As detailed in § III-D, ENDBOX is able to execute middlebox functions on encrypted traffic. The following four proposals also target this problem. BlindBox [15] presents an encryption scheme to perform a limited set of computations on encrypted traffic, but at a much lower cost than traditional homomorphic encryption. In mcTLS [13] and mbTLS [14] packets are encrypted in a way such that middleboxes that require access can decrypt them. SGX-Box [52] utilises SGX on centralised middleboxes to enable DPI on encrypted network traffic. Similarly to ENDBOX, TLS session keys are securely shared with the enclave.

VII. CONCLUSION

In this paper, we presented ENDBOX, a scalable system that enables the secure deployment and execution of middlebox functions on untrusted client machines. For typical middlebox functions, it scales linearly with the number of clients, thereby achieving a 2.6× to 3.8× higher throughput than a traditional deployment at the core of a managed network. Despite being distributed, configuration changes to ENDBOX-based middlebox services are centrally controlled and enforced. Finally, encrypted application traffic can be efficiently and securely decrypted and filtered using ENDBOX, due to its location at the client side.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewers for their valuable feedback. This work has received funding from the EU's Horizon 2020 research and innovation programme under grant agreements 645011 (SERECA) and 690111 (SecureCloud).

REFERENCES

[1] Cisco Visual Networking Index, "The zettabyte era–trends and analysis," *Cisco white paper*, 2013.
[2] Kaspersky Lab, "Global IT Security Risks Survey 2014 – Distributed Denial of Service (DDoS) Attacks," https://goo.gl/dbg3wZ.
[3] Verisign Blog, "Verisign Q1 2016 DDos Trends: Attack Activity Increases 111 Percent Year Over Year," https://goo.gl/Srm3cW.
[4] J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy *et al.*, "Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service," in *ACM SIGCOMM'12*.
[5] C. Lan, J. Sherry, R. A. Popa, S. Ratnasamy, and Z. Liu, "Embark: Securely Outsourcing Middleboxes to the Cloud," in *USENIX NSDI'16*.
[6] H. Ballani, P. Costa, C. Gkantsidis, M. P. Grosvenor *et al.*, "Enabling End-Host Network Functions," in *ACM SIGCOMM'15*.
[7] W. Zhang, G. Liu, A. Mohammadkhan, J. Hwang *et al.*, "SDNFV: Flexible and Dynamic Software Defined Control of an Application- and Flow-Aware Data Plane," in *Middleware'16*.
[8] M. Feilner, *OpenVPN: Building and integrating virtual private networks*. Packt Publishing Ltd, 2006.
[9] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek, "The Click modular router," *ACM Transactions on Computer Systems*, 2000.
[10] EFF, "We're Halfway to Encrypting the Entire Web," https://goo.gl/VdUj5b, 2017.
[11] D. Naylor, A. Finamore, I. Leontiadis, Y. Grunenberger *et al.*, "The cost of the S in HTTPS," in *ACM CoNEXT'14*.
[12] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson, "Analyzing forged SSL certificates in the wild," in *IEEE S&P 2014*.
[13] D. Naylor *et al.*, "Multi-Context TLS (mcTLS): Enabling Secure In-Network Functionality in TLS," in *ACM SIGCOMM'15*.
[14] D. Naylor *et al.*, "And then there were more: Secure communication for more than two parties," in *CoNEXT'17*.
[15] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy, "BlindBox: Deep Packet Inspection over Encrypted Traffic," in *ACM SIGCOMM'15*.
[16] 1&1 Internet Ltd., "IP Spoofing: Simple manipulation of data packets by attackers," https://goo.gl/Dn1CaV, 2017.
[17] D. Kreutz *et al.*, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, 2015.
[18] B. Han *et al.*, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, 2015.
[19] J. Soares *et al.*, "Toward a telco cloud environment for service functions," *IEEE Communications Magazine*, 2015.
[20] C. Dixon, H. Uppal, V. Brajkovic, D. Brandon *et al.*, "ETTM: a scalable fault tolerant network manager," in *USENIX NSDI'11*.
[21] S. Gueron, "A Memory Encryption Engine Suitable for General Purpose Processors." *IACR Cryptology ePrint Archive*, 2016.
[22] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," in *HASP'13*.
[23] S. Arnautov, B. Trach, F. Gregor, T. Knauth *et al.*, "SCONE: Secure Linux Containers with Intel SGX," in *USENIX OSDI'16*.
[24] C.-C. Tsai, D. E. Porter, and M. Vij, "Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX," in *USENIX ATC'17*.
[25] S. Shinde, D. L. Tien, S. Tople, and P. Saxena, "PANOPLY: Low-TCB Linux Applications With SGX Enclaves," in *NDSS'17*.
[26] S. Brenner, C. Wulf, D. Goltzsche, N. Weichbrodt *et al.*, "SecureKeeper: Confidential ZooKeeper using Intel SGX," in *Middleware'16*.
[27] Y. Xu, W. Cui, and M. Peinado, "Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems," in *IEEE SP'15*.
[28] N. Weichbrodt, A. Kurmus, P. Pietzuch, and R. Kapitza, "AsyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves," in *ESORICS'16*.
[29] J. Van Bulck, F. Piessens, and R. Strackx, "SGX-Step: A practical attack framework for precise enclave execution control," 2017.
[30] J. Seo, B. Lee, S. Kim, M.-W. Shih *et al.*, "SGX-Shield: Enabling address space layout randomization for SGX programs," in *NDSS'17*.
[31] M.-W. Shih, S. Lee, T. Kim, and M. Peinado, "T-SGX: Eradicating controlled-channel attacks against enclave programs," in *NDSS'17*.
[32] A. Garg and A. N. Reddy, "Mitigation of DoS attacks through QoS regulation," *Microprocessors and Microsystems*, 2004.
[33] H. Nguyen and V. Ganapathy, "EnGarde: Mutually-Trusted Inspection of SGX Enclaves," in *IEEE ICDCS'17*.
[34] M. Green, R. Droms, R. Housley, P. Turner, S. Fenter, "Data Center use of Static Diffie-Hellman in TLS 1.3," https://goo.gl/95FaWD.
[35] E. Rescorla, "Update on TLS 1.3 Middlebox Issues," https://goo.gl/zCUuRG, 2017.
[36] Intel Corp, "Intel Software Guard Extensions for Linux OS (Intel SGX) SDK," https://01.org/intel-software-guard-extensions, 2017.
[37] P.-L. Aublin, F. Kelbert, D. O'Keeffe, D. Muthukumaran *et al.*, "TaLoS: Secure and Transparent TLS Termination inside SGX Enclaves," Imperial College London, Tech. Rep. 2017/5, Mar. 2017.
[38] M. Orenbach, P. Lifshits, M. Minkin, and M. Silberstein, "Eleos: ExitLess OS Services for SGX Enclaves," in *EuroSys '17*.
[39] S. Checkoway and H. Shacham, "Iago Attacks: Why the System Call API is a Bad Untrusted RPC Interface," in *ASPLOS'13*.
[40] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks." in *USENIX LISA'99*.
[41] A. V. Aho and M. J. Corasick, "Efficient string matching: an aid to bibliographic search," *Communications of the ACM*, 1975.
[42] W. Sun and R. Ricci, "Fast and flexible: Parallel packet processing with GPUs and Click," in *ACM/IEEE ANCS'13*.
[43] Alexa., http://www.alexa.com/, 2017.
[44] T. Karagiannis *et al.*, "Network Exception Handlers: Host-network Control in Enterprise Networks," in *ACM SIGCOMM'08*.
[45] L. Lamport *et al.*, "Paxos made simple," *ACM Sigact News*, 2001.
[46] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *iNetSec'15*.
[47] X. Yuan, X. Wang, J. Lin, and C. Wang, "Privacy-preserving deep packet inspection in outsourced middleboxes," in *IEEE INFOCOM'16*.
[48] H. Duan, X. Yuan, and C. Wang, "LightBox: SGX-assisted Secure Network Functions at Near-native Speed," *arXiv:1706.06261*, 2017.
[49] M. Coughlin, E. Keller, and E. Wustrow, "Trusted Click: Overcoming Security issues of NFV in the Cloud," in *ACM SDN-NFV Security'17*.
[50] D. Kuvaiskii, S. Chakrabarti, and M. Vij, "Snort Intrusion Detection System with Intel Software Guard Extension," *arXiv:1802.00508*, 2018.
[51] B. Trach *et al.*, "ShieldBox: Secure Middleboxes using Shielded Execution," in *ACM SOSR'18*, 2018.
[52] J. Han, S. Kim, J. Ha, and D. Han, "SGX-Box: Enabling Visibility on Encrypted Traffic using a Secure Middlebox Module," in *ACM APNet'17*.

https://doi.org/10.24355/dbbs.084-201807101413-0