

# Launching into Cyber Security June 2022



Search forums


## Collaborative Learning Discussion 2

### Summary Post

 [Settings](#) ▼

[◀ Initial post](#)

Display replies in nested form



Summary Post

by [Nomusa Majola](#) - Monday, 8 August 2022, 11:43 PM

Introduction

Securing networks are very challenging considering that operation, maintenance, and security is very reliant on low level end user configuration and involves the vulnerability of the end user's infrastructure. Software defined networks specifically are radically agile and dynamically evolving but the rigidity of the underlying infrastructure means it's almost impossible to innovate and improve at the same pace. Unfortunately, mechanism for automatic and simultaneous responsiveness are not readily available.

Key issues and solutions

There are numerous threats encountered, predominantly being data leaks, malicious data manipulation, DDOS and unauthorised access. For purposes of this discussion, I will unpack some strategies or solutions employed by security professionals to build defences, identify threats and also secure software defined networks.

Separating the data and the control plane allows for a centralised software program to control the entire network. This is where integrating cloud computing and Software defined networks becomes key. This also allows entities to reduce capital expenditure as the burden to secure shared and becomes the responsibility of the cloud computing provider and the vendor. As cloud computing becomes the standard form of data storage, it is important for security frameworks to be entrenched in the organisation security and risks regularly monitored as regulation transparency of third party software is not always forthcoming (Anderson, 2019). Integration of these two technologies enhances the manageability of controlling the underlying network structure by allowing programming to be done on the cloud. This does come with its own set of problems which are overcome with encryption prior to storage in a cloud and key based authentication.

Protocol attacks are often able to bypass firewalls especially if they are not properly configured. Running penetration tests on a regular basis will enhance the security strategy by enabling the business to identify weaknesses in their network before attackers can. Although Next Generation Firewalls are costly and process intensive, they do incorporate more advanced security functions

Relying on multiple distributed servers which are housed in different areas reduces the risk of total access restrictions. This also allows remote servers to act as backup and pick up traffic until the system is restored. This does come with challenges as there is restricted servers, slower response times and ultimately increased cost.

Key based authentication uses both public and private keys factors to confirm the identity of the user.

Users are provided with asymmetric keys which are stored in the system they are accessing while the private keys are only maintained on the specific device the user connects with. Similarly security tokens are programmed with information that authenticates the user. Since they are a physical device they are plugged into the system to allow the user to gain access to the specified network as normally seen in the banking sector. Solutions like 2 factor authorisation are cumbersome and end users tend to not always use them

Conclusion

There are a number of solutions available for securing and increasing defences within the cyberspace. Due to the environment being overly agile, it becomes a constant marathon to remain ahead of security threats. Incorporating security at development stage is key but also enabling ongoing programmability for the network infrastructure without necessarily changing the underlying infrastructure. Network security principle based on the idea of “never trust, always verify” should become the basis for any security specialist.

References

- Shaghaghi, A., Kaafar, M.A., Buyya, R., Jha, S. (2020). Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions. In: Gupta, B., Perez, G., Agrawal, D., Gupta, D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. [https://doi.org/10.1007/978-3-030-22277-2\\_14](https://doi.org/10.1007/978-3-030-22277-2_14)
- Niranjnamurthy, M. and Chahar, D., 2013. The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(7), pp.2885-2895
- Singh, B., 2011. *Network Security and Management*. PHI Learning Pvt. Ltd..
- Gupta, B.B. and Akhtar, T., 2017. A survey on smart power grid: frameworks, tools, security issues, and solutions. *Annals of Telecommunications*, 72(9), pp.517-549.
- Patel, N.S. and Rekha, B.S., 2014. Software as a Service (SaaS): security issues and solutions. *International Journal of Computational Engineering Research*, 4(6), pp.68-71.
- Seyyed Mohammad Safi, Ali Movaghar, Mohammad Ghorbani, Privacy protection scheme for mobile social network, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 7, 2022, Pages 4062-4074,
- G. McGraw, "Software security," in *IEEE Security & Privacy*, vol. 2, no. 2, pp. 80-83, March-April 2004, doi: 10.1109/MSECP.2004.1281254.
- Anderson, R., 2020. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Indianapolis, USA: Wiley.