REFERENCES

[1] Massimiliano Albanese, Ermanno Battista, and Sushil Jajodia. 2015. A deception based approach for defeating OS and service fingerprinting. In *Communications and Network Security (CNS), 2015 IEEE Conference on*. IEEE, 317–325.

[2] Massimiliano Albanese, Ermanno Battista, and Sushil Jajodia. 2016. Deceiving Attackers by Creating a Virtual Attack Surface. In *Cyber Deception*. Springer, 169–201.

[3] Mohammed H Almeshekah and Eugene H Spafford. 2014. Planning and integrating deception into computer security defenses. In *Proceedings of the 2014 Workshop on New Security Paradigms Workshop*. ACM, 127–138.

[4] Mohammed H Almeshekah and Eugene H Spafford. 2016. Cyber security deception. In *Cyber Deception*. Springer-Verlag, 25–52.

[5] Tansu Alpcan and Tamer Başar. 2010. *Network security: A decision and game-theoretic approach*. Cambridge University Press.

[6] Nicola Basilico and Nicola Gatti. 2011. Automated Abstractions for Patrolling Security Games.. In *AAAI*.

[7] Nicola Basilico, Nicola Gatti, and Francesco Amigoni. 2012. Patrolling security games: Definition and algorithms for solving large instances with single patroller and single intruder. *Artificial Intelligence* 184 (2012), 78–123.

[8] David Barroso Berrueta. 2003. A practical approach for defeating Nmap OS-Fingerprinting. *Retrieved March* 12 (2003), 2009.

[9] Christopher M Bishop. 2006. *Pattern recognition and machine learning*. springer.

[10] Thomas E Carroll and Daniel Grosu. 2011. A game theoretic investigation of deception in network security. *Security and Communication Networks* 4, 10 (2011), 1162–1172.

[11] Karel Durkota, Viliam Lisỳ, Branislav Bošanskỳ, and Christopher Kiekintveld. 2015. Approximate solutions for attack graph games with imperfect information. In *International Conference on Decision and Game Theory for Security*. Springer, 228–249.

[12] Karel Durkota, Viliam Lisỳ, Branislav Bosanskỳ, and Christopher Kiekintveld. 2015. Optimal Network Security Hardening Using Attack Graph Games.. In *IJCAI*. 526–532.

[13] Vindu Goel and Nicole Perlroth. 2016 (accessed September 10, 2017). *Yahoo Says 1 Billion User Accounts Were Hacked*. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

[14] Ines Gutzmer. 2017 (accessed October 15, 2017). *Equifax Announces Cybersecurity Incident Involving Consumer Information*. https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[15] Sushil Jajodia, Noseong Park, Fabio Pierazzi, Andrea Pugliese, Edoardo Serra, Gerardo I Simari, and VS Subrahmanian. 2017. A Probabilistic Logic of Cyber Deception. *IEEE Transactions on Information Forensics and Security* 12, 11 (2017), 2532–2544.

[16] Rob Joyce. 2016. Disrupting Nation State Hackers. USENIX Association, San Francisco, CA.

[17] Christopher Kiekintveld, Viliam Lisỳ, and Radek Píbil. 2015. Game-theoretic foundations for the strategic use of honeypots in network security. In *Cyber Warfare*. Springer, 81–101.

[18] Aron Laszka, Yevgeniy Vorobeychik, and Xenofon D Koutsoukos. 2015. Optimal Personalized Filtering Against Spear-Phishing Attacks.. In *AAAI*. 958–964.

[19] Gordon Fyodor Lyon. 2009. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.

[20] Mandiant. 2013. APT1: Exposing One of ChinaâĂŹs Cyber Espionage Units. (2013).

[21] NIST. 2017. *National Vulnerability Database*. https://nvd.nist.gov/.

[22] Jeffrey Pawlick and Quanyan Zhu. 2015. Deception by design: evidence-based signaling games for network defense. *arXiv preprint arXiv:1503.05458* (2015).

[23] Radek Pıbil, Viliam Lisỳ, Christopher Kiekintveld, Branislav Bošanskỳ, and Michal Pechoucek. 2012. Game theoretic model of strategic honeypot selection in computer networks. *Decision and Game Theory for Security* 7638 (2012), 201–220.

[24] Aaron Schlenker, Haifeng Xu, Mina Guirguis, Chris Kiekintveld, Arunesh Sinha, Milind Tambe, Solomon Sonya, Darryl Balderas, and Noah Dunstatter. 2017. Don't Bury your Head in Warnings: A Game-Theoretic Approach for Intelligent Allocation of Cyber-security Alerts. (2017).

[25] Edoardo Serra, Sushil Jajodia, Andrea Pugliese, Antonino Rullo, and VS Subrahmanian. 2015. Pareto-optimal adversarial defense of enterprise systems. *ACM Transactions on Information and System Security (TISSEC)* 17, 3 (2015), 11.

[26] Milind Tambe. 2011. *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge University Press.