

EXHIBIT C

rec.games.netrek

Search this group

Search Groups

Help getting res-rsa working with server...

[Options](#)

☆ 2 messages - [Collapse all](#)

Dave Ahn [View profile](#)

[Hide options](#) Nov 15 1994, 2:50 pm

Newsgroups: **rec.games.netrek**
From: **ahn@wfu.edu (Dave Ahn)**
Date: **15 Nov 1994 02:22:21 GMT**
Local: **Mon, Nov 14 1994 9:22 pm**
Subject: **Help getting res-rsa working with server...**

[Reply to author](#) | [Forward](#) | [Print](#) | [Individual message](#) | [Show original](#) | [Report this message](#) | [Find messages by this author](#)

Hello,

I'm trying to build the vanilla bronco server from csuchico.edu with RSA support. I've been able to build the binaries (daemons, etc) without any problems, but I can't get the genkeys to create a set of keys for my server. I've tried compiling genkeys under several platforms (SunOS 4.1.3, Solaris 2.x, HP-SUX 9.04, Linux 1.1.62 w/gcc 2.5.8) but fails to generate a set of keys.

While I understand the necessities of RSA encryption between client and server, I don't seem to have very clear documentation on how it is implemented on the server side. From what I've been able to make out,

- (1) the server maintains a list of public keys which allows certain "blessed clients" to connect to the server and rejecting unblessed or expired clients.
- (2) the server (or rather an update daemon) downloads these public keys once a day to maintain an updated list at all times.
- (3) the server can have its own RSA keys from which the public key can be distributed to be included in a special "blessed" client (i.e. if I want to have a client with special features that take advantage of special features of the server)

Is this correct? If so, then if I do not want any specialized clients, I do not have to create a set of keys using genkeys, right?

I would appreciate any help and info you can give me.
Thanks,
Dave.

PS. Also, if I want to open up my server to the netrek community, is there any special procedure I need to follow?

--

Dave Ahn Internet: ahn@hbar.phy.wfu.edu, ahn@indigo2.medeng.wfu.edu

Discussions

[+ new post](#)

[About this group](#)

[Subscribe to this group](#)

This is a Usenet group - [learn more](#)

Sponsored Links

Only \$89/Year. 30 Day Money-Back Guarantee, 24/7 Support. Order Now!
www.HostMySite.com

[Public Key Certificates](#)
Contract With the DoD Via Digital Certification. Get Set Up In 48 Hours
www.IdenTrust.com

[\\$9 - SSL Certificates](#)
Issued in 3 minutes, trusted by all browsers, no paperwork required.
www.positiveSSL.com

Related Pages

[Redhat Security Update Fixes Samba "send_mailslot\(\)" Vulnerability](#)
FrSIRT - 10 hours ago
A vulnerability has been identified in various Redhat products, ...

[29.6 Installation](#)
wks.uts.ohio-state.edu

[Building and Installing the Distribution](#)
www.eecis.udel.edu

[BigAdmin - Submitted Tech Tip: Installing OpenSSH on the Solaris 8 ...](#)
This tip offers a list of resources with suggestions on how to ...
www.sun.com

"When you were born you cried, and the world rejoiced. Try to live your life so that when you die you will rejoice, and the world will cry." -1/2 jj^2

[Reply to author](#) [Forward](#)

Nick Trown [View profile](#)

[Hide options](#) Nov 18 1994, 11:15 am

Newsgroups: **rec.games.netrek**

From: **trown@ecst.csuchico.edu (Nick Trown)**

Date: **17 Nov 1994 16:36:47 GMT**

Local: **Thurs, Nov 17 1994 11:36 am**

Subject: **Re: Help getting res-rsa working with server...**

[Reply to author](#) | [Forward](#) | [Print](#) | [Individual message](#) | [Show original](#) | [Report this message](#) | [Find messages by this author](#)

In article <3a960t\$3kv@eis.wfunet.wfu.edu>, Dave Ahn <ahn@wfu.edu> wrote:
>Hello,

|
|I'm trying to build the vanilla bronco server from csuchico.edu with
|RSA support. I've been able to build the binaries (daemons, etc)
|without any problems, but I can't get the genkeys to create a set of
|keys for my server. I've tried compiling genkeys under several platforms
|(SunOS 4.1.3, Solaris 2.x, HP-SUX 9.04, Linux 1.1.62 w/gcc 2.5.8) but
|fails to generate a set of keys.

|While I understand the necessities of RSA encryption between client and
|server, I don't seem to have very clear documentation on how it is
|implemented on the server side. From what I've been able to make out,
|(1) the server maintains a list of public keys which allows certain
|"blessed clients" to connect to the server and rejecting unblessed
|or expired clients.
|(2) the server (or rather an update daemon) downloads these public keys
|once a day to maintain an updated list at all times.
|(3) the server can have its own RSA keys from which the public key can
|be distributed to be included in a special "blessed" client (i.e.
|if I want to have a client with special features that take advantage
|of special features of the server)

|Is this correct? If so, then if I do not want any specialized clients,
|I do not have to create a set of keys using genkeys, right?

Yes this is correct. If you don't want to have your own specialized clients
then simply run the updated program. This is described in (2). This will
contact the metaserver to download the keys. This is how most servers such
as wormhole, calvin, bigbang, rosebud, etc to it. It save the admin. alot
of work.

|
|I would appreciate any help and info you can give me.
|Thanks,
|Dave.

http://groups.google.com/group/rec.games.netrek/browse_frm/thread/4da4c5af59745a61/fde76eab98a25b8a

| PS. Also, if I want to open up my server to the netrek community, is there
| any special procedure I need to follow?

When you're ready to have your server put on the metaserver send me mail.

Nick

[Reply to author](#) [Forward](#)

End of messages

[« Back to Discussions](#)

[« Newer topic](#) [Older topic »](#)

[Create a group](#) - [Google Groups](#) - [Google Home](#) - [Terms of Service](#) - [Privacy Policy](#)

©2007 Google