Conclusion

The paper present some of the security issue, challenge and solution of virtualization in the virtual machine. Technology is growing more complex every single day giving more room for vulnerability. Virtualization should be made in a way that the security is the main concern to the environment. As the security technology advance, we could be said the same to the hacker who adapting with new security technology. Virtualization in virtual machine environment should be designed in such a way that giving little or no chance at all to the attacker to exploit the vulnerability on a virtual machine.

Virtualization brings a lack of added security to the environment. The key issue of the virtual machine is the fact that virtual machine represents the logical instance of an underlying system [1]. There are many virtualization technologies available on the market which some of them are open source and free and some of them we have to pay to use the technology underlying different security approach on the virtual machine.

Most of the security issue presented here are related to the hypervisor and the host. If the host and the hypervisor are compromised the attacker can gain sensitive information from a user and the security approach from the respective virtual machine is irrational. To solve the security issue, a user must aware of new security patches from vendor to avoid the risk of hypervisor being compromised.

Virtualization is the best solution to cut down operational cost in today's computing but if we neglected the security issue it will posing risk to the environment.

Reference

[1] <http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf>