Game Theory Meets Network Security

A Tutorial

Quanyan Zhu
New York University
Brooklyn, New York
qz494@nyu.edu

Stefan Rass
Universitaet Klagenfurt
Klagenfurt, Austria
stefan.rass@aau.at

ABSTRACT

The increasingly pervasive connectivity of today's information systems brings up new challenges to security. Traditional security has accomplished a long way toward protecting well-defined goals such as confidentiality, integrity, availability, and authenticity. However, with the growing sophistication of the attacks and the complexity of the system, the protection using traditional methods could be cost-prohibitive. A new perspective and a new theoretical foundation are needed to understand security from a strategic and decision-making perspective. Game theory provides a natural framework to capture the adversarial and defensive interactions between an attacker and a defender. It provides a quantitative assessment of security, prediction of security outcomes, and a mechanism design tool that can enable security-by-design and reverse the attacker's advantage. This tutorial provides an overview of diverse methodologies from game theory that includes games of incomplete information, dynamic games, mechanism design theory to offer a modern theoretic underpinning of a science of cybersecurity. The tutorial will also discuss open problems and research challenges that the CCS community can address and contribute with an objective to build a multidisciplinary bridge between cybersecurity, economics, game and decision theory.

CCS CONCEPTS

• **Security and privacy → Network security**; • **Mathematics of computing**; • **Theory of computation → Algorithmic game theory and mechanism design**;

KEYWORDS

Game theory, Network security, Defense strategy, Mechanism design, Decision theory, Security economics

ACM Reference Format:
Quanyan Zhu and Stefan Rass. 2018. Game Theory Meets Network Security: A Tutorial. In *CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security Oct. 15–19, 2018, Toronto, ON, Canada,* Jennifer B. Sartor, Theo D'Hondt, and Wolfgang De Meuter (Eds.). ACM, New York, NY, USA, Article 4, 3 pages. https://doi.org/10.1145/3243734.3264421

CCS '18, October 15–19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5693-0/18/10.
https://doi.org/10.1145/3243734.3264421

1 TUTORIAL DESCRIPTION

Contemporary information and communication technology evolves fast not only in terms of the level of sophistication but also regarding its diversity. The increasing complexity, pervasiveness, and connectivity of today's information systems brings up new challenges to security, and the cyberspace has become a playground for people with all levels of skills and all kinds of intention (positive and negative). With 24/7 connectivity having become an integral part of people's daily life, protecting information, identities, and assets has gained more importance than ever. Traditional security has accomplished a long way toward protecting well-defined goals such as confidentiality, integrity, availability, and authenticity (CIA+). Cryptography is a solid theoretic foundation for security which relies on the secrecy of cryptographic keys. However, for attackers who can steal full cryptographic keys as in advanced persistent threats (APTs) or social engineering attacks, the assumption of key secrecy fails, and they can penetrate the system. A new perspective and a new theoretical foundation are needed to capture scenarios where an attacker can completely compromise a system, and a defender aims to protect the system without the assumption of key secrecy.

Game-theoretic models are natural frameworks to capture the adversarial and defensive interactions between players [9, 14, 15, 20, 21, 30, 42, 48, 53, 59]. Game theory can provide a quantitative measure of the quality of protection with the concept of Nash equilibrium where both defender and an attacker seek optimal strategies, and no one has an incentive to deviate unilaterally from their equilibrium strategies despite their conflict for security objectives. The equilibrium concept also provides a quantitative prediction of the security outcomes of the scenario the game model captures. With the quantitative measures of security, game theory makes security manageable beyond the strong qualitative assurances of cryptographic protections. Extending this approach to mechanism design provides system designers freedom to shift the equilibrium and the predicted outcomes toward ones that are favored by the defender or the system designer via an elaborate design of the game structure.

For more than a decade now, the interest in the field has proliferated, and game- and decision theory has become a systematic and well proven powerful theoretic underpinning of today's security research. Somewhat different from standard security definitions, game- and decision theory adopts a different and more economic viewpoint: security is not the absence of threats, but the point where attacking a system has become more expensive than not attacking. Starting from a game- and decision-theoretic root thus achieves the most elegant type of self-enforcing security, by analyzing and creating incentives to encourage actively honest behaviors rather than preventing maliciousness. At the same time, the economic

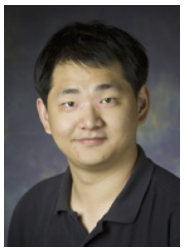
approach to security is also essential as it parallels the evolution of today's attackers. Cybercrime has grown into a full-featured economy, maintaining black markets, supply chains, and widely resembling an illegal counterpart of the of the official software market. Traditional security remains an important foundation to tackle the issue from below, but game- and decision theory offers a top-down view by adopting the economic and strategic view of the attackers too, and as such complements purely technological security means. The optimum is achieved when both routes are taken towards meeting in the middle, which is what game and decision theory aims to achieve.

The objective of this tutorial is to introduce diverse methodologies from game theory that include mechanism design, incentive analysis, decision-making under incomplete information, and dynamic games to provide solid underpinnings of a science of cybersecurity. The tutorial will be organized to connect different classes of games with different sets of security problems. For example (1) Stackelberg and multi-layer games for proactive defense [8, 26, 44, 46–48, 52, 56, 58], (2) network games for cyber-physical security that deals with critical infrastructure protection and information assurance [3, 15, 21, 32–36], (3) dynamic games for adaptive defense for network security [9, 16, 17, 24, 42, 43, 54, 55, 57], and (4) mechanism design theory for economics of network security that investigates resource allocation methodologies [2, 5, 11, 13, 37, 40, 49–51].

From the perspective of cybersecurity, the topics of this tutorial will cover recent applications of game theory to several emerging topics such as cross-layer cyber-physical security [6, 21, 29, 35, 45, 53], cyber deception [14, 22, 23, 25, 42, 59], moving target defense [18, 19, 44], critical infrastructure protection [3, 4, 12, 15, 16, 28, 30], adversarial machine learning [26, 27, 31, 38, 39], insider threats [1, 2], and cyber risk management [7, 10, 13, 41]. The tutorial will also discuss open problems and research challenges that the CCS community can address and contribute. With the objective to build a multidisciplinary bridge between cybersecurity, economics, game and decision theory, this tutorial will review basic concepts and provide an overview of recent advances in the field to CCS community with the hope to establish a community interest in the science of security and cross-disciplinary researches.

The potential audience includes researchers from academia and industry, including PhD and graduate students. Some background in network security and knowledge of basic optimization and data science is helpful but not necessary. The tutorial takes 1.5 hours.

2 AUTHOR BIOGRAPHY



Quanyan Zhu received B. Eng. in Honors Electrical Engineering from McGill University in 2006, M.A.Sc. from University of Toronto in 2008, and Ph.D. from the University of Illinois at Urbana-Champaign (UIUC) in 2013. After stints at Princeton University, he is currently an assistant professor at the Department of Electrical and Computer Engineering, New York University. He is a recipient of many awards including NSERC Canada Graduate Scholarship (CGS), Mavis Future Faculty Fellowships, and NSERC Postdoctoral Fellowship (PDF). He spearheaded and chaired INFOCOM Workshop on Communications and Control on Smart Energy Systems (CCSES), and Midwest Workshop on Control and Game Theory (WCGT). His current research interests include resilient and secure interdependent critical infrastructures, energy systems, cyber-physical systems, and cyber-enabled sustainability. He is a recipient of best paper awards at 5th International Conference on Resilient Control Systems, and 18th International Conference on Information Fusion. He has served as the general chair of the 7th Conference on Decision and Game Theory for Security (GameSec) in 2016 and International Conference on NETwork Games, COntrol and OPtimisation (NETGCOOP) in 2018. Website: http://wp.nyu.edu/quanyan

Stefan Rass graduated with a double master degree in mathematics and computer science from the Universitaet Klagenfurt in 2005. He received a PhD degree in mathematics in 2009, and habilitated on applied computer science and system security in 2014. His research interests cover decision theory and game-theory with applications in system security, as well as complexity theory, statistics and information-theoretic security. He authored numerous papers related to security and applied statistics and decision theory in security. He (co-authored) the book "Cryptography for Security and Privacy in Cloud Computing", published by Artech House, and edited the Birkhäuser Book "Game Theory for Security and Risk Management: From Theory to Practice" in the series on Static & Dynamic Game Theory: Foundations & Applications. He participated in various nationally and internationally funded research projects, as well as being a contributing researcher in many EU projects and offering consultancy services to the industry. Currently, he is an associate professor at the AAU, teaching courses on algorithms and data structures, theoretical computer science, complexity theory, security and cryptography. Website: https://www.syssec.at/en/team/rass

REFERENCES

[1] Casey, W., Morales, J. A., Wright, E., Zhu, Q., and Mishra, B. Compliance signaling games: toward modeling the deterrence of insider threats. *Computational and Mathematical Organization Theory 22*, 3 (2016), 318–349.

[2] Casey, W. A., Zhu, Q., Morales, J. A., and Mishra, B. Compliance control: Managed vulnerability surface in social-technological systems via signaling games. In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats* (2015), ACM, pp. 53–62.

[3] Chen, J., Touati, C., and Zhu, Q. A dynamic game analysis and design of infrastructure network protection and recovery. *ACM SIGMETRICS Performance Evaluation Review 45*, 2 (2017), 128.

[4] Chen, J., and Zhu, Q. Interdependent network formation games with an application to critical infrastructures. In *American Control Conference (ACC), 2016* (2016), IEEE, pp. 2870–2875.

[5] Chen, J., and Zhu, Q. Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach. *IEEE Transactions on Information Forensics and Security* (2017).

[6] Chen, J., and Zhu, Q. Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach. *IEEE Transactions on Information Forensics and Security 12*, 11 (2017), 2736–2750.

[7] Chen, J., and Zhu, Q. Security investment under cognitive constraints: A gestalt nash equilibrium approach. In *Information Sciences and Systems (CISS), 2018 52nd Annual Conference on* (2018), IEEE, pp. 1–6.

[8] Clark, A., Zhu, Q., Poovendran, R., and Başar, T. Deceptive routing in relay networks. In *Decision and Game Theory for Security*. Springer, 2012, pp. 171–185.

[9] Farhang, S., Manshaei, M. H., Esfahani, M. N., and Zhu, Q. A dynamic bayesian security game framework for strategic defense mechanism design. In *Decision and Game Theory for Security*. Springer, 2014, pp. 319–328.

[10] Fung, C. J., and Zhu, Q. Facid: A trust-based collaborative decision framework for intrusion detection networks. *Ad Hoc Networks 53* (2016), 17–31.

[11] Hayel, Y., and Zhu, Q. Attack-aware cyber insurance for risk sharing in computer networks. In *Decision and Game Theory for Security*. Springer, 2015, pp. 22–34.

[12] Hayel, Y., and Zhu, Q. Resilient and secure network design for cyber attack-induced cascading link failures in critical infrastructures. In *Information Sciences and Systems (CISS), 2015 49th Annual Conference on* (2015), IEEE, pp. 1–3.

[13] Hayel, Y., and Zhu, Q. Epidemic protection over heterogeneous networks using evolutionary poisson games. *IEEE Transactions on Information Forensics and Security 12*, 8 (2017), 1786–1800.

[14] Horák, K., Zhu, Q., and Bošanskỳ, B. Manipulating adversary?s belief: A dynamic game approach to deception by design for proactive network security. In *International Conference on Decision and Game Theory for Security* (2017), Springer, pp. 273–294.

[15] Huang, L., Chen, J., and Zhu, Q. A large-scale markov game approach to dynamic protection of interdependent infrastructure networks. In *International Conference on Decision and Game Theory for Security* (2017), Springer, pp. 357–376.

[16] Huang, L., and Zhu, Q. Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks. In *ACM SIGMETRICS Performance Evaluation Review* (2018).

[17] Huang, L., and Zhu, Q. Analysis and computation of adaptive defense strategies against advanced persistent threats for cyber-physical systems. In *International Conference on Decision and Game Theory for Security* (2018).

[18] Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., and Wang, X. S. *Moving target defense: creating asymmetric uncertainty for cyber threats*, vol. 54. Springer Science & Business Media, 2011.

[19] Maleki, H., Valizadeh, S., Koch, W., Bestavros, A., and van Dijk, M. Markov modeling of moving target defense games. In *Proceedings of the 2016 ACM Workshop on Moving Target Defense* (2016), ACM, pp. 81–92.

[20] Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR) 45*, 3 (2013), 25.

[21] Miao, F., Zhu, Q., Pajic, M., and Pappas, G. J. A hybrid stochastic game for secure control of cyber-physical systems. *Automatica 93* (2018), 55–63.

[22] Pawlick, J., Colbert, E., and Zhu, Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *arXiv preprint arXiv:1712.05441* (2017).

[23] Pawlick, J., Colbert, E., and Zhu, Q. Modeling and analysis of leaky deception using signaling games with evidence. *arXiv preprint arXiv:1804.06831* (2018).

[24] Pawlick, J., Farhang, S., and Zhu, Q. Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats. In *Decision and Game Theory for Security*. Springer, 2015, pp. 289–308.

[25] Pawlick, J., and Zhu, Q. Deception by design: evidence-based signaling games for network defense. *arXiv preprint arXiv:1503.05458* (2015).

[26] Pawlick, J., and Zhu, Q. A Stackelberg game perspective on the conflict between machine learning and data obfuscation. In *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on* (2016), IEEE, pp. 1–6.

[27] Pawlick, J., and Zhu, Q. A Mean-Field Stackelberg Game Approach for Obfuscation Adoption in Empirical Risk Minimization. *arXiv preprint arXiv:1706.02693* (2017).

[28] Pawlick, J., and Zhu, Q. Proactive defense against physical denial of service attacks using poisson signaling games. In *International Conference on Decision and Game Theory for Security* (2017), Springer, pp. 336–356.

[29] Pawlick, J., and Zhu, Q. Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. *IEEE Transactions on Information Forensics and Security 12*, 12 (2017), 2906–2919.

[30] Rass, S., Alshawish, A., Abid, M. A., Schauer, S., Zhu, Q., and De Meer, H. Physical intrusion games–optimizing surveillance by simulation and game theory. *IEEE Access 5* (2017), 8394–8407.

[31] Wang, W., and Zhu, Q. On the detection of adversarial attacks against deep neural networks. In *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense* (2017), ACM, pp. 27–30.

[32] Xu, Z., and Zhu, Q. A cyber-physical game framework for secure and resilient multi-agent autonomous systems. In *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on* (2015), IEEE, pp. 5156–5161.

[33] Xu, Z., and Zhu, Q. Cross-layer secure cyber-physical control system design for networked 3d printers. In *American Control Conference (ACC), 2016* (2016), IEEE, pp. 1191–1196.

[34] Xu, Z., and Zhu, Q. A Game-Theoretic Approach to Secure Control of Communication-Based Train Control Systems Under Jamming Attacks. In *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles* (2017), ACM, pp. 27–34.

[35] Xu, Z., and Zhu, Q. Secure and practical output feedback control for cloud-enabled cyber-physical systems. In *Communications and Network Security (CNS), 2017 IEEE Conference on* (2017), IEEE, pp. 416–420.

[36] Yuan, Y., Zhu, Q., Sun, F., Wang, Q., and Basar, T. Resilient control of cyber-physical systems against denial-of-service attacks. In *Resilient Control Systems (ISRCS), 2013 6th International Symposium on* (2013), IEEE, pp. 54–59.

[37] Zhang, R., and Zhu, Q. Attack-Aware Cyber Insurance of Interdependent Computer Networks.

[38] Zhang, R., and Zhu, Q. A game-theoretic defense against data poisoning attacks in distributed support vector machines. In *Decision and Control (CDC), 2017 IEEE 56th Annual Conference on* (2017), IEEE, pp. 4582–4587.

[39] Zhang, R., and Zhu, Q. A game-theoretic approach to design secure and resilient distributed support vector machines. *IEEE Transactions on Neural Networks and Learning Systems* (2018).

[40] Zhang, R., Zhu, Q., and Hayel, Y. A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks. *IEEE Journal on Selected Areas in Communications 35*, 3 (2017), 779–794.

[41] Zhang, R., Zhu, Q., and Hayel, Y. A bi-level game approach to attack-aware cyber insurance of computer networks. *IEEE Journal on Selected Areas in Communications 35*, 3 (2017), 779–794.

[42] Zhang, T., and Zhu, Q. Strategic defense against deceptive civilian gps spoofing of unmanned aerial vehicles. In *International Conference on Decision and Game Theory for Security* (2017), Springer, pp. 213–233.

[43] Zhu, Q., and Başar, T. Dynamic policy-based ids configuration. In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on* (2009), IEEE, pp. 8600–8605.

[44] Zhu, Q., and Başar, T. Game-theoretic approach to feedback-driven multi-stage moving target defense. In *International Conference on Decision and Game Theory for Security* (2013), Springer, pp. 246–263.

[45] Zhu, Q., and Basar, T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. *Control Systems, IEEE 35*, 1 (2015), 46–65.

[46] Zhu, Q., Bushnell, L., and Basar, T. Game-theoretic analysis of node capture and cloning attack with multiple attackers in wireless sensor networks. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on* (2012), IEEE, pp. 3404–3411.

[47] Zhu, Q., Clark, A., Poovendran, R., and Basar, T. Deceptive routing games. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on* (2012), IEEE, pp. 2704–2711.

[48] Zhu, Q., Clark, A., Poovendran, R., and Basar, T. Deployment and exploitation of deceptive honeybots in social networks. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on* (2013), IEEE, pp. 212–219.

[49] Zhu, Q., Fung, C., Boutaba, R., and Başar, T. A game-theoretical approach to incentive design in collaborative intrusion detection networks. In *Game Theory for Networks, 2009. GameNets' 09. International Conference on* (2009), IEEE, pp. 384–392.

[50] Zhu, Q., Fung, C., Boutaba, R., and Başar, T. Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks. *Selected Areas in Communications, IEEE Journal on 30*, 11 (2012), 2220–2230.

[51] Zhu, Q., Gunter, C. A., and Basar, T. Tragedy of anticommons in digital right management of medical records. In *HealthSec* (2012).

[52] Zhu, Q., Li, H., Han, Z., and Basar, T. A stochastic game model for jamming in multi-channel cognitive radio systems. In *ICC* (2010), pp. 1–6.

[53] Zhu, Q., and Rass, S. On multi-phase and multi-stage game-theoretic modeling of advanced persistent threats. *IEEE Access 6* (2018), 13958–13971.

[54] Zhu, Q., Tembine, H., and Başar, T. Heterogeneous learning in zero-sum stochastic games with incomplete information. In *Decision and Control (CDC), 2010 49th IEEE Conference on* (2010), IEEE, pp. 219–224.

[55] Zhu, Q., Tembine, H., and Basar, T. Network security configurations: A nonzero-sum stochastic game approach. In *American Control Conference (ACC), 2010* (2010), IEEE, pp. 1059–1064.

[56] Zhu, Q., Tembine, H., and Basar, T. Hybrid learning in stochastic games and its applications in network security. *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control* (2013), 305–329.

[57] Zhu, Q., Yuan, Z., Song, J. B., Han, Z., and Basar, T. Dynamic interference minimization routing game for on-demand cognitive pilot channel. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* (2010), IEEE, pp. 1–6.

[58] Zhu, Q., Yuan, Z., Song, J. B., Han, Z., and Başar, T. Interference aware routing game for cognitive radio multi-hop networks. *Selected Areas in Communications, IEEE Journal on 30*, 10 (2012), 2006–2015.

[59] Zhuang, J., Bier, V. M., and Alagoz, O. Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *European Journal of Operational Research 203*, 2 (2010), 409–418.