Charting the Cyber-Physical System Security Landscape

PhD Candidacy Exam

Miguel A. Arroyo
miguel@cs.columbia.edu

Department of Computer Science
Columbia University

Nov 27th, 2018
10 A.M.
1401 NWC

1 Candidate Research Area Statement

Cyber-Physical Systems (CPS) are critical to multiple aspects of our daily lives. The dual operating nature and highly integrated control of CPS means that they not only inherit problems from traditional computing systems (ie. software vulnerabilities, hardware side-channels, etc), but introduce challenges of their own. The fundamental question that then arises is: to what degree can existing security techniques help and what new opportunities exist?

A cyber-physical system's feedback loop between the continuous analog (physical) and discrete digital (cyber) domains requires a re-evaluation of computer security principles & techniques to expose threats and defensive opportunities that can leverage their unique characteristics.

2 Faculty Committee Members

The candidate respectfully solicits the guidance and expertise of the following faculty members and welcomes suggestions for other important papers and publications in the exam research area.

- Prof. Suman Jana
- Prof. Simha Sethumadhavan
- Prof. Jeannette Wing

3 Exam Syllabus

The papers have broad coverage in the space of CPS, which are needed to make a fair assessment of these systems unique aspects that lead to new threats and defensive opportunities.

- I begin with attack papers that exploit various properties of CPS to identify threat vectors and additionally expose challenges faced from both an attacker's and defender's perspective.
- Next, I provide an overview of defensive techniques proposed across various CPS domains. I mainly focus on techniques that leverage the unique characteristics of these systems. These techniques may protect one or more CPS component.
- Finally, I conclude by highlighting opportunities for future work.

Table 1 categorizes attack papers according to the components they target. Table 2 categorizes techniques according to defensive objectives and highlights components they protect.

Component	References
Control	
Software Vulnerabilities	
Software vulnerabilities such as memory safety, concurrency, etc.	Szekeres et al. [1]
Algorithmic	
Violation of assumptions in control algorithms due to adversarial behavior.	Liu et al. [2] Dadras et al. [3]
Communication	
Network Protocols	
Vulnerabilities in protocols, topology, etc.	Checkoway et al. [4]
Sensing & Actuation	
Signal Spoofing	
Modification of an analog signal being sensed.	Shoukry et al. [5] Kune et al. [6] Son et al. [7] Park et al. [8]
Visual Spoofing	
Modification of a visual environment.	Davidson et al. [9] Eykholt et al. [10]

Table 1: CPS Threat Vectors

Objective	References	Component		
		Control	Comm.[1]	S&A
Prevention				
Authentication				
Verification of valid system component interaction.	Shoukry et al. [11]	–	–	✓
Formal Methods				
Sound verification of system properties.	Mitra et al. [12]	✓	–	–
	Bohrer et al. [13]	✓	–	–
Memory Safety				
Enforcement of memory safety related properties.	Clements et al. [14]	✓	–	–
Resilient Control				
Algorithms resilient to adversarial behavior.	Ivanov et al. [15]	✓	–	✓
System Architecture				
Structural organization of system components for high security assurance.	Liu et al. [16]	✓	–	✓
Detection				
Attestation				
Verification of system trustworthiness.	Valente and Cárdenas [17]	✓	–	✓
	Chen et al. [18]	✓	–	–
Intrusion Detection				
Monitor system properties for violations.	Cho et al. [19]	✓	–	✓
	Urbina et al. [20]	✓	–	✓
	Cheng et al. [21]	✓	–	–
Vulnerability Discovery				
Determine presence of system correctness errors (i.e. bugs).	Corteggiani et al. [22]	✓	–	–
	Pustogarov et al. [23]	✓	–	–
Mitigation				
Reconfiguration				
Ability to perform self-recovery.	Abdi et al. [24]	✓	–	✓
	Kong et al. [25]	✓	–	✓

Table 2: Defensive Techniques

[1] To the best of my knowledge no existing papers leverage unique CPS properties to protect Communication.

References

[1] L. Szekeres, M. Payer, T. Wei, and D. Song. Sok: Eternal war in memory. In *2013 IEEE Symposium on Security and Privacy*, pages 48–62, May 2013. doi: 10.1109/SP.2013.13.

[2] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-894-0. doi: 10.1145/1653662.1653666. URL http://doi.acm.org/10.1145/1653662.1653666.

[3] Soodeh Dadras, Ryan M. Gerdes, and Rajnikant Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '15, pages 167–178, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3245-3. doi: 10.1145/2714576.2714619. URL http://doi.acm.org/10.1145/2714576.2714619.

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX Security Symposium 2011, Proceedings*. USENIX Association, 2011. URL http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf.

[5] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *Proceedings of the 15th International Conference on Cryptographic Hardware and Embedded Systems*, CHES'13, pages 55–72, Berlin, Heidelberg, 2013. Springer. ISBN 978-3-642-40348-4. doi: 10.1007/978-3-642-40349-1_4. URL http://dx.doi.org/10.1007/978-3-642-40349-1_4.

[6] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159, May 2013. doi: 10.1109/SP.2013.20.

[7] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 881–896, Washington, D.C., 2015. USENIX Association. ISBN 978-1-931971-232. URL https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son.

[8] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. This ain't your dose: Sensor spoofing attack on medical infusion pump. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX, 2016. USENIX Association. URL https://www.usenix.org/conference/woot16/workshop-program/presentation/park.

[9] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. Controlling uavs with sensor input spoofing attacks. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX, 2016. USENIX Association. URL https://www.usenix.org/conference/woot16/workshop-program/presentation/davidson.

[10] Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, Amir Rahmati, and Dawn Song. Robust physical-world attacks on machine learning models. *CoRR*, abs/1707.08945, 2017. URL http://arxiv.org/abs/1707.08945.

[11] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 1004–1015, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3832-5. doi: 10.1145/2810103.2813679. URL http://doi.acm.org/10.1145/2810103.2813679.

[12] S. Mitra, T. Wongpiromsarn, and R. M. Murray. Verifying cyber-physical interactions in safety-critical systems. *IEEE Security Privacy*, 11(4):28–37, July 2013. ISSN 1540-7993. doi: 10.1109/MSP.2013.77.

[13] Brandon Bohrer, Yong Kiam Tan, Stefan Mitsch, Magnus O. Myreen, and André Platzer. Veriphy: Verified controller executables from verified cyber-physical system models. In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI 2018, pages 617–630, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5698-5. doi: 10.1145/3192366.3192406. URL http://doi.acm.org/10.1145/3192366.3192406.

[14] A. A. Clements, N. S. Almakhdhub, K. S. Saab, P. Srivastava, J. Koo, S. Bagchi, and M. Payer. Protecting bare-metal embedded systems with privilege overlays. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 289–303, May 2017. doi: 10.1109/SP.2017.37.

[15] Radoslav Ivanov, Miroslav Pajic, and Insup Lee. Attack-resilient sensor fusion for safety-critical cyber-physical systems. *ACM Trans. Embed. Comput. Syst.*, 15(1):21:1–21:24, February 2016. ISSN 1539-9087. doi: 10.1145/2847418. URL http://doi.acm.org/10.1145/2847418.

[16] Jed Liu, Joe Corbett-Davies, Andrew Ferraiuolo, Alexander Ivanov, Mulong Luo, G. Edward Suh, Andrew C. Myers, and Mark Campbell. Secure autonomous cyber-physical systems through verifiable information flow control. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS-SPC '18, pages 48–59, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5992-4. doi: 10.1145/3264888.3264889. URL http://doi.acm.org/10.1145/3264888.3264889.

[17] Junia Valente and Alvaro A. Cárdenas. Using visual challenges to verify the integrity of security cameras. In *Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015, pages 141–150, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3682-6. doi: 10.1145/2818000.2818045. URL http://doi.acm.org/10.1145/2818000.2818045.

[18] Y. Chen, C. M. Poskitt, and J. Sun. Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system. In *2018 IEEE Symposium on Security and Privacy (SP)*, volume 00, pages 240–252. doi: 10.1109/SP.2018.00016. URL doi.ieeecomputersociety.org/10.1109/SP.2018.00016.

[19] Kyong-Tak Cho, Kang G. Shin, and Taejoon Park. Cps approach to checking norm operation of a brake-by-wire system. In *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, ICCPS '15, pages 41–50, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3455-6. doi: 10.1145/2735960.2735977. URL http://doi.acm.org/10.1145/2735960.2735977.

[20] David I. Urbina, Jairo A. Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1092–1105, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4139-4. doi: 10.1145/2976749.2978388. URL http://doi.acm.org/10.1145/2976749.2978388.

[21] Long Cheng, Ke Tian, and Danfeng (Daphne) Yao. Orpheus: Enforcing cyber-physical execution semantics to defend against data-oriented attacks. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, ACSAC 2017, pages 315–326, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-5345-8. doi: 10.1145/3134600.3134640. URL http://doi.acm.org/10.1145/3134600.3134640.

[22] Nassim Corteggiani, Giovanni Camurati, and Aurélien Francillon. Inception: System-wide security testing of real-world embedded systems software. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 309–326, Baltimore, MD, 2018. USENIX Association. ISBN 978-1-931971-46-1. URL https://www.usenix.org/conference/usenixsecurity18/presentation/corteggiani.

[23] Ivan Pustogarov, Thomas Ristenpart, and Vitaly Shmatikov. Using program analysis to synthesize sensor spoofing attacks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, pages 757–770, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-4944-4. doi: 10.1145/3052973.3053038. URL http://doi.acm.org/10.1145/3052973.3053038.

[24] Fardin Abdi, Chien-Ying Chen, Monowar Hasan, Songran Liu, Sibin Mohan, and Marco Caccamo. Guaranteed physical security with restart-based design for cyber-physical systems. In *Proceedings of*

the 9th ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS '18, pages 10–21, Piscataway, NJ, USA, 2018. IEEE Press. ISBN 978-1-5386-5301-2. doi: 10.1109/ICCPS.2018.00010. URL https://doi.org/10.1109/ICCPS.2018.00010.

[25] Fanxin Kong, Meng Xu, James Weimer, Oleg Sokolsky, and Insup Lee. Cyber-physical system checkpointing and recovery. In *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*, ICCPS '18, pages 22–31, Piscataway, NJ, USA, 2018. IEEE Press. ISBN 978-1-5386-5301-2. doi: 10.1109/ICCPS.2018.00011. URL https://doi.org/10.1109/ICCPS.2018.00011.