drawn from the expressions of intent for the legislation from the Parliamentary debate[9] and in UK legal practice the courts do sometimes go back to the official record (Hansard) when faced with problems of interpretation.

In the final analysis one must conclude that the noble aim of restricting the availability of hacking tools is not something that it is possible to resolve solely by finding an appropriate form of words. Prosecutorial policy decisions will have to be taken, balancing on the one hand the need to make more difficult casual attack on information systems against the need for tools to protect legitimate users. Where bad prosecution decisions have been made one pities the lay jury of ordinary citizens who may have to listen to opposing experts arguing about the extent of "dual use" of a particular tool and then having to infer what was going on in the mind of a system administrator, penetration tester, or software distributor.

[8] For what it is worth, on my advice

[9] http://www.publications.parliament.uk/pa/cm200506/cmstand/d/st060328/am/60328s02.htm

On behalf of the legitimate activities of system administrators and investigators, one would hope that the onus would be on a Prosecutor to show ill intent. Skilled forensic technicians have got used to using timelines of activity, web- email and other types of traffic to show the intent and state of mind of an accused. But these may not help in the present circumstances, where a defendant may find himself having to demonstrate an *absence* of knowledge that a utility was likely to be used by some-one to commit an offence.

Peter Sommer

Peter Sommer is Senior Research Fellow at the Information Systems Integrity Group at the London School of Economics. He has been providing expert testimony in the English courts for 20 years. His instructions have included cases of global hack attacks, large-scale software piracy, paedophiliac rings, high-value frauds and terrorism. He is Joint Lead Assessor for the Digital Evidence speciality at the UK's Council for the Registration of Forensic Practitioners.