Towards a Hardware/Software Co-Design Approach for CPS and IoT Security

Anomadarshi Barua (anomadab@uci.edu)

Introduction

My research sits at the intersection of hardware and software layers in CPSs and IoTs, exploring how interactions of cyber and physical components open a “Pandora’s Box” of unknown threats, specifically about how they affect the safety and controllability of closed-loop control from sensing to actuation. CPSs and IoTs are engineered systems that are built from, and depend upon the seamless integration of computation and physical components. Most attacks on CPSs and IoTs can be propagated from the physical domain to the cyber domain or vice-versa and hence, can be termed as cross-domain attacks. To understand these cross-domain attacks, a very different set of methodologies and tools are needed. Moreover, as these cross-domain attacks involve hardware and software layers, defenses against these vulnerabilities also demand new hardware/software co-design approaches to detect, contain and isolate vulnerabilities in CPSs and IoTs. **My recent and ongoing studies investigate technological threats to the safety of CPSs and IoTs. Themes I also investigate include CPS’s forensics and provenance, hardware and microarchitectural security, machine learning in embedded systems, low-power hardware and algorithms for robust defense, and distributed data architecture in CPSs and IoTs (Figure 1).**

My doctoral work addresses the cross-domain vulnerabilities in CPSs/IoTs and provide defenses in multiple contexts. **The outcome of my doctoral research results in the following assisted grants (future grants will be proposed to NSF: ENG & CISE and to NIH & DARPA)**:

- **NSF EAGER (ECCS-2028269, $300,000)**
- **Cisco Research ($100,000)**
- **NIH (1R41DA049615-01A1 and R41DA049615)**

My future research centers around achieving the following ***short and long-term goals*** covering the large picture of CPS and IoT security:

1. ***Short-term goals:*** My short-term goal is to keep continuing my research to find the loopholes that exist along the physical and cyber cross-domain layers. For example, during my Ph.D. study, I find a few interesting vulnerabilities present in CPS’s sensors that also get media coverage. I will keep continuing to discover loopholes **not only limited to the sensor domain** but also in other domains, such as **programmable logic controllers (PLCs), cloud infrastructures, embedded systems, and memory controllers** in CPSs. I will also consider **CPS forensics and attack provenance** to trace the loopholes and correct them accordingly.
2. ***Long-term goals:*** My long-term goals are to create tools and new architectures for safe and secured CPSs and IoTs. I will explore the possibility of providing **analog signal encryption** as a defense for sensors and PLCs that will simultaneously work for in-band and out-band fake injected input signals in real time without hampering the existing data processing speed or bandwidth of the CPSs or IoTs. I will explore analog signal encryptions for sensors with a focus on **spread-spectrum and channel encryption** using different traditional **numerical approaches and machine learning (ML) based data-centric approaches**. I will also re-engineer the **in-sensor computations, proposed first in one of my works [6],** and will prove its superiority compared to near-memory computations in terms of preserving security and bandwidth. I will work on a **new distributed sensor architecture** to support **my proposed in-sensor computation approach for CPS forensics** that will integrate sensors in a well-organized way and optimizes the whole end-to-end CPSs. This will certainly trigger the industry-academia collaboration with a probability of new spin-offs from academia.

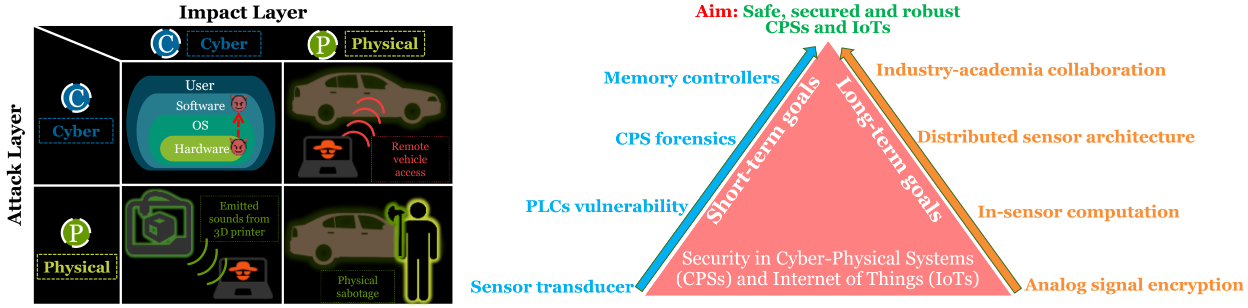

Figure 1: (Left) A cross-domain attack and defense research. (right) My short-term and long-term research goals.

Background and Current Work

My current research covers a few short and long-term goals regarding cross-domain attacks and defenses for achieving a safe and secured CPS and IoT. The representative works in my current research can be categorized into the following themes.

Finding vulnerabilities in CPSs and IoTs (*1. Short-term goals*)

Leaking Deadly pathogens. A Negative Pressure Room (NPR) is an essential requirement by the Bio-Safety Levels (BSLs) in biolabs because it maintains a negative pressure inside with respect to the outside reference space so that microbes are contained inside of an NPR [1]. Nowadays, differential pressure sensors (DPSs) are used in NPRs to control and monitor the negative pressure in an NPR. We demonstrate a non-invasive and stealthy attack on NPRs by spoofing a DPS at its resonant frequency. The main contributions are: (i) We show that DPSs used in NPRs typically have resonant frequencies in the audible range. (ii) We use this finding to design malicious music to create resonance in DPSs, resulting in an overshooting of the DPS's normal pressure readings. (iii) We show how the resonance in DPSs can fool the NPR, turning its negative pressure to a positive one, causing a potential *leak* of deadly microbes from NPRs. Moreover, we demonstrate our attack at a real-world NPR located in an anonymous FDA approved bioresearch facility.

BayesImposter: Weaponizing a Siemens PLC with Rowhammer. Over the last six years, several papers used memory deduplication to trigger various security issues, such as leaking heap address and causing bit-flip in the physical memory, by providing identical copies of a physical page. Recent works use a brute-force approach to create identical copies of a physical page that is an inaccurate and time-consuming primitive from the attacker's perspective. Our work begins to fill this gap by providing a structured way to duplicate a physical page in cloud settings in the context of industrial control systems (ICSs). Here, we show a new attack primitive - *BayesImposter*, which can duplicate the .bss section of the target DLL file of cloud protocols using *Bayesian estimation* [2]. Our approach results in less memory (i.e., 4 KB compared to GB) and time (i.e., 13 minutes compared to hours) compared to the brute-force approach used in recent works. We create a real-world automation platform using an automated high-bay warehouse and industrial-grade SIMATIC S7-1500 PLC from Siemens and demonstrate that *BayesImposter* can predictively inject false commands causing possible machine failure in the target ICS.

Hall Spoofing. Nowadays, smart sensors and transducers are tightly integrated into power CPSs. This integration opens the "Pandora's Box" of unknown threats that could come from very unconventional ways. We demonstrate a noninvasive attack that could come by spoofing the Hall sensor of power systems by using an external magnetic field [3, 4, 5]. We demonstrate how an attacker can camouflage an attack tool and place it near a target power grid and can intentionally perturb grid voltage and frequency and can inject false real and reactive power into the grid. We also show the consequences of the attack on a scaled-down power grid with a commercial 140 W grid-tied inverter from Texas Instruments. We can achieve a 31.52% change in output voltage, 3.16x (-6dB to -11dB) increase in low-frequency harmonics power, and 3.44x increase in real power. To the best of our knowledge, this is the first methodology that highlights the possibility of such an attack that might lead to grid blackout in a weak grid.

Providing defenses for CPSs and IoTs (*1. Short-term goals + 2. Long-term goals*)

HALC. Several papers have been published over the last ten years to provide a defense against intentional spoofing of sensors. However, these defenses would only work against those spoofing signals, which have a separate frequency from the original signal being measured. These defenses would not work if the spoofing attack signal (i) has a frequency equal to the frequency of original signals, (ii) has zero frequency, and (iii) is strong enough to drive the sensor output close to its saturation region. We proposed defense HALC [6] that can detect and contain all types of strong and weak magnetic spoofing, such as constant, sinusoidal, and pulsating magnetic fields, in real-time. HALC works up to ~9000 G of external magnetic spoofing up to 150 kHz, whereas existing defenses work only when the spoofing signals have a separate frequency from the original signal being measured. HALC utilizes the analog and digital cores to achieve a constant computational complexity O(1). We have tested HALC on ten different industry-used Hall sensors from four manufacturers and demonstrated its efficacy in two practical systems: a grid-tied solar inverter and a rotation-per-minute measurement system.

PreMSat. Existing defenses do not work against a strong magnetic spoofing attack that can drive the passive Hall sensor output in its saturation region. We name this as the saturation attack. In the saturation region, the output gets flattened, and no information can be retrieved, resulting in a denial-of-service attack on the sensor. Our work provides a defense named PreMSat against the saturation attack on passive Hall sensors. The core idea behind PreMSat [7] is that it can generate an internal magnetic field having the same strength but in opposite polarity to external magnetic fields injected by an attacker. Therefore, the generated internal magnetic field by PreMSat can nullify the injected external field while preventing: (i) intentional spoofing in the sensor's linear region, and (ii) saturation attack in the saturation region. PreMSat can prevent the magnetic saturation attack up to ~4200 A-t within a frequency range of 0Hz--30kHz with low cost (~$14), whereas the existing works cannot prevent saturation attacks with any strength. We create a prototype of PreMSat and evaluate its performance in a practical system - a grid-tied solar inverter.

Brain-Inspired algorithm for one-pass real-time learning and anomaly detection. A neuro-cognitive inspired architecture named as Hierarchical Temporal Memory (HTM) is proposed for anomaly detection and simultaneous data prediction in real-time for smart grid uPMU data. The key technical idea is that the HTM learns *a sparse distributed temporal representation* of sequential data that turns out to be very useful for anomaly detection and simultaneous data prediction in real-time [8, 9, 10]. Our results show that the proposed HTM can predict anomalies within 83% - 90% accuracy for three different application profiles, namely Standard, Reward Few False Positive, and Reward Few False Negative for two different datasets. We show that the HTM is competitive with five state-of-the-art algorithms for anomaly detection. Moreover, for the multi-step prediction in the online setting, the same HTM also performs well and is also competitive with six state-of-the-art prediction algorithms. We demonstrate that the same HTM model can be used for both the tasks and can learn online in one-pass, in an unsupervised fashion and adapt to changing statistics.

Future Directions on Hardware/Software Co-design for CPS and IoT Security

The *usability and efficiency* of defenses in CPSs and IoTs cannot be achieved *alone* by only hardware or only software modifications; instead, a hardware/software (HW-SW) co-design [11] approach is required. For example, sensors in CPS should be redesigned from the transducer level to in-sensor levels. **My future research [12] will involve CPS forensics, attack provenance, building smart transducers, and designing intelligent algorithms for in-sensor and distributed sensor architecture to secure CPSs and IoTs. We explain the paths below to achieve this roadmap.**

1. Encryption of analog signal (*1. Short-term goals + 2. Long-term goals*)

One of the main reasons for CPS vulnerability is the legitimate analog signal, which is going to be measured by the sensor, is not encrypted before going into the transducer. Therefore, the attacker can use a fake signal to corrupt the legitimate signal. This problem can be solved by encrypting the legitimate analog signal with a key in the ***analog domain*** and decrypting the legitimate signal on the transducer side using the same key. My future research will explore analog domain encryption in the following ways: ***First,*** I will explore the padding of an orthogonal noise with the legitimate signal to hide the information from the attack surface. This method is known as analog scrambling. ***Second,*** I will explore the mapping of the legitimate signal into the broad spectrum. This technique is known as frequency spread spectrum and can be adopted in the sensor domain. In one recent ongoing project [13], I am exploring this technique for sensor data encryption. According to preliminary results, this method has promising data obfuscation capabilities.

2. Modifying the transducer (*1. Short-term goals*)

The transducer must be resilient enough to reject the injected fake signal. As a transducer is an entry point to the sensor, if a transducer can reject the fake signal, this approach would diminish the burden of using a complex encryption algorithm in the sensor hardware. I would like to explore the possibility of modifying the transducer for all sensors in general similar to the ***differential transducer technique***. In a differential transducer approach, two transducers are placed inside a sensor in a differential manner to reject ***common-mode*** noise. As the injected fake signal is common to the differential transducers, the injected fake signal can be considered as common-mode noise and can be eliminated from the sensor at the ***transducer level***. Though this strategy is quite novel, it has its own implementation challenge for all types of sensors. Research along this direction would be *influential* in the future for secured CPSs and IoTs.

3. In-sensor computations for CPS and IoT security (*1. Long-term goals*)

The core idea behind ***in-sensor computation*** is that the sensing and computations of signals will be implemented in the sensor-domain; instead of implemented inside a discrete system controller. In-sensor computation will have ***analog and digital cores*** for HW-SW co-design implementation. The analog and digital cores will work ***parallelly*** in two separate paths to process inputs enabling faster signal processing. In-sensor computation will be much low-power, faster, and will not hamper the existing speed of CPSs and IoTs. The in-sensor computation can be also used to prevent sensors from going into saturation as in the saturation region, the output gets flattened, and no information can be retrieved, resulting in a DoS attack. This attack is known as saturation attack. The core idea behind preventing a saturation attack is to generate an internal signal, which has the *same* strength but in *opposite polarity* to the injected fake signal, so that the internal signal can nullify the injected fake signal. We conceptualized this idea for Hall sensors by providing a defense named *PreMSat* using in-sensor computations. I would like to extend my research experience from *PreMSat* to other sensor types as well [7].

4. CPS forensics and attack provenance (*1. Short-term goals + 2. Long-term goals*)

CPS logs are invaluable for forensic audits. However, CPS logs grow so large because of their underlying complexity, and often fine grains logs are quickly discarded to minimalize the cost related to data storage and data processing. This also creates problems by preventing the provenance-based investigation techniques that have gained popularity in the literature. Encouragingly, forensically-informed methods for reducing the size of system logs are a subject of frequent study. Unfortunately, many of these techniques are designed for an offline reduction in a central server, meaning that the up-front cost of log capture, storage, and transmission must still be paid at the endpoints. Therefore, I am proposing and will research ***in-sensor CPS forensics*** for data off-loading from the server that will result in less data storage and transmission to the server ***as most of the forensics and attack provenance*** will be performed inside of sensors.

5. Distributed sensor architecture for CPS and IoT security (*1. Long-term goals*)

Today, data is generated with higher velocity and higher volume than can be feasibly stored, raising the need for new algorithms, software abstractions, and systems. Majority of these data are coming from different sensors in CPSs and IoTs. However, today's CPS architecture is missing *distributed sensor systems* which will help to provide ***distributed online data processing***. The idea of distributed online data processing will be accomplished inside of the ***distributed sensor systems*** *enabling less data handling by the main system controller. This will enable comparatively low-power and* low-complexity algorithms running inside *distributed sensor systems*. A viable option can be using machine learning (ML) algorithms to create an appropriate ***context*** and ***abstraction*** of the sensor data [14] from *distributed sensor systems.* Therefore, during an attack, the sensor data can be recovered from a proper context using abstracted sensor data. The data abstraction can be made intelligent and adaptive to tackle the continuous change of the sensor environment. A low-power ML algorithm named as Hierarchical Temporal Memory (HTM) to detect *contex-aware* anomaly detection on the sensor data can be explored in this context. My previous research experience on this will help to build the distributed sensor architecture.

Conclusion: The Hardware/software co-design approach integrates all the CPSs components in a well-organized way and optimizes the whole end-to-end CPSs. I would like to continue to collaborate with both academia and industry and investigate all the promising opportunities discussed here and push design and optimization of modern defenses for the CPS and IoT security to the next level.

References

1. **A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music.**
Anomadarshi Barua, Yonatan Gizachew Achamyeleh, M. A. Al Faruque. To appear at the 29th ACM Conference on Computer and Communications Security (ACM CCS), 2022.

2. **BayesImposter: Bayesian Estimation Based .bss Imposter Attack on Industrial Control Systems.**
Anomadarshi Barua, Lelin Pan, M. A. Al Faruque. To appear at Annual Computer Security Applications Conference (ACSAC), 2022.

3. **Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter.**
Anomadarshi Barua and M. A. Al Faruque. 29th USENIX Security Symposium (USENIX Security 2020), pp. 1273-1290, 2020.

4. **The Hall Sensor Security.**
Anomadarshi Barua and M. A. Al Faruque. Encyclopedia of Cryptography, Security and Privacy, Springer Nature, 2021-22.

5. **Noninvasive Sensor-Spoofing Attacks on Embedded and Cyber-Physical Systems.**
Anomadarshi Barua and M. A. Al Faruque. IEEE 38th International Conference on Computer Design (ICCD), pp. 45-48, 2020.

6. **HALC: A Real-time In-sensor Defense against the Magnetic Spoofing Attack on Hall Sensors.**
Anomadarshi Barua, M. A. Al Faruque. 25th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2022.

7. **PreMSat: Preventing Magnetic Saturation Attack on Hall Sensors**
Anomadarshi Barua, M. A. Al Faruque. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Aug 31:438-62, 2022.

8. **Hierarchical temporal memory based one-pass learning for real-time anomaly detection and simultaneous data prediction in smart grids.**
Anomadarshi Barua, D Muthirayan, PP Khargonekar, M. A. Al Faruque. IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1770-1782, 2022.

9. **Hierarchical Temporal Memory Based Machine Learning for Real-Time, Unsupervised Anomaly Detection in Smart Grid**
Anomadarshi Barua, D. Muthirayan, P. P. Khargonekar and M. A. Al Faruque. ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), pp. 188-189, 2020.

10. **Brain-Inspired Golden Chip Free Hardware Trojan Detection.**
S. Faezi, R. Yasaei, **Anomadarshi Barua,** M. A. Al Faruque. IEEE Transactions on Information Forensics and Security, pp. 2697-2708, 2021.

11. **Analog and digital co-design techniques to mitigate non-invasive spoofing attack on magnetic sensors.**
M. A. Al Faruque and **Anomadarshi Barua**. US Patent App. 17/518,483, 2022.

12. **Sensor Security: Current Progress, Research Challenges, and Future Roadmap.**
Anomadarshi Barua, M. A. Al Faruque. To appear at the 41st International Conference on Computer-Aided Design (ICCAD), 2022.

13. **Spreading Magnetic Transduction Medium for Securing Voltage and Current Magnetic Sensors against EMI Spoofing.**
Anomadarshi Barua, Mohammad Abdullah Al Faruque. Under review at a top anonymous conference to be appeared in 2023.

14. **Tool of Spies: Leaking your IP by Altering the 3D Printer Compiler.**
S. R. Chhetri, **Anomadarshi Barua,** S. Faezi, F. Regazzoni, A. Canedo and M. A. Al Faruque. IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 667-678, 1 March-April 2021.