CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

Request for Information on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan

Respondents:

- Matthew Wright (Matthew.Wright@rit.edu), Professor of Computing Security and Director of the Center for Cybersecurity
- S. Jay Yang (Jay.Yang@rit.edu), Professor and Chair of Computer Engineering

Center of Cybersecurity (http://cybersecurity.rit.edu/), Rochester Institute of Technology

1. What innovative, transformational technologies have the potential to greatly enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?

- **Anticipatory Cyber Defense**: trusted and explainable AI for predictive cyber situation awareness and threat forecasting [Fava08, Okutan18, Yang14].
- **Adaptive Infrastructure**: beginning with end-user systems, having adaptive components adds cost to adversary to deter attacks and to realize robust cyber defense.
- **Interdisciplinary Effects**: cross-disciplinary research is needed to understand human behavior, monetary effects, domestic and international policies, business operations, and technology invention/adoption on cybersecurity.
- **Operating on Encrypted Data**: This mentioned briefly in the 2016 Strategic Plan, but it is a potential game changer for both security and privacy. If individuals' data is only ever stored and processed in encrypted forms by third parties, then protections are much stronger than if data is in the clear [Hu17].
- **Wireless-based Authentication**: Many IoT devices lack the power for strong cryptographic authentication, but they have wireless connectivity that can be leveraged for authentication [Rahbari18].

4. What challenges or objectives not included in the 2016 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those capabilities and objectives should be strategic priorities.

Cyberattack Scenario Generation is a critical necessity to advance cybersecurity research and effective workforce development. In most other fields of study, practical examples are keys to generation of novel approaches, assessment of solutions, and basis for education. In cybersecurity, cyberattack scenarios, tactics, exploits, and behaviors change rapidly, and require sustainable generation and sharing of attack scenarios. Research work that leverage advances in, e.g., generative adversarial networks and simulation [Moskal18, Krall16] to generate cyberattack

scenarios with limited real-world data will be critical to the continuous advancement in cyber defense against evolving adversarial activities.

Measurement of Security Deployment. The 2016 Strategic Plan includes measurement of adversary effort, but much remains to be done to understand the extent and effectiveness of existing security deployments, such as DNSSEC [Chung17a,b], Certificate Authority Authorization (CAA) [Scheitle '18], or OCSP Stapling [Chung18]. Only be measuring and understanding these deployments can we know how what has gone right, what has gone wrong, and how to move forward more productively.

Wireless Security. The 2016 Strategic Plan addresses wireless very briefly, but this needs to be emphasized much more. A huge amount of traffic is now wireless, and this is increasing all the time. 5G is coming, which will open up more uses of wireless and constant high-speed connectivity. Even data centers are starting to go wireless. Not only is it critical to secure our wireless connections from jamming [Rahbari16, Krunz18] and eavesdropping [Rahbari15,17,18a], but wireless connections also offer new opportunities to add security [Rahbari18b].

Vehicular Security. With the coming of autonomous vehicles and the increases in vehicular interfaces and connectivity, addressing vehicular security should be upgraded to a first-class priority in the field of cybersecurity. The unique challenges of securing vehicles have not been clearly understood and addressed.

Traffic analysis is a major area that is not addressed in the 2016 Strategic Plan and should be added. As more and more of our networked communications become encrypted, attackers will shift to learning about our communications and activity patterns through traffic analysis techniques that exploit the metadata of our connections. For example, the websites you visit can reveal a lot about you -- religious interests, health issues, financial information and activity, romantic engagements, and more. Given that ISPs can gather and sell this kind of data [Fung17], more companies will be accessing it and storing it, potentially insecurely. Protections against this kind of metadata snooping and analysis are becoming increasingly more important, and we need to increase our understanding of existing protections (such as Tor) and their limitations.

5. *What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?*

The future cybersecurity workforce needs to be trained to have the ability to work alongside powerful AI technologies, with an emphasis on **critical thinking skills, creativity,** and **professional communications**. An example of this is the Collegiate Penetration Testing Competition (CPTC: https://nationalcptc.org/), hosted each year at RIT. In this competition, students work together like a professional pentesting team, getting goals and rules of engagement from a client, using their creativity and skills to attack the target network, and presenting their findings in both oral and written forms in a professional manner. This competition tests skills and abilities that will not be made irrelevant (in the near term) by an AI equipped with security tools. Similar efforts, both in competitions but also core education and outreach, need to be built in every area of security, with a clear eye towards whether the focus is on skills that will endure as technology advances.

6. *What other research and development strategies, plans, or activities, domestic or in other countries, should inform the U.S. Federal cybersecurity R&D strategic plan?*

International coalition through academic collaborations: a limitation today in advancing research and workforce development for cybersecurity at U.S. is the lack of collaboration beyond geographic boundaries. While security in general is a sensitive matter between sovereign states, cybersecurity inherently sees no such limits, and, in fact, often takes advantage of such limits. Foster collaborative research advances, curriculum and pedagogy development, as well as exchange best practices, cultural and policy differences, are among the benefits that will outweigh the concerns of data and intellectual property sensitivity. Investment to encourage international collaboration, especially at the intersect of cybersecurity with AI, IoT/CPS, and Quantum Computing, broadens the opportunity and innovative approaches to combat increasingly diverse and fast evolving malicious activities. A Global Cybersecurity Consortium formed by academic institutions expands student and faculty experiences, use-cases, transition-to-practice opportunities, and creates a venue for government and industry partners to leverage the eco-system generated by such coalition.

References

[Chung17a] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson, "A Longitudinal, End-to-End View of the DNSSEC Ecosystem," In Proceedings of the USENIX Security Symposium (Security '17), Vancouver, BC, Canada, August 2017.

[Chung17b] Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson, "Understanding the Role of Registrars in DNSSEC Deployment," In Proceedings of the ACM Internet Measurement Conference (IMC'17), London, United Kingdom, November 2017.

[Chung18] Taejoong Chung, Jay Lok, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, John Rula, Nick Sullivan, and Christo Wilson, "Is the Web Ready for OCSP Must Staple?," in Proceedings of the ACM Internet Measurement Conference (IMC '18), Boston, USA, November 2018.

[Fava08] D. Fava, S. Byers, S. J. Yang, "Projecting Cyber Attacks through Variable Length Markov Models," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp.359-369, September 2008.

[Fung17] B. Fung, "The House just voted to wipe away the FCC's landmark Internet privacy protections," Washington Post, Mar. 28, 2017, Accessed at https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/ on Jan. 15, 2019.

[Hu17] Hu, Peizhao, Sherman SM Chow, and Asma Aloufi. "Geosocial query with user-controlled privacy." In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 163-172. ACM, 2017.

[Krall16] A. Krall, M. E. Kuhl, **S. J. Yang**, and S. Moskal, "Estimating the Likelihood of Cyber Attack Penetration using Rare-Event Simulation," in Proceedings of 2016 IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016), December 6-9, Athens, Greece.

[Krunz18] Marwan Krunz, Berk Akgun, Peyman Siyari, Hanif Rahbari, Rashad Eletreby, and Ozan Koyluoglu, "Systems and Methods for Securing Wireless Communications," U.S. Patent App. 15/336,070 (granted Sep. 4, 2018)

[Moskal18] S. Moskal, S. J. Yang, and M. Kuhl, “Cyber Threat Assessment via Attack Scenario Simulation using an Integrated Adversary and Network Modeling Approach,” Journal of Defense Modeling and Simulation, Vol. 15, No.1, pp.13-29, 2018.

[Okutan18] A. Okutan, G. Werner, S. J. Yang, and K. McConky, “Forecasting Cyberattacks with Incomplete, Imbalanced, and Insignificant Data,” Springer Journal on Cybersecurity, 1:15, December, 2018.

[Rahbari15] Rahbari, Hanif, and Marwan Krunz. “Secrecy beyond encryption: Obfuscating transmission signatures in wireless communications.” IEEE Communications Magazine 53, no. 12 (2015): 54-60.

[Rahbari16] Rahbari, Hanif, and Marwan Krunz, “Rolling Preambles: Mitigating Stealthy FO Estimation Attacks in OFDM-based 802.11 Systems” 4th IEEE Conference Communications and Network Security (CNS 2016), October 2016.

[Rahbari17] Rahbari, Hanif, and Marwan Krunz. "Exploiting Frame Preamble Waveforms to Support New Physical-Layer Functions in OFDM-Based 802.11 Systems." IEEE Transactions on Wireless Communications 16, no. 6 (2017): 3775-3786.

[Rahbari18a] Rahbari, Hanif, Peyman Siyari, Marwan Krunz, and Jung-Min Jerry Park. “Adaptive Demodulation for Wireless Systems in the Presence of Frequency-Offset Estimation Errors.” In IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 1592-1600. IEEE, 2018.

[Rahbari18b] Rahbari, Hanif, Jinshan Liu, and Jung-Min Jerry Park. “SecureMatch: Scalable Authentication and Key Relegation for IoT Using Physical-Layer Techniques.” In 2018 IEEE Conference on Communications and Network Security (CNS), pp. 1-9. IEEE, 2018.

[Scheitle18] Quirin Scheitle, Taejoong Chung, Jens Hiller, Oliver Gasser, Johannes Naab, Roland van Rijswijk-Deij, Oliver Hohlfeld, Ralph Holz, Dave Choffnes, Alan Mislove, and Georg Carle, “A First Look at Certification Authority Authorization (CAA),” ACM SIGCOMM Computer Communications Review (CCR), April 2018.

[Yang14] S. J. Yang, H. Du, J. Holsopple, and M. Sudit, “Attack Projection for Predictive Cyber Situation Awareness,” book chapter in A. Kott, R. Erbacher, and C. Wang (Eds.), Cyber Defense and Situational Awareness, Springer, pp. 239-261, 2014.