Information Systems Frontiers (2021) 23:263–267
https://doi.org/10.1007/s10796-021-10134-8

Seeking Foundations for the Science of Cyber Security

Editorial for Special Issue of Information Systems Frontiers

Shouhuai Xu[1] · Moti Yung[2] · Jingguo Wang[3]

Accepted: 31 March 2021 / Published online: 28 April 2021

1 Introduction

Cyber security (or cybersecurity) has become a fundamental issue which deeply affects citizen's lives (including their privacy), the public's economic prosperity, and national security. The high frequency of media reports on high-profile cyber attacks, which cause substantial and, at times, catastrophic damages, highlights that cyberspace is a very fragile and vulnerable ecosystem, and that our understanding of cybersecurity and our capability of defending cyberspace are far from adequate. This is true despite the numerous advancements and breakthroughs in some fields of cybersecurity. One outstanding example is cryptography, which has been built on a firm foundation in Computational Complexity Theory, starting with a number of breakthroughs, e.g. Diffie and Hellman (1976), Rivest et al. (1978), Goldwasser and Micali (1982), and Yao (1982). However, there are many cyber attacks that go beyond the standard cryptographic threats models, such as attacks which can compromise cryptographic private keys by directly stealing memory pages (e.g., Harrison and Xu (2007)), or indirectly exploiting side-channel attacks (e.g., Kocher (1996)). The state-of-the-art is that we are far from being capable of adequately dealing with such attacks in practice, as discussed in Xu and Yung (2009). Indeed, it would be fair to say, cybersecurity as a whole is still an art, partially because its many aspects (e.g., defense operations) are largely heuristics without scientific rigor.

It is interesting to note that the importance of putting cybersecurity on firm foundations were not widely recognized until perhaps the 2008 Science of Security Workshop (https://cps-vo.org/group/SoS/). This event has triggered a number of explorations, including: Schneider (2011), Kott (2014), Xu (2014a), Xu (2014b), Xu (2019), Xu (2020), Roque et al. (2016), Herley and van Oorschot (2017), and Spring et al. (2017). These endeavors suggest that it is far from clear in terms of what would be the foundations for the Science of Cyber Security. This is not surprising because cyber security turns out to be an extremely difficult problem, owing to many factors, such as: (i) the *scale* of cyberspace, where billions of devices are interconnected and must be considered holistically; (ii) the *complexity* of cyberspace in terms of the interdependence and interactions among its *cyber-physical-human* components; (iii) the *adversarial intelligence* that attackers possess as skilled human beings which is on par with defenders; (iv) the *asymmetry* between attackers who only need to identify and exploit a single vulnerability, and defenders who must seek to prevent or block each and every vulnerability; (v) the difficulty in *quantifying* cybersecurity from a whole-system (rather than building-blocks) perspective; and (vi) the multidisciplinary nature of cybersecurity, technologically speaking, and especially the involvement of human beings as users, attackers, and defenders.

The above discussion suggests that it must take an extensive community wide effort to investigate the foundations for the Science of Cyber Security. This motivated the creation of the new series of International Conference on Science of Cyber Security (SciSec) in 2018. The mission of SciSec is to catalyze and foster such a research community. SciSec focuses on a unique set of topics. As shown in the Call For Papers of SciSec (cf. https://scisec.org), the topics of interest include, but are not limited to, the

✉ Shouhuai Xu
sxu@uccs.edu

Moti Yung
moti@cs.columbia.edu

Jingguo Wang
jwang@uta.edu

[1] Department of Computer Science, University of Colorado Colorado Springs, Colorado Springs, CO, USA

[2] Google and Department of Computer Science, Columbia University, New York, NY, USA

[3] Department of Information Systems, University of Texas at Arlington, Arlington, TX, USA

following: "(1) cybersecurity dynamics; (2) cybersecurity metrics and measurements; (3) first-principle cybersecurity modeling and analysis; (4) cybersecurity data analytics; (5) quantitative risk management for cybersecurity; (6) big data for cybersecurity; (7) artificial intelligence and machine learning to cybersecurity; (8) economics approaches to cybersecurity; (9) social sciences approaches to cybersecurity; (10) statistical physics approaches to cybersecurity; (11) complexity sciences approaches to cybersecurity; (12) experimental cybersecurity; (13) macroscopic cybersecurity; (14) statistics approaches to cybersecurity; (15) human factors for cybersecurity; (16) compositional security; (17) biology-inspired approaches to cybersecurity; (18) synergetics approaches to cybersecurity."

2 The Special Issue

The present special issue consists of four invited papers whose earlier versions were presented at The Second International Conference on Science of Cyber Security (SciSec'2019). All these papers contain significant extensions based on the feedback received at the conference, and went through two rounds of independent reviews per the criteria of the Information Systems Frontier journal. These papers fall into three topics of SciSec, namely *experimental cybersecurity* or more specifically deceptive cyber defense, *cybersecurity data analytics*, and *human factors in cybersecurity* or more specifically game-theoretic modeling of human behavior.

Deceptive cyber defense is an important approach to cyber security which is little understood. The paper by Huang et al. (2021), entitled "HoneyGadget: A Deception Based Approach for Detecting Code Reuse Attacks," advances the state-of-the-art in deceptive cyber defense, by proposing and evaluating a new deception mechanism that aims at actively detecting ongoing code reuse attacks.

Cybersecurity data analytics aims at leveraging real-world data to deepen our understanding of attacks, and helping achieve more effective cyber defense. The paper by Xia et al. (2021), entitled "LogGAN: a Log-level Generative Adversarial Network for Anomaly Detection using Permutation Event Modeling," proposes a cutting-edge Generative Adversarial Network (GAN) method in systems anomaly detection. The paper by Roy and Chen (2021), entitled "DeepRan: Attention-based BiLSTM and CRF for Ransomware Early Detection and Classification," pushes the frontier in ransomware detection, by leveraging deep learning techniques.

Game-theoretic modeling of cyber security, including human behavior, is an active research topic. The paper by Xue et al. (2021), entitled "Incentive Mechanism for Rational Miners in Bitcoin Mining Pool," presents a novel game-theoretic model of user behaviors in the Bitcoin network, more specifically it covers designing incentive mechanism design for Bitcoin miners and analyzing their properties.

3 Future Research

There are many open problems that are yet to be tackled. We next highlight a few of them.

First, corresponding to the aforementioned *scale* of cyberspace, we immediately encounter the scalability barrier, which is fundamentally related to the *state-space explosion* problem as discussed in Xu (2014a), Xu (2019), and Xu (2020). While there have been some significant progress in this regard (e.g., Xu et al. (2015b), Zheng et al. (2015), Zheng et al. (2018), Lin et al. (2019), and Han et al. (2020)), there are many problems that are yet to be addressed (cf. Xu (2020)).

Second, corresponding to the aforementioned *complexity* of cyberspace in terms of the interdependence and interactions among its cyber-physical-human components, we encounter the challenges of *high nonlinearity*, as shown in Xu et al. (2012), Xu et al. (2014), Zheng et al. (2018), and Lin et al. (2019), and *dependence* between random variables and stochastic processes (or time series), as shown in Xu and Xu (2012), Da et al. (2014), Xu et al. (2015a), and Fang et al. (2021). One outstanding research problem is to model and characterize coordinated defense against coordinated attacks (cf. Xu (2008)). Another outstanding research problem is to model and characterize large-scale adaptive and proactive defenses against adaptive attacks. Yet another outstanding open problem is to understand and manage the *transient* behavior in the evolution of cybersecurity state of (say) enterprise networks. This is important because, often, mathematical tools can only characterize *asymptotic* (e.g., equilibrium) behaviors. While important for sure, it is imperative to understand the transient behaviors, which often have to be dealt with using data-driven approaches, highlighting the importance of cybersecurity data analytics (e.g., Zhan et al. (2013), Zhan et al. (2015), Chen et al. (2015), Xu et al. (2017), Peng et al. (2017), Xu et al. (2018), Fang et al. (2019), and Fang et al. (2021)).

Third, corresponding to the aforementioned *adversarial intelligence* that attackers are as skilled human beings as defenders, we encounter a range of challenges, including adversarial evasion attacks against malware detectors, *uncertainty* of models and parameters, the absence of data label ground truth (when applicable), the availability of partial (rather than full) information, and the treatment of cyber attacker/defender human factors (including their cognitive capabilities). There are some initial efforts towards ultimately tackling these problems (e.g., Li et al.

(2020), Li et al. (2021a), Du et al. (2018), and Rodriguez et al. (2020)).

Fourth, corresponding to the aforementioned *asymmetry* that inherently benefits the attacker, researchers have been studying how to detect software vulnerabilities so as to hopefully patch them before they are discovered by attackers (e.g., Li et al. (2018), Li et al. (2021c), Zou et al. (2019), and Li et al. (2021d)). However, many problems remain open, including the explainability and robustness of such detectors against adversarial attackers (cf. Zou et al. (2021) and Li et al. (2021b)).

Fifth, corresponding to the aforementioned difficulty in *quantifying* cyber security from a whole-system perspective, the research community must tackle the barriers of cyber security trustworthiness metrics, broadly defined to include security metrics, resilience metrics, and agility metrics (cf. Pendleton et al. (2016) and Cho et al. (2019)) and their measurements. There are a sequence of ongoing research activities in this regard (e.g., Li et al. (2011), Xu and Xu (2012), Han et al. (2014), Wang et al. (2015), Chen et al. (2018a), Chen et al. (2018b), Mireles et al. (2019), and Liu et al. (2021)).

Sixth, corresponding to the aforementioned multidisciplinary nature of cyber security, we observe that Science of Cyber Security would demand the research community to understand not only the security properties and behavior of information technologies, but also their ripple effects on individuals, organizations, and the society (e.g., Wang et al. (2019)). This multidisciplinary nature, naturally calls for international collaborations, which motivated the creation of the new conference series of SciSec. One problem of particular interest is: Which discipline can contribute to solve what kinds of concrete cyber security problems that may not be solved by other disciplines? Answering this question will likely lead to *holistic* and *end-to-end* cyber defense solutions.

With this special issue, we hope that more researchers will find, both, the emerging field of Science of Cyber Security and the SciSec Conference interesting, and more importantly, raise their passion and engagement in elevating the art of cybersecurity to a science, which cannot be achieved without a concert community effort. We look forward to seeing a community working together.

Acknowledgements We sincerely thank the authors who submitted their papers to SciSec'2019 and to this special issue, the Program Committee of SciSec'2019 for selecting papers for its Proceedings, the Organization Committee of SciSec'2019 for making the conference successful, and the reviewers for this special issue.

References

Chen, H., Cho, J., Xu, S. (2018a). Quantifying the security effectiveness of firewalls and dmzs. In *Proc. HoTSoS'2018* (pp. 9:1–9:11).

Chen, H., Cho, J., Xu, S. (2018b). Quantifying the security effectiveness of network diversity. In *Proc. hoTSos'2018* (p. 24:1).

Chen, Y., Huang, Z., Xu, S., Lai, Y. (2015). Spatiotemporal patterns and predictability of cyberattacks. *PLoS One*, *10*(5), e0124, 472.

Cho, J., Xu, S., Hurley, P., Mackay, M., Benjamin, T., Beaumont, M. (2019). Stram: Measuring the trustworthiness of computer-based systems. *ACM Comput Surv*, *51*(6), 128:1–128:47.

Da, G., Xu, M., Xu, S. (2014). A new approach to modeling and analyzing security of networked systems. In *Proc. HotSoS'14* (pp. 6:1–6:12).

Diffie, W., & Hellman, M.E. (1976). New directions in cryptography. *IEEE TransInformTheory IT-22*, 644–654.

Du, P., Sun, Z., Chen, H., Cho, J.H., Xu, S. (2018). Statistical estimation of malware detection metrics in the absence of ground truth. *IEEE T-IFS*, *13*(12), 2965–2980.

Fang, X., Xu, M., Xu, S., Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *EURASIP J Information Security*, *2019*, 5.

Fang, Z., Xu, M., Xu, S., Hu, T. (2021). A framework for predicting data breach risk: Leveraging dependence to cope with sparsity. *IEEE Trans Inf Forensics Secur*, *16*, 2186–2201.

Goldwasser, S., & Micali, S. (1982). Probabilistic encryption and how to play mental poker keeping secret all partial information. In *ACM STOC* (pp. 365–377).

Han, Y., Lu, W., Xu, S. (2014). Characterizing the power of moving target defense via cyber epidemic dynamics. In *HotSoS* (pp. 1–12).

Han, Y., Lu, W., Xu, S. (2020). Preventive and reactive cyber defense dynamics with ergodic time-dependent parameters is globally attractive. arXiv:2001.07958.

Harrison, K., & Xu, S. (2007). Protecting cryptographic keys from memory disclosures. In *IEEE/IFIP DSN'07* (pp. 137–143).

Herley, C., & van Oorschot, P.C. (2017). Sok: Science, security and the elusive goal of security as a scientific pursuit. In *2017 IEEE symposium on security and privacy (SP)* (pp. 99–120).

Huang, X., Yan, F., Zhang, L. (2021). Honeygadget: A deception based approach for detecting code reuse attacks. *Information Systems Frontiers*, *23*(2). https://doi.org/10.1007/s10796-020-10014-7.

Kocher, P. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Proc. CRYPTO 96, Springer-Verlag, pp 104–113, lNCS 1109*.

Kott, A. (2014). *Towards fundamental science of cyber security*, (pp. 1–13). New York: Springer.

Li, D., Li, Q., Ye, Y., Xu, S. (2020). Sok: Arms race in adversarial malware detection. arXiv:2005.11671.

Li, D., Li, Q., Ye, Y., Xu, S. (2021a). A frameowrk for enhancing deep neural networks against adversarial malware examples. *IEEE Transactions on Network Science and Engineering (TNSE)*, *8*, 736–750.

Li, X., Parker, P., Xu, S. (2011). A stochastic model for quantitative security analyses of networked systems. *IEEE Transactions on Dependable and Secure Computing*, *8*(1), 28–43.

Li, Z., Zou, D., Xu, S., Ou, X., Jin, H., Wang, S., Deng, Z., Zhong, Y. (2018). Vuldeepecker: A deep learning-based system for vulnerability detection. In: *Proc. NDSS'18*.

Li, Z., Tang, J., Zou, D., Chen, Q., Xu, S., Zhang, C., Li, Y., Jin, H. (2021b). Robustness of deep learning-based vulnerability detectors: Attack anddefense. under review.

Li, Z., Zou, D., Xu, S., Jin, H., Zhu, Y., Chen, Z., Wang, S., Wang, J. (2021c). Sysevr: A framework for using deep learning to detect software vulnerabilities. IEEE Transactions on Dependable and Secure Computing (accepted for publication).

Li, Z., Zou, D., Xu, S., Jin, H., Zhu, Y., Zhang, Z., Chen, Z., Li, D. (2021d). Vuldeelocator: A deep learning-based system for detecting and locating software vulnerabilities. Under review.

Lin, Z., Lu, W., Xu, S. (2019). Unified preventive and reactive cyber defense dynamics is still globally convergent. *IEEE/ACM Trans Netw*, *27*(3), 1098–1111.

Liu, Z., Zheng, R., Lu, W., Xu, S. (2021). Using event-based method to estimate cybersecurity equilibrium. *IEEE CAA J Autom Sinica*, *8*(2), 455–467.

Mireles, J., Ficke, E., Cho, J., Hurley, P., Xu, S. (2019). Metrics towards measuring cyber agility. *IEEE T-IFS*, *14*(12), 3217–3232.

Pendleton, M., Garcia-Lebron, R., Cho, J., Xu, S. (2016). A survey on systems security metrics. *ACM Comput Surv*, *49*(4), 62:1–62:35.

Peng, C., Xu, M., Xu, S., Hu, T. (2017). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, *44*(14), 2534–2563.

Rivest, R., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Rodriguez, R.M., Golob, E., Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. CoRR (to appear in Frontiers in Psychology-Cognition). arXiv:2007.04932.

Roque, A., Bush, K., Degni, C. (2016). Security is about control: insights from cybernetics. In *Proc. HotSoS* (pp. 17–24).

Roy, K.C., & Chen, Q. (2021). Deepran: Attention-based bilstm and crf for ransomware early detection and classification. *Information Systems Frontiers*, *23*(2). https://doi.org/10.1007/s10796-020-10017-4.

Schneider, F. (2011). Blueprint for a science of cybersecurity. Tech. rep. Cornell University.

Spring, J., Moore, T., Pym, D. (2017). Practicing a science of security: A philosophy of science perspective. In *Proc. NSPW* (pp. 1–18).

Wang, J., Gupta, M., Rao, H.R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91–112.

Wang, J., Shan, Z., Gupta, M., Rao, H.R. (2019). A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts. *MIS Quarterly, 43*(2).

Xia, B., Bai, Y., Yin, J., Li, Y., Xu, J. (2021). Loggan: a log-level generative adversarial network for anomaly detection using permutation event modeling. *Information Systems Frontiers*, *23*(2). https://doi.org/10.1007/s10796-020-10026-3.

Xu, M., & Xu, S. (2012). An extended stochastic model for quantitative security analysis of networked systems. *Internet Mathematics*, *8*(3), 288–320.

Xu, M., Da, G., Xu, S. (2015a). Cyber epidemic models with dependences. *Internet Mathematics*, *11*(1), 62–92.

Xu, M., Hua, L., Xu, S. (2017). A vine copula model for predicting the effectiveness of cyber defense early-warning. *Technometrics*, *59*(4), 508–520.

Xu, M., Schweitzer, K.M., Bateman, R.M., Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE T-IFS*, *13*(11), 2856–2871.

Xu, S. (2008). Collaborative attack vs. collaborative defense (pp. 217–228).

Xu, S. (2014a). Cybersecurity dynamics. In *Proc. HotSoS'14* (pp. 14:1–14:2).

Xu, S. (2014b). Emergent behavior in cybersecurity. In *Proc. HotSoS* (pp. 13:1–13:2).

Xu, S. (2019). Cybersecurity dynamics: A foundation for the science of cybersecurity. In *Proactive and dynamic network defense* (pp. 1–31).

Xu, S. (2020). The cybersecurity dynamics way of thinking and landscape (invited paper). In *ACM Workshop on Moving Target Defense*.

Xu, S., & Yung, M. (2009). Expecting the unexpected: Towards robust credential infrastructure. In *Financial Crypto* (pp. 201–221).

Xu, S., Lu, W., Xu, L. (2012). Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights. *ACM TAAS, 7*(3).

Xu, S., Lu, W., Xu, L., Zhan, Z. (2014). Adaptive epidemic dynamics in networks: Thresholds and control. *ACM TAAS, 8*(4).

Xu, S., Lu, W., Li, H. (2015b). A stochastic model of active cyber defense dynamics. *Internet Mathematics*, *11*(1), 23–61.

Xue, G., Xu, J., Wu, H., Lu, w., Xu, L. (2021). Incentive mechanism for rational miners in bitcoin mining pool. *Information Systems Frontiers*, *23*(2). https://doi.org/10.1007/s10796-020-10019-2.

Yao, A.C. (1982). Theory and application of trapdoor functions. In *Proc. 23rd IEEE Symp. on Foundations of Comp. Science* (pp. 80–91). Chicago: IEEE.

Zhan, Z., Xu, M., Xu, S. (2013). Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *IEEE T-IFS, 8*(11).

Zhan, Z., Xu, M., Xu, S. (2015). Predicting cyber attack rates with extreme values. *IEEE T-IFS*, *10*(8), 1666–1677.

Zheng, R., Lu, W., Xu, S. (2015). Active cyber defense dynamics exhibiting rich phenomena. In *Proc. HotSoS*.

Zheng, R., Lu, W., Xu, S. (2018). Preventive and reactive cyber defense dynamics is globally stable. *IEEE TNSE*, *5*(2), 156–170.

Zou, D., Wang, S., Xu, S., Li, Z., Jin, H. (2019). μvuldeepecker: A deep learning-based system for multiclass vulnerability detection. IEEE Transactions on Dependable and Secure Computing, pp 1–1. https://doi.org/10.1109/TDSC.2019.2942930.

Zou, D., Zhu, Y., Xu, S., Li, Z., Jin, H., Ye, H. (2021). Interpreting deep learning-based vulnerability detector predictions based on heuristic searching. *ACM Transactions on Software Engineering and Methodology, 30*(2).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Shouhuai Xu is the Gallogly Chair Professor in Cybersecurity, Department of Computer Science, University of Colorado, Colorado Springs (UCCS). Prior to joining UCCS, he was a Full Professor in the Department of Computer Science, University of Texas at San Antonio. He is the founding director of the Laboratory for Cybersecurity Dynamics (LCD). He pioneered the Cybersecurity Dynamics approach as foundation for the emerging science of cyber security, including: first-principle cybersecurity modeling and analysis (the x-axis); cybersecurity data analytics (the y-axis); and cybersecurity metrics (the z-axis). He co-initiated the International Conference on Science of Cyber Security and is serving as its Steering Committee Chair. His research has been supported by ARO, ARL, AFOSR, AFRL, NSF, and ONR. He has served a Program Committee co-chair of SciSec'2019, SciSec'2018, ICICS'18, NSS'15 and Inscrypt'13. He has been an Associate Editor of IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), IEEE Transactions on Information Forensics and Security (IEEE T-IFS), and IEEE Transactions on Network Science and Engineering (IEEE TNSE). He received a PhD degree in Computer Science from Fudan University. His website is at https://xu-lab.org.

Moti Yung is a Security and Privacy Research Scientist with Google, with main interests in Cryptography, Security, and Privacy. He graduated from Columbia University in 1988 and is an adjunct senior research faculty at Columbia till today. In parallel to Columbia he has had an industrial research career, working at places like IBM, RSA Labs. (EMC), Snap, and now Google. Yung is a fellow of ACM, IEEE, the International Association for Cryptologic Research (IACR), and the European Association for Theoretical Computer Science (EATCS). Among his awards are ACM's SIGSAC Outstanding Innovation Award in 2014, the 2018 IEEE Computer Society W. Wallace McDowell Award, and the 2021 IEEE Computer Society Women of ENIAC Computer Pioneer Award. His research covers broad areas: from the theory and foundations, to applied systems, and actual engineering efforts of cryptography, privacy, and secure systems. His website is at http://www.cs.columbia.edu/~moti/.

Jingguo Wang is a Professor of Information Systems, College of Business, University of Texas at Arlington (UTA). He earned his Ph.D. from University at Buffalo, State University of New York. His work has been published in the leading journals of Information Systems including MIS Quarterly, Information Systems Research, Journal of Management Information Systems, and Journal of the Association for Information Systems. His current research interests focus on information security, mostly investigating security behavior of end users and risk management practices of organizations. He has been serving as an associate editor of MIS Quarterly Special Issue on Information Systems Security in a Digital Economy. He is currently serving as a coordinating editor of Information Systems Frontier, an associate editor of The Journal of the Association for Information Systems, Information Systems Journal, Decision Support Systems, and on the editorial board of Journal of Database Management. He also served as an associate editor of ICIS track in Security and Privacy and track in Social Media and Digital Collaboration, a review coordinator of WITS, and a program co-chair of Dewald Roode Workshop (IFIP WG8.11/WG11.13). He has been on the Program Committees of a number of international conferences/ workshops, and a reviewer for various journals. His research has been supported by the National Science Foundation and the University of Texas at Arlington. His website is at https://blog.uta.edu/jingguo/.