Research Statement

Mohit Kumar Jangid (jangid.6@osu.edu)

I entered into computer security with fascination and curiosity at the art and craft of breaking system software and appreciating the complex beauty of cryptography. I believe in approaching problems fundamentally and systematically, which takes a longer route but yields sustainable, impactful solutions targeting root causes. Since security reasoning is a complex process, manual approaches are ineffective in the presence of large-scale systems, applications, and protocols, resulting in various flaws and attacks. For instance, the attack on Needham Schroeder Public Key protocol [41], a three-entity protocol, was discovered after 12 years by Lowe [36].

Fundamental and automated security solutions can tackle scale to large complex systems and provide comprehensive coverage beyond human reasoning ability. In this direction, Formal methods are one approach to the reason for rigorous security and privacy. Formal methods not only reason security from the correct construction philosophy but also provide an automated or semi-automated process for verification. At the current stage, formal methods face several challenges of scalability to large programs, verification gap, weak hardware-software contract, the composition of proofs, state-space explosion and non-termination, etc. However, many inspiring research works on large-scale protocols, such as TLS 1.3 [18, 22, 9], the Noise framework [27, 35], Signal [17, 16, 34], 5G authentication key exchange [8], IEEE 802.11's WPA2 [19] are gradually bridging the gaps. In the same spirit, I am excited to contribute and help resolve these challenges while also enjoying the work that aligns with my values.

Thesis Research

During my PhD, I spent time understanding state-of-the-art formal verification techniques and the underlying mathematical background. I have directed my focus to challenge the limitations of symbolic formal methods by expanding them to new directions of systems and privacy. In particular, with my colleagues, I have performed comprehensive formal investigations using symbolic verification tool Tamarin [39] in three research areas. First, modeling enclave programs to detect state continuity vulnerability [31], which is published in USENIX Security 2021. Second, modeling complex Bluetooth pairing protocols [33], which is published in NDSS 2023. Lastly, we systematically expose the root causes of a new privacy terrain: preferred network list-based privacy attacks. These three directions of research are summarized below:

- **Potential and Challenges of Modeling Intel SGX Enclave Programs** [31]. Intel SGX [30, 38, 6] enables hardware-protected security, which has opened avenues for confidential computing and secure client authentication. However, enclave programs, when faced with a strong adversary such as a malicious operating system, can be subject to state continuity vulnerability. As such, we made a first attempt towards extending Tamarin to program logic for SGX enclaves with the powerful SGX threat model and formally reason about the state continuity property. In this effort, we developed a detailed model for three open-source SGX applications: (1) Sawtooth [2, 4, 3] (a blockchain framework), (2) BI-SGX [42] (a confidential cloud platform), and (3) SGXEnabledAccess [10] (a secure remote monitoring framework for IoT devices). In the respective applications, our model discovers three categories of flaws that allow violation of state continuity in three categories: the trusted computing base states are stored in monotonic counters, global variables, and data in the sealed storage. Enhancing the trust, the proposed countermeasures are verified in the patched version of the models.

- **Potential and Challenges of Modeling Complex Bluetooth Pairing** [33]. Bluetooth is one of the most widely used wireless protocols for connecting versatile devices such as IoT devices, desktops, and laptops. The security of Bluetooth communication is centered on two apparently secure pairing protocols: *Passkey Entry* and *Numeric Comparison*. Our model consists of these challenging, and long Bluetooth pairing protocols with a detailed Bluetooth environment of device access control, human interaction, and human errors. The generic design of our modal allowed us to uncover five attacks: three existing — Static Passcode [43], Reflection [14], and Method Confusion [45]; and two new attacks — Group Guessing and Ghost Attack. These attacks demonstrate the effectiveness of our augmented formal verification.

- **Potential and Challenges of Modeling Allowlist Privacy Attack [In-Progress]**. With the growth of wireless IoT devices, various novel replay and relay-based privacy risks emerge. The complexity of these

privacy risks increases due to the diversity of communication mediums, authentication methods, and data-sharing structures across different contexts. Consequently, many clever privacy attacks expose the social relationship [11, 20], trace geographic location [15, 40, 46], and predict user interest [23, 12, 21]. Therefore, there is a lack of root causes and systemization for these privacy violations. In this research, we investigate recent location-tracking attacks and systemize them to build a robust science that explain the root causes of the privacy flaw. Our research identifies privacy flaws in prominent wireless protocols and explains the required conditions and threat model leading to the attacks. The proposed countermeasures are acknowledged by industry standards and verified in our formal model. Two research papers in this direction are currently in-progress.

Other Research

- **TEE-based V2V Protocol** [32]. Collaborative networks of Connected and Autonomous Vehicles (CAVs) can improve traffic safety and efficiency by exchanging information on congestion, can lower costs associated with medical care, emergency services, employment, insurance, and legal procedures, and benefit the national economy [5, 1]. CAVs face challenges of fast and scalable communication for real-time cross-vehicle interactions and ensuring security and privacy amidst a vast attack surface. In this research, we introduce a new V2V protocol design using a trusted execution environment (TEE). Supported by preliminary experiments, our design accomplishes authentication, privacy, accountability, revocation, scalability, and efficiency objectives. We hope to inspire future research using this initiative.
- **Social Darknet Network** [24, 25]. In this interdisciplinary research, we collaborated with the Department of Sociology and Criminal Justice. Our aim was to study the social networks of online drug trade markets and devise strategies to deteriorate illegal operations. In this research, I developed a powerful automation to collect the trading operation metrics from popular drug market websites. The automation took four days to run continuously to collect sellers, buyers, drug attributes, geolocation, and timeline. After text processing over the data, we built a social graph network representing seller-buyer interactions. The network was analyzed from different perspectives of buyer-seller relationships, the prevalence of drugs, changes in the network over time, and geographical relations with the drug transactions. This technical contribution was acknowledged in the journals Socio-Economic Review 2023 [25] and American Journal of Sociology 2021 [24].

Research Vision

During my research, I observed some key gaps that are limiting current standards of automated security and privacy verification. I envision working in the following directions toward my research vision.

- **Next 2 Years**
  - **Gap in Efficient Proof Heuristics**: Due to undecidability results in proving the properties of a given system [26, 28, 13], most verification relies on human heuristics. For example, Tamarin uses an intuitively defined next constraints selection algorithm to iterate over complete model states and proof tree sequences. These heuristics are designed based on expert experiences in proving the properties of standard protocols and systems. Relying on human experience can be limited compared to scalable machine-learning comprehension of finding optimal paths for proof completion. By capturing the patterns of existing protocol proofs, machine learning can guide the algorithm with broader common sense. Similarly, many principles of state space exploration of mature fuzzing tools can be borrowed to enhance proof heuristics.
  - **Gap in Efficient Privacy Verification Techniques**: Formalizing privacy is still a young field in the research community. In the literature, there are very few proofs of privacy properties (e.g. observational equivalence) compared to trace-based properties [29]. Observational equivalence property is harder to encode in formal techniques because they require comparing the structure of the modeled system, which needs large state space coverage and unconventional reasoning of indistinguishability. A subset of observational equivalence can be captured using diff-equivalence, which is adopted in mainstream symbolic tools to compare two systems having the same structure but differing in one term. However, diff-equivalence modeling requires limiting the system's functionality – eliminating condition checks to deal with processing randomized messages [7, 29].

Subsequently, it limits the classes of privacy captured by these tools. To enhance the privacy capturing techniques, I plan to establish the formalization for the preferred network list based privacy attack using process algebra and gain insight for effective capturing of observational equivalence.

- **Next 5 Years**
  - **Building Blocks for Foundational Automated Security.** In the past 20 years, a plethora of formal verification and automated reasoning tools have been developed. All these tools have different strengths and weaknesses. Such a heterogeneous nature of growth can paralyze formal verification efforts if not aligned with a universal method. I wish to compose universal and modularized automated security verification blocks. I hope that by making these blocks generic, a large number of people can contribute to making it robust and practical. For example, by Initiating and organising a research conference among different formal method communities; working on formal method tools that can interchangeably convert from formal languages to binary executable programs (e.g., F* [44]); and devising methods to interchangeability convert from one language to another (e.g., applied pi-calculus to multiset rewriting rules) would bring uniformity to formal methods.
  - **Distributed Computing Security.** Distributed computing is complex and powerful. Given the growth of IoT in the home, manufacturing industries, and transportation sectors, utilizing the power of distributed systems would provide novel directions for creating cryptographic systems and defenses. Not only will these systems be tolerant of a single point of failure – but computationally efficient by distributing the workload (e.g., Rollback protection for trusted execution [37]). I wish to expand cryptosystems that utilize distributed systems well to provide better security and privacy.

Execution of Research Vision

Throughout my PhD research, I had the privilege of working under the guidance of esteemed senior students who have since become faculties, such as Xiaokuan Zhang (George Mason University, USA), Guoxing Chen (Shanghai Jiao Tong University, China), and Yue Zhang (Drexel University, USA). My advisors, Dr. Zhiqiang Lin (The Ohio State University), Dr. Yinqian Zhang (Southern University of Science and Technology), and Dr. Manoj Singh Gaur (IIT Jammu), along with my friend Bahruz Jabiyev (PostDoc at Dartmouth College), have also played a crucial role in shaping my research journey. I am eager to continue this collaborative spirit and build momentum in my future research endeavors. To accelerate my research, I will collaborate with the formal methods and machine learning communities. My past and recent experiences with Dr. Cas Cremers (CISPA Helmholtz Center for Information Security in Saarbruecken, Germany) and Dr. Stéphanie Delaune (Institute for Research in Computer Science and Random Systems), who have done foundational work in formal methods, can help me with formal method expertise. Further, Dr Srinivasan Parathaarty will be my lead for the machine learning direction. I will approach my research vision ideas in a spiral fashion: by building a small prototype to show the promising direction, then gradually building up to a fully-fledged solution.

During my research, I developed a grant proposal to bridge the gaps in verification techniques. During my prospective faculty position, I plan to submit the proposal to leading grant agencies in India. Further, as instilled by my advisors, I will keep the research standard to the top tiers of research conferences: IEEE S&P, USENIX, NDSS, and CCS. I will require several resources for my research, including IoT devices, personal phones and laptops, and cloud computing services. These tools will enable me to conduct both local case studies and heavy experiments on formal verification.

My research vision will have two impacts. First, it will bring automation to formal methods, thereby reducing the need for strenuous human effort. Second, it will promote the "analysis-prior-to-deployment" design philosophy, thereby enhancing assurance in security.

References

[1] Ensuring American Leadership in Automated Vehicle Technologies. https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf. (Accessed on 12/24/2021).

[2] Hyperledger Sawtooth. Retrieved January 20, 2021 from https://www.hyperledger.org/use/sawtooth.

[3] Hyperledger Sawtooth-PoET patch. Retrieved January 12, 2021 from https://github.com/hyperledger/sawtooth-poet/commit/6f9db4998a11b427c6a24ea42f9891cb9ff0101e.

[4] Hyperledger Sawtooth-PoET vulnerable. Retrieved January 12, 2021 from https://github.com/hyperledger/sawtooth-core/releases/tag/v1.0.5, Filepath /consensus/poet/sgx/sawtooth_poet_sgx/libpoet_enclave/poet_enclave.cpp.

[5] Traffic Safety: Raising Spending Could Save Lives and Money. https://www.cnbc.com/2015/12/14/traffic-safety-raising-spending-could-save-lives-and-money.html. Accessed on 01/04/2022.

[6] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In *Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*, volume 13, page 7. ACM New York, NY, USA, 2013.

[7] David Baelde, Stéphanie Delaune, and Solène Moreau. A method for proving unlinkability of stateful protocols. In *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, pages 169–183. IEEE, 2020.

[8] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, page 1383–1396. ACM, 2018.

[9] K. Bhargavan, B. Blanchet, and N. Kobeissi. Verified models and reference implementations for the TLS 1.3 standard candidate. In *2017 IEEE Symposium on Security and Privacy*, pages 483–502, Los Alamitos, CA, USA, may 2017. IEEE Computer Society.

[10] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, and Y. T. Hou. Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in iot. *IEEE Transactions on Information Forensics and Security*, 14(7):1830–1842, 2019. Github: https://github.com/fishermano/SGXEnabledAccess.

[11] Ningning Cheng, Prasant Mohapatra, Mathieu Cunche, Mohamed Ali Kaafar, Roksana Boreli, and Srikanth Krishnamurthy. Inferring user relationship from hidden information in wlans. In *MILCOM 2012-2012 IEEE Military Communications Conference*, pages 1–6. IEEE, 2012.

[12] Maxim Chernyshev, Craig Valli, and Peter Hannay. On 802.11 access point locatability and named entity recognition in service set identifiers. *IEEE Transactions on Information Forensics and Security*, 11(3):584–593, 2015.

[13] Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune. From security protocols to pushdown automata. *ACM Transactions on Computational Logic (TOCL)*, 17(1):1–45, 2015.

[14] Tristan Claverie and José Lopes Esteves. Bluemirror: Reflections on bluetooth pairing and provisioning protocols. In *2021 IEEE Security and Privacy Workshops (SPW)*, pages 339–351, 2021.

[15] Peter Cohan. How nordstrom uses wifi to spy on shoppers, forbes magazine. 2013. Retrieved April 19, 024 from https://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/?sh=6b402de44362.

[16] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. *Journal of Cryptology*, 33(4):1914–1983, 2020.

[17] Cas Cremers, Jaiden Fairoze, Benjamin Kiesl, and Aurora Naska. Clone detection in secure messaging: Improving post-compromise security in practice. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 1481–1495. Association for Computing Machinery, 2020.

[18] Cas Cremers, Marko Horvat, Jonathan Hoyland, Samuel Scott, and Thyla van der Merwe. A comprehensive symbolic analysis of TLS 1.3. In *ACM SIGSAC Conference on Computer and Commuincations Security*, pages 1773–1788. ACM, October 2017.

[19] Cas Cremers, Benjamin Kiesl, and Niklas Medinger. A formal analysis of IEEE 802.11's wpa2: Countering the kracks caused by cracking the counters. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1–17. USENIX Association, August 2020.

[20] Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli. Linking wireless devices using information contained in wi-fi probe requests. *Pervasive and Mobile Computing*, 11:56–69, 2014.

[21] Ante Dagelić, Toni Perković, Bojan Vujatović, and Mario Čagalj. Ssid oracle attack on undisclosed wi-fi preferred network lists. *Wireless Communications and Mobile Computing*, 2018, 2018.

[22] A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, J. Protzenko, A. Rastogi, N. Swamy, S. Zanella-Beguelin, K. Bhargavan, J. Pan, and J. K. Zinzindohoue. Implementing and proving the TLS 1.3 record layer. In *2017 IEEE Symposium on Security and Privacy*, pages 463–482, 2017.

[23] Adriano Di Luzio, Alessandro Mei, and Julinda Stefa. Mind your probes: De-anonymization of large crowds through smartphone wifi probe requests. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9. IEEE, 2016.

[24] Scott W Duxbury and Dana L Haynie. Shining a light on the shadows: Endogenous trade structure and the growth of an online illegal market. *American Journal of Sociology*, 127(3):787–827, 2021.

[25] Scott W Duxbury and Dana L Haynie. Network embeddedness in illegal online markets: Endogenous sources of prices and profit in anonymous criminal drug trade. *Socio-Economic Review*, 21(1):25–50, 2023.

[26] Shimon Even and Oded Goldreich. On the security of multi-party ping-pong protocols. In *24th Annual Symposium on Foundations of Computer Science (sfcs 1983)*, pages 34–39. IEEE, 1983.

[27] Guillaume Girol, Lucca Hirschi, R. Sasse, D. Jackson, C. Cremers, and David Basin. A spectral analysis of noise: A comprehensive, automated, formal analysis of diffie-hellman protocols. In *USENIX Security Symposium*, 2020.

[28] Nevin Heintze and J Doug Tygar. A model for secure protocols and their compositions. *IEEE transactions on software engineering*, 22(1):16–30, 1996.

[29] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for verifying privacy-type properties: the unbounded case. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 564–581. IEEE, 2016.

[30] Matthew Hoekstra, Reshma Lal, Pradeep Pappachan, Vinay Phegade, and Juan Del Cuvillo. Using innovative instructions to create trustworthy software solutions. *HASP@ ISCA*, 11(10.1145):2487726–2488370, 2013.

[31] Mohit Kumar Jangid, Guoxing Chen, Yinqian Zhang, and Zhiqiang Lin. Towards formal verification of state continuity for enclave programs. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 573–590. USENIX Association, August 2021.

[32] Mohit Kumar Jangid and Zhiqiang Lin. Towards a TEE-based V2V Protocol for Connected and Autonomous Vehicles. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2022.

[33] Mohit Kumar Jangid, Yue Zhang, and Zhiqiang Lin. Extrapolating formal analysis to uncover attacks in bluetooth passkey entry pairing. In *Network and Distributed Systems Security (NDSS) Symposium*, 2023.

[34] N. Kobeissi, K. Bhargavan, and B. Blanchet. Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach. In *IEEE European Symposium on Security and Privacy*, pages 435–450, 2017.

[35] N. Kobeissi, G. Nicolas, and K. Bhargavan. Noise explorer: Fully automated modeling and verification for arbitrary noise protocols. In *2019 IEEE European Symposium on Security and Privacy*, pages 356–370, 2019.

[36] Gavin Lowe. Breaking and fixing the needham-schroeder public-key protocol using fdr. In *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, pages 147–166. Springer, 1996.

[37] Sinisa Matetic, Mansoor Ahmed, Kari Kostiainen, Aritra Dhar, David Sommer, Arthur Gervais, Ari Juels, and Srdjan Capkun. ROTE: Rollback protection for trusted execution. In *26th USENIX Security Symposium*, pages 1289–1306, Vancouver, BC, August 2017. USENIX Association.

[38] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R Savagaonkar. Innovative instructions and software model for isolated execution. *Hasp@ isca*, 10(1), 2013.

[39] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The tamarin prover for the symbolic analysis of security protocols. pages 696–701, 2013.

[40] ABM Musa and Jakob Eriksson. Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of the 10th ACM conference on embedded network sensor systems*, pages 281–294, 2012.

[41] Roger M Needham and Michael D Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[42] Aoi Sakurai. BI-SGX: Secure Cloud Computation. *58th SIGBIO Bioinformatics Study Group, Japan*, 2019. Website: https://bi-sgx.net/, Github: https://github.com/hello31337/BI-SGX.

[43] Da-Zhi Sun, Yi Mu, and Willy Susilo. Man-in-the-middle attacks on secure simple pairing in bluetooth standard v5.0 and its countermeasure. *Personal Ubiquitous Comput.*, 22(1):55–67, February 2018.

[44] Nikhil Swamy, Cătălin Hriţcu, Chantal Keller, Aseem Rastogi, Antoine Delignat-Lavaud, Simon Forest, Karthikeyan Bhargavan, Cédric Fournet, Pierre-Yves Strub, Markulf Kohlweiss, et al. Dependent types and multi-monadic effects in f. In *Proceedings of the 43rd annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 256–270, 2016.

[45] Maximilian von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. Method confusion attack on bluetooth pairing. *Under submission*, 2020.

[46] Yue Zhang and Zhiqiang Lin. When good becomes evil: Tracking bluetooth low energy devices via allowlist-based side channel and its countermeasure. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 3181–3194, 2022.