





























- [26] Open Networking Foundation. Threat analysis for the sdn architecture. pages 1–21, 2016.
- [27] Yang Gao and Mingdi Xu. Defense against software-defined network topology poisoning attacks. *Tsinghua Science and Technology*, 28(1):39–46, 2022.
- [28] Sana Habib, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupe. Mitigating threats emerging from the interaction between sdn apps and sdn (configuration) datastore. In *Proceedings of the 2022 on Cloud Computing Security Workshop*, pages 23–39, 2022.
- [29] Sungmin Hong, Lei Xu, Haopei Wang, and Guofei Gu. Poisoning network visibility in software-defined networks: New attacks and countermeasures. In *Ndss*, volume 15, pages 8–11, 2015.
- [30] Tao Hu, Zehua Guo, Peng Yi, Thar Baker, and Julong Lan. Multi-controller based software-defined networking: A survey. *IEEE access*, 6:15980–15996, 2018.
- [31] Tao Hu, Zhen Zhang, Peng Yi, Dong Liang, Ziyong Li, Quan Ren, Yuxiang Hu, and Julong Lan. Seapp: A secure application management framework based on rest api access control in sdn-enabled cloud environment. *Journal of Parallel and Distributed Computing*, 147:108–123, 2021.
- [32] Xinli Huang, Peng Shi, Yufei Liu, and Fei Xu. Towards trusted and efficient sdn topology discovery: A lightweight topology verification scheme. *Computer Networks*, 170:107119, 2020.
- [33] Juniper. Junos space datasheet. <https://www.juniper.net/us/en/products/sdn-and-orchestration/junos-space-datasheet.html>.
- [34] Peyman Kazemian, Michael Chang, Hongyi Zeng, George Varghese, Nick McKeown, and Scott Whyte. Real time network policy checking using header space analysis. In *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*, pages 99–111, 2013.
- [35] Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mohsen Guizani, and Muhammad Khurram Khan. Topology discovery in software defined networks: Threats, taxonomy, and state-of-the-art. *IEEE Communications Surveys & Tutorials*, 19(1):303–324, 2016.
- [36] Ahmed Khurshid, Xuan Zou, Wenxuan Zhou, Matthew Caesar, and P. Brighten Godfrey. VeriFlow: Verifying Network-Wide invariants in real time. In *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*, pages 15–27, Lombard, IL, April 2013. USENIX Association.
- [37] Jiwon Kim, Benjamin E Ujcich, and Dave Jing Tian. Intender: Fuzzing {Intent-Based} networking with {Intent-State} transition guidance. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 4463–4480, 2023.
- [38] Diego Kreutz, Fernando MV Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, 2014.
- [39] Chanhee Lee, Changhoo Yoon, Seungwon Shin, and Sang Kil Cha. Indago: A new framework for detecting malicious sdn applications. In *2018 IEEE 26th International Conference on Network Protocols (ICNP)*, pages 220–230. IEEE, 2018.
- [40] Charles E. Leiserson. Fat-trees: Universal networks for hardware-efficient supercomputing. *IEEE Transactions on Computers*, C-34(10), 1985.
- [41] He Li, Peng Li, Song Guo, and Shui Yu. Byzantine-resilient secure software-defined networks with multiple controllers. In *2014 IEEE International Conference on Communications (ICC)*, pages 695–700. IEEE, 2014.
- [42] Tong Li, Jinqiang Chen, and Hongyong Fu. Application scenarios based on sdn: an overview. In *Journal of Physics: Conference Series*, volume 1187, page 052067. IOP Publishing, 2019.
- [43] Yassine Maleh, Youssef Qasmaoui, Khalid El Gholami, Yassine Sadqi, and Soufyane Mounir. A comprehensive survey on sdn security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments*, 9(2):201–239, 2023.
- [44] Stephanos Matsumoto, Samuel Hitz, and Adrian Perrig. Fleet: Defending sdns from malicious administrators. In *Proceedings of the third workshop on Hot topics in software defined networking*, pages 103–108, 2014.
- [45] Colin Scott Murphy. The pox network software platform. <https://github.com/noxrepo/pox>, 2013. Accessed on 2023-06-19.
- [46] Ajay Nehra, Meenakshi Tripathi, Manoj Singh Gaur, Ramesh Babu Battula, and Chhagan Lal. Sldp: A secure and lightweight link discovery protocol for software defined networking. *Computer Networks*, 150:102–116, 2019.
- [47] Ajay Nehra, Meenakshi Tripathi, Manoj Singh Gaur, Ramesh Babu Battula, and Chhagan Lal. Tilak: A token-based prevention approach for topology discovery threats in sdn. *International Journal of Communication Systems*, 32(17):e3781, 2019.
- [48] Samsung Newsroom. Samsung expands its lineup of sdn solutions. <https://news.samsung.com/global/samsung-expands-its-lineup-of-sdn-solutions>, 2021.
- [49] Tri-Hai Nguyen and Myungsik Yoo. Analysis of link discovery service attacks in sdn controller. In *2017 International Conference on Information Networking (ICOIN)*, pages 259–261. IEEE, 2017.
- [50] University of Adelaide. Topology zoo. <http://www.topology-zoo.org/dataset.html>.
- [51] Panagiotis Papadimitriou, Ali Dasdan, and Hector Garcia-Molina. Web graph similarity for anomaly detection. *Journal of Internet Services and Applications*, 1:19–30, 2010.
- [52] Karl Pertsch, Youngwoon Lee, and Joseph Lim. Accelerating reinforcement learning with learned skill priors. In *Conference on robot learning*, pages 188–204. PMLR, 2021.
- [53] Philip Porras, Seungwon Shin, Vinod Yegneswaran, Martin Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for openflow networks. In *Proceedings of the first workshop on Hot topics in software defined networks*, pages 121–126, 2012.
- [54] Chao Qi, Jiangxing Wu, Hongchao Hu, Guozhen Cheng, Wenyan Liu, Jianjian Ai, and Chao Yang. An intensive security architecture with multi-controller for sdn. In *2016 IEEE conference on computer communications workshops (infocom wkskps)*, pages 401–402. IEEE, 2016.
- [55] Ryan Izard Qing Wang, Geddings Barrineau. Floodlight sdn openflow controller. <https://github.com/floodlight/floodlight>, 2016. Accessed on 2023-06-19.
- [56] Christian Röpke and Thosten Holz. Preventing malicious sdn applications from hiding adverse network manipulations. In *Proceedings of the 2018 Workshop on Security in Software-defined Networks: Prospects and Challenges*, pages 40–45, 2018.
- [57] Stuart J Russell and Peter Norvig. *Artificial intelligence: a modern approach*. Malaysia: Pearson Education Limited., 2016.
- [58] Arash Shaghghi, Mohamed Ali Kaafar, Rajkumar Buyya, and Sanjay Jha. Software-defined network (sdn) data plane security: issues, solutions, and future directions. *Handbook of Computer Networks and Cyber Security*, pages 341–387, 2020.
- [59] Arash Shaghghi, Salil S. Kanhere, Mohamed Ali Kaafar, and Sanjay Jha. Gwardar: Towards protecting a software-defined network from malicious network operating systems. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–5, 2018.
- [60] Richard Skowryra, Lei Xu, Guofei Gu, Veer Dedhia, Thomas Hobson, Hamed Okhravi, and James Landry. Effective topology tampering attacks and defenses in software-defined networks. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 374–385. IEEE, 2018.
- [61] Dylan Smyth, Sean McSweeney, Donna O’Shea, and Victor Cionca. Detecting link fabrication attacks in software-defined networks. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–8. IEEE, 2017.
- [62] Amin Tootoonchian and Yashar Ganjali. Hyperflow: A distributed control plane for openflow. In *Proceedings of the 2010 internet network management conference on Research on enterprise networking*, volume 3, 2010.
- [63] ONF TS-009. Openflow switch specification version 1.3.2. <https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.3.2.pdf>.
- [64] Yuchia Tseng, Farid Nait-Abdesselam, and Ashfaq Khokhar. A comprehensive 3-dimensional security analysis of a controller in software-defined networking. *Security and Privacy*, 1(2):e21, 2018.
- [65] Yuchia Tseng, Montida Pattaranantakul, Ruan He, Zonghua Zhang, and Farid Nait-Abdesselam. Controller dac: Securing sdn controller with dynamic access control. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2017.
- [66] Benjamin E Ujcich, Samuel Jero, Anne Edmundson, Qi Wang, Richard Skowryra, James Landry, Adam Bates, William H Sanders, Cristina Nita-Rotaru, and Hamed Okhravi. Cross-app poisoning in software-defined networking. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 648–663, 2018.
- [67] Benjamin E Ujcich, Samuel Jero, Richard Skowryra, Adam Bates, William H Sanders, and Hamed Okhravi. Causal analysis for {Software-Defined} networking attacks. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3183–3200, 2021.
- [68] Raniyah Wazirali, Rami Ahmad, and Suheib Alhiyari. Sdn-openflow topology discovery: an overview of performance issues. *Applied Sciences*, 11(15):6999, 2021.
- [69] Alan Weissberger. Comcast: Onf trellis software is in production together with l2/l3 white box switches. <https://techblog.comsoc.org/2019/09/14/comcast-puts-onf-trellis-software-into-production/>.
- [70] Tracy Yang. Picos 4.4.4 configuration guide (special release): Ecmp select group. <https://pica8-fs.atlassian.net/wiki/spaces/PicOS444beta/pages/115898390/Ecmp+Select+Group>.
- [71] Tracy Yang. Picos 4.4.4 configuration guide (special release): ovs-ofctl add-flow <bridge> <flow>. <https://pica8-fs.atlassian.net/wiki/spaces/PicOS444beta/pages/115900326/ovs-ofctl+add-flow+bridge+flow>.
- [72] Ch Yoon and S Lee. Attacking sdn infrastructure: Are we ready for the next-gen networking? *BlackHat-USA-2016*, pages 17–18, 2016.
- [73] Yuan Zhang, Lin Cui, Wei Wang, and Yuxiang Zhang. A survey on software defined networking with multiple controllers. *Journal of Network and Computer Applications*, 103:101–118, 2018.
- [74] Haifeng Zhou, Chunming Wu, Chengyu Yang, Pengfei Wang, Qi Yang, Zhouhao Lu, and Qiumei Cheng. Sdn-rdcd: A real-time and reliable method for detecting compromised sdn devices. *IEEE/ACM transactions on networking*, 26(5):2048–2061, 2018.