

Living in the Internet of Things

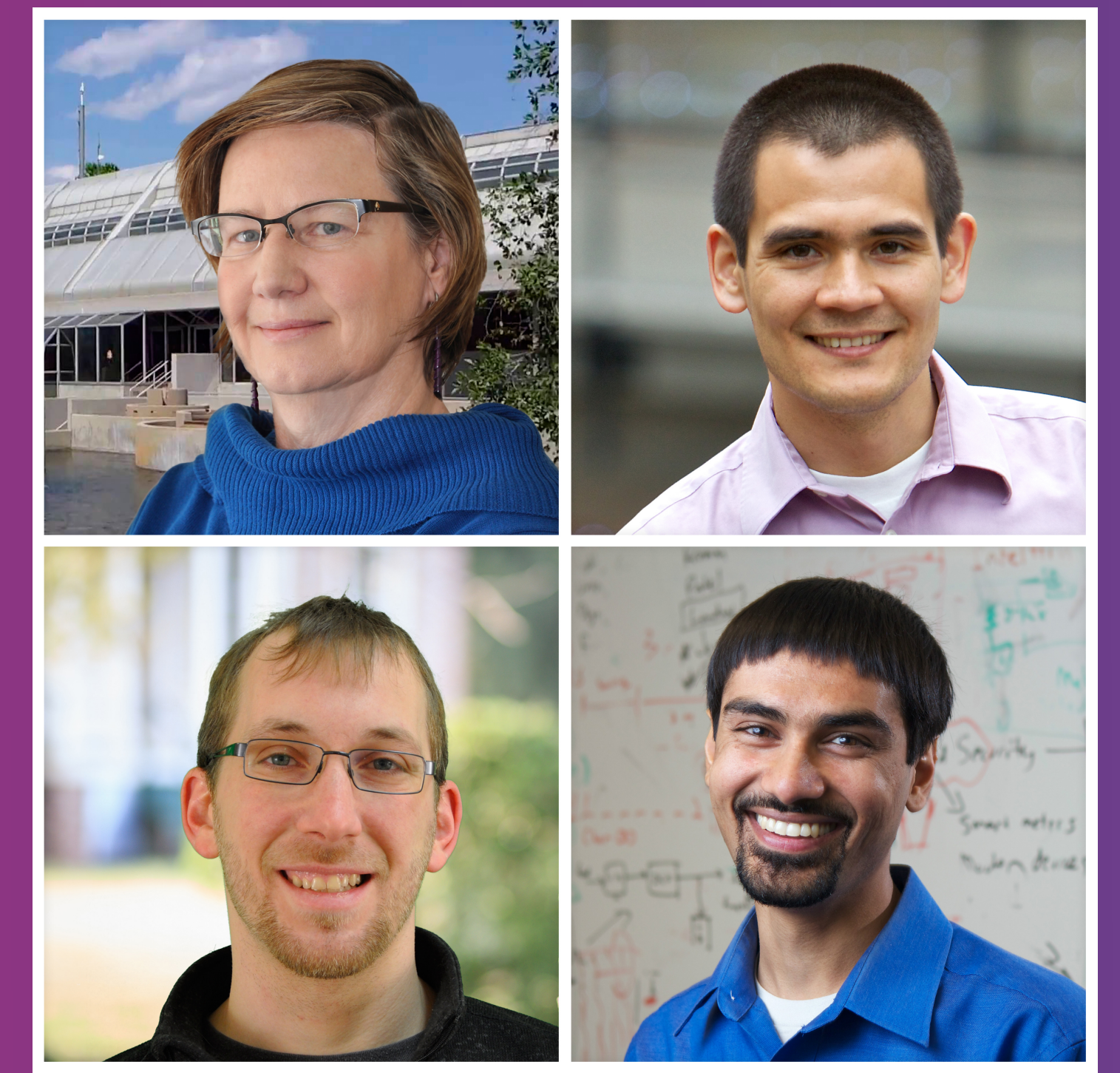
CNS 1565252, CNS 1565375

L. Jean Camp¹, Tadayoshi Kohno², Ryan Henry^{1,3}, Shwetak Patel²

¹Indiana University, ²University of Washington, ³University of Calgary in Alberta

iot.sice.indiana.edu

Security and privacy for an Internet of Things (IoT) ecosystem requires addressing human aspects and technical aspects in a holistic, multidisciplinary manner and bringing those to the public in forms that are usable and impactful.

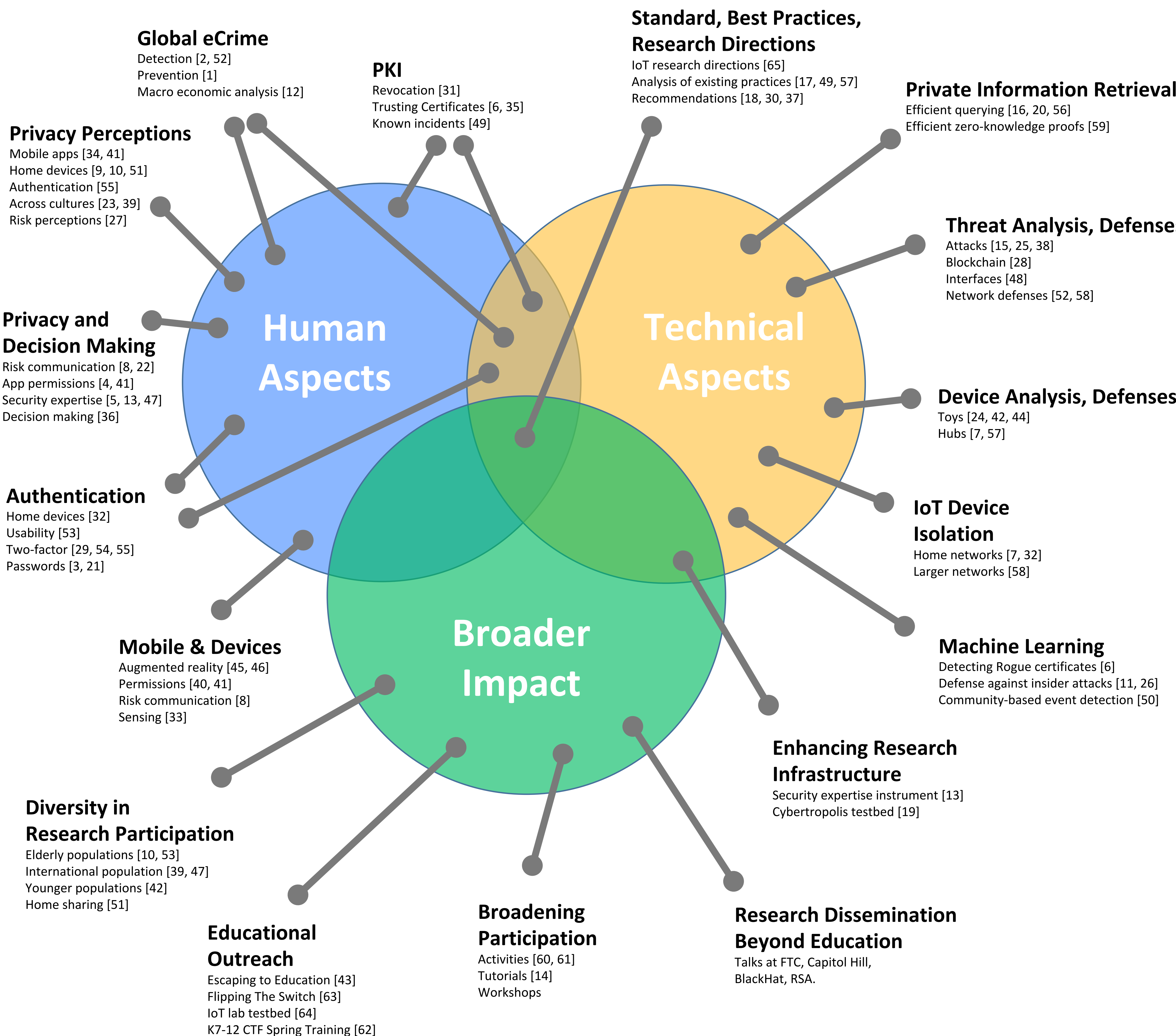


References (Papers, Events, Talks)

1. K. Benton and L. J. Camp, "Firewalling Scenic Routes: Preventing Data Exfiltration via Political and Geographic Routing Policies," in Proceedings of the ACM Workshop on Automated Decision Making for Active Cyber Defense, 2016.
2. K. Benton, L. J. Camp, and M. Swamy, "Borgo: A BGP speaker built for defending against bad routes," in Proceedings of IEEE Military Communications Conference (MILCOM) 2016.
3. L. J. Camp, J. Abbott, and S. Chen, "CPasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication," in Proceedings of the Hawaii International Conference on System Sciences (HICSS) 2016.
4. P. Rajivan and L. J. Camp, "Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices," in Proceedings of the SOUPS Workshop on Privacy Indicators 2016.
5. P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "What Can Johnny Do? Factors in an End-User Expertise Instrument," in Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA) 2016.
6. Z. Dong, K. Kane, and L. J. Camp, "Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks," in ACM Transactions on Privacy and Security, 2017.
7. A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," in PerCom Workshop on Pervasive Smart Living Spaces, 2017.
8. B. Momenzadeh and L. J. Camp, "Peeling the Lemons Problem with Risk Communication for Mobile Apps," Indiana University Bloomington, Technical Report TR736, 2017.
9. E. Zheng, S. Mare, and F. Roesner, "End User Security and Privacy Concerns with Smart Homes," in Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2017.
10. L. Huber and L. J. Camp, "User-Driven Design in Smart Homes: Ethical Aspects," in Handbook of Smart Homes, Health Care and Well-Being, Springer International Publishing, 2017.
11. P. Moriano, J. Pendleton, S. Rich, and L. J. Camp, "Insider Threat Event Detection in User-System Interactions," in Proceedings of the International Workshop on Managing Insider Security Threats, 2017.
12. P. Moriano, S. Achar, and L. J. Camp, "Incompetents, criminals, or spies: Macroeconomic analysis of routing anomalies," Computers & Security, 2017.
13. P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an end user security expertise instrument," Information & Computer Security, 2017.
14. R. Henry, "Tutorial: Private Information Retrieval," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2017.
15. R. Nandakumar, A. Takakuwa, T. Kohno, and S. Gollakota, "CovertBand: Activity Information Leakage Using Music," in Proceedings of Ubicomp, 2017.
16. S. M. Hafiz and R. Henry, "Querying for Queries: Indexes of Queries for Efficient and Expressive IT-PIR," in ACM SIGSAC Conference on Computer and Communications Security, 2017.
17. A. Dingman, G. Russo, G. Osterholt, T. Uffelmann, and L. J. Camp, "Poster: Good Advice That Just Doesn't Help," in Proceedings of the IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), 2018.
18. B. Momenzadeh, H. Dougherty, M. Remmel, S. Myers, and L. J. Camp, "Best Practices Would Make Things Better in IoT," under review, 2018.
19. G. M. Deckard, "Cyberterrorism: breaking the paradigm of cyber-ranges and testbeds," in Proceedings of the IEEE International Symposium on Technologies for Homeland Security, 2018.
20. G. Yaroslavtsev and A. Vadapalli, "Massively Parallel Algorithms and Hardness for Single-Linkage Clustering under p Distances," in Conference on Machine Learning (ICML), 2018.
21. J. Abbott, D. Galcaro, and L. J. Camp, "Factors Influencing Password Reuse: A Case Study," in the 46th Research Conference on Communications, Information, and Internet Policy, 2018.
22. J. Abbott, P. Rajivan, Z. Dong, S. Chen, and J. Blythe, "Instrumenting Simple Risk Communication for Safer Browsing," in Proceedings of the Security & Human Behavior Workshop, 2018.
23. J. Dev, S. Das, and L. J. Camp, "Privacy Practices, Preferences, and Compuncions: WhatsApp Users in India," in HAISA 2018.
24. J. Streiff, O. Kenny, S. Das, A. Leeth, and L. J. Camp, "Who's Watching Your Child? Exploring Home Security Risks with Smart Toy Bears," in IoTDI 2018.
25. K. Eykholt et al., "Physical Adversarial Examples for Object Detectors," in Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2018.
26. P. Moriano, J. Pendleton, S. Rich, and L. J. Camp, "Stopping the Insider at the Gates: Protecting Organizational Assets through Graph Mining," in Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2018.
27. P. van Schaik, et al., "Security and privacy in online social networking: Risk perceptions and precautionary behavior," in Computers in Human Behavior, 2018.
28. R. Henry, A. Herzberg, and A. Kate, "Blockchain Access Privacy: Challenges and Directions," IEEE Security Privacy, vol. 16, no. 4, 2018.
29. S. Das, A. Dingman, and L. J. Camp, "Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key," in Conference on Financial Cryptography (FC) 2018.
30. S. Das, J. Dev, and K. Sriniwasan, "Modularity is the Key A New Approach to Social Media Privacy Policies," in Mexican Conference on Human-Computer Interaction, 2018.
31. S. Myers and A. Shull, "Practical Revocation and Key Rotation," in Topics in Cryptology - CT-RSA 2018, 2018.
32. W. He et al., "Rethinking Access Control and Authentication for the Home Internet of Things (IoT)," in Proceedings of the USENIX Security Symposium (USENIX Security), 2018.
33. A. Marakakis, E. Wang, S. Patel, and M. Goel, "Challenges in Realizing Smartphone-Based Health Sensing," in IEEE Pervasive Computing, vol. 18, no. 2, 2019.
34. A. S. M. Noman, S. Das, and S. Patil, "Techies Against Facebook: Understanding Negative Sentiment Toward Facebook via User Generated Content," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), 2019.
35. H. Hadan, N. Serrano, S. Das, and L. J. Camp, "Making IoT Worthy of Human Trust," in Social Science Research Network (SSRN), 2019.
36. J. Abbott, G. Gao, and P. Shih, "Green: A Carbon Footprint Calculator Designed for Calculation in Context," in Information in Contemporary Society, 2019.
37. J. Abbott, H. MacLeod, N. Nurain, G. Ekobe, and S. Patil, "Local Standards for Anonymization Practices in Health, Wellness, Accessibility, and Aging Research at CHI," in CHI 2019.
38. K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahamti, C. Xiao, A. Prakash, T. Kohno, D. Song, "Robust Physical-World Attacks on Deep Learning Visual Classification," in the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
39. J. Dev, et al., "Personalized WhatsApp Privacy: Demographic and Cultural Influences on Indian and Saudi Users," in Social Science Research Network (SSRN), 2019.
40. J. Schubauer, A. Raymond, and D. Madappa, "Over-Privileged Permission: Using Technology and Design to Create Privacy Compliance," in IAC17: Research Conference on Innovation and the Transformation of Consumer Law, 2019.
41. J. Schubauer, D. Argast, J. Camp, and S. Patil, "Apps, Code, Culture, and Market Reform: Examining Influences on Android Permissions in the United States, South Korea, and Germany," in the 47th Research Conference on Communications, Information, and Internet Policy (TPRC), 2019.
42. J. Streiff and S. Das, "Eyes in Your Child's Bedroom: Exploiting Child Data Risks with Smart Toys," BSides MSP, 2019.
43. J. Streiff, C. Justis, and L. J. Camp, "Escaping to Cybersecurity Education: Using Manipulative Challenges to Engage and Educate," in Proceedings of the European Conference on Games Based Learning, 2019.
44. J. Streiff, "Bears, Unicorns, & Crocspots. Oh My! An Introduction to Internet of Things (IoT) Threat Modeling Education," in Proceedings of the AI & Connected Conference, 2019.
45. K. Lebeck, T. Kohno, and F. Roesner, "Enabling Multiple Applications to Simultaneously Augment Reality: Challenges and Directions," in Proceedings of the International Workshop on Mobile Computing Systems and Applications (HotMobile), 2019.
46. K. Ruth, T. Kohno, and F. Roesner, "Secure Multi-User Content Sharing for Augmented Reality Applications," in Proceedings of the USENIX Security Symposium (USENIX Security), 2019.
47. L. J. Camp, et al., "Conceptualizing Human Resilience in the Face of the Global Epidemiology of Cyber Attacks," in HICSS 2019.
48. M. Palekar, E. Fernandes, and F. Roesner, "Analysis of the Susceptibility of Smart Home Programming Interfaces to End User Error," in IEEE Workshop on the Internet of Safe Things (SafeThings), 2019.
49. N. Serrano, H. Hadan, and L. J. Camp, "A Complete Study of P.K.I. (PKI's Known Incidents)," in TPRC 2019.
50. P. Moriano, J. Finke, and Y.-Y. Ahn, "Community-Based Event Detection in Temporal Networks," in Scientific Reports, vol. 9, no. 1, 2019.
51. S. Mare, F. Roesner, and T. Kohno, "Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts," under review 2019.
52. P. Moriano, R. Hill, and L. J. Camp, "Using Bursty Announcements for Early Detection of BGP Routing Anomalies," in CoRR, vol. abs/1905.05835, 2019.
53. S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards Implementing Inclusive Authentication Technologies for Older Adults," in SOUPS Workshop Who Are You? Adventures in Authentication (WAY), 2019.
54. S. Das, B. Wang, and L. J. Camp, "MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content," in HAISA, 2019.
55. S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," in HAISA, 2019.
56. S. M. Hafiz and R. Henry, "A Bit More Than a Bit Is More Than a Bit Better: Faster (essentially) optimal-rate many-server PIR," in Privacy Enhancing Technologies (PoPETs), 2019.
57. S. Mare, L. Girvin, F. Roesner, and T. Kohno, "Consumer Smart Homes: Where We Are and Where We Need to Go," in HotMobile Workshop, 2019.
58. V. Andalibi, D. Kim, and L. J. Camp, "Throwing MUD into the FOG: Defending IoT and Fog by expanding MUD to Fog network," in Proceedings of the USENIX Workshop on Hot Topics in Edge Computing (HotEdge), 2019.
59. W. Black and R. Henry, "There Are 10 Types of Vectors (and Polynomials): Efficient Zero-Knowledge Proofs of 'One-Hotness' via Polynomials with One Zero," in IACR Cryptology ePrint Archive, vol. 2019.
60. K. Kabe, Students Get Education. CyberSecurity Brown County Democrat. 2019.
61. J. Streiff, Capturing Education: CTF and IoT in K-12 Education. Luddy Hall Pathfinders Night Session. 2019.
62. J. Streiff, Flipping the Switch: Cybersecurity Workshop Session at Indiana Department of Education (IDoE), Indian's Annual K-8 Computer Science Conference 2019.
63. J. Streiff, How Santa knows if you are Naughty or Nice: How your IoT toys can spy on you. SPICE Colloquium. 2019.
64. I. Evtimov, E. Fernandes, K. Koscher, F. Roesner, T. Kohno, "IoT lab: A platform for research and education," forthcoming 2019.
65. L. Camp et al., "Towards a Secure IoT: Directions for IoT Research", under review, 2019.

Acknowledgements

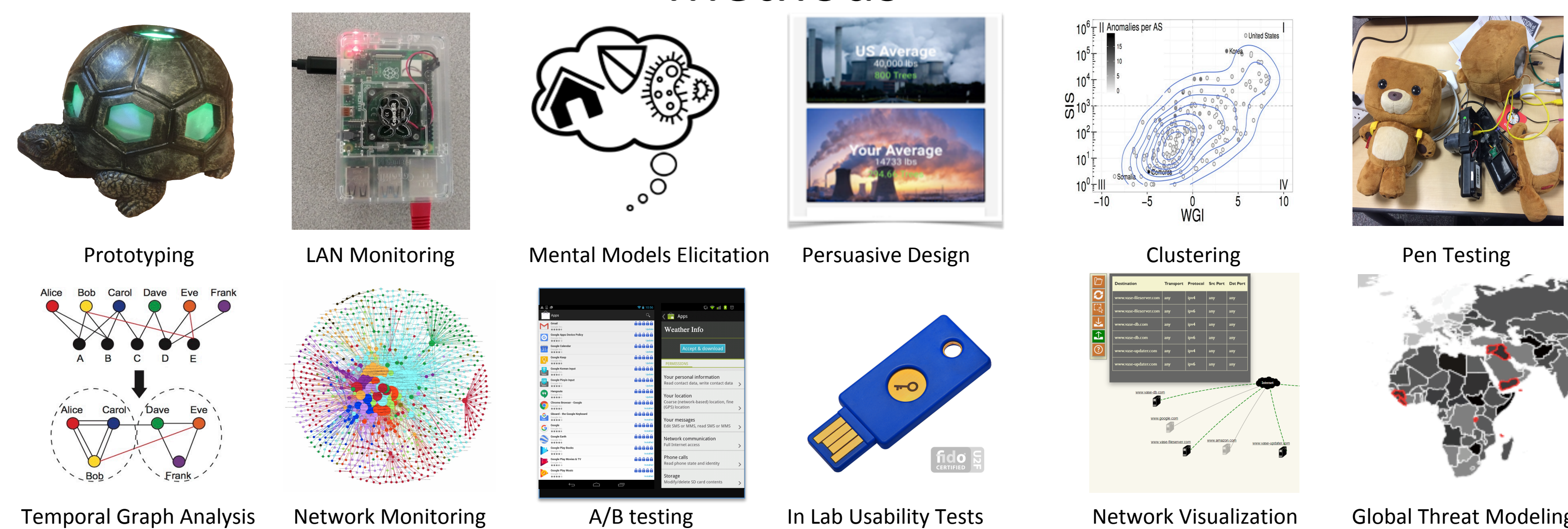
This research was supported in part by the National Science Foundation under CNS 1565252 and CNS 1565375 as well as the partners identified below. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the the US Government, the National Science Foundation, nor Indiana University or University of Washington.



Partners



Methods



Organized Events



The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
October 28-29, 2019 | Alexandria, Virginia

Award ID#: 1565252, 1565375

