Security Researcher Wanted

Dead

or

Alive

1 Everything in Moderation

I have always avoided extreme exercise. I have always avoided extreme discomfort - like camping, military service or opera. But most of all, I have always avoided extreme views – particularly those weird extreme views about the right to privacy, right to pursue your vocation and other rights associated with Big-Brother that some security experts get roped into.

The truth is I don't mind if people want to watch what I do on CCTV - That would mean watching me work my arse-off trying to correct the mistakes of someone who proves natural selection is a myth.

If you want to listen-in to what I say I think that's brilliant, it can only be a good thing. Nobody has to do so covertly; I'll go to any conference or venue. But if they must, so be it. Surely, It will raise the average knowledge/intelligence levels in the world.

And as long as people don't steal any money from me, people can look at my computer records. They will only learn what lots of people already know, that I am a highly skilled, over weight and under-appreciated bloke.

But I feel I have to speak up when Big Brother makes it harder to earn a living – its too bloody hard as it is. And recent amendments to the Computer Misuse Act does exactly that So here it is, I'm "Give-in it to the Man ".

2 The Computer Misuse Act 1990

This was the UKs' first attempt at criminalising naughtiness on computers. Fundamentally, it wasn't effective and didn't really act as a deterrent An extract from my Amazon Top 500 Security Text book " How to cheat at Managing Information Security" shown below outlines its coverage

> *The Computer Misuse Act 1990 creates three distinct criminal offences:*
>
> ***1.*** *Unauthorised access to computers including the illicit copying of software held in any computer. This carries a penalty of up to six months imprisonment or up to a £5000 fine and will be dealt with by magistrate. This covers hobby hacking and potentially penetration testing.*
> ***2.*** *Unauthorised access with intent to commit or facilitate commission of further offences (like Fraud or Theft), which covers more serious cases of hacking with a criminal intent. This has a penalty of up to five years imprisonment and an unlimited fine. As it is a serious offence it will be trialable (12 jolly good men)*
> ***3.*** *Unauthorised modification of computer material, which includes the intentional and unauthorised destruction of software or data; the circulation of "infected" materials on-line("virus").; and the unauthorised addition of a password to a data file ("crypto virus"). This offence also carries a penalty of up to five years imprisonment and an unlimited fine. It is also a serious offence so it will be trialable (12 jolly good men)*
>
> *This act has been the chief means of dealing with unauthorised access like hacking. However, it has been heavily criticised – I remember one of my old bosses giving lectures and stating that "you practically had to be standing over the offenders shoulder while he was doing it to get a conviction"*

But more than that, in typical Anglo-Saxon stupidity and laziness, we sighed, said ho-hum, clapped politely whatever politician it was that passed the act, shouting "good effort old chap" -- and left it for well over a decade.

Significant drawbacks of the original act include;

* Poor definitions
* Low fines compared to the damage that can be caused by an applicable offense
* Not addressing virus writers, only the guy that sends it out.
* Not addressing DDOS attacks.

My ex-boss's comments did have some validity but the real problem was the judiciary, all those lovely lawyers and judges could read the statutes well enough but had really no terms of reference on which to apply them. At that time most, judges still had assistants who had electric typewriters, rather than PC and Macs. To a lesser extent, the same was true of all the lawyers and the LEAs. This is an opinion formed from first hand experience from work as an expert witness on the "Cash for Rides" case.

3 The Computer Misuse Act (Ammended)

The misuse act has been very significantly changed not by a new act but by two further cover-all acts. The first, the Police and Justice Act 2006, made virtually any type of security research a criminal offence. The second (**the Serious Crime Act 2007**) watered down these draconian measures a little but it is clear to see how many types of security research could leave a successful researcher liable to imprisonment.

The new powers slipped into effect on Wednesday, 1 October 2008 with no fuss and little splash. Lets look at the act as is now, a task in itself as it has been made up as a series of deltas, and I'll show you why I'm vexed.

Computer misuse offences 1 & 2 have changed very little – for all intents and purposes, the only notable amendment is the punishment - the fines and term of imprisonment will increase.

The real "greater good" of the act has been added in offense-3. The previous offence "Unauthorised modification of computer material" has been replaced by a new offence "Unauthorised acts with intent to impair or with recklessness as to impairing, operation of a computer". This was put in place by Police and Justice Act 2006 and has only been modified slightly by the Serious Crime Act 2007,

3.1 The Good

3 (1) A person is guilty of an offence if
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer; or
(c) to impair the operation of any such program or the reliability of any such data;

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to
(a) any particular computer;
(b) any particular program or data; or
(c) a program or data of any particular kind.

(5) In this section
(a) a reference to doing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) 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 ten years or to a fine or to both

“So!”, you ask “Where’s the good in that,? looks like a load of lawyer weasel words to me!!” you say. And you’d be right Weasel Words indeed. But it does do what Lord Northesk tried many years before. It makes DOS and DDOS attacks a crime.

3(2) clearly is describing a DOS attack. A ***Denial of Service*** attacks or sometimes known ***as Disruption of Service*** attacks are launched by a bad guy with the intent of making that target computer unusable – typically by making it hang, loop or overwhelming the target by sending a flood of traffic.

And during the early Noughties (2000-2005) , the online gambling, banking and shopping industries were held to ransom with DDOS attacks and the attackers have not been heavily perused. Similarly, malevolent code writers have often escaped prosecution.

This act should change that.

3.2 The Bad and The Ugly

And this is why I am vexed. Look at clause 3A(1). A perfectly sensible clause that makes designing something destructive. Then look at 3A2.

Making, supplying or obtaining articles for use in offence under section 1 or 3

3A (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article 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 supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) 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.

(4) In this section "article" includes any program or data held in electronic form.

(5) 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.

If someone believes it could be used to commit an offense. Well when I wrote an exploit for my last Zero-day vulnerability, fatajack, I wrote it to highlight a known flaw and I published it to encourage manufacturers to correct the fix. I was doing what was industry standard practice. But it worked and I had freely distributed it - so it would be impossible to refute that *someone out there, across the millions that have access to the internet, could use it.* It is infact *likely* so I have committed a crime.

As a security expert, I have written and published dozens of stack-overflow, scanners and password cracks with intent of driving my point home – a security audit with key points including theoretical vulnerabilities will be ignored. But now when I do it I will be committing a crime.

Will it stop me – Hell No!