Publications

Advancing Security of Public Infrastructure using Resilience and Economics

1. Adepu S. and Mathur A., "An Agent-based Framework for Simulating and Analysing Attacks on CPS," 15th International Conference on Algorithms and Architectures for Parallel Processing
2. Adepu S. and Mathur A., "An Investigation into the Response of a Water Treatment System to Cyber Attacks," The 17th IEEE International Symposium on High Assurance Systems Engineering (HASE) 2017
3. Adepu S. and Mathur A., "Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plan," Asia CCS 2016
4. Adepu S. and Mathur A., "Generalized attacker and attack models for Cyber Physical Systems," The 40th IEEE Computer Society International Conference on Computers, Software & Applications
5. Adepu S. and Mathur A., "Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study," 2nd Asia Pacific Conference on Complex Systems Design and Management
6. Adepu S. and Mathur A., "Using Process Invariants to Detect Cyber Attacks on a Water Treatment System," ICT Systems Security and Privacy Protection 2016
7. Adepu S. and Mathur A., "Detecting Multi-Point Attacks in a Water Treatment System Using Intermittent Control Actions,"Singapore Cyber Security R&D Conference (SG-CRC 2016)
8. Adepu S., Shrivastava S., and Mathur A., "Argus: An Orthogonal Defense Framework," IEEE computing magazine, Cyber Physical Security and Privacy Joint Special issue with IEEE intelligent Systems
9. Adepu S., Mishra G. and Mathur A., "Access Control in Water Distribution Networks: A Case Study", 2017 IEEE International Conference on Software Quality, Reliability & Security
10. Adepu S., and Mathur A., "From Design to Invariants: Detecting Attacks on Cyber Physical Systems", 2017 IEEE International Conference on Software Quality, Reliability & Security
11. Adepu S., Prakash J., and Mathur A., "WaterJam: An Experimental case study of Jamming Attacks on a Water Treatment System", 2017 IEEE International Conference on Software Quality, Reliability & Security
12. Ahmed C. M., Adepu S., Mathur A., "Limitations of State Estimation Based Cyber Attack Detection Schemes in Industrial Control Systems," Smart City Security and Privacy Workshop (SCSP-W) CPS Week 2016
13. Ahmed C. M., Murguia C., Ruths J., "Model-based Attack Detection Scheme for Smart Water Distribution Networks", ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017
14. Ahmed C. M. and Mathur A., "Hardware Identification via Sensor Fingerprinting in a Cyber Physical System", 2017 IEEE International Conference on Software Quality, Reliability & Security
15. Antonioli D., Ghaeini H. R., Adepu S., Ochoa M., and Tippenhauer N. O., "Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3", 3rd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)

Research
‹ Projects
Publications
Reports
‹ Testbeds

16. Chamambaz M., Notarstefano G., Bouffanais R., “Randomized Constraints Consensus for Distributed Robust Linear Programming”, The 20th World Congress of the International Federation of Automatic Control, 9-14 July 2017
17. Chamanbaz M., Notarstefano G., Bouffanais R., “A Distributed Ellipsoid Algorithm for Uncertain Convex Problems: A Randomized Approach,” 56th IEEE Conference on Decision and Control 2017
18. Chen Y., Poskitt C. M., and Sun J., “Towards Learning and Verifying Invariants of Cyber-Physical Systems by Code Mutation”, accepted at Formal Methods 2016
19. Chen Y., Poskitt C.M. , Sun J., “Learning from Mutants: Using Code Mutation to Learn and Monitor Cyber-Physical System Invariants,” IEEE Symposium on Security and Privacy 2018
20. Goh J., Adepu S., Junejo K. N., and Mathur A., “A Dataset to Support Research in the Design of Secure Water Treatment Systems,” The 11th International Conference on Critical Information Infrastructures Security
21. Goh, Adepu S, Tan M. and Lee Z. S., ” Anomaly Detection in Cyber Physical Systems using Recurrent Neural Networks”, Workshop on Security issues in Cyber Physical Systems (SecCPS) @ HASE 2017
22. Inoue J. , Yamagata Y., Chen Y., Poskitt C.M., and Sun J., “Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning,” IEEE International Conference on Data Mining Workshops: Data Mining for Cyberphysical and Industrial Systems (DMCIS 2017)
23. Junejo K. N. and Yau D., “Data Driven Physical Modelling for Intrusion Detection in Cyber Physical Systems,” Singapore Cyber Security R&D Conference 2016
24. Junejo K. N., Goh J., “Attack Detection and Classi cation in Cyber Physical Systems Using A Machine Learning Approach,” 2nd ACM Cyber-Physical System Security Workshop
25. Mathur A., “SecWater: A Multi-Layer Security Framework for Water Treatment Plants,” CySWATER ’17 Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks
26. Mujeeb A. C., Reddy V., Mathur A., “WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems”, 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater) 2017
27. Murguia C. and Ruths J., “Characterization of a CUSUM Model-Based Sensor Attack Detector,” IEEE 55th Conference on Decision and Control
28. Murguia C. and Ruths J., “CUSUM and x2 Attack Detection of Compromised Sensors,” Multi-conference on Systems and Control 2016
29. Murguia C., Ruths J., Nijmeijer H., “Robust Network Synchronization of Time-Delayed Coupled Systems,” 6th IFAC International Workshop on Periodic Control Systems
30. Murguia C., van de Wouw N., Ruths J., “Reachable Sets of Hidden CPS Sensor Attacks: Analysis and Synthesis Tools”, IFAC 2017 World Congress
31. Nguyen H. H., Tan R., Yau D. K. Y, “Collaborative Demand-Response Load Management with Safety Assurance in Smart Grids,” ACM Transactions on Cyber-Physical Systems
32. Pal K., Adepu S., Goh J., ” Effectiveness of Association Rules Mining for Invariants Generation in Cyber-Physical Systems “, The 18th IEEE International Symposium on High Assurance Systems Engineering (HASE) 2017
33. Qadeer R., Murguia C., Ahmed C.M., and Ruths J., “Multistage Downstream Attack Detection in a Cyber Physical System,” CyberICPS Workshop 2017, in conjunction with ESORICS 2017
34. Rocchetto M. and Tippenhauer N.O., “Towards Formal Security Analysis of Industrial Control Systems”, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017
35. Rocchetto M. and Tippenhauer N. O., “CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions,” ICFEM 2016
36. Rocchetto M. and Tippenhauer N. O., “On Attacker Models and Profiles for Cyber-Physical Systems,” ESORICS 2016 (European Symposium on Research in Computer Science)
37. Sabaliauskaite G., Adepu S., “Integrating Six-Step Model with Information Flow Diagrams for Comprehensive Analysis of Cyber-Physical System Safety and Security”, The 18th IEEE International Symposium on High Assurance Systems Engineering (HASE) 2017
38. Sugumar G. and Mathur A., “Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control Systems”, 2017 IEEE International Conference on Software Quality,

Reliability & Security
39. Taormina R., Galelli S., "Real-time detection of cyber-physical attacks on water distribution systems using deep learning," World Environmental & Water Resources Congress 2017
40. Taormina R., Galelli S., Tippenhauer N. O., Ostfeld A., "Assessing the effect of cyber-physical attacks on water distribution systems," World Environmental & Water Resources Congress
41. Taormina R., Galelli S., Tippenhauer N. O., Salomons E., Ostfeld A., "Simulation of Cyber-Physical Attacks on Water Distribution Systems with EPANET," Singapore Cyber Security R&D Conference 2016
42. Taormina R., Galelli S., Tippenhauer N. O., Salomons E., Ostfeld A., "Characterizing cyber-pysical attacks on water distribution systems," Journal of Water Resources Planning and Management
43. Umer A.M., Junejo K.N., Mathur A., and Adepu S., "Integrating design and data centric approaches to generate invariants for distributed attack detection," 3rd ACM Workshop on CPS Security and Privacy
44. Wang J., Sun J, Yuan Q. and Pang J., "Should We Learn Probabilistic Models for Model Checking? A New Approach and an Empirical Study," 20th International Conference on Fundamental Approaches to Software Engineering (FASE) in ETAPS 2017
45. Wang J.Y., Sun J. and Qin S.Q., "Verifying Complex Systems Probabilistically through Learning, Abstraction and Refinement", 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)

Autonomous Vehicle Security

1. Cui J., Sabaliauskaite G., "How to Align the Safety and Security for Autonomous Vehicles?," The Second International Conference on Cyber-Technologies and Cyber-Systems (CYBER) 2017
2. Cui J., Sabaliauskaite G., "US^2: An Unified Safety and Security Analysis Method for Autonomous Vehicles," Future of Information and Communication Conference (FICC) 2018
3. Cui J., Sabaliauskaite G., "Integrating Autonomous Vehicle Safety and Security Using the Six-Step Model, ISO 26262, SAE J3061, and SAE J3016," CYPHY: Security Issues and Solutions for Cyber-Physical Systems, The Second International Conference on Cyber-Technologies and Cyber-Systems (CYBER) 2017

Cyber Physical System Protection

1. Adepu S. and Mathur A., "An Agent-based Framework for Simulating and Analysing Attacks on CPS," 15th International Conference on Algorithms and Architectures for Parallel Processing
2. Adepu S. and Mathur A., "An Investigation into the Response of a Water Treatment System to Cyber Attacks," The 17th IEEE International Symposium on High Assurance Systems Engineering (HASE)
3. Adepu S. and Mathur A.,"Generalised attacker and attack models for Cyber Physical Systems,", IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016)
4. Adepu S. and Mathur A., "Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study," 2nd Asia Pacific Conference on Complex Systems Design and Management
5. Adepu S. and Mathur A., "Using Process Invariants to Detect Cyber Attacks on a Water Treatment System," ICT Systems Security and Privacy Protection 2016
6. Adepu S. Mathur A., Jackson D. and Kang E. "Model Based Security Analysis of a Water Treatment System," 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS'16)
7. Adepu S., and Mathur A., "An Experimental Investigation into Detecting Cyber Attacks on a Water Treatment System Using Process Invariants," 7th International Conference on Cyber-Physical Systems (ICCPS)
8. Antonioli D., Agrawal A., Tippenhauer N. O., "Towards High Interaction Virutal ICS Honeypots-in-a-box", CPS-SPC16 Workshop
9. Chen X., Lei L., Zhang H., Yuen C. "On the Secrecy Outage Capacity of Physical Layer Security in Large-Scale MIMO Relaying Systems with Imperfect CSI," IEEE International Conference on Communications (IEEE ICC 2014)

10. Chen X., Sun J. and Sun M., “A Hybrid Model of Connectors in Cyber-Physical Systems.” 16th International Conference on Formal Engineering Methods (ICFEM 2014).
11. Chen X., Sun J., Sun M., “A Hybrid Model of Connectors in Cyber-Physical Systems,” ICFEM 2014: 59-74
12. Dau S. H., Song W., Yuen C., “On Block Security of Regenerating Codes at the MBR Point for Distributed Storage Systems,” IEEE International Symposium on Information Theory (IEEE ISIT 2014)
13. Dau S. H., Song W., Yuen C., “On Simple Multiple Access Networks,” IEEE Journal on Selected Topics in Communications, Nov 2014
14. Dau S. H., Song W., Yuen C., “Secure Erasure Codes with Partial Decodability,” IEEE International Conference on Communications (ICC2015)
15. Dau S. H., Song W., Yuen C., “Weakly secure MDS codes for simple multiple access networks,” IEEE International Symposium on Information Theory (IEEE ISIT 2015)
16. Hao J., Kang E., Jackson D., Sun J., “Adaptive Defending Strategy for Smart Grid Attacks.” SEGS@CCS 2014: 23-30.
17. Kang E., Adepu S., Mathur A. and Jackson D., “Model Based Security Analysis of a Water Treatment System”, SEsCPS 2016, ICSE Workshop
18. Kong P., Li Y., Chen X., Sun J., Sun M. and Wang J., “Towards Concolic Testing for Hybrid Systems.” FM 2016.
19. Li L., Jun S., and Dong J. S., “A Formal Specification and Verification Framework for Timed Security Protocols.” IEEE Transactions on Software Engineering. Under Review.
20. Li L., Jun S., Liu Y., Dong J. S., “Practical Analysis Framework for Software-based Attestation Scheme.” 16th International Conference on Formal Engineering Methods (ICFEM 2014).
21. Li L., Jun S., Liu Y., Dong J. S., “TAuth: Verifying Timed Security Protocols.” ICFEM 2014: 300-315.
22. Li L., Pang J., Liu Y., Jun S., Dong J. S., “Symbolic Analysis of an Electric Vehicle Charging Protocol.” ICECCS 2014: 11-18.
23. Li Li, Jun Sun, Yang Liu, Jin Song Dong., “Verifying Parameterized Timed Security Protocols.” FM 2015: 342-359
24. Li Li, Jun Sun and Jin Song Dong., “Automated Verification of Timed Security Protocols with Clock Drift.” FM 2016.
25. Mathur A. and Tippenhauer N. O., “SWaT: Secure Water Treatment Testbed for Research and Training in the Design of Industrial Control Systems,” IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016)
26. Sabaliauskaite G., Adepu S., and Mathur A., “A six-step model for safety and security analysis of complex cyber-physical systems”, The 7th international conference “Complex Systems Design & Management” (CSD&M)
27. Sun Y., Li W., Song W., Yuen C., “False Data Injection Attacks with Local Topology Information against Linear State Estimation,” IEEE PES Innovative Smart Grid Technologies 2015 Asian Conference (IEEE ISGT-Asia 2015)
28. Tan T. H., Sun J., Xue Y., Chen M., Dong J. S., Liu Y., “Optimizing Selection of Competing Features via Feedback-Directed Evolutionary Algorithms,” International Symposium on Software Testing and Analysis (ISSTA 2015)
29. Urbina D. I., Giraldo J., Cárdenas A. A., Tippenhauer N. O., Valente J., Faisal M., Ruths J., Candell R., and Sandberg H., “Limiting The Impact of Stealthy Attacks on Industrial Control Systems”, CCS 2016
30. Urbina D., Giraldo J. and Cardenas A., Tippenhauer N. O., “Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed,” Singapore Cyber Security R&D Conference (SG-CRC 2016)
31. Wang J. and Sun J., “Verifying Complex Systems Probabilistically through Learning, Abstraction and Refinement.” TACAS 2016. Submitted.
32. Yuen C., “Achievable Ergodic Secrecy Rate for MIMO SWIPT Wiretap Channels,” IEEE International Conference on Communications (IEEE ICC 2015)
33. Yuen C., “On the Existence of MDS Codes Over Small Fields With Constrained Generator Matrices,” IEEE International Symposium on Information Theory (IEEE ISIT 2014)

Network Engineering Techniques for Wireless Security

1. C. Cheng, J. Lee, T. Jiang, and T. Takagi, “Security analysis and improvements on two

homomorphic authentication schemes for network coding," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 993-1002, May 2016

2. C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Secret group key generation in physical layer for mesh topology" in Proc. IEEE Global Commun. Conf., San Diego, CA, Dec. 2015, pp. 1-6
3. C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," IEEE Transactions on Wireless Communications, vol. 15, no. 2, pp. 1517-1530, Feb. 2016
4. C. D. T. Thai, J. Lee, C. Cheng, and T. Q. S. Quek, "Physical-layer secret key generation with untrusted relays" in Proc. IEEE Global Commun. Conf., Workshop on Trusted Communications with Physical Layer Security, Austin, TX, Dec. 2014, pp. 1–6
5. F. Wang, X. Yuan, J. Lee, and T. Q. S. Quek, "Wireless MIMO switching with trusted and untrusted relays: degrees of freedom perspective," in Proc. IEEE Int. Conf. Commun., London, UK, Jun. 2015, pp. 1-6
6. J. Lee and T. Q. S. Quek, "Device-to-device communication in wireless mobile social networks," in Proc. IEEE Semiannual Veh. Technol. Conf., Seoul, Korea, May 2014
7. J. Lee, J. Ryu, C. D. T. Thai, J. Wang, F. Wang, and T. Q. S. Quek, "Friends or foes – the design of confidential cooperative communication with untrustworthy relay," IEEE Commun. Mag.
8. J. Ryu, J. Lee, and T. Q. S. Quek, "Confidential cooperative communication with trust degree of potential eavesdroppers," IEEE Transactions on Wireless Communications
9. J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Secure communication via jamming in massive MIMO Rician channels" in Proc. IEEE Global Commun. Conf., Workshop on Massive MIMO: From theory to practice, Austin, TX, Dec. 2014, pp. 1–6
10. J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," IEEE Trans. Wireless Commun., vol. 14, no. 12, pp. 6854-6868, Dec. 2015
11. Jong Yeol Ryu, Jemin Lee, and Tony Q. S. Quek, "Trust degree based beamforming for MISO cooperative communication system," IEEE Communications Letters, vol. 19, no. 11, Nov. 2015
12. L. Q. Duy, T. Q. S. Quek, and J. Lee, "A game theoretic model for enabling honeypots in IoT networks," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumper, Malaysia, May 2016
13. P. Mohapatra, N. Pappas, J. Lee, T. Q. S. Quek, and V. Angelakis, "Stability region of 2-user full-duplex broadcast channel with secrecy constraint," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumper, Malaysia, May 2016
14. R. Hsu, J. Lee, and T. Q. S. Quek, "Reliable and Privacy Preserving Secure D2D Communication in LTE-A,? in Proc. ACM Int. Conf. on Security and Privacy in Wireless and Mobile Networks, New York, NY, Jun. 2015
15. R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "GRAAD: Group anonymous and accountable D2D communication in mobile networks," IEEE/ACM Transactions on Networking
16. R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "ReSIoT: Reconfigurable security for IoT," IEEE Wireless Communications
17. S.-Y. Chang, J. Lee, and Y.-C. Hu, "Noah: Keyed noise flooding for wireless confidentiality," in Proc. ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), Cancun, Mexico, Nov. 2015, pp. 141- 148

Research & Security Innovation Lab for IoT

1. Sachidananda, V., Toh, J., Siboni, S., Shabatia, A., Elovici Y., "Poster: Towards Exposing Internet of Things: A Roadmap", ACM Conference on Computer and Communications Security (CCS) 2016: 1820-1822
2. Siboni, S., Shabatia, A., Tippenhauer, N., Lee, J., Elovici, Y., "Advanced Security Testbed Framework for Wearable IoT Devices", ACM Transactions on Internet Technology (TOIT), 16(4): 26:1-26:25 (2016)
3. Meidan, Y., Bohadana, M., Shabati, A., Elovici, Y., Ochoa, M., Tippenhauer, N., Guarnizo, J.,D., "Poster: ProfilIoT: A Machines learning Approach for IoT Device Identification Based on Network Traffic Analysis", The 32nd ACM Symposium on Applied Computing (SAC 2017)
4. Guarnizo, J., Tambe, A., Bhunia, S., Ochoa, M., Tippenhauer, N., Shabtai, A., Elovici, Y., "SIPHON : Towards Scalable High-Interaction Physical Honeypots", 3rd ACM Cyber-Physical System Security Workshop (CPSS 2017), pp. 57- 68
5. Siby, S., Maiti, R., Tippenhauer, N., "IoTScanner: Detecting Privacy Threats in IoT

Neighborhoods", 3rd International Workshop on IoT Privacy, Trust, and Security (IoTPTS), pp. 23- 30

6. Sachidananda, V., Toh, J., Siboni, S., Shabati, A., Elovici, Y., "Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things" 3rd International Workshop on IoT Privacy, Trust, and Security (IoTPTS), pp. 3-10
7. Maiti, R., Siby, S., Sridharan, R., Tippenhauer, N., "Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios", 22nd European Symposium on Research in Computer Security (ESORICS), pp.247-264
8. Antonioli, D., Siby, S., Tippenhauer, N., "Practical Evaluation of Passive COTS Eavesdropping in 802.11b/n/ac WLAN", International Conference on Cryptology and Network Security (CANS 2017)

Security by Design for Interconnected Critical Infrastructures

1. Ahmed C. M., Murguia C., Ruths J., "Model-based Attack Detection Scheme for Smart Water Distribution Networks," ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017

Cyber Patrol

1. Elovici Y., Toh, J., "Cyber Security Patrol – Detecting Fake and Vulnerable WiFi-Enabled Printers", The 32nd ACM Symposium on Applied Computing (ACM SAC) 2017, pp. 535- 542
