Bibliography

[1] A. Press, "Un hacked in apparent espionage operation: report," *New York Post*, 2020.

[2] E. Nakashima and J. Greene, "Hospitals being hit in coordinated, targeted ransomware attack from russian-speaking criminals," *The Washington Post*, 2020.

[3] S. R. Choudhury, "New zealand's stock exchange halts trading for third day in a row," *CNBC*, 2020.

[4] R. Lagerström, C. Baldwin, A. MacCormack, D. Sturtevant, and L. Doolan, "Exploring the relationship between architecture coupling and software vulnerabilities," in *Engineering Secure Software and Systems*, E. Bodden, M. Payer, and E. Athanasopoulos, Eds. Cham: Springer International Publishing, 2017, pp. 53–69.

[5] P. Johnson, D. Gorton, R. Lagerström, and M. Ekstedt, "Time between vulnerability disclosures: A measure of software product vulnerability," *Computers Security*, vol. 62, pp. 278–295, 2016.

[6] O. Depren, M. Topallar, E. Anarim, and M. Ciliz, "An intelligent intrusion detection system (ids) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713–722, 2005, cited By 287.

[7] R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," in *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, 2017, pp. 141–147.

[8] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[9] T. T. Nguyen and G. Armitage, “A survey of techniques for internet traffic classification using machine learning,” *IEEE communications surveys & tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

[10] N. Friedman, D. Geiger, and M. Goldszmidt, “Bayesian network classifiers,” *Machine Learning*, vol. 29, pp. 131–163, 1997.

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network anomaly detection: Methods, systems and tools,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[12] C. Chow and C. Liu, “Approximating discrete probability distributions with dependence trees,” *IEEE transactions on Information Theory*, vol. 14, no. 3, pp. 462–467, 1968.

[13] C. Bielza and P. Larrañaga, “Discrete bayesian network classifiers: A survey,” *ACM Comput. Surv.*, vol. 47, no. 1, 2014.

[14] C. R. de Sá, C. Soares, A. Knobbe, P. Azevedo, and A. M. Jorge, “Multi-interval discretization of continuous attributes for label ranking,” in *Discovery Science*, J. Fürnkranz, E. Hüllermeier, and T. Higuchi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 155–169.

[15] J. Dougherty, R. Kohavi, and M. Sahami, “Supervised and unsupervised discretization of continuous features,” in *Machine Learning Proceedings 1995*, A. Prieditis and S. Russell, Eds. San Francisco (CA): Morgan Kaufmann, 1995, pp. 194 – 202.

[16] J. McHugh, “Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory,” *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, p. 262–294, 2000.

[17] N. Moustafa and J. Slay, “Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set),” in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[18] J. P. Anderson, “Computer security threat monitoring and surveillance,” *Technical Report, James P. Anderson Company*, 1980.

[19] M. Ekstedt, R. Lagerström, J. Jacobsson, M. Wällstedt, and P. Eliasson, “An attack simulation language for the it domain,” in *Graphical Models for Security: 7th International Workshop, GraMSec 2020, Boston, MA, USA, June 22, 2020 Revised Selected Papers*. Springer Nature, p. 67.

[20] D. Elsner, P. Aleatrati Khosroshahi, A. D. MacCormack, and R. Lagerström, “Multivariate unsupervised machine learning for anomaly detection in enterprise applications,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[21] A. K. Ghosh and A. Schwartzbard, “A study in using neural networks for anomaly and misuse detection.” in *USENIX security symposium*, vol. 99, 1999, p. 12.

[22] L. Khan, M. Awad, and B. Thuraisingham, “A new intrusion detection system using support vector machines and hierarchical clustering,” *The VLDB journal*, vol. 16, no. 4, pp. 507–521, 2007.

[23] B. Balajinath and S. Raghavan, “Intrusion detection through learning behavior model,” *Computer Communications*, vol. 24, no. 12, pp. 1202 – 1212, 2001.

[24] S. Mukherjee and N. Sharma, “Intrusion detection using naive bayes classifier with feature reduction,” *Procedia Technology*, vol. 4, p. 119–128, 2012.

[25] A. Panigrahi and M. R. Patra, “Anomaly based network intrusion detection using bayes net classifiers,” 2019.

[26] F. Y. Nia and M. Khalili, “An efficient modeling algorithm for intrusion detection systems using c5.0 and bayesian network structures,” in *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 2015, pp. 1117–1123.

[27] R. Najafi and M. Afsharchi, “Network intrusion detection using tree augmented naive-bayes,” in *The Third International Conference on Contemporary Issues in Computer and Information Sciences (CICI)*, 2012, pp. 396–402.

[28] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke, “Can the common vulnerability scoring system be trusted? a bayesian analysis,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1002–1015, 2018.