Innovative Engineering Outreach Using Intel® Security and Embedded Tools

Raghudeep Kannavara¹, Patrick Schaumont², Michail Maniatakos³, Michael A. Smith⁴, Scott Buck⁵
¹, ⁴ Intel Corporation, USA, ² ECE Department, Virginia Tech, Blacksburg, VA, USA, ³ ECE Department, NYU Abu Dhabi, United Arab Emirates

Abstract—During Spring 2013, the Evaluation Platforms Program from Intel and the Intel Software and Services Group donated Intel® Atom™ processor based development kits to the Electrical and Computer Engineering (ECE) Departments at Virginia Tech University and Polytechnic Institute of New York University (NYU Poly). The goal was to enable engineering faculty to develop projects based on Intel® security and embedded tools. The projects thus developed, key learnings and project outcomes are elucidated in this paper. Further, we evaluate the outreach projects to highlight the two different, yet important approaches to security curriculum development emphasizing security engineering versus security attacks.

Keywords—Computer Security; Embedded Platforms; Intel® Atom™ Processors; Engineering Outreach;

I. INTRODUCTION

The rise of intelligent embedded computing has vastly changed the way we interact with technology. From smartphones to connected cars, the Internet of Things (IoT) has revolutionized our lives, empowering us with new capabilities and enabling us to be more productive in our daily activities. On the other hand, the rise of security risks to embedded computing cannot be disregarded. The rapid evolution and commoditization of technology due to the growth in manufacturing prowess and optimization of supply chain logistics has raised many security challenges. As Intel seeks to create and extend computing technology to connect and enrich the lives of every person on earth, ensuring the security of this connected ecosystem comprising of hardware, software and information is critical. Building, testing and deploying technology that is secure and reliable requires human resources with engineering skills that can comprehend the risks to new technology. This implies industry and academia must work ever so closely to hone the necessary security skills in emerging engineering talent by developing and diffusing education on the latest in technology.

With this motivation, during the Spring of 2013, the Evaluation Platforms Program from Intel [11] and Intel Software and Services Group donated Intel® Atom™ processor based embedded PCs to the Electrical and Computer Engineering (ECE) Departments at Virginia Tech University and Polytechnic Institute of New York University (NYU Poly). The primary goal of our outreach was to enable engineering faculty to develop projects based on Intel security and embedded tools, thus fostering a cohesive curriculum program that develops a pipeline of capable students who understand security challenges and how Intel® technology can help solve those questions. Beyond accomplishing our primary goal, we believe our outreach also serves the important purpose of highlighting the two distinctive aspects that define the learning objectives and teaching methods of a security curriculum. While traditional approach to security curriculum is to imbibe a security engineering mindset, of late, incorporating an “ethical hacker” mindset has become necessary as well to enable effective security validation. Thus, in this paper, we showcase the usage of Intel® security and embedded tools in security curriculum development while comparing and contrasting the outreach projects to highlight the necessity of “security engineering” versus “security attacker” approaches to security curriculum development.

This paper is organized as follows. Section 2 elaborates the nuances in security curriculum development. Section 3 describes our efforts towards a reusable curriculum. Section 4 briefly introduces the embedded development kits used in the university outreach. Section 5 and 6 explain the outreach with Virginia Tech University and Polytechnic Institute of New York University respectively. Section 7 sets the conclusion and provides insights into potential future directions and collaboration opportunities.

II. SECURITY EDUCATION

The primary goal of security education is to raise awareness of computer security issues to computing students at all levels. We need to proactively identify opportunities to augment and develop security curriculum at key schools, empower students to analyze systems security risks, enable students to reason about system security properties and teach students how to exploit platform capabilities. Security curricula must address three dimensions, which include Vulnerability analysis to identify what system threats exist, Mitigations to identify how to defend against the identified threats and Validation to verify that the mitigations address the threats identified. In essence, security training has two distinctive approaches. The learning objectives and teaching methods can impart security

* Other names and brands may be claimed as the property of others
engineering skills that enable the students to architect, design and implement secure systems with a goal to defend or protect. On the other hand, the learning objectives and teaching methods can emphasize an “ethical hacker” or an attacker mindset that enables the students to reverse engineer, find security defects, perhaps exploit security systems and thus develop appropriate mitigations. Imparting security training that equally addresses both these approaches is vital in developing competent computer security professionals while incorporating these fundamental concepts into the security curriculum will also raise the bar on systems security. Beyond these two approaches, there are additional materials and topics which are being incorporated into state of the art security curricula. These topics underscore security enforcement and emphasize policy, compliance, legalities, and user experience and privacy issues. Overall, conceptualization, secure architecture, design, security validation and adherence to policies or protocols are integral constituents in a product’s security development life cycle. Although in figure 1, we depict these three aspects of security curriculum development, in our outreach, we do not explore the third aspect of security enforcement.

In reality, perfect security does not exist; any implementation has at least one weakest link. Either from an engineer’s perspective or an attacker’s perspective, it is crucial to identify and acknowledge the weakest link. For example, the weakest link in an encryption scheme may be defined by the cryptographic key-length. An algorithm's key length is distinct from its cryptographic security, which is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. The security of an algorithm cannot exceed its key length, since any algorithm can be cracked by brute force [7]. On the other hand, side-channel attacks, for example, show that cryptographic key-length is not always the weakest link, since a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be used to infer cryptographic keys to break the system. While these are specific examples that highlight the weakest link in an encryption scheme, there are always numerous other avenues that can make or break a cryptographic system. In this paper, the outreach with Virginia Tech University highlights security engineering curriculum development that emphasizes protecting the “weakest link” and the outreach with Polytechnic Institute of New York University highlights security attack curriculum development that emphasizes exploiting the “weakest link”.

III. TOWARDS A REUSABLE CURRICULUM

The Intel® Software Academic Program provides collaborative Intel® software and education material for faculty teaching parallel programming, security, embedded systems, perceptual computing and mobile computing [10]. Intel has a long history of supporting advanced curriculum development and the increasing reliance on information security is an important part of Intel’s next generation hardware and software

![Security Curriculum Development Diagram](image-url)

Fig 1. Aspects of Security Curriculum Development

* Other names and brands may be claimed as the property of others
systems. The focus of our outreach was security curriculum development with the goal to develop collaborative education materials that faculty could leverage for teaching security courses and laboratory experiments. Collateral developed for this effort includes books, evaluation hardware and teaching aids on security experiments and course modules, which would be made available to the faculty. The laboratory experiments can run directly on the students’ laptops or desktop machines without requiring access to specialized hardware. These laboratory modules are hosted online with the Intel® Software Academic Program for easy access and broader dissemination across the security community. They can also be used in general aspects of computer security instruction at both the undergraduate and graduate level. Further, these modular laboratory experiments can easily be incorporated in broader electrical and computer engineering courses to inject security concepts into the coursework.

IV. INTEL® ATOM™ PROCESSOR DEVELOPMENT KIT

Intel® Embedded Alliance introduces the BIS-6630, a power-performance efficient 12W compact fanless embedded PC developed around the Intel® Atom™ processor N2800 at 1.8 GHz [6]. The platform comes with a Fedora clone pre-installed, but also supports embedded development using the Yocto® project, Windows® 7 Embedded, Windows 7, and future Linux® systems. The BIS-6630’s fan-less, rich with I/Os, easy access drive bay design makes it perfect for embedded and industrial applications. These characteristics of the BIS-6630 also make it an ideal development kit for students to build, experiment and demonstrate Electrical and Computer engineering laboratory projects including computer security projects - the focus of our outreach.

Fig. 2. BIS-6630 Norco development kits (Intel® Atom™ processor development kits)

V. OUTREACH WITH VIRGINIA TECH

In this section we describe our outreach with Virginia Tech University. We briefly discuss the learning objectives, project description, student learnings and project results.

A. Learning Objectives

Handheld computing is an emerging market with increasingly complex and powerful processors to provide wide range of services to the end user. Current processors targeted at the handheld market contain several coprocessors and accelerators which can perform specialized functions, such as signal processing and video acceleration, without burdening the main processor. Information security is a common requirement for those platforms as well. High-performance implementations are also important for handheld computing platforms. Faster cryptography may enable higher levels of equivalent security, or higher availability of handheld computing resources for other tasks. New applications enabled by mobile computing, such as e-cash and privacy-friendly attributes make extensive use of cryptographic primitives [1].

With this in focus, during Spring 2013, Dr. Patrick Schaumont, currently an Associate Professor at the Bradley Department of Electrical and Computer Engineering, Virginia Tech, designed and taught ECE 5984 Handheld Computer Security, a graduate level course. The objectives of the course were to enable the students to design implementations of common cryptographic operations in software and hardware by integrating common cryptographic algorithms into cryptographic protocols that operate on handheld computers. Meeting these learning objectives required analyzing the threats, comprehending implementation-level attacks and designing transformations on cryptographic hardware and software of a handheld computer to mitigate implementation-level attacks. As one of the teaching methods used to meet the learning objectives of ECE 5984 Handheld Computer Security, Dr. Schaumont leveraged the Intel® Atom™ processor development kits to design a semester wide course project, a brief description of which is provided in the next section.

B. Brief Project Description

Public key cryptographic algorithms like RSA, DSA and elliptic curve cryptography (ECC) are needed to support key exchange and signature protocols. ECC is a public key crypto system gaining popularity in recent times because of its shorter key sizes, compared to other public key cryptographic systems. ECC involves point multiplication on elliptic curves over prime fields or binary fields. This point multiplication involves doubling and adding points on an elliptic curve which in turn depend on the modular arithmetic in the underlying field. Majority of ECC running time is spent in doing modular multiplication in the underlying field. Therefore significant performance gains can be achieved if we can accelerate this modular multiplication. With this in view, as part of the course project, students used the Intel® Atom™ processor development kits to investigate and optimize vector processing techniques to accelerate modular multiplications in prime fields using the Intel® Streaming SIMD Extensions 2 (Intel® SSE2) instruction-set extensions in Intel® Atom™ processor.

* Other names and brands may be claimed as the property of others
optimized implementation runs almost three times faster than the modular multiplication on standard GMP library.

The project enabled the students to research techniques to optimize cryptographic algorithms for Intel architecture to build secure and fast cryptographic systems. We note that, in general, performance-optimization and risk-mitigation are independent design concerns [9]: a fast implementation is not necessarily side-channel-free and vice versa. In this project, the emphasis was on performance improvement.

C. Key Learnings and Project Outcome

The students’ project work focused on efficient implementation of modular arithmetic which forms the basis for ECC, by exploiting the capabilities of SIMD coprocessors in Intel® Atom™ processors. Implementing modular multiplication using Intel® SSE2 to optimize cryptographic algorithms for Intel® architecture required careful evaluation of the advantages and disadvantages of the methodology while using advanced architectural features. Via hands-on demonstration and detailed performance analysis, the students learned that their implementations, which use National Institute of Standards and Technology (NIST) standard prime-field curves, run much faster than the OpenSSL versions of the same ECC operations on the same processor. The students comprehend that accelerating basic cryptographic operations on mobile platforms can have large impact on the performance of secure mobile applications. The students documented their experimental observations in their conference submission titled “SIMD Acceleration of Modular Arithmetic on Contemporary Embedded Platforms” to the IEEE High Performance Extreme Computing Conference (HPEC), which was a nominated Best Paper Award candidate.

With regards to evaluating the course meeting the learning objectives, Dr. Schaumont conducted a student survey towards course completion. 56% of the students responded to the survey, of which nearly 44% of the students rated their abilities as “Good” towards meeting the learning objectives, while nearly 33% of the students rated their abilities as “Excellent” towards meeting the learning objectives. This shows that a majority of the students appreciated the teaching aids and methods used to incorporate a security mindset to the curriculum.

VI. OUTREACH WITH NYU POLY

In this section we describe our outreach with NYU Poly. We briefly discuss the learning objectives, project description, student learnings and project results.

A. Learning Objectives

Security has always been a major concern in computing and communications systems. Substantial research has been devoted to develop, evaluate and standardize cryptographic algorithms, key management practices and security protocols. Before the advent of attacks based on side channel analysis, it was typically assumed that cryptographic algorithms usually implemented in software or hardware on physical devices were “black-boxes” whose internals can neither be observed nor interfered with by any malicious entity. Based on these assumptions, the level of security was widely quantified in terms of the mathematical properties of the cryptographic algorithms and their key sizes [8]. These assumptions do not take into account the serious threat that a side-channel attack poses to the security of cryptographic modules. These attacks use information from the physical implementation of a cryptosystem, such as its timing information, power consumption, electromagnetic leaks, or even sound, which are exploited to derive the cryptographic keys. A secure cryptographic system must ensure that the cryptographic keys are not revealed in any way. In consequence, cryptographic implementations have to be evaluated for their resistivity to such attacks necessitating the adoption of physical security validation during the development of cryptographic systems. The incorporation and testing of different countermeasures against such attacks during the development phase has consequently become a necessity.

With this in view, during Spring 2013, Dr. Michail Maniatakos, currently an Assistant Professor of Electrical & Computer Engineering, NYU Abu Dhabi, developed and taught EL9433 Modern Microprocessors, a graduate level course. The learning outcomes anticipated were to enable the students to understand basic concepts of modern microprocessor design and basic stages and tools leading to the development of such systems by analyzing performance, power and manufacturing requirements. The course covered most aspects of modern microprocessors pre- and post- deployment which include conceptualization, architecture, design, fabrication, testing and security. Topics such as performance versus security tradeoffs, adding Design for Testability features, memory hierarchy choices were emphasized while requiring the students to focus on industrially relevant solutions. In order to meet the learning objectives of EL9433 Modern Microprocessors, Dr. Maniatakos leveraged the Intel® Atom™ processor development kits to design a semester wide course project, a brief description of which is provided in the next section.

B. Brief Project Description

Timing attacks are a class of side channel attacks that were developed with the realization that encryption devices give the attacker more information than previously thought. Timing attacks watch the data movement in and out of the CPU or of the memory (or cache) and determine a secret key (such as an AES key) by analyzing the variations in the time taken to execute cryptographic algorithms. The existence of side channel attacks was already known and taken into consideration when Advanced Encryption Standard (AES) was developed to replace the old Data Encryption Standard by NIST [2][3]. But the AES candidates that were chosen, even after the evaluation of their security, were prone to specific timing attacks against systems that use table lookups by taking advantage of the information leakage caused by cache misses, since the AES candidates chosen relied on large table lookups to improve the performance of their algorithm. Side channel attacks, in general, can provide valuable information about the cryptographic system’s hardware and software implementations and operations on data including secret keys and messages. Therefore, it is important to study side channel
attacks to develop countermeasures that are resistant to such attacks and diminish information leakage that comes with encryption devices. With this motivation, as part of the course project, students used the Intel® Atom™ processor development kit as a server in client-server architecture, to investigate and present several tests to demonstrate the effectiveness of cache-timing attacks against AES on Intel® microprocessors while providing detailed analysis.

The project provided the students an opportunity to perform power and performance analysis on modern Intel microprocessor architecture using benchmark applications, while comprehending the engineering tradeoffs necessary to improve microprocessor security. For example, due to performance overhead, a mobile platform may not be able to go past a 128-bit security parameter without proper optimizations, therefore hindering the designer’s security hardening efforts.

C. Key Learnings and Project Outcome

In order to launch a successful attack, the students divided the attack into three phases, which include preparation for the attack, carrying out the attack, and finally analysis of the attack. The preparation phase required collecting data to build the baseline profile of timing information, by setting the AES key in the server to all zeros and observing the server as it reacts to different size packets. The attack phase required setting a random secret AES key instead of a known AES key and performing the same information collection activity. Finally the analysis phase required correlating the timing information collected during the preparation and attack phases to output potential keys that produce large correlations which can be combined with the output from the server to derive the potential AES key [3]. By means of analysis, the students demonstrate that advances in Intel processor architecture, introduction of AES-NI and improvements in cache implementation make timing based side channel attacks harder to implement on contemporary microprocessors. The students comprehend that modern Intel multicore processors have complicated cache architecture and provide instruction level support for secure and fast cryptographic operations, thus lowering the risk of cache timing attacks. Leveraging the knowledge gained, the students developed a comprehensive tutorial titled “Tutorial to Demonstrate a Cache-timing Attack on AES on an Intel Atom™ processor” [3]. The tutorial is hosted online to enable easy access and broader sharing across the security community.

With regards to evaluating the course meeting the learning objectives, Dr. Maniatakos conducted a student survey towards course completion. 45% of the students responded to the survey, of which nearly 67% of the students agreed that, the course effectively promoted the learning objectives to a “Very Great Extent” and added “Great” value to their education. Although, among the students who responded, nearly 45% felt the course was “Too Hard”, nearly 56% agreed that the course was overall “Great”, which shows that the additional effort to augment a security mindset to the curriculum was appreciated by a majority of the students.

VII. CONCLUSIONS AND FUTURE WORK

With the rise in embedded computing and the corresponding increase in security threats faced by the digital economy and modern society, computer security has come to the forefront. Developing and imparting education in computer security is vital to ensuring future engineers have the necessary skills to comprehend the new security threats and conceive appropriate mitigations enabling them to build, validate and deploy complex technology. With this motivation, in this paper, we described our efforts to collaborate with the academy to develop security curriculum. We further described the two distinctive approaches to security curriculum development that are equally important to foster competent security professionals. Incorporating an attacker mindset, as demonstrated in our outreach with NYU Poly, while being able to build secure cryptographic schemes, as demonstrated in our outreach with Virginia Tech, are important skills sought in modern security professionals. Ultimately, these combined skills will raise the bar on systems security. Although our outreach described in this paper focused on graduate students, it is imperative that we include undergraduate students as well. We believe that our outreach is a step in the right direction to impart security training to emerging engineers. Further, our outreach emphasizes the fact that industry and academia should closely collaborate to develop and diffuse security education on the latest in technology to hone the necessary security skills in emerging engineering talent. We also note that developing reusable and modular security courses and experiments enables injecting security concepts into the broader electrical and computer engineering curriculum.

Thus we conclude this paper with a brief note on future collaboration opportunities. Intel recently introduced the Intel® Galileo development boards featuring the new Intel® Quark™ technology to universities worldwide [5]. The new microcontroller boards enable university students to innovate at the lower end of the spectrum with inventions that will be compatible with other Intel Architecture devices in the Internet of Things. Similar to our outreach using Intel® Atom™ processor based embedded boards; incorporating Intel® Quark™ technology and Intel® Galileo boards in security curriculum development will spur further innovation across the computing spectrum.

ACKNOWLEDGMENT

The authors would like to thank Curtis Durrant, Joy Shetler, Haidong Xia, Yvonne Davis, Evaluation Platforms Program from Intel, Intel® Software Academic Program and Intel Software and Services Group, for supporting this initiative.

REFERENCES


* Other names and brands may be claimed as the property of others.


* Other names and brands may be claimed as the property of others