2021 ASEE ANNUAL CONFERENCE

Virtual Meeting | July 26–29, 2021 | Pacific Daylight Time

ASEE

Paper ID #35654

2020 BEST PIC I PAPER WINNER - Hands-On Cybersecurity Curriculum Using a Modular Training Kit

Mr. Asmit De, Pennsylvania State University

Asmit De is a PhD Candidate in Computer Engineering at PennState. His research interest is in developing secure hardware and architectures for mitigating system vulnerabilities. Asmit received his B. Tech degree in Computer Science and Engineering from National Institute of Technology Durgapur, India in 2014. He worked as a Software Engineer in the enterprise mobile security team at Samsung R&D Institute, India from 2014 to 2015. He has also worked as a Design Engineer Intern in the SoC Template team at SiFive Inc. developing security IPs in summer 2019.

Dr. Mohammad Nasim Imtiaz Khan
Mr. Abdullah Ash Saki
Mr. Md Mahabubul Alam
Mr. Taylor Steven Wood, Pennsylvania State University
Dr. Matthew Johnson, Pennsylvania State University
Mr. Manoj Varma Saripalli
Ms. Yu Xia
Dr. Stephanie Cutler, Pennsylvania State University
Swaroop Ghosh, Pennsylvania State University
Dr. Kathleen M. Hill
Dr. Annmarie Ward

ASEE'S VIRTUAL CONFERENCE
At Home with Engineering Education JUNE 22 - 26, 2020 #ASEEVC
Paper ID #31471

Hands-On Cybersecurity Curriculum using a Modular Training Kit

Mr. Asmit De, The Pennsylvania State University

Asmit De is a PhD Candidate in Computer Engineering at PennState. His research interest is in developing secure hardware and architectures for mitigating system vulnerabilities. Asmit received his B. Tech degree in Computer Science and Engineering from National Institute of Technology Durgapur, India in 2014. He worked as a Software Engineer in the enterprise mobile security team at Samsung R&D Institute, India from 2014 to 2015. He has also worked as a Design Engineer Intern in the SoC Template team at SiFive Inc. developing security IPs in summer 2019.

Mr. Mohammad Nasim Imtiaz Khan, The Pennsylvania State University

Nasim is a final year Doctorate student. His research interest is hardware security.

Mr. Karthikeyan Nagarajan, Pennsylvania State University

Karthikeyan is a second-year doctoral student in the School of Electrical Engineering and Computer Science of The Pennsylvania State University (Penn State), under the advisement of Dr. Swaroop Ghosh. Karthikeyan received his Bachelors ('15) and Masters ('17) from the Department of Electrical and Computer Engineering at Georgia Institute of Technology. Before starting his Ph.D., Karthikeyan was a Technology Analyst at the firm GrowthPilot in Atlanta and has also worked as a Systems Solutions Intern at Samsung Semiconductor in San Jose. His research interests include hardware security and low-power circuit design. Currently, he is exploring the security and privacy aspects of emerging non-volatile memories like STTRAM, MRAM and RRAM, and their cryptographic applications. He is a student member of IEEE.

Mr. Abdullah Ash Saki, Pennsylvania State University
Mahabubul Alam, Pennsylvania State University

Mahabubul Alam received his B.Sc. degree in electrical and electronic engineering from the Bangladesh University of Engineering and Technology (BUET) in 2015. He is currently pursuing a Ph.D. degree in electrical engineering at Pennsylvania State University. He was an ASIC Physical Design Engineer with PrimeSilicon Technologies. He was an Intern with Qualcomm Flarion Technologies in 2018. His current research interests include quantum circuit noise resilience, optimization techniques/design automation, and hardware security.

Mr. Taylor Steven Wood, Pennsylvania State University, University Park

Taylor received his B.S. degree in Physics from Brigham Young University, after which he worked for 5 years as a semiconductor engineer for Micron Technology in Boise, ID, specializing in numerical and computational data analysis. During this time, he also volunteered extensively with the educational arm of the Micron Foundation, bringing inquiry-based STEM outreach lessons to K-12 classrooms throughout the Boise area and serving as a career mentor to high school students interested in pursuing engineering as a career. Taylor's role at CSATS focused on interfacing with science and engineering research faculty to develop and implement K-12 teacher professional development. Currently, Taylor is pursuing a doctorate degree in Materials Science and Engineering and Penn State University.

Dr. Matthew Johnson,

Matt is an Assistant Professor with the Center for Science and the Schools in the College of Education at Penn State University. His research interests focus on how teachers learn about epistemic practices of engineers through in-service teacher professional development programs and how they provide opportunities for students to engage in them to learn disciplinary content.

Mr. Manoj Varma Saripalli, The Pennsylvania State University
Ms. Yu Xia, Pennsylvania State University

Yu Xia is a doctoral candidate in Learning, Design, and Technology program in College of Education and research assistant in Leonhard Center for Enhancement of Engineering Education in College of Engineering at Penn State. She is currently doing research of collaborative learning in various learning contexts.

Dr. Stephanie Cutler, Pennsylvania State University, University Park

Stephanie Cutler has a Ph.D. in Engineering Education from Virginia Tech. Her dissertation explored faculty adoption of research-based instructional strategies in the statics classroom. Currently, Dr. Cutler works as an assessment and instructional support specialist with the Leonhard Center for the Enhancement of Engineering Education at Penn State. She aids in the educational assessment of faculty-led projects while also supporting instructors to improve their teaching in the classroom. Previously, Dr. Cutler worked as the research specialist with the Rothwell Center for Teaching and Learning Excellence Worldwide Campus (CTLE - W) for Embry-Riddle Aeronautical University.

Dr. Swaroop Ghosh, Penn State

Swaroop Ghosh received the B.E. (Hons.) from IIT, Roorkee, India, the M.S. degree from the University of Cincinnati, Cincinnati, and the Ph.D. degree from Purdue University, West Lafayette. He is an assistant Professor at Penn State University. Earlier, he was with the faculty of University of South Florida. Prior to that, he was a Senior Research and Development Engineer in Advanced Design, Intel Corp. At Intel, his research was focused on low power and robust embedded memory design in scaled technologies. His research interests include low-power circuits, hardware security, quantum computing and digital testing for nanometer technologies.

Dr. Ghosh served as Associate Editor of the IEEE Transactions On Computer-Aided Design (2019-) and IEEE Transactions On Circuits and Systems I (2014-2015) and as Senior Editorial Board member of IEEE Journal of Emerging Topics on Circuits and Systems (JETCAS) (2016-2018). He served as Guest Editor of the IEEE JETCAS (2015-2016) and IEEE Transactions On VLSI Systems (2018-2019). He has also served in the technical program committees of ACM/IEEE conferences such as, DAC, ICCAD, CICC, DATE, ISLPED, GLSVLSI, Nanoarch and ISQED. He served as Program Chair of ISQED (2019) and DAC Ph.D. Forum (2016) and track (co)-Chair of CICC (2017-2019), ISLPED (2017-2018) and ISQED (2016-2017).

Dr. Ghosh is a recipient of Intel Technology and Manufacturing Group Excellence Award in 2009, Intel Divisional Award in 2011, Intel Departmental Awards in 2011 and 2012, USF Outstanding Research Achievement Award in 2015, College of Engineering Outstanding Research Achievement Award in 2015, DARPA Young Faculty Award (YFA) in 2015, ACM SIGDA Outstanding New Faculty Award in 2016, YFA Director's Fellowship in 2017, Monkowsky Career Development Award in 2018, Lutron Spira Teaching Excellence Award in 2018 and Dean's Certificate of Excellence in 2019. He is a Senior member of the IEEE and the National Academy of Inventors (NAI), and, Associate member of Sigma Xi. He serves as a Distinguished Speaker of the Association for Computing Machinery (ACM) for a 3 year term (2019-2022).

Dr. Kathleen M. Hill, Pennsylvania State University
Dr. Annmarie Ward

Hands-On Knowledge on Cybersecurity with a Self-Learning Kit

Abstract

There is an exponential growth in the number of cyber-attack incidents resulting in significant financial loss and national security concerns. Secure cyberspace has been designated as one of the National Academy of Engineering (NAE) Grand Challenges in engineering. Broadly, the security threats are targeted on software programs, operating system and network with the intention to launch confidentiality, integrity and availability violations. Existing undergraduate and graduate-level cybersecurity education curriculum rely primarily on didactic teaching methods with little focus on student centered, inquiry-based teaching, known to improve student learning. With growing number of security incidents taking place, it is of utmost importance to prepare a workforce equipped with knowledge of the threat space and existing state-of-the-art solutions. Such comprehensive understanding is only possible by a dedicated hands-on course on cybersecurity where students can learn the key concepts by editing the hardware, software and OS, and, network policies. Unfortunately, such extensive and deep flexibilities are not provided in current cybersecurity curriculum.

In this paper, we introduce a hands-on and modular self-learning Cybersecurity Training (CST) Kit to advance cybersecurity education. Students can promptly apply newly acquired knowledge on the CST Kit as part of the learning process. This Kit accompanies Do-It-Yourself (DIY) training modules that is used to model and investigate cybersecurity issues and their prevention to all levels of the cybersecurity workforce, including undergraduate and graduate students and K-12 science and technology teachers. The Kit also covers various aspects of cybersecurity issues including, hardware, software, operating system and network security. A coursework has been developed on hardware security for senior undergraduate and graduate students using the Kit. A preliminary survey conducted among students who were introduced to the modular board to implement hardware security threats such as, side-channel attack shows an 120% improvement in their understanding after the CST Kit based activities. The components of the CST Kit have also been used in a 4-day summer workshop for K-12 teachers. Teachers took pre- and post- concept inventories to assess their learning of content throughout the workshop and the results indicated improvement of 58%. These assessments focused on vulnerabilities and specific types of attacks, system security, data transmission and encryption, permutations and combinatorics, and binary numbers.

1. Introduction

There is an exponential growth in the number of cyber-attack incidents in the recent years resulting in significant financial loss and national security concerns. Secure cyberspace has been designated as one of the National Academy of Engineering (NAE) Grand Challenges in engineering. Broadly, the security threats are targeted on software programs, operating system and network with the intention to launch confidentiality, integrity and availability violations. Existing undergraduate and graduate-level cybersecurity education curriculum introduces the threats and countermeasures at the theoretical level. Therefore, the students are not exposed to practical understanding and lack technical insights. In addition, these efforts rely primarily on didactic teaching methods with little focus on student centered, inquiry-based teaching, known to improve student learning. With growing number of security incidents taking place, it is utmost important to prepare a workforce equipped with knowledge of the threat space and existing state-of-the-art solution. Such comprehensive understanding could only be possible by a dedicated hands-on course on cybersecurity where students can learn the key concepts by editing the hardware, software and OS, and, network policies. Unfortunately, such extensive and deep flexibilities are not provided in current cybersecurity curriculum. Therefore, we have designed a hands-on and self-learning Cybersecurity Training (CST) Kit and Do-It-Yourself (DIY) training modules which can advance cybersecurity education among students and professionals through it. This modular kit-based training approach has shown to be effective due to its simplicity, and hands-on practical demonstration setups, requiring little to no extra infrastructure setup.

Existing undergraduate (UG) and graduate-level cybersecurity education curriculum conveys the software, Operating System (OS), network and hardware level security threats with little consideration to the underlying role played by the system memories. The concepts are covered in isolation which fail to provide the desired visibility to the students. Furthermore, the courses introduce the threats and countermeasures at a theoretical level. Therefore, the students are not exposed to practical understanding and hence, lack technical insights. With the growing number of security incidents taking place, it is of utmost importance to prepare a workforce equipped with knowledge of the threat space on memories and the existing state-of-the-art solutions. Such comprehensive understanding can only be possible by a dedicated hands-on course on cybersecurity where students can learn the key concepts by editing the hardware, software and OS, and, network policies. Unfortunately, such extensive and deep flexibilities are not provided in current cybersecurity curriculum.

Furthermore, there is a definite gap in the Computer Science (CS) background of underrepresented minorities, including women as they enter undergraduate level educational institutions [1]. In the past, mandatory K-12 CS education has consisted largely of learning to use various software rather than including concepts, skills and practices needed by computer science engineers and technicians. Very little attention has been paid to developing the skills needed to prepare the students for entering the CS workforce. Recently, there has been a new emphasis on computer science education at the K-12 level by Pennsylvania and numerous other states. Components of this emphasis can be seen in the K12 Computer Science Framework [1], which provides guidelines for the development of intellectual skills and conceptual understanding of essential CS practices. This Framework proposes to bring CS to all students, not just a fortunate few. Students with the depth of understanding have mostly been self-motivated and self-taught. Pennsylvania has just recently determined that certain CS courses will be counted towards fulfilling science course requirements. With the inevitable development of standards for CS education, there will be a need for project-based curricula that incorporate important elements of computer science, engineering and technology, and create engaging and meaningful classroom projects exemplifying real-world CS endeavors in which all students can participate.

To address these concerns for developing students' computer science skills and, understanding and awareness of cybersecurity issues across multiple educational levels, we have developed and piloted a Do-It-Yourself (DIY) modular Cybersecurity Training (CST) Kit with the accompanying modular curriculum at variable levels. The Kit allows the students to test the concepts taught in class on real hardware immediately. It facilitates hands-on assignment where the students assemble modular hardware components and modify program binaries to achieve the desired goals. The Kit is based on a previously developed apparatus [2] for testing the impact of cybersecurity threats on magnetic memories. This existing apparatus was designed by an UG student as part of Honors Thesis and was used to demonstrate cybersecurity threats on memories [3]. The results obtained from this apparatus has been published in IEEE conferences and the UG students trained using this board have successfully competed in worldwide cybersecurity competitions [4]. The CST Kit will serve as a hands-on tool for use in several instructional settings to teach cybersecurity.

Modular hands-on-labs have been shown to improve learning. Several such labs or modular kits have already been developed in different domains to advance education. In [7], a modular microcontroller kit has been designed to teach various aspects of embedded operating systems. In [8], modular hands-on labs and courses have been developed to teach digital forensics. Similarly, in [9], modular online labs and lectures have been created to teach cybersecurity. A hardware security book accompanied with a Hardware Hacking platform in [10] provides theory and hands-on training on hardware security issues in all forms of electronic hardware.

This paper explores if hands-on learning, based on the simple, inexpensive DIY kit enable student learning. The results show that students can recreate the attack scenarios to study various aspects of cybersecurity vulnerabilities and threats, and, develop/validate their countermeasures on the DIY kit. *To the best of our knowledge, this is the first holistic attempt to advance cybersecurity education through a hands-on activity-based modular Kit*. In future, the recorded lecture of topic will be uploaded before every class with the intention of preparing the students for CST Kit activities and group discussions in class. Consequently, this will bind pedagogical techniques such as, classroom flipping [5], un-lecturing [6] and group learning in the course to create an engaging classroom environment. Group-based activities and final projects on the Kit will allow transfer of learning and motivate the students.

The rest of the paper is organized as follows: Section 2 provides the details of the CST kit and its components; Section 3 describes our piloting and evaluation strategy; and Section 4 draws the conclusion.

2. Cybersecurity Training Kit

The Cybersecurity Training Kit (CST) and associated Do-It-Yourself (DIY) training modules are designed to model and investigate cybersecurity issues and their prevention to all levels of the cybersecurity workforce, including undergraduate and graduate students, community, K-12 science and technology teachers, and industry professionals. The kit covers all aspects of cybersecurity issues including, hardware, software, operating system and network security.

The kit hardware consists of several boards that is designed to train and teach different aspects of cybersecurity. For our first iteration of the kit, we have setup the following hardware modules:

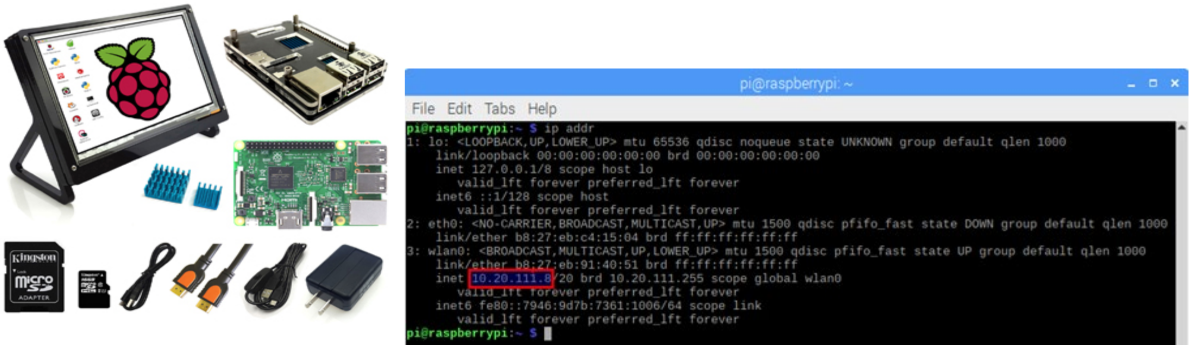
- CSTM01: Raspberry Pi for Cryptography, Software and Network Security
- CSTM02: FPGA Board for Side Channel Attacks on Cryptographic Algorithms
- CSTM03: FPGA Board for System Security Attacks on Embedded Systems
- CSTM04: FPGA Board for Magnetic Attacks on Emerging NVMs

Each of these hardware modules can be individually used to learn about a specific aspect of cybersecurity. The hardware modules are pre-configured to demonstrate the attacks and in some cases the defenses. The hardware setups are also accompanied by software required to interface with the boards. To complete the learning experience, DIY training modules are provided with each hardware setup. We will explain in detail the contents of each module.

CSTM01: Raspberry Pi for Cryptography, Software and Network Security

Basic cybersecurity education comes from knowing how to be a good digital citizen. That involves, among several things, learning about password etiquette and understanding their weaknesses, recognizing email phishing attempts and how to prevent being a victim of it. We have prepared a Raspberry Pi board to teach passwords and password cracking, phishing, network security and basics of cryptography (Fig. 1).

The Raspberry Pi comes with a Jupyter notebook that teaches the basic of programming using Python. Students can learn and write their own code that aids in the future activities of the module. We created activities to convey how to create strong passwords, and the students can write Python code to attempt to brute-force and crack weak passwords. Activities involving phishing include recognizing phishing attempts, and an example attack to demonstrate the consequences of becoming a victim of a phishing attempt. We teach about network security using Wireshark demonstrations, where a student can attempt to sniff an unsecure network communication. An activity is created to demonstrate how encrypting communication channels



```
pi@raspberrypi:~ $ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether b8:27:eb:c4:15:04 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether b8:27:eb:91:40:51 brd ff:ff:ff:ff:ff:ff
    inet 10.20.111.8/20 brd 10.20.111.255 scope global wlan0
       valid_lft forever preferred_lft forever
    inet6 fe80::7946:9d7b:7361:1006/64 scope link
       valid_lft forever preferred_lft forever
pi@raspberrypi:~ $
```

Fig. 1. CSTM01 Raspberry Pi kit and wireshark activity

may prevent sniffing attacks. This leads into learning the importance of securing network traffic, and encryption. We also teach basics of cryptography and ciphers using simple step-by-step code. Students can use the code from their Jupyter notebook to learn and try encryption/decryption using simple ciphers such as Caesar Cipher.

Learning Aim: The aim of this module is to introduce students to cybersecurity so that they can be aware of common threats and take basic countermeasures. The hands-on activities in the Raspberry Pi provides a practical glimpse of cybersecurity threats and aids in the learning process. The students need no additional equipment to use this module.

Module Components: To replicate this module, only a Raspberry Pi [11] board is required. Jupyter notebooks can be easily set up to run interactive python scripts [12,13]. Network sniffing can be demonstrated by installing Wireshark in the Raspberry Pi [14].

CSTM02: FPGA Board for Side Channel Attacks on Cryptographic Algorithms

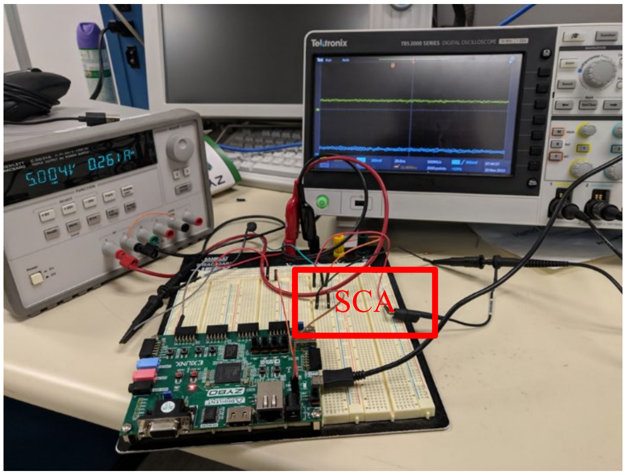


Fig. 2. CSTM02 hardware module

Modern cryptographic algorithms deployed in current systems are mathematically sound and secure. However, due to the specific nature of implementation in hardware, they may leave some side-channel signatures that may be leveraged to attack the cryptosystem. We have prepared a module with a FPGA, Breadboard and SCA Resistance as shown in Fig. 2, that can be used to exploit a hardware implementation of a cryptosystem.

The software provided along with the board consists of the hardware implementation code of several cryptosystems such as RSA, AES, etc. The code is flexible enough to be modified by students to experiment with different types of attacks.

Learning Aim: The aim of this module is to let the students experiment with the different cryptosystems and try to obtain power or timing side-channel signatures and reverse engineer the crypto key. The students require access to a computer, oscilloscope and power supply.

Module Components: To replicate the module, the components required are (i) FPGA board [15], (ii) 1Ω SCA Resistor, (iii) Breadboard and wires, (iv) RTL for a cryptosystem that can be run on the FPGA. The SCA resistance is inserted before the power source to the FPGA. RTL for cryptosystems are publicly available [16] and can be synthesized using Xilinx tools to run on the FPGA.

CSTM03: FPGA Board for System Security Attacks on Embedded Systems

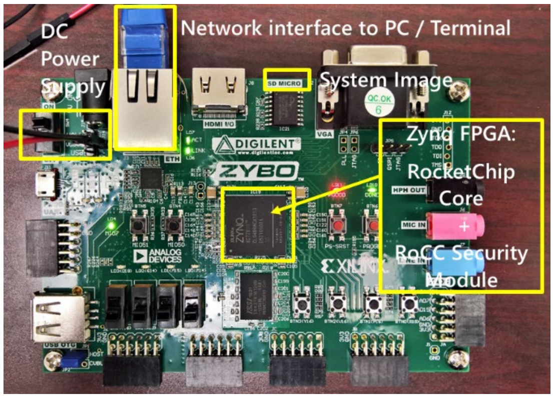

DC Power Supply
Network interface to PC / Terminal
System Image
Zynq FPGA: RocketChip Core
RoCC Security Module

Fig. 3. CSTM03 hardware module

Embedded systems are resource constrained which makes them compromise on security. System applications designed for such systems may often suffer from system security vulnerabilities such as buffer overflows. We have prepared a module with a FPGA that instantiates a RISC-V SoC and demonstrates common system security vulnerabilities as shown in Fig. 3.

The software provided along with the board consists of the hardware bitstream of the RISC-V RocketChip SoC that can be flashed to the FPGA. Sample vulnerable programs and attack payloads are provided to try out on the system. To demonstrate a defense against such attacks, we have also built hardware-based solutions and created a 'secure' version of the system. The students can run the same attack code on both the unprotected and protected versions of the systems and observe the behavior. The students can also write their own code and try to attack them on the system.

Learning Aim: The aim of this module is to let the students experiment with different types of system security attacks and build defenses around them. The open-source Rocket-Chip platform helps students design configure and customize the SoC code with ease. The provided toolchain and compilers help the students compile their own programs for running on the system. The students only require access to a computer to use this module.

Module Components: The module can be designed using just a FPGA [15]. The source code of the RocketChip system is available at [17] and can be compiled using the provided tools. The basic system security attacks and defenses can be modeled following [18] for the students to try out.

CSTM04: FPGA Board for Magnetic Attacks on Emerging NVMs

The emerging memory technologies offer higher density, lower cost/static power operation compared to conventional memories such as Static RAM (SRAM) or Dynamic RAM (DRAM). One flavor of emerging memory is Magnetic RAM (MRAM) which stores data in terms of magnetic orientation of a ferromagnetic layer. However, MRAM is susceptible to external magnetic field. An adversary can corrupt the stored memory in MRAM by applying a higher external magnetic field compared its tolerance.

We have prepared a module using a Xilinx Virtex-5 FPGA which is programmed to run specific March tests on the DUT. The FPGA is interfaced with a PC to acquire test results for flexible test automation and data analysis. This approach allows for easy replacement of the DUT and avoids any need for manual entry of results. Furthermore, this framework is modular which is amenable to new test routines and new flavors of memory such as: STT-MRAM and Ferroelectric RAM (FeRAM). We used commercially available toggle MRAM in 2 MB TSOP-44 packages manufactured by Everspin Technologies. The module setup is shown in Fig. 4.

The module is associated with an interfacing software that can be used to read and write data to the MRAM memory. The bitstream provided can be readily flashed onto the FPGA. Students can use the interfacing software to populate and monitor the memory cells of the MRAM. The attacks can be tried out by using commercially available strong magnets by bringing them in proximity to the MRAM to observe data corruption.

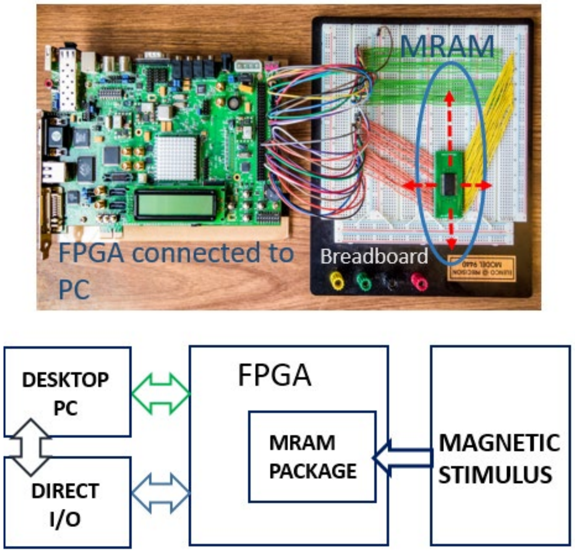


Fig. 4. CSTM04 hardware module

Learning Aim: The aim of this module is to enlighten the students regarding the susceptibility of the emerging memory technologies to external magnetic fields. The students can investigate basic countermeasures such as physical shielding of the memory.

Module Components: The following components are required to replicate the module: (i) FPGA board [19], (ii) MRAM [20], (iii) Breadboard and wires, (iv) Neodymium magnet [21]. The board setup and attacks can be modeled based on [3] for the students to try out.

3. Implementation and Piloting

3.1 Hardware security course

A 3-tier coursework is being developed to provide cybersecurity education to Junior and Senior-level undergraduate students, graduate students and professionals. The CST kit was piloted as part of a graduate level course titled EE/CSE597 Introduction to Hardware Security. The course introduces basic cybersecurity and then delves deeper into hardware and systems security. Modules CSTM02 and CSTM03 were used to supplement the topics of side-channel attacks and system security issues. Total enrollment of the course was 9.

The students completed surveys which included a pre-survey earlier in the semester and a post-survey after the middle of the semester. Generic to the surveys are three sets of rating questions about the importance of 8 topics to future career, about student interests in the same 8 topics, and about student confidence in carry out 12 types of tasks respectively. The pre-survey was then followed by 4 knowledge questions and a confidence rating for each question. The post-survey was followed by the 4 sets of knowledge questions and confidence level rating, again followed by three additional open-ended questions. All rating questions were assessed on a 5-point Likert scale (e.g., Not at all important = 1; Slightly important = 2; Somewhat important = 3; Important

= 4; Very important = 5). A summary of pre- and post- survey results are shown in Table I.

Pre-survey: In student rating of the 8 topics in terms of their importance to future career, *Integration of security as a design metric* received the highest mean score (*M* = 4.07), while *Counterfeit Electronics* was rated the least important (*M* = 2.71). In student rating of the 8 topics in terms of how much they were interested in, *Secure hardware for software security* received the highest mean score (*M* = 4.36), while again *Counterfeit Electronics* was rated the least important (*M* = 3.36). In student rating of their confidence in completing the 12 tasks, *Appropriately assess the relevance of my knowledge and skills to a project* received the highest mean score (*M* = 3.79), while *Talk about a project design using other discipline language* was

Table I – Summary Table for the Comparisons between Pre- and Post- Survey Results

Statement	Pre	Post
	M(SD)	M(SD)
Rate how* important *the following topics are to your future career:		
Integration of security as a design metric	**4.07(1.07)**	**4.43(0.79)**
Understanding cybersecurity attack to provide countermeasures	4.00(1.24)	**4.43(0.79)**
State-of-the-art security methods	4.00(1.11)	4.29(0.76)
Secure hardware for software security	3.79(1.12)	**4.43(0.79)**
Protecting intellectual property against piracy and tampering	3.57(1.34)	4.27(0.76)
Detection and isolation of hardware Trojans	3.21(1.12)	4.00(1.00)
Emerging nanotechnologies	3.00(1.18)	3.86(1.07)
Counterfeit Electronics	2.71(1.14)	3.57(0.79)
Rate how* interested *you are in the following topics:		
Secure hardware for software security	**4.36(1.22)**	4.14(0.69)
Understanding cybersecurity attack to provide countermeasures	4.29(1.14)	4.29(0.76)
State-of-the-art security methods	4.23(1.17)	4.29(0.49)
Integration of security as a design metric	3.93(1.39)	**4.43(0.54)**
Emerging nanotechnologies	3.71(1.27)	3.71(0.76)
Detection and isolation of hardware Trojans	3.57(1.22)	4.00(0.82)
Protecting intellectual property against piracy and tampering	3.50(1.23)	3.86(0.38)
Counterfeit Electronics	**3.36(1.39)**	**3.14(0.90)**
Appropriately assess the relevance of my knowledge and skills to a project.	**3.79(0.80)**	4.14(0.90)
Accurately evaluate how much my knowledge and skills contribute to a project	3.79(0.70)	**4.29(0.76)**
Clearly identify the type of knowledge and skills I bring to a project.	3.71(0.91)	**4.29(0.76)**
Be proactive in working on design problems with those from different disciplines	3.50(0.65)	4.14(0.69)
Examine a design issue from my teammate's perspective	3.43(0.65)	4.00(0.82)
Think of ways other members have influenced a project in a way that represents their academic disciplines.	3.29(1.00)	4.14(0.90)
Discuss the contributions other disciplines have made to a project	3.21(0.98)	**3.86(1.07)**
Accurately assess the extent to which my mastery of these knowledge and skills are adequate for a project.	3.21(0.80)	4.00(0.82)
Provide input to others from different disciplines	3.14(1.03)	4.14(0.69)
Clearly identify the type of knowledge and skills possessed by teammates from other disciplines	3.07(1.07)	4.00(0.82)
Accurately recognize goals that reflect the disciplinary backgrounds of other team members	3.00(1.18)	4.00(0.82)
Talk about a project design using other discipline language	**2.86(1.17)**	**3.86(1.07)**

rated as the least confident (*M* = 2.86). A total of 13 students completed 4 sets of knowledge questions and confidence level rating in the survey. There were 8, 6, 10, and 3 students who provided the correct answers respectively.

Post-survey: In student rating of the 8 topics in terms of their importance to future career, 3 topics received the highest scores: *Integration of security as a design metric* (*M* = 4.43)*, Understanding cybersecurity attack to provide countermeasures* (*M* = 4.43)*, and Secure hardware for software security* (*M* = 4.43), while *Counterfeit Electronics* continued to be rated as the least important (*M* = 3.57). In student rating of the 8 topics in terms of how much they were interested in, *Integration of security as a design metric* (*M* = 4.43), while again *Counterfeit Electronics* was rated the least important (*M* = 3.14). In student rating of their confidence in completing the 12 tasks, two tasks that rated the highest scores differed from pre-survey; they are *Clearly identify the type of knowledge and skills I bring to a project* (*M* = 4.29) and *Accurately evaluate how much my knowledge and skills contribute to a project* (*M* = 4.29), while *Talk about a project design using other discipline language* was again rated as the least confident (*M* = 3.86), with an addition one, Discuss the contributions other disciplines have made to a project (*M* = 3.86). A total of 7 students completed 4 sets of knowledge questions and confidence level rating in the survey. There were 3, 6, 7, and 7 students who provided the correct answers respectively. The evaluation showed a 58% improvement in their learning of the content after using the CSTM02 and CSTM03 modules as summarized in Table II:

Table II – Course Evaluation

	Average points earned	**Percentage Correct**
Pre-test	2.08	41.54%
Post-test	3.29	65.8%

Two additional open-ended questions were asked in post-survey. For the first question of *what elements of this activity were helpful to your learning*, students talked about a few topics: use of the CST hardware setup, oscilloscope, RTL coding, FPGA implementation, the real-life visualization of the power plots, practical programming experience, among which FPGA implementation was talked about 3 times.

3.2 K-12 teacher workshop

The CSTM01 module of the CST kit was also used in a 4-day summer workshop for K-12 teachers (Fig. 5). Teachers took pre- and post- concept inventories to assess their learning of content throughout the workshop. These assessments focused on vulnerabilities and specific types of attacks, system security, data transmission and encryption, permutations and combinatorics, and binary numbers.

The workshop was designed to build the teachers' capacity to better understand aspects of cybersecurity and to apply their skills in a culminating challenge at the end of the week. The final challenge was designed as a mock forensic investigation in which a man was murdered when he uncovered an embezzlement scheme at his company. Teachers were given "police reports" on each of the victims, each of whom had a Raspberry Pi with files and emails on for the

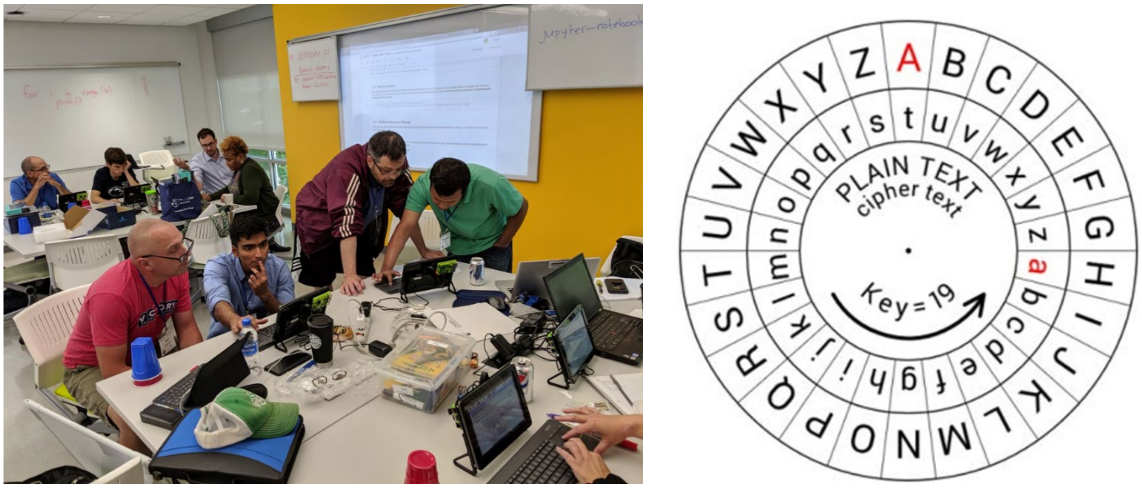

jupyter-notebook
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key = 19

Fig. 5. K-12 teacher workshop and Caesar Cipher activity

teachers to investigate. The following concepts were applied through participation in the final challenge:

1. Passwords should be strong – passwords to the computers of the suspects were found by reading the police report (i.e., pet's name, etc.)
2. Networks can be monitored – teachers used Wireshark on the fictional company's "server" to identify that there was an unusually high amount of activity on the embezzler's computer
3. Simple passwords can be discovered with brute force techniques – teachers used the program they wrote to hack into encrypted folders of communications between the embezzler and the hired murderer.
4. Ciphers – teachers used the program they wrote to crack Caesar Ciphers to read the communications between the embezzler and the murderer.

Teachers used these skills to identify the suspects that should be arrested. We have offered to lend these Raspberry Pis to the teachers if they want to run this activity with their students.

A total of 11 teachers from various backgrounds such as Math, Physics, Computer Science, Technology Education participated in the workshop. The evaluation showed a 120% improvement in their learning of the content after using the CSTM01 module as summarized in the Table III:

Table III – K-12 Teacher Workshop Evaluation

	Average points earned	**Percentage Correct**
Pre-test	5	33.33%
Post-test	11	73.33%

In addition, we evaluated the workshop and the teachers' experience. We used Likert Scale questions to ask if the goals were accomplished, their understanding enhanced, and asked them to rate the instructors, activities, and facilities. In addition, we asked for feedback on the workshop's strengths and weaknesses, how they plan to incorporate these activities into their

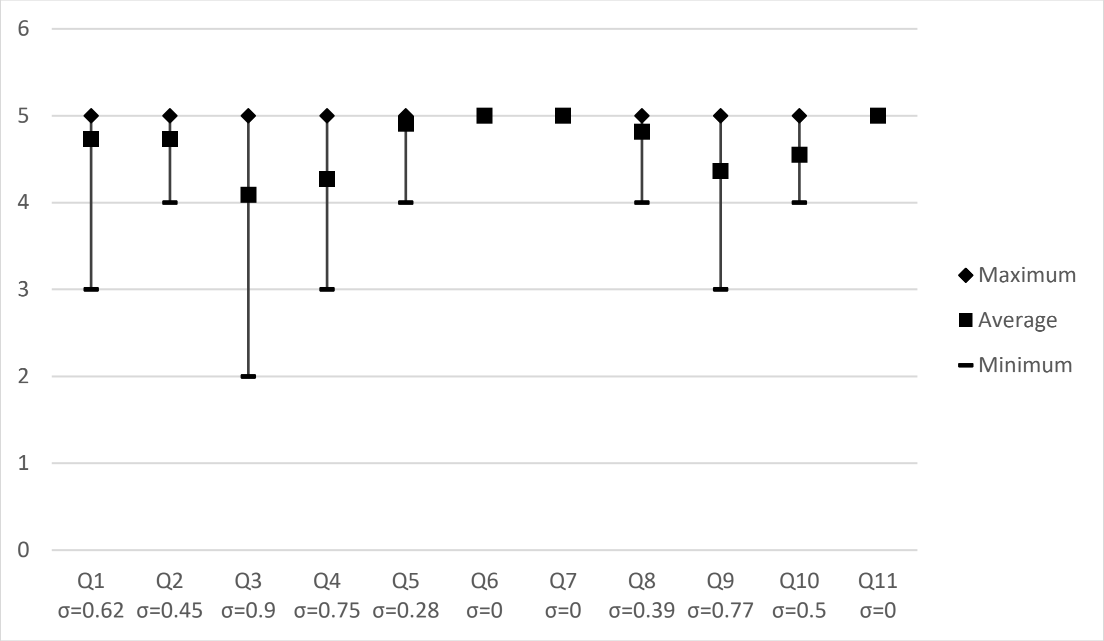


Fig. 6. K-12 Teacher Workshop Feedback Summary

Table IV – Feedback Questionnaire

	Question
Q1	The goals and objectives were clearly specified at the beginning of the workshop.
Q2	My understanding of this topic has been enhanced.
Q3	The content is relevant to the science curriculum I teach.
Q4	I will be able to apply what I learned into my classroom instruction.
Q5	The workshop activities were carefully planned, well organized, and well executed.
Q6	The presenter was knowledgeable about the content.
Q7	I felt comfortable asking the instructors questions.
Q8	The presenter's instructional techniques facilitated my learning.
Q9	I had sufficient time to complete all required tasks.
Q10	I had sufficient time to reflect on what I had learned.
Q11	The facilities were conducive to my learning.

curriculum, and for suggestions for improvement. Fig. 6 summarizes the feedback based on the questions provided in Table IV. It is evident that the workshop received scores of more than 4 out of 5 for all the questions. They also found that the instructional techniques including the hardware resources facilitated their learning (Q8) and were comfortable in applying the techniques in their classroom (Q4).

3.3 Future adoption of the CST Kit

The CST Kit is flexible to be adopted to different security courses at different education levels. For example, a Tier-1 (Beginner) course developed around the kit will contain course modules to explain the components of computer and introduce the basic concepts of cybersecurity to the students. The objective is to pique the students' curiosity in cybersecurity concepts and issues. The course can be offered to junior undergraduate students with basic knowledge of computers and hardware. CSTM01 is an ideal module for this course, and the basic (unmodified) Kit can be used to demonstrate various security vulnerabilities and convey possible solutions.

A Tier-2 (Intermediate) course can contain modules with the objective to provide thorough understanding of cybersecurity threats and solutions to the students. The course can be offered to senior undergraduate and graduate students who have taken courses on computer networks, operating systems and computer architecture. All the kit modules can be used as teaching aids for this course. Students will be expected to try out the different attack methodologies and defenses using the kit.

A Tier-3 (Advanced) course can be aimed to impart an in-depth knowledge of cybersecurity threats and solutions. The course can be offered to graduate students and professionals who have already passed the proposed intermediate level cybersecurity course. The kit can be used as a starting framework for aiding course labs and projects, where the students will be encouraged to experiment and develop new security attack and defense capabilities.

In future, we plan to expand the CST kit to include the following modules (among others):

- Network security attacks, such as Heartbleed [22]
- System security vulnerabilities, such as Spectre and Meltdown [23]
- Simulated hardware trojan attacks and defenses [24]

These modules will cover some infamous attacks in cybersecurity, that will help in greatly expanding the knowledge from our existing simulated attack modules through actual real-world exploits. We also plan to introduce a new area of hardware security through simulated hardware trojans in systems to demonstrate system level attacks that stem from such hardware vulnerabilities.

4. Conclusion

In this work, we presented a modular Cybersecurity Training Kit (CST) that aids in cybersecurity education starting from high school to industry professionals. The hardware as well as software of the kit is customizable which will allow easy adoption of the kit in wide range of cybersecurity courses and workforce levels. The components of the CST kit can be used to foster interest in and enhance cybersecurity education with underrepresented and underserved students at the high school and technical college level via teacher professional development and subsequent engagement of their students in Classroom Cybersecurity Challenges. Collaboration and dissemination can be promoted by sharing the curriculum with academic and industrial collaborators. Our pilot course and teacher workshop showed encouraging results and we hope to continue developing the CST kit and curricula around it.

Acknowledgement

This work is supported by National Science Foundation (NSF) [DGE 1723687, 1821766, CNS 1722557, 1801534; CCF 1718474] and Semiconductor Research Corporation (SRC) [2847.001, 2727.001].

References

[1] K-12 Computer Science Framework. (2016). Retrieved from http://www.k12cs.org.

[2] Holst, Alexander and Swaroop Ghosh. "Quantified Analysis of Magnetic Attack on Commercial Magnetic RAM Chip." Hardware Demonstration in Hardware Oriented Security and Trust (HOST), 2016, Online: http://www.hostsymposium.org/host2016/hardware-demo-list_2016.php

[3] A. Holst, J. Jang and S. Ghosh, "Investigation of magnetic field attacks on commercial Magneto-Resistive Random Access Memory," 2017 18th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, 2017, pp. 155-160.

[4] CSAW Embedded Security Challenge, https://www.csaw.io/esc

[5] Berrett, Dan. "How 'flipping' the classroom can improve the traditional lecture." The chronicle of higher education 12 (2012): 1-14.

[6] Furman, Burford J. "The un-lecture: a computer-assisted curriculum delivery approach for the effective teaching of mechanical design." In Frontiers in Education Conference, 1996. FIE'96. 26th Annual Conference., Proceedings of, vol. 3, pp. 1379-1382. IEEE, 1996.

[7] Crompton, Brittany, et al. "Cybersecurity Awareness Shrewsbury Public Schools." (2016).

[8] Yier Jin and Cliff Zou, "Cyberforensic.net – Training Many to Fight Cyber Crime." http://cyberforensic.net/articles/Jin_Zou.pdf

[9] Wenliang Du and Ronghua Wang, "SEED: A Suite of Instructional Laboratories for Computer Security Education (Extended Version)." In The ACM Journal on Educational Resources in Computing (JERIC), Volume 8, Issue 1, March 2008.

[10] Bhunia, Swarup, and Mark Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.

[11] Raspberry Pi, https://www.raspberrypi.org/

[12] Jupyter Notebooks, https://jupyter.org/

[13] Raspberry Pi computing using Jupyter Notebooks, https://www.hackster.io/mjrobot/rpi-physical-computing-using-jupyter-notebook-056fa8

[14] Network monitoring using Wireshark in Raspberry Pi, https://zone13.io/post/wifi-monitoring-using-raspberry-pi/

[15] Xilinx Zynq-7000 FPGA, https://store.digilentinc.com/zybo-z7-zynq-7000-arm-fpga-soc-development-board/

[16] RSA Verilog implementation, https://github.com/Rajandeep/RSA-CRYPTOSYSTEM-using-verilog

[17] RocketChip generator, https://github.com/chipsalliance/rocket-chip

[18] A. De, A. Basu, S. Ghosh and T. Jaeger, "FIXER: Flow Integrity Extensions for Embedded RISC-V," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 2019, pp. 348-353.

[19] Xilinx Virtex-7 FPGA, https://www.xilinx.com/products/boards-and-kits/ek-v7-vc707-g.html

[20] Everspin MRAM, https://www.everspin.com/file/157247/download

[21] N52 Neodymium Magnets, https://www.amazon.com/40x20mm-Neodymium-Permanent-Strongest-Powerful/dp/B07KF61YZT/

[22] Heartbleed bug, https://heartbleed.com/

[23] Spectre and Meltdown vulnerabilities, https://meltdownattack.com/

[24] A. De, M. Nasim Imtiaz Khan, K. Nagarajan and S. Ghosh, "HarTBleed: Using Hardware Trojans for Data Leakage Exploits," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 4, pp. 968-979, April 2020.