

Launching into Cyber Security June 2022



Search forums

Collaborative Learning Discussion 2


Initial Post

 [Settings](#) ▾

[◀ Initial post](#)

[Initial Post ▶](#)

Display replies in nested form



Initial Post
by [Nomusa Majola](#) - Monday, 1 August 2022, 3:26 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 specifical 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 two strategies employed by cyber security professionals to build defences for software defined networks.

One strategy to reducing security problems is separating the data and the control plane allowing 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 is more reliant and becomes the primary responsibility of the cloud computing provider.

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

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. The server with then authenticate by requesting the user to decrypt with the corresponding private key.

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. This tool is normally used by the financial services industry in South Africa

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 get ahead of those that pose security threats. Incorporating security at development stage is key but also enabling ongoing programmability for the network infrastructure without necessarily changing the underlying infrastructure. I believe that will be more sustainable long term.

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
- NiranjanaMurthy, 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.

Maximum rating: -

[Permalink](#) [Reply](#) [Export to portfolio](#)



Peer Response

by [Laura Saxton](#) - Wednesday, 3 August 2022, 9:14 AM

Nomusa, thank you for this very interesting post. You have clearly defined the benefits of centralized software as well as cryptography use in security management. You mention that cloud computing security is the “primary responsibility of the cloud computing provider” – do you see any issues of security transparency in this arrangement? If so, how might these be mitigated?

As cloud computing becomes the standard form of data storage, it is important for security frameworks to be utilized by businesses, as regulation transparency of third party software is not always forthcoming (Anderson, 2019).

One framework of interest is Covington et al.’s (2008) usage control (UCON) based security framework. This model is a successor of the policy-enforcement-implementation (PEI) framework, and “[presents] an access control model” (Covington et al., 2008: 4). UCON has six components: subjects and their attributes, objects and their attributes, rights, authorizations, obligations, and conditions which “support attribute mutability and decision continuity by leveraging a hybrid approach of attribute acquisitions and event-based updates” (Covington et al., 2008: 34). Open LDAP and Open SSL are used for security enforcement, along with the extensible access control markup language (XACML) “to enforce policy specification” (Chang et al., 2016: 25) aligned with the framework’s security approach.

Though the above security framework is robust, it does not provide a proposed large-scale business application. Chang et al. (2016) have attempted to fill this gap with the cloud computing adoption framework (CCAF). This framework seeks to implement three layers of security to be deployed “to an on-premise OpenStack cloud environment” (Chang et al., 2016: 39), with particular attention to large scale data structures (50 TB of data was shown to be read in less than 7000 s). Results from the prototype found that common malware (viruses and trojans) were blocked with an F-measure of 0.9975, while SQL injections deployed against MySQL and MongoDB were blocked with response times “constant at 0.20 and 0.40 s, rather than 1000 s per simple request” (Chang et al., 2016: 40).

Though the above frameworks may add a layer of protection for businesses with large databases,



there still remains the question of the amount of security a business is expected to provide along with third party vendors.

Resources

Anderson, R., 2020. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis, USA: Wiley.

Chang, V., Kuo, Y.-H. and Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, [online] 57, pp.24–41. doi:10.1016/j.future.2015.09.031.

Covington, M.J., Zhang, X., Nakae, M., and Sandhu, R. (2008). Toward a Usage-Based Security Framework for Collaborative Computing Systems. *ACM Transactions on Information and System Security*, 11(1), pp.1–36. doi:10.1145/1330295.1330298.

[Permalink](#) [Show parent](#) [Reply](#)



Peer Response

by [Maryam Al-Shibani](#) - Thursday, 4 August 2022, 10:30 AM

Nomusa, it was very interesting reading your post on how to secure the network. You have emphasized on the importance of the ongoing threats the network is exposed to and thereby, the ongoing security countermeasures to keep the risks in an acceptable level while not affecting the underlying infrastructure.

The employment of the separation of the data and control panel as well as encryption and key based authentication would mitigate the risk of data leaks, malicious data manipulation, etc. to ensure a secure environment. Although as you mentioned, all countermeasures has weakness.

According to Lee (2012), the entire system would be affected in the case of denial of service attack. To illustrate the point, moving the environment to the cloud would not mean securing it from DOS attacks the environment will still be in risk of such an attack. In the case of such an attack, data will not be affected due to encryptions, however, the availability of the service would be affected as the whole cloud would be disturbed and will not be possible to gain access to it at that time. In some small organizations the availability of services can be disturbed without affecting the organization, however, this is dependent on the organizations business some organization would not accept this risk as availability would be a major issue for them. Moreover, The use of key authentication mechanism has its short comes as stated by Kambourakis et al. (2004), however, the use of SSL (Secure Sockets Layer) mechanism can overcome these issues.

References

Kambourakis, G., Rouskas, A. & Gritzalis, S. (2004) Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication systems. *EURASIP Journal on Wireless Communications and Networking*. Available from: <https://link.springer.com/content/pdf/10.1155/S1687147204403016.pdf> [Accessed 29 July 2022].

Lee, K. (2012) Security Threats in Cloud Computing Environments. *International Journal of Security and Its Application*. 6(4) Available from: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.4573&rep=rep1&type=pdf> [Accessed 29 July 2022].

[Permalink](#) [Show parent](#) [Reply](#)





Re: Initial Post

by [Chak Kwan Lee](#) - Monday, 8 August 2022, 5:36 AM

Nomusa, it was very interesting reading your post on how to secure the network. Authenticator is a really common and easy way to protect the network security, due to Data breaches have become the new normal. The stolen data in the first half of 2017 exceeded the total in 2016. These attacks have hit the world's largest retail supply chains (Target, Home Depot, TJX), restaurants (Hyatt, Hilton), Internet companies (Yahoo, eBay, LinkedIn), and many others, stealing massive amounts of their customer's to access the account's password information. Once credentials are obtained, criminals can hijack these accounts (and other services that share passwords) to empty property, steal more confidential personal information, and buy goods and services in your name.

Billions of login credentials are currently circulating on the dark web. Last year, Yahoo alone admitted to hacking 3 billion user records. In December 2017, an underground website was found to have a database of 1.4 billion stolen accounts available to hackers, the largest known case to date.

When placing an order under 2FA, you can also verify the second "identity verification" based on the items required by the user account: you cannot perform the second verification personally. information (mother's first name), information that you hold personally (e.g. sent via text message, app or software lock [dongle]), protection of any customer from personal characteristics (e.g. authentication). This article focuses on the second category, codes that are subject to constant change and post-use security vulnerabilities, which are sent via text messages or applications on devices/computers to achieve their goals quickly.

References

Trendmicro---- <https://blog.trendmicro.com>

[Permalink](#) [Show parent](#) [Reply](#)

[◀ Initial post](#)

[Initial Post ▶](#)

