

## RE: Is SSH worth it??

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-10/0121.html>

---

**From:** Louis Erickson ([LErickson@ariba.com](mailto:LErickson@ariba.com))

**Date:** 10/09/02

From: Louis Erickson <[LErickson@ariba.com](mailto:LErickson@ariba.com)>

To: "'Andre Guimaraes'" <[Andre.Guimaraes@talli.ibest.com.br](mailto:Andre.Guimaraes@talli.ibest.com.br)>, Trevor Cushen <[Trevor.Cushen@sysnet](mailto:Trevor.Cushen@sysnet)>

Date: Wed, 9 Oct 2002 10:06:35 -0700

May I ask a question or two? See below...

> -----Original Message-----

> **From:** Andre Guimaraes [<mailto:Andre.Guimaraes@talli.ibest.com.br>]

> **Sent:** Tuesday, October 08, 2002 11:26 AM

> **To:** Trevor Cushen; [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

> **Subject:** RES: Is SSH worth it??

>

>

> *I dont like RSA without passwords caus if your machine gets*

> *compromised, the*

> *attacker would have root access to another machines in your network.*

Why would the attacker have root access to another machine in my network?

If I am using keys for the root account, then they would, but if I'm using a user account, I don't see where they would. Is there something I don't know?

> *When I needed automated scripting using ssh and scp I used*

> *this programming*

> *language called EXPECT, perl includes a module that*

> *implements the expect*

> *language. It goes something like this:*

>

> *exec ssh myhost "commands" (could be scp myfile myhost:path)*

> *expect yes/no*

> *send yes\r*

> *expect assword*

> *send my\_password*

>

> *Just to make the figure.*

So, how is having the text of your password stored in the Expect script better than having keys? As I see it, if they compromise the machine with this, they get the actual password. If they compromise the machine with keys, they get access to the other machine, but don't know the password.

## SecurityFocus BASICS: RE: Is SSH worth it??

Is there something I'm not understanding here?

I've used this same mechanism myself, and our security staff was quite unhappy with the solution, because it left the password in plain text in the Expect script.

They offered two ways around this, both of which we've used.

One way is when you boot your machine, it asks for the password, which you must key in. It is therefore not stored on disc. (It is in memory, but that's apparently a risk they could live with.)

The other – and the one I prefer – is to use a scheduled task/cron event as the trusted account to encrypt (gpg or whatever) the files, then to move them to a drop directory where an untrusted user account can read them. That untrusted account uses authorized keys to copy them via script, and then they can be stored on the other end, and decrypted if needed.

Both are more complex, but mean you don't have a password floating in a text file, or authorized keys for an important account.

---

- **Previous message:** [Hudak, Tyler: "RE: securing my new wireless router"](#)
- **Maybe in reply to:** [Trevor Cushen: "Is SSH worth it??"](#)
- **Next in thread:** [Godfrey, Tyler: "RE: Is SSH worth it??"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)