C. Comparison of VPN Solutions

This section compares and evaluates the performance results as well as important non-functional aspects that distinguish the studied VPN solutions.

1) Performance: Fig. 3 summarizes the individual performance rankings for each platform. Since the platforms contained Ethernet devices of different speeds, the measurements were normalized to the same order of magnitude, in order to make their relative distance from the baseline (the theoretically possible) comparable. The evaluation showed a clear trend towards the latest approaches MACsec and Wireguard. While MACsec (together with IPsec) was consistently best or second best performing solution for latency, Wireguard showed the highest throughput achievable (or line speed) on 4 of 5 platforms.

For 10 Gbit/s links, the equations seem to change considerably. In order to saturate these links, hardware support for encryption and big CPUs are not sufficient anymore and the bottleneck moved somewhere else. Where to, we can only speculate.

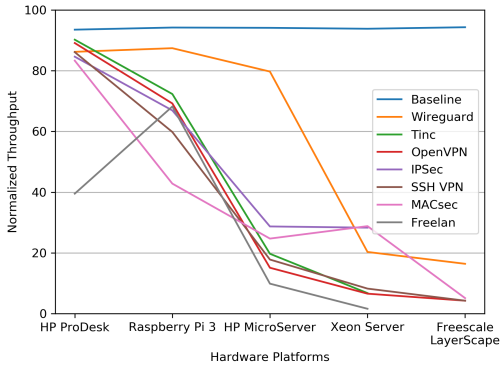
2) Non-functional Aspects: The customary and established solutions (OpenVPN, IPsec, Tinc, Secure Shell) offer a multitude of ciphers to choose from. And, while variety is ostensibly a good feature, it has detrimental effects as well.

Some solutions offer ciphers in their documentation, but once configured just do not work (see Table III) and furthermore, the sets of working algorithms change between platforms. We could not find conclusive evidence as to why this is the case. It is at least puzzling, as all platforms ran an up-to-date Linux kernel, with, in most cases, a current software distribution on top (see Table II). Some ciphers even worked on none of the tested platforms. Within the ciphers that did work, some individual ciphers (e. g. Whirlpool, MCDC-2) always showed abysmal performance. The modes of operation CFB1 and CFB8 also performed very badly, independently of the configured cipher. Other ciphers showed very good and very poor performance depending on the platform (e. g. BLAKE2). Furthermore, some ciphers are so old, that they have been broken by now, and must be considered insecure. Blowfish was proposed in 1993 and is even still the default setting for OpenVPN. Legacy support cannot be used as an argument here. Performance of the ciphers between platforms also differs widely. If performance actually is an issue, tweaking of the individual system becomes necessary and as we have showed, this is a non-trivial task.

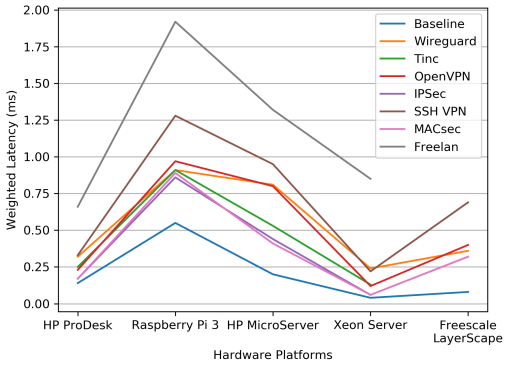
This wealth of options, that probably accumulated over many years of development and maintenance of each VPN software, seems to make it hard to manage it. In our minds, users would be better served, if the configurable cipher sets would be drastically reduced.

On contrast, the new approaches MACsec and especially Wireguard go in the opposite direction and do not offer the user multiple ciphers, thereby eliminating the chance for misconfiguration. Additionally, this gives the software developers the chance to address performance and compatibility issues, that may arise on different hardware and operating system architectures. Therefore, we clearly recommend the use of those two solutions, wherever possible.

[9]Normalization factors for the platforms were 0.1, 1, 0.1, 0.01, 0.1



(a) Throughput ranking.[9]



(b) Latency ranking.

Figure 3: General performance rankings of solutions over all platforms.

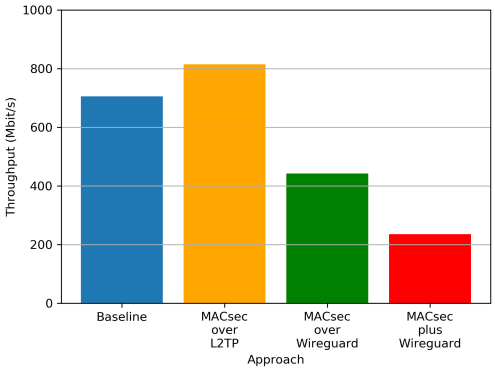
D. Extended Setting

Fig. 4 shows the achieved throughput and latency performances of each approach.

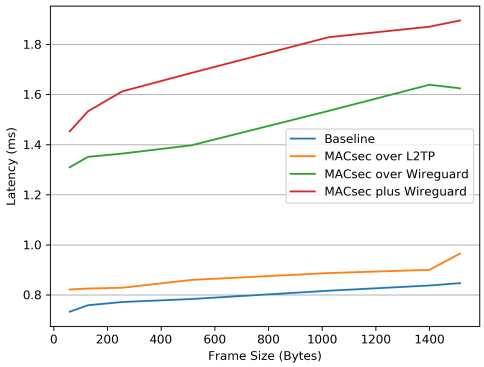
The throughput of the baseline measurement is lower than the measurement for MACsec/L2TP. This is probably due to the measurement tools rate adjustment algorithm getting confused by the setup, meaning the data flows being interrupted by multiple send and receive queues of the different involved devices. The measured CPU usage does not indicate a bottleneck.

The performance of the 'MACsec over L2TP'-approach shows almost line speed. This is no surprise, as the gateways only relay already encrypted frames. Yet, with the other two approaches, the performance drops considerably. The additional encryption steps performed on the gateways, have big impact. The additional Wireguard tunnel within the second approach halves achieved throughput and almost doubles latency. The further step of the third approach of de- and encrypting the MACsec frames on the gateways halves the achievable throughput yet again.

For resource restricted environments, where performance is non the less an issue, it seems unfeasible to protect communication data within and in between LANs with conventional means (second and third approach). Therefore, the aforementioned trade-off between configuration complexity and performance should be answered individually depending on



(a) Throughput comparison.



(b) Latency comparison.

Figure 4: Performance comparison of different approaches of the extended gateway setting.

the use case. The first prototypical approach of just relaying MACsec frames should be investigated further.

VI. Conclusion

This study investigated different software solutions on how to securely interconnect local area networks. Non-functional aspects as well as their performance were analyzed, discussed and compared.

The classic and well established solutions, like OpenVPN and IPsec, were found to exhibit significant drawbacks in the face of new and upcoming solutions. We believe, that these, namely MACsec and Wireguard, should be preferred in the future, where and whenever possible.

This study also revealed starting points for future research. ChaCha/Poly1305 performed best in resource restricted environments, where AES hardware acceleration within the CPU did not exist. It might therefore be promising to include this cipher into other VPN solutions and protocols in order to increase their performance in certain use cases. Furthermore, extended security schemes, that already protect communication data within a LAN should be further researched in order to be used efficiently.

References

[1] K. Ahmed, N. S. Nafi, J. O. Blech, M. A. Gregory, and H. Schmidt. Software defined industry automation networks. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–3, Nov 2017.

[2] A. Alshalan, S. Pisharody, and D. Huang. A survey of mobile vpn technologies. *IEEE Communications Surveys Tutorials*, 18(2):1177–1196, Secondquarter 2016.

[3] A. Bluschke, W. Bueschel, M. Hohmuth, F. Jehring, R. Kaminski, K. Klamka, S. Koepsell, A. Lackorzynski, T. Lackorzynski, M. Matthews, P. Rietzsch, A. Senier, P. Sieber, V. Ulrich, R. Wiggers, and J. Wolter. fastvpn - secure and flexible networking for industry 4.0. In *Broadband Coverage in Germany; 12th ITG-Symposium*, pages 1–8, April 2018.

[4] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah. Performance evaluation and analysis of layer 3 tunneling between openssh and openvpn in a wide area network environment. In *2015 International Conference on Computing, Communication and Security (ICCCS)*, pages 1–4, Dec 2015.

[5] B. Czybik, S. Hausmann, S. Heiss, and J. Jasperneite. Performance evaluation of mac algorithms for real-time ethernet communication systems. pages 676–681, 07 2013.

[6] J. A. Donenfeld. WireGuard: Next Generation Kernel Network Tunnel. Technical report, www.wireguard.com, 2018.

[7] S. Dubroca. MACsec: Encryption for the wired LAN. In *netdev 1.1*. Red Hat, February 2016.

[8] S. Escher and S. Köpsell. Durchführung eines integrierten Anti-Phishing-Trainings. In *Christian Paulsen (Hg.): Sicherheit in vernetzten Systemen. 23. DFN-Konferenz*, 2018.

[9] A. Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired.com, September 2018.

[10] Industrial Internet Consortium. *Industrial Networking Enabling IIoT Communication*, August 2018.

[11] S. Khanvilkar and A. Khokhar. Virtual private networks: an overview with performance evaluation. *IEEE Communications Magazine*, 42(10):146–154, Oct 2004.

[12] I. Kotuliak, P. Rybar, and P. Trúchly. Performance comparison of ipsec and tls based vpn technologies. 10 2011.

[13] A. Lakbabi, G. Orhanou, and S. E. Hajji. Vpn ipsec amp; ssl technology security and management point of view. In *2012 Next Generation Networks and Services (NGNS)*, pages 202–208, Dec 2012.

[14] J. Lau and M. Townsley. Layer Two Tunneling Protocol - Version 3 (L2TPv3). RFC 3931, March 2005.

[15] H. Mao, L. Zhu, and H. Qin. A comparative research on ssl vpn and ipsec vpn. In *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4, Sep. 2012.

[16] S. Narayan, K. Brooking, and S. de Vere. Network performance analysis of vpn protocols: An empirical comparison on different operating systems. In *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, volume 1, pages 645–648, April 2009.

[17] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero. An experimental security analysis of an industrial robot controller. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 268–286, May 2017.

[18] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The first collision for full sha-1. pages 570–596, 07 2017.

[19] A. V. Uskov. Information security of ipsec-based mobile vpn: Authentication and encryption algorithms performance. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1042–1048, June 2012.

[20] M. H. M. Zaharuddin, R. A. Rahman, and M. Kassim. Technical comparison analysis of encryption algorithm on site-to-site ipsec vpn. In *2010 International Conference on Computer Applications and Industrial Electronics*, pages 641–645, Dec 2010.

[21] Z. Zhipeng, S. Chandel, S. Jingyao, Y. Shilin, Y. Yunnan, and Z. Jingji. Vpn: a boon or trap? : A comparative study of mpls, ipsec, and ssl virtual private networks. In *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, pages 510–515, Feb 2018.

[22] ZVEI. *The Reference Architectural Model Industrie 4.0 (RAMI 4.0)*, April 2015.