

[Full-Disclosure] Administrivia

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2002-08/0516.html>

From: Scott Francis (full-disclosure@lists.netsys.com)

Date: 08/16/02

From: full-disclosure@lists.netsys.com (Scott Francis)

Date: Fri, 16 Aug 2002 12:53:20 -0700

--yzvKDKJiLNESc64M

Content-Type: text/plain; charset=us-ascii

Content-Disposition: inline

Content-Transfer-Encoding: quoted-printable

(I finally feel like some productive discussion is going on, even if it's not directly related to security concerns per se. I should probably move this to a philosophical forum. Long discourse follows; please hit 'd' if you're not interested.)

On Fri, Aug 16, 2002 at 03:29:17AM -0500, sockz@email.com said:

[snip]

> *It was refreshing to read your email. I agree with you on many points and
> couldn't resist the urge to reply.*

thanks, this is what I'm trying to promote – discussion about problems and real action that can be taken, pros and cons.

> *ARE hackers. but like i said, this is just a minor point. the big part =
of
> the argument is that through public discussion of security issues you have
> morons leeching off the ideas of those with intelligence. people cease to
> work for themselves. taht and its just plain stupid to begin with. hack=
ers
> aren't after security. they're after security that can be compromised.*

I mostly agree with your statement, especially about people leeching off the work of others (Jeff Goldblum's line from 'Jurassic Park' comes to mind – "You stood on the shoulders of geniuses ..." unfortunately, I couldn't find it in the script archive online, and I can't remember from the movie well enough to quote verbatim.) However ... 'hackers aren't after security. they're after security that can be compromised' I disagree with. I know that is the motivation for some hackers. I consider myself to be a hacker, however, and I have motivations in addition to the lure of exploring systems and networks that aren't mine – it's the lure of learning, of creating and =

Full-Disclosure: [Full-Disclosure] Administrivia

of
discovering new things. None of which are necessarily tied to what might mo=
re
accurately be termed 'cracking'.

> > *would not have a problem keeping it there. My issue is, when exploits a=
nd
> > holes stay private, it means that a small group of individuals is able =
to do
> > some very nasty stuff to people that have no means of protecting themse=
lves.
> > Being on the receiving end of that kind of attack is frustrating and ca=
n be
> > rather scary at times.
>=20
> yes. but that's life, Scott. and in many ways, if you think about it, w=
e're
> all better off in a scenario like that.
> a) it restores the "knowledge =3D power" relationship -- forcing all the =
stupid
> people to stay stupid and not rise to fame on the shoulders of others.
> b) when an exploit is known to only a small covert group, it cannot be us=
ed
> by many other people. hence, fewer people are affected by that exploi=
t.*

A secret involving more than one person doesn't remain a secret very long. =
No
matter how small and covert the group, people (especially hackers) cannot
resist the temptation to brag about secret knowledge. This is how exploits
that start out as private knowledge to a small group make their way into the
hands of those with malicious intent, and eventually appear as tools for use
by the script kiddies.

I am currently of the opinion that restricting knowledge to those that
generate it will merely delay the inevitable. The knowledge _will_ get out,
and when it does, if there is no place for admins to look in order to prote=
ct
themselves, those with malice aforethought will cause harm with the
knowledge. As an admin, I don't like this scenario. I have the utmost respe=
ct
for the skills of those that find bugs and exploits; however, I also know
that there simply are not enough hours in the day for every admin out there
to personally audit every software package and OS under his/her control to
find the same bugs that the underground is finding.

I think Raschid hit it on the head when he proposed the teaching of ethics
alongside information and skills. Higher ethical standards among the
underground is, I believe, the key to making the model you proposed work,
without raping the general public and those of us responsible for protecting
various of them (admins).

Full-Disclosure: [Full-Disclosure] Administrivia

- > *c) the fewer internet security companies you have, the better. why? because*
- > *they are _companies_ and the fundamental focus of any company is profit.*
- > *while their core function may be security, it is the exploitation and*
- > *careful manipulation of that core function that is used for profit. HE=*
- NCE
- > *you have more capitalists trying to exploit the security fears and*
- > *inhibitions of people like e-business executives where it is UNECESSARY.*
- > *the entire security industry is HOLDING BACK e-business because it gene=*
- rates
- > *fear and paranoia in order to generate profit.*

agreed; when business entered the Net it ceased to be a cooperative, academic learning effort and became a money-making business model. This is the core of the problems we're seeing today in many sectors of the Net. I don't know if this can be undone, but my optimistic side clings to the notion that the people still have the power to beat back corporatism. As hippie or socialistic as it may sound, cooperative effort created the Net, and cooperative effort can recreate it and help it become what we want it to – a tool for connecting people and disseminating knowledge, rather than just another means of making a buck.

- > *so the part where one individual may suffer isn't of any great concern. =*
- you
- > *remove the security industry and you remove this 'desire for profit' that=*
- has

I think the root of the problem is much deeper than the security industry – after all, Microsoft (for instance) is a great example of a company that has hurt the public and purposefully done things that were morally wrong in order to make a profit. It's the corporate mentality that has taken over the Net that is the problem; the current state of the security industry is merely a symptom.

- > *managed to latch itself onto the minds of programmers. its not about pro=*
- fit.

While that's true, those programmers _do_ have to pay the rent, feed themselves and support their families. If they shouldn't do it by using their security skills to make money, what do you suggest instead? Writing new software for profit can be a good model, but it can also be terribly abused (MSFT, etc.).

- > *its about information. its about intelligence. to put a price on intellig=*
- ence
- > *is to devalue humanity.*

Full-Disclosure: [Full-Disclosure] Administrivia

And so we return, full circle, to the old manifesto – 'Information wants to be free.'

>> *I used to think the solution was full disclosure of all information – after*
>> *all, hackers used to have the motto "Information wants to be free", and =*
this
>> *was the motivation in days gone by. What I'm sensing now is that attitude has*
>> *been replaced by cynicism as hackers, working for the good of the community,*
>> *have had their work stolen by greedy corps.*
>=20
> *YES!!!! YES THAT IS EXACTLY RIGHT! And it has changed the psyche/mindset =*
of
> *those who used to call themselves 'hackers'. they have changed into profiteers*
> *who's only concern is public glory, money, and having their ego stroked. =*
greed

Some have that motivation. I think many more have simply found that skills that were once just something with which they pursued a hobby, can now pay the rent. Is it wrong to take such skills and try to support oneself? This is a difficult situation – how can a hacker use his/her skills to pay the bills, and yet not create a situation as seems to exist now, where the only motivation is money and fame, and the spirit of cooperation and learning has been crushed by the bottom line?

> *like that isn't human and it isn't smart. anyone who argues that its the*
> *challenge of uncovering an exploit that leads them to post information on*
> *something like bugtraq, is lying. its not the challenge that motivates them.*
> *its the public recognition that they're after... the recognition that they*
> *have *some* kind of intelligence capable of meeting that challenge.*

In the old phreaking days, information was generated by curious hackers and traded around in the underground. Some folks abused the info, but most of them were merely curious explorers, and those with a desire to keep on learning. When it was discovered that there was money to be made in the flow of this information, the modern security industry was born.

>> *So maybe the solution now is more along the lines of what Raschid said –*
>> *hackers banding together, closing ranks, keeping the info and techniques =*
and
>> *knowledge available, but available to the underground, and most importantly,*
>> *making sure ethics (along the lines of what Raschid said) are passed on.*
>>=20
>> *The idea that with great power comes great responsibility is one that I =*

think

>> *is missed sometimes, especially in newer hackers who are merely in a rush for*

>> *power or glory.*

>=20

> *this is perfectly true. and real power is not overt in its nature. real power*

> *is covert. it is hidden and unseen. if knowledge = 3D power then it stands to*

> *reason that those who give out their information give away their power. = what*

True. The tinfoil hat brigade would tell you that the real power in this world has been hidden and silent for centuries now, and that everything the common person associates with power is merely a sham.

> *you end up with is an immature society thats conditioned to dealing with = power*

> *by giving it away because they have no idea how to handle it responsibly.*

This is definitely a lesson of history – power that is not used will be taken

by someone who will use it.

> *furthermore you have power being given to those who wouldn't normally have*

> *knowledge of the vulnerability. and with that you have those morons out = there*

> *who are not able to handle the information in a responsible manner. THIN= K=20*

That is the crux of my dissonance on this subject – if information is made public, it's exploited by those after a buck. If it's kept private, it inevitably leaks to those in the underground who will use it irresponsibly. The only solution I have been able to come up with is Raschid's call to ethics.

> *ABOUT IT. if you were smart enough to discover a way to compromise a system*

> *in the first place, your first reaction isn't going to be as stupid as to = tell*

> *every script kiddie you see. nor are you going to go and exploit it without*

There are exceptions, of course. The lure of fame and ego can be very strong.

> > *Is there no room anymore for the original definition of the word? (referring*

> > *to ESR's jargon file entry) It looks like the definition being embraced = is*

> > *the criminal one (i.e. hacker being akin to a cracker, somebody who breeds*

aks

> > *into other machines, rather than a hacker being someone who creates things).*

>=20

> *[next bit is actually from the end but i put it here cuz its relevant]*

>=20

> > *The name 'hacker', until recently, did not mean somebody who breaks into*

> > *systems. Some would argue that the meaning you ascribe to it is what has*

> > *sullied its reputation; that the true meaning of hacker is more along t=*

he

> > *lines of the jargon file entry.*

> >=20

> > <http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html>

>=20

> *true. i dont refer to "crackers" as such. i did at one stage but really, =*

its

> *just a whitehat term that allows whitehats to call themselves hackers, and*

> *real hackers end up not being hackers at all. eric may be right in the*

> *origins of the word, but society changes. the word "gay" is a good exampl=*

e of

> *that. or "faggot". i mean if you look up the word "faggot" in the diction=*

ary

> *it gives you something completely different to the meaning we have for it*

> *today.*

Very good points. Language certainly does evolve; maybe I just wish that it hadn't evolved in this one area. I miss the hacker, in the traditional sense of J. Random Hacker. I think the spirit is still alive, but I don't know wh=

at

to call it now. 'Hacker' seems to have taken on a different meaning.

> *eric also suggests that a person isn't labelled a hacker unless someone*

> *else labels them a hacker. and i think thats kinda stupid. a person whos*

> *hacking activites are THAT known to a community (of any sort) isn't a*

> *hacker. they're an "imbecile". people exist outside of labels, Scott.*

In the sense of the current definition of 'hacker' I'd agree with you. In ESR's original definition, I tend to agree with him – a true hacker of the old skool tended to have skills that were recognized by his/her peers. I think that's what ESR was trying to say. Wrt labels, I also agree – in fact, I think labels can often cause more harm than benefit.

> *you could say someone is an accountant who occasionally dabbles in the art*

> *of magic. whether you see them as a mage or an accountant is beside the*

> *point. the point being that books are still balancing and you are still*

> *find them strangely charming. you could call them a janitor and still see*

> *the same effect.*

nod

Full-Disclosure: [Full-Disclosure] Administrivia

> > *The law has a tendency to condemn blackhats, to date. :) (Those that are
> > caught, anyway.)
> =20
> yep. but only stupid and irresponsible blackhats get caught.. those who =
dont*

get caught, or abuse knowledge in such a way as to create a situation where they can _be_ caught (i.e. if you're acting ethically, you have no fear of being caught, because you're not doing anything to be caught for. Obviously, this assumes a benevolent and uncorrupt legal/moral system, and such is not currently the case in most countries and governments.)

> *know how to handle their power... those who are looking for scene status =
or
> seek some other un-intellectual goal. and if you look at a lot of the po=
licy*

Ego has been the single biggest downfall of hackers/crackers in the history of the Net. Of course, ego has also been the motivation behind some great work, as Larry Wall noted ("The 3 great qualities of a programmer: laziness, impatience and hubris").

> *drawn up in the past few years to deal with blackhat hackers, you have to
> realise that it has come as a result of the security industry's grip of
> paranoia over luddites. and i can tell you that most of the policy makers=
(be*

Anti-virus vendors are a good example here. Viruses and worms were interesting when the idea first appeared, back in the day. They have _long_ since _stopped_ being a challenge. I'm pretty certain no serious hacker bothers with writing viruses anymore; the challenge just isn't there. It's old hat; there are even GUI virus creation tools these days (have been for a while, actually.) If there were not money to be made selling AV products, I very strongly suspect that the much-vaunted virus "threat" would simply disappear, because the financial motivation for protection relies on the existence of a threat in the first place. Remove the financial motivation, and unless the threat has a separate reason for existence, it will disappea=
r.

I would not at all be surprised to learn that various AV vendors are, directly or indirectly, keeping the threat alive in order to keep sales ali=
ve.

> *they politicians or beaurcrats) aren't all that computer savvy. when look=
ing
> for information they go to a security company and that company tells them=
to
> be scared. so even though they may learn as they go along, what they lear=
n is
> based on this notion of "the internet is scary, its not secure, and hacke=
rs
> are everywhere just waiting to pounce!".*

Full-Disclosure: [Full-Disclosure] Administrivia

Reminds me so much of the news media. When I first moved to LA from the midwest, I was amazed at the lack of serious news content on the local TV stations. It was like the tabloids, converted to video, and they were competing for the biggest shock value. The discovery was made long ago that sex (and shock) sells, and when news becomes a business venture, instead of a journalistic undertaking, I guess it's no surprise that real hard news is dropped in favor of whatever lurid fluff boosts ratings.

- > *a smart hacker will work in collusion with the government, just like your*
- > *media moguls work with politicians. or like law enforcement agencies work*
- > *with your ISP. like i said, real power is covert. and if you have that kind*
- > *of power its very hard for someone to take it away from you. because they*
- > *dont know you have it.*

Exactly. man, I feel myself growing more paranoid by the second.

> *Hope this made my previous posts a bit clearer.*

Very much so. Thanks for writing. I haven't had a good thought-provoking discussion, especially touching on ethics, since I left college. To the naysayers: while this thread may not technically fit the topic, I think in the long run it will be more valuable than discussion of the 37th javascript hole in MSIE this year, etc.

The Internet community contains some of the best minds on the planet. We can do great things when we work together; history has shown this, and financial motivation need not be present. The bulk of the Net, and the tools that make it run and that we use on it, came out of a spirit of cooperation between hackers. That spirit continues today, but sometimes it can be hard to see amongst all the dollar signs. Let's bring that back.

(Yes, I may be naive and optimistic – it doesn't mean I'm not right.)

```
--=20
--=3D Scott Francis || darkuncle (at) darkuncle (dot) net =3D-
  GPG key CB33CCA7 has been revoked; I am now 5537F527
    illum oportet crescere me autem minui
```

```
--yzvKDKJiLNESc64M
Content-Type: application/pgp-signature
Content-Disposition: inline
```

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (FreeBSD)
```

```
iD8DBQE9XVgwWaB7jFU39ScRApEQAJ99ThTky35+pYtjbj434webLvKj+wCffBOq
p6lw6BgG6AdQAbxBFoqf58c=
=mprd
-----END PGP SIGNATURE-----
```

--yzvKDKJiLNESc64M--