

Re: A repository changed its public key?

Source: <http://linux.derkeiler.com/Newsgroups/alt.os.linux.suse/2008-01/msg00934.html>

- *From:* houghi <houghi@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 24 Jan 2008 13:06:19 +0100
-

birre wrote:

Since we must trust the distributor of our system, I should prefer that they also update my system with the keys from the contributors they trust, so I don't fall in the trap to trust a key from some false contributor.

Somebody who is good now can be bad tomorrow. Such is trust. The question is how big the risk is.

I have not the skill to validate the keys, other then hope the site is intact and the key is real.

Indeed, but that does not mean that the key can be trusted. However the risks are minimal. At this moment the risk is more academic then real life.

Many users of linux is trained by the windows software where they learn to click on anything even if they have no chance to know what to answer.

I is very well trained to do the same thing in Linux. This has nothing to do with Linux or Windows. It has everything to do with human nature. It also can have something to do with liability, like the stoopid sticker on many apliences to warn you for idiotic things.

Like the antivirus program say they have virus, and are asked if they will remove it. (yes or no) , and they call me.
I ask them "what program ask that", and they say, "I don't know"
So, maybe it was the virus itself or the antivirus program, who know.

Or hitting [ENTER] after ``rm -rf b[tab]`` and then realizing that you are root AND in / and not a user in ~/tmp/. What I have done is put the `-rf` at the end of the command.

Re: A repository changed its public key?

Also there are other times in Linux that I ignored popups and warnings. I am now using Linux for several years, so I can not blame Windows for my behaviour anymore.

It must not be like this with keys, someone we trust must trust them first so we don't get fooled so easy.

That depends on what risks you are willing to take. As a homeuser or small business, there is no problem. However if you so desire, you can meet people in real life who can then sign keys. On FOSDEM there is such a keysigning each year.

As I do want to keep my internet name as much separated as my real life alter ego, I can not produce any papers confirming who I am, without making a link between the two.

That means you can NEVER completely trust me to be me, even when I give you my public key.

The problem with risk is that people can not understand what risk really is, even if you give them the numbers.

The risk of getting killed by a traffic accident is much, much higher than being killed in a terrorist attack. Yet the amount spent on one is much, much higher and has a much greater impact than on the other.

As long as we can not say that a risk is 0, people will use it to scare people into doing stupid things.

That all said, it is good that the GP asked the question. He was uncertain and sought confirmation. He did not panic with "OMG!!!! I AM HACKED!!!!" He just looked for confirmation in a situation that could be strange.

The first time I had such a thing happening was when I re-installed a machine and my ssh connections started to give errors.

houghi

—

Theologians can persuade themselves of anything. Anyone who can worship a trinity and insists that his religion is a monotheism can believe anything — just give him time to rationalize it.

Robert A. Heinlein, JOB: A Comedy of Justice

.