OpenNebula - Bug #493
Weak secuirty model in OpenNebula

02/21/2011 04:07 AM - Carsten Friedrich

Status:	Closed	**Start date:**	02/21/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	worksforme	**Pull request:**	
Affected Versions:			

Description

I consider the current security and especially authentication model used in OpenNebula as weak as:

- All RPC requests are transmitted in plain text.
- Passwords are transmitted in plain text and stored in plain text in OpenNebula (I understand that they are hashed, but as this is done on the client side it only makes the password more complicated, it does not encrypt it. I.e. the password hash is basically a more complicated plain text password based on the original password.
- If external authentication schemes are used, e.g. LDAP, password are not even hashed. This also makes authentication code more complicated as the client needs to decide whether to hash the password based on the authentication scheme used (which it should not need to care about).

I think to fix these issues, OpenNebula needs to:

- Use secure RPC to encrypt all RPC traffic.
- Send passwords un-hashed over the encrypted RPC and have the server take care of hashing when it is needed.

Associated revisions

Revision 0b36571b - 09/28/2017 03:03 PM - Juan Jose Montiel Cano

B #5119: Removed vnet if user can not reserve (#493)

Revision 55908c1b - 09/28/2017 03:04 PM - Juan Jose Montiel Cano

B #5119: Removed vnet if user can not reserve (#493)

(cherry picked from commit 0b36571b23259e089764c05127d4288c9e69be3b)

History

#1 - 02/21/2011 10:03 AM - Ruben S. Montero

- Status changed from New to Closed

- Resolution set to worksforme

RPC calls can be easily tunneled through HTTPS proxy, so addressing all your concenrs

#2 - 02/21/2011 11:27 PM - Carsten Friedrich

HTTPS proxy can be used to address the first issue, the other two still remain:

- Passwords should not be stored in plain text by OpenNebula. A simple misconfiguration e.g. as happened in http://lists.opennebula.org/pipermail/users-opennebula.org/2011-February/004018.html will expose all passwords and allow any user to act as any other user. Storing plain password is just a bad idea from a security perspective if it can be avoided.

- Clients should not need to know what authentication scheme OpenNebula uses internally to decide whether to hash passwords or not.

#3 - 02/21/2011 11:47 PM - Ruben S. Montero

That is also address by the auth drivers, you can check for example the SSH module at http://www.opennebula.org/documentation:rel2.0:users