

Re: [OT] The PGP Signed Posts Farce

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2003-10/3822.html>

From: Peter T. Breuer (*ptb_at_it.uc3m.es*)

Date: 10/30/03

Date: Thu, 30 Oct 2003 22:40:03 GMT

Alan Connor <zzzzzz@xxx.yyy> wrote:

- > *On Thu, 30 Oct 2003 20:13:14 GMT, dkoleary@attbi.com <dkoleary@attbi.com> wrote:*
- > *What I've been saying, which you actually know perfectly well, is that*
- > *PGPsigs don't do anything real about preventing impersonation or*
- > *establishing a persons identity.*

Oh yes they do (strike "person", and replace with "virtual being").

- > *You see, I could easily get a PGPsig/key in any name I chose to put*
- > *in my headers up there. As could anyone.*

So? How would that affect us? If you choose to use that name and that key and keep it a secret, then we can all verify that it's the virtual entity with that key and name posting all the time, every time it does. End. You are happy, and we are happy.

If you wish to pass the key and the name to your friends, then you create a larger, multibody, virtual entity, by your own volition. That might make your imprimature worthless, or it might not. Some artists discovered this problem a long time ago – if they let other people sign works as them, they get more sales, but the value of each goes down, because people stop trusting in them. So sensible people who are interested in using their signature as a mark of identity don't pass it out. But nothing physically stops you passing your key out, any more than anything physically stops you passing out the password to your account, or the keys to your safe.

Normal people don't do that because it has the opposite effect to what they are interested in achieving – keeping a unique mark of identity.

If you pass out your key, then you allow somebody to sign posts with your imprimature, and "impersonate" you. If that is your aim, fine. Companies do this. Microsoft does it, for example. I have a departmental key! It is a normal mode of behaviour and marks a group identity. But ONE group identity.

So there you are – two alternative behaviours, both discussed, neither a problem to anyone, let alone us!

> *That's merely one of the reasons why PGPsig/keys are a waste of time.*

No, it's completely irrelevant.

> *Personally I think anyone that uses their real name on the Usenet is
> a fool.*

Oh, why? Perhaps you'd like to tell Linus Torvalds that? Or a whole host of people, including me!

> *Nor do I believe that someone with a PGPsig key, a website with family
> photos, and an address in a phonebook someplace, all with the same name,
> are necessarily who and where they say they are.*

And so what? Why should you care? What you DO know is that they have the key they claim to have. If they have that key for the purpose of identifying themselves, then they will keep it secret from others.

> *All of these things are easy as pie to create or acquire, as are ISP
> accounts under false names: They accept Money Orders.*

Good. All the more digital identities to authenticate then! Maybe they even pay using paypal!!! Good job they can identify themselves to paypal.

> *The Internet is the Land of Illusions, and anyone who thinks it will ever
> be anything else is a fool.*

Oh, the ironnnnnnnny.

> *Do you know where I am? Here's a clue: No one around me, from dawn until
> dark, can ever be heard speaking English.*

I know, I know, they're all moaning and screaming and jibbering.

> *Now take a look at my headers. Here's another clue: Earthlink doesn't
> offer any service within hundreds of miles (at least) of my location.*

Oh, it's you posting from earthlink, is it? I thought that was us. I thought you were the one posting from elsewhere.

> *And I am not even very good at this sort of thing.*

Fantastic. Next you are going to discover that IP addresses don't fix your geographic location, no?

They just fix your IP address. Surprise, surprise.

But then geographic location is useless for figuring out which IP address you are posting from.

comp.os.linux.misc: Re: [OT] The PGP Signed Posts Farce

Just as who you are on Earth is useless for helping us figure out which virtual being you are, and what its paypal accounts are, and how much money is in them, and what other virtual identities it has payed monies to in the past.

Going to "get it" soon, are we?

Peter