

Re: Question about rsync

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2008-03/msg00328.html>

- *From:* David Brown <david.brown@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 23 Mar 2008 14:34:25 +0100
-

Unruh wrote:

David Brown <david.brown@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> writes:

Unruh wrote:

Jack Snodgrass <jacks_temp_id_bf2142@xxxxxxxxxxx>
writes:

<snip>

If you use rsyncd, it's faster (non-ssh) and
you can do

It is faster because it is unencrypted. Not a great idea if you
are backing
up unless you do not care if everyone can read the stuff being
transferred.

Unencrypted transfers are only faster than encrypted ones if the bottleneck is
processor speed, rather than link speed (or if you are

No, unencrypted transfers are always faster but the speed difference is
negligible if the link is the slowest item.

Fair enough.

passing compressible data over a link that does transparent compression, such

Re: Question about rsync

as openvpn or ssh -C, since encrypted data is uncompressible). For many online backup operations, the link is the bottleneck, so encryption is free.

However, the idea of "always use encryption because everyone can read the data being transferred" is basically FUD in most cases. If you've got a backup running between two sites, then the data moves from the one server, through your switches and gateways on to your ISP, through the internet infrastructure, and back out at the other side. At what point is it realistic to think that an attacker would be listening in to this

"through your switches and gateways on to your ISP, through the internet infrastructure, and back out at the other side"

Again – at which point is it realistic to think an attacker will be listening here? Anyone with evil intent who has direct network access along this path has far more power than just sniffing rsync traffic – rsync sniffing is unlikely to be your major problem. Anyone looking for access to your files and who has this kind of physical access is probably going to find a faster and easier method.

The most important aspect of security is improving your weakest links – when you are at the stage that the easiest method(s) of attack is physical (such as stealing the servers), or personal (such as rubber hose cryptoanalysis), then your job as IT security is pretty much done (for now!). It makes sense to take easy steps to increase security if you can – an attacker might not have the same opinion about the easiest method(s) of attack as you. But if you can be confident that wire-tapping the network path between two computers is a minimal risk, then encrypting traffic along that path is not necessary.

traffic? It is *very* difficult to compromise the security of a decent ISP in order to sniff out traffic like that – hacking into the trunk internet exchanges would be even harder. Even if you managed it, with

It depends on who is doing the sniffing. "Reading passport applications" is even harder.

People will try harder to beat systems if the rewards are greater – obviously the effort you make into securing a system is determined by the worth of the data, and the likelihood of an attack.

rsync you only get bits of changed data – you'd need to monitor the line (capturing enormous quantities of data) for months to get anything sensible.

Re: Question about rsync

It is **vastly** easier for an attacker to use other methods

Nonsense. Any file you created today is sent out in its entirety.

I'm not sure on that – the information on the rsync website is not clear here, but it contains information about an algorithm aimed precisely at transferring only those parts of a file that have changed. Of course, for new files, that means the whole file.

In a great many cases, however, single files are of little use on their own. If you want to steal some software I've written, you'll get pretty bored waiting for all the files to be transferred via rsync as they are not all changed on a regular basis.

(bribe one of your IT staff, for example, or steal some login passwords) if they want to get your data. So unless you are doing a backup of a nuclear missile design, encryption on an rsync backup will only make a realistic difference if your network topology is such that the traffic is accessible by more people (such as the notorious "disgruntled employee").

Of course, since encryption here is free, it is still worth using even for its tiny real-world benefits. If nothing else, it keeps you in the habit for when it **does** matter.

Yes. Precisely.

Security is a process, and it starts with thinking about the situation, not with automatic rules that must always be applied at all times.

And as a process it should not be such that it needs to be thought about each time it is used. It should be robust, even to human forgetfulness. Making it a habit is part of that process.

I agree there – and it can make sense to make encryption of traffic a habit, and part of mandatory procedures. But I'm cautioning against complacency and lack of thought for the security needs of a given system – the idea that you **always** need strong encryption for any transfer can quickly lead to the mistake that strong encryption is all you ever need.

Re: Question about rsync