Abstract

Software Defined Network is developed by the demand of large business organization. Software Defined Network (SDN) is a new network architecture that provides central control over the network. SDN achieve the centralized control by separating the network control from forwarding and is directly programmable. In SDN there is a controller which controls the entire network. The main benefit of SDN is the centralized control and network control programmability. central control is the major advantage of SDN but it leads to central point of failure. The programmability of network control leads to another vulnerabilities. However, before any large scale deployments, it is important to understand security issues arising from this new technology. This survey paper deal with SDN security issues and 9 security mechanism.

References

3. Seugwon Shin, Phillip Porras, Vinod Yeegneswaran, Martin Fong, GuoFeiGu, Mabry Tyson: “FRESCO: Modular Composable Security Services for Software-Defined Networks”, February 2013

Index Terms

Computer Science Security

Keywords

Software Defined Networking, DoS Attack, OpenFlow