

Re: Secure backup on remote untrusted server over slow line?

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-06/0476.html>

From: Iwo Mergler (Iwo.mergler@soton.sc.philips.com)

Date: 06/12/02

Date: Wed, 12 Jun 2002 16:16:49 +0100

From: Iwo Mergler <Iwo.mergler@soton.sc.philips.com>

Preben Bohn wrote:

>

> *Hi all, I hope the subject says it all... :-)*

>

> *If not, here's my problem, I really hope someone can help me:*

>

> *I want to backup my linux server (~10GB data) on a remote server over a*

> *slow line (~200 kbps). I only need a snapshot at say 1 days interval.*

> *The changes to the server data are relatively small so an incremental*

> *scheme is the way to go (and with 10GB over 200 kbps it is the only way*

> *:)).*

>

> *The problem is that the remote server is "public" available, so I need*

> *to encrypt the data somehow. Does anyone have any good ideas to how I*

> *can accomplish this?*

>

> *My own ideas:*

> *1) Make a secure filesystem on my own server and rsync the filesystem*

> *file to the remote server. The problem with this approach is that*

> *according to <http://rsync.samba.org/fom-serve/cache/60.html> rsync*

> *requires at least 3*(the filesize)? free space on the remote server to*

> *do this, and I havn't got that much... Also it seems like a waste of*

> *processing power to encrypt the entire filesystem, when I only need to*

> *encrypt what I send to (and store on) the remote server... This leads me*

> *to option 2:*

>

> *2) Make a program myself that reads /dev/hdXX in blocks, encrypt the*

> *block, compare a checksum of this block to the corresponding checksum on*

> *the remote server's block, and transfer the local block if they are*

> *different. I'll probably face some problems with the disk changing while*

> *reading, and such...?*

>

If you do it blockwise, you can't have the filesystem mounted at the same time. All kind of amusing stuff can happen if your backup races with a metadata update.

comp.os.linux.security: Re: Secure backup on remote untrusted server over slow line?

Use a backup program to create a single file. Compress it, split off the header and keep it on the local machine. Encrypt the rest with something secure and send it.

If you want a reasonably simple, but safe encryption, you could generate a key from truly unpredictable data (record your local waterfall) which is as long as the file you want to send. XOR the data with it, bit by bit. Same for decryption. As long as nobody can get hold of the CD-ROM with the key, the code is virtually unbreakable.

On the other hand, you could write the backup to a CD-ROM in the first place. :^)

Kind regards,

Iwo

- *Next message:* [Wojtek Walczak: "Re: blackhole.pl / tcp 1190"](#)
- *Previous message:* [-alls-: "iptables: state & forward confusion"](#)
- *In reply to:* [Preben Bohn: "Secure backup on remote untrusted server over slow line?"](#)
- *Next in thread:* [Preben Bohn: "Re: Secure backup on remote untrusted server over slow line?"](#)
- *Reply:* [Preben Bohn: "Re: Secure backup on remote untrusted server over slow line?"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)