Academic Papers

Faculty and Staff Information Security Awareness and Behaviors

Johnathan M. Yerby, Kevin S. Floyd

🕑 2:00 PM to 2:35 PM 📍 La Salle A

The purpose of this study was to determine the information security awareness and behaviors that faculty and staff report. A sample of 321 participants consisting of 164 faculty and 157 staff members from a public, state university located in the Southeastern United. The results indicate that overall, faculty and staff have high to moderate levels of information security awareness and behaviors. An independent samples t-test found that there was no significant difference in security awareness, but there were four behaviors differences between faculty and staff. Participants that reported higher levels of security policy awareness demonstrated significantly more secure behaviors in ten of the 18 items measured. Given these findings, comprehensive security awareness training will be essential for institutions of higher education as a means of minimizing threats to information technology resources.

Example Security Injections for Hardware Courses

Chenyang (Nick) Li, Sohum Sohoni, John Acken

🕑 2:30 PM to 3:00 PM 📍 La Salle B

This paper gives examples of security injections in computer engineering courses, including courses on hardware design. More broadly, the paper aims to show how knowledge of hardware and software implementations relate to security exploits is important for students who design computer hardware, and how knowledge of the hardware and architectural features is important for those who focus on computer security. The paper provides examples to illustrate the impact of the knowledge of underlying architectural optimizations and hardware limitations on security features and exploits. Examples of educational tools and methods for integrating security education in context in the computer engineering curriculum are also described.

Examining the Level of Education Factors on Reducing Data Security Breaches

Steven Brown, Oscar Ukpere

🕑 2:35 PM to 3:05 PM 📍 La Salle A

The purpose of this quantitative correlational research study was to examine the relationship between the levels of educational factors possessed by information security managers (ISMs) and the number data security breaches in their organizations. Previous research reported that levels of educational factors have an increasing impact on the reduction of organizations' data breaches, leading researchers to conclude that various levels of educational factors are effective in implementing appropriate controls to address data breaches. A quantitative correlational study was used to determine the relationship between data security breaches and ISMs' levels of educational factors (level of completed formal education, number of professional certifications, number of training programs, and years of work experience) to provide quantifiable data on data security breaches. Data analysis revealed a significant, positive correlational relationship between the reduction of organizations' data breaches (dependent variable) and each of the four independent variables (levels of formal education, completed data security certifications, on-the-job training, and hands-on experience).

IoTCP: A Novel Trusted Computing Protocol for IoT

Paul Wang, Amjad Ali, Ujjwal Guin, Anthony Skjellum

🕓 3:05 PM to 3:35 PM 📍 La Salle A

The ability to understand, predict, secure and exploit the vast array of heterogeneous network of things is phenomenal. With the ever-increasing threats to cyber physical systems and Internet of Things, security on those networks of data-gathering sensors and systems has become a unique challenge to industries as well as to military in the battlefield. To address those problems, we propose a trusted computing protocol that employs discrete Trusted Platform Modules and Hardware Security Modules for key management, a blockchain-based package verification algorithm for over-the-air security, and a secure authentication mechanism for data communication. The IoT-based Trusted Computing Protocol implements integrated hardware security, strong cryptographic hash functions, and peer-based blockchain trust management. We have tested the protocol under various circumstances where devices have built-in securities while others do not. We apply the new protocol to a SCADA system that contains more than 3,000 edge devices. The preliminary results show that proposed protocol establishes trust, improves security, integrity, and privacy.

NICERC's Cyber Interstate: The Next Generation of Cyber Worker can be Found at the Intersection for Classroom Content and Teacher Support

Chuck Gardner

🕓 3:35 PM to 4:05 PM 📍 La Salle A

Since 2012, the National Integrated Cyber Education Research Center has existed with the express goal of supporting local workforce development in the areas of STEM, cyber, and computer science. In that time, a variety of subject matter experts have contributed to writing content that is now in use by more than 8,000 teachers across the country. In addition to providing that content to United States public school teachers at no cost, the organization and subject matter experts also provide free professional development to ensure that teachers are as prepared as possible when they present this content in their classrooms. Lastly, the organization also provides opportunities for extracurricular engagement by students outside of the traditional classroom model. Content for events such as robotics competitions, science fairs, and maker spaces are also provided by the organization. This paper will investigate a variety of research studies that support the organization's mission as well as particular studies that identify the organization's offerings as a critical need to education in the 21st century.

A Study of the Evolution of Secure Software Development Architectures

Leah Winkfield, Yen-Hung Hu, Mary Ann Hoppa

🕓 4:05 PM to 4:35 PM 📍 La Salle A

Emerging technologies such as containers, microservices, DevOps, Agile software development life cycle (SDLC), and cloud-native applications have gained popularity and traction in the industry and among enterprises. These modern application technologies and architectures are being adopted because they enable greater flexibility, scalability, portability and more rapid development. Consequently, how to build and maintain secure applications and systems is being reevaluated. Since the total responsibility is now larger and more complex, the application developer role is expanding to include greater security obligations and concerns. This paper explores the evolution of software development architectures and consequent implications on security, to better understand the technology landscape driving this change and its impacts on application development. To remain competitive, organization must be prepared to invest in ongoing training of their developers in the latest best practices. To remain relevant, higher education must adapt curriculums to prepare future professionals in the appropriate cybersecurity and secure coding practices to match the development shifts observed in industry.

All About SQL Injection Attacks

Vinitha Subburaj, Daniel Thomas Loughran, Mayar Kefah Salih

🕓 4:35 PM to 5:05 PM 📍 La Salle A

With advancements in Internet technologies, there is an increasing growth of applications that are web based. With smaller software development cycles and faster delivery, security has become an important issue. There are many types of security attacks that are made on Web applications and SQL injection attack is one type of an attack. Recently, studies have shown that more and more web applications are getting attacked by different types of SQL injection attacks. To effectively detect and prevent these attacks, a deeper understanding on the different types of SQL injection attacks, the nature of the attacker, and the mechanism used is very important. This paper discusses details that one would need to understand all about SQL injection attacks. This paper presents a detailed study of most recent SQL injection attacks on web applications, SQL injection prevention and detection mechanisms. The classification of different types of SQL injection attacks, prevention and detection mechanisms discussed in this paper highlights the need for future improvements in the detection and prevention mechanisms to secure web applications from SQL injection attacks.

Quantum Key Exchange Simulator

Michael McGregor

🕓 5:05 PM to 5:35 PM 📍 La Salle A

Quantum cryptography and key exchange is an important and challenging topic for cybersecurity and information assurance students, and one that is difficult to teach without an appropriate demonstration platform. In this paper, we describe the background of quantum key exchange (QKE) theory, modern implementations of QKE, and the role it plays in classical, symmetric key cryptography. We present a QKE simulator that can be used by educators to aid in the teaching of quantum key exchange concepts and processes. The simulator provides a hands-on learning mechanism with which the participants interact. It is designed to be engaging and practical for students to use by supporting the ability to walk through phases of quantum key exchange, pausing at each step, to facilitate discussion and comprehension of this complex security topic.

QUSAIM: A Multi-dimensional Quantum Cryptography Game for Cyber Security

Abhishek Parakh

🕓 5:35 PM to 6:00 PM 📍 La Salle A

Discovering and predicting a gamer's behavior and adapting the game environment to improve the learning is a challenging task in any game-based learning environment. QuaSim is a gamified intelligent tutoring system (ITS) developed to teach quantum cryptography. In QuaSim, students solve problems related to quantum cryptography through different lessons/game plans. In this paper, we provide an overview of QuaSim, and our approach to analyzing students' performance and gameplay behavior based on activity sequence modelling and clustering. We present the results of our analysis and identify different student groups having distinct gaming patterns and problem-solving behaviors. Finally, we discuss the pre- and post-game survey results.

Presentations

RESCUE: A Cloud-based System for Cybersecurity Ed & Training

Anyi Liu, Dong Han, Huirong Fu

🕒 2:00 PM to 2:30 PM 📍 La Salle B

With the proliferation of the technology of virtualization, Software-Defined Network (SDN) and Network Function Virtualization (NFV), cloud computing has become a vital building block of the high-performance and low-cost computing paradigm serving for various educational purposes. In this paper, we first describe a free framework, namely ReScuE (Range for Security Education), which is a cloud-based networked virtual environment dedicated for cybersecurity education. We leverage the state-of-the-art technologies of SDN and NFV and elaborate the solutions to tackle the technical challenges of deploying ReScuE upon the underlying cloud infrastructure. Then, we present a set of hands-on labs that teach the students how to perform offensive, defensive, and forensic analysis tasks with the techniques and tools on the top of ReScuE. Finally, we tested both ReScuE and the hands-on labs with two groups of undergraduate students. Through the post-lab assessment and feedbacks, we gain some insights of how to effectively promote the wide adoption of the cybersecurity-related hands-on labs to the undergraduate and graduate-level courses at different educational institutions (e.g., community colleges, 4-years universities, and post-graduate schools).

Inter-Disciplinary Capacity Building in Cybersecurity

Shamik Sengupta, William Doherty

🕒 3:00 PM to 3:30 PM 📍 La Salle B

Recent literature recognizes that cybersecurity education should include skills outside of the traditional computing space to best prepare the workforce for current and future challenges. To address this need, a team from the University of Nevada, Reno and Truckee Meadows Community College created and pilot tested libraries of interdisciplinary modules that integrate cybersecurity concepts from Information System, Justice, Political Science and Computer Science. The modules are designed to be integrated into existing courses in any related discipline. Quantitative and qualitative data was gathered from each participating course to evaluate the effect of the module on student awareness and knowledge of the related cybersecurity topic.

A GenCyber Camp Case-Study: Teaching Defensive Programming at the Pre-University Level Using A Novel Data-Tampering Theme

Ankur Chattopadhyay, Elizabeth Quigley, Sallie Petty

🕒 3:30 PM to 4:00 PM 📍 La Salle B

The current IEEE/ACM curricular recommendations and the latest CSEC2017 cybersecurity curriculum guidelines advocate for the inclusion of software security related topics within the present computing disciplinary knowledge-areas. Recent statistics estimate that 90% of reported security incidents result from exploits against defects in the code-design of commonly used software. With the rising demand for cybersecurity workforce, as we look to prepare our youth in cybersecurity, a lack of basic-awareness and understanding of software security may expose our young generation to cyber attacks. For this matter, it is important to teach software security related topics to pre-university learners at an early age. However, even though there are several software security based curriculum development initiatives at the university level, there are limited pre-university focused initiatives in this context, and none of them focus on the theme of data tampering in parameter passing. Therefore, in order to bolster the ongoing efforts in K-12 towards building hands-on software security learning modules and to introduce the topic of parameter-passing based data-tampering, we have designed a unique lesson-plan on defensive-programming for educating pre-university students about relevant secure-coding topics, like parameter passing, function vulnerabilities, buffer-misbehavior, integer error and buffer overflow. This paper describes our creative pre-university educational module on software security, which has been successfully used to conduct several hands-on workshop sessions with middle school students (grades 6-9) as part of our NSA/NSF GenCyber camp-program. Our paper also presents the survey-data collected from the workshop-participants for gauging their interests in the covered topics as well as the overall impact of the lesson-plan leading to new knowledge insights and improved awareness levels, in an effort to evaluate our nifty experiential learning module as a potential outreach vehicle for engaging pre-university students.

LVA: A Network Monitoring and Visualization System for Cyber Defense Competitions

Claude Turner, Rolston Jeremiah, Dwight Richards, Jie Yan

4:00 PM to 4:30 PM La Salle B

This work presents the network monitoring and visualization application, LUCID Network Monitoring and Visualization Application (LVA); a Node.js app that uses D3 for dynamic generation of graphical units. The system is targeted to intermediary or expert spectators at cyber defense competitions. It leverages several open source components for collecting and processing network data. Results are then sent to a visualization component for interpretation by a scoring algorithm and presentation methods. The LVA consists of several sub-systems, including its core visualization component and the following external components: Node.js, Linux Auditd kernel facility, Redis server, MySQL server, Syslog-ng, Nagios network monitor and Snort intrusion detection system. Blue teams in the competition network are monitored by Auditd, Snort, and Nagios (monitors). Syslog-ng clients on the blue team machines or on machines in the administrative domain watch log files generated by the respective monitors for events of interest. These events of interest are then sent to a centralized syslog-ng server. The syslog-ng server in turn sends the data to a Redis server, also running in the administrative domain. Redis is an in-memory database utilized by LVA to listen for messages submitted to channels marked by keys. Received messages are then transmitted to clients over a web-socket connection. Specifically, they are sent to the core LVA visualization app, which processes each message, scores it, and displays it appropriately in a browser in format that depends on its source or data type.

Teaching Cyber Security Concept though IOT application based on Raspberry Pi

Ravi Rao

4:30 PM to 5:00 PM La Salle B

Currently, we are witnessing a massive increase in internet-of-things applications, which involves low-cost devices connected to the internet. This has been accompanied by an increase in cybersecurity breaches. Consequently, it has become important to teach students both about the internet-of-things applications, and their accompanying cybersecurity risks. This poses a dual challenge of creating the necessary course materials in each area, and teaching them concurrently in a single course.

In the current paper, we discuss the introduction of cybersecurity concepts in an embedded systems course. We present our experience with the students who were taught this material during the Fall 2017 semester at Fairleigh Dickinson University. Though some of the basic concepts can be taught in one course, the learning curve is quite steep. The students were taught Python programming, the Linux environment, embedded systems programming and computer networking concepts within a single course. They were able to successfully complete a lab devoted to filtering internet traffic through the use of firewalls.

The course material we are developing could serve as a model for other institutions at the graduate and undergraduate levels. Other instructors and course developers could likely benefit from our experience.

Discovering Patterns and Sentiments about Hacking from Tweets

Azene Zenebe, Jessica C. Alcindor

🕔 5:00 PM to 5:30 PM 📍 La Salle B

As different events occur, people use social media to express their opinions about events, products and issues. It is useful to gage awareness and watchfulness of users on cyber security. This paper used analytics using twitter data as the main source and IBM's Watson Analytics software – an advanced cognitive and analytic solution, to identify different insights including trends and sentiments on the hacking subject. The tweets in English with the timeframe from May 2015 to June 2017 were selected. Twenty-five thousands (25,000) tweets that have #hacking were retrieved, relevant data were extracted and analyzed. We identified an increasing trend on the public interest on Hacking as well as more positive than negative sentiments about hacking. The results of this study encourage cyber security professionals and others to utilize big data that exist in social media such as Twitter and Facebook, and advanced analytics software to understand user awareness and discover actionable information for decision-making. Future research will focus on both topic modeling, and correlation and regression analysis among the discovered insights, actual threats and hacking incidents.

Preserving Cell Phone Privacy

William Butler

🕔 5:30 PM to 6:00 PM 📍 La Salle B

Operators of international mobile subscriber identity (IMSI) catcher technology are compromising consumer cellphone privacy within the United States. These compromises of consumer cellphone privacy are illegal intercepts and man-in-the-middle attacks. Despite efforts by organizations concerned with privacy, such as the American Civil Liberties Union, to inform the U.S. Congress and the public of the threat, no significant legislation has resulted to protect consumers from direct network interceptions and attacks. Scientists and software and hardware vendors are developing countermeasures; however, these measures have not been categorized within an accepted framework such as the National Institute of Standards and Technology Risk Management Framework for consumers to evaluate these countermeasures against the three pillars of cybersecurity, namely, confidentiality, integrity, and availability. Five themes emerged from the results of this study identifying issues focused on consumers, hardware and software providers, network providers and standards making bodies. Based on these themes recommendations are presented for adoption to begin to address IMSI catcher issue.

Lightning Talks

New Approaches to Cyber Security Education (NACE)

Debasis Bhattacharya

🕓 2:00 PM to 2:15 PM 📍 La Salle C

Cybersecurity has become a prevalent topic in many colleges, but how it should fit into the overall educational process is still not fully understood. A cybersecurity project at the University of Hawaii Maui College (UHMC), funded by the NSF SFS and ATE program, spans multiple disciplines and targets women and minorities.

Chief Information Security Officers (CISOs) as Endangered Species: Is the CISO high turnover problem a Mirage?

Frank Lin, Conrad Shayo

🕓 2:20 PM to 2:35 PM 📍 La Salle C

CISOs average job tenure is about 18 months in the USA. Although we know that such high turnover is a problem, it keeps happening. The impact of such turnovers has not been ascertained. The purpose of this panel is to explore the cost of CISO turnovers and strategies that may be used to increase their tenure. Many studies have found that retention of IT employees is important because when they leave their jobs, they leave with priceless and difficult to replace organizational knowledge, skills, and abilities (Wang & Kaarst-Brown 2014; Tnay, Othman, Siong, & Lim, 2013). Besides, it takes money and time to train a replacement CISO, who is most likely going to leave in a few months. The exploration of the CISO turnover problem will focus on the following: What is the organizational cost of replacing a CISO? Why are fired CISOs getting hired immediately? Why do some CISOs decide to run to the hills after a short tenure? What strategies can organization leaders use to retain their CISOs? Which strategies are working and which are not, and why? (Lee, C. Lee, C.C. & Kimb, S. 2016; Waldman, Carter & Hom, 2015). We hope this discussion panel will contribute to our understanding of the forces and determinants of CISO turnover and retention. Moreover, we intend to gather some survey data to continue with this line of research.

We Are Fighting A Cyber War Right Now

Humayun Zafar

🕓 2:40 PM to 3:05 PM 📍 La Salle C

There is no denying it, we are fighting a cyber war right now. The responsibility undoubtedly lies with humans. Cybersecurity experts, such as the FBI and others have confirmed that the biggest weakness in in cybersecurity is human error. IBM in a study revealed that 95% of all security incidents involved some form of human error (e.g. phishing scams, falling victim to advanced persistent threats etc.). Is the issue lack of investment in this arena? Not at all. Firms continue to spend millions on security technologies. The only issue is that all it does is to make an executive feel safe as opposed to being safe. For years people have also been talking about training as the best way of ensuring that human errors are reduced. That's somewhat true. The only issue is that instead of looking at training at a macro level, we have to consider training at a group level. That is essentially why even with an industry that focuses exclusively on cybersecurity training programs, we continue to have higher rates of security breaches due to human error.

We investigated this issue in the healthcare and financial services arenas.

Designing and Delivering a Cybersecurity Curriculum for Middle Schools

Yesem Kurt Peker, Hillary Fleenor

🕓 3:10 PM to 3:25 PM 📍 La Salle C

The need for highly trained computing professionals continues to grow in our nation and throughout the world. Research has shown that more and more of these technology positions require a level of skill that cannot be accomplished in a university program without prior computing experience. This is also true for cybersecurity, one of the most in-demand fields today. Primary and secondary schools are essential for exposing students to computing and security topics at earlier ages in order to achieve levels of expertise needed by industry, government, and other organizations. It is also essential to attract a more diverse student body into the field. In this work, the authors develop a middle school cybersecurity curriculum to achieve two goals: 1) increase student knowledge in cybersecurity topics and 2) increase student interest in cybersecurity in general as well as a possible career path. The team consists of a tenure track assistant professor in computer science with a background in cybersecurity and an expertise in cryptography; a lecturer/outreach coordinator with a master's in computer science, a master's in education, and previous experience teaching middle school; and a current middle school teacher certified in business education. In the current (2017-2018) school year the team members have been collaborating to deliver the cybersecurity curriculum in two grade 8 classes, a total of 60 students, in a Title I middle school in the U.S. Almost all students in the two classes are African American and more than 50% are female. The curriculum includes standards, objectives, and lessons for implementation within a year-long business and computer science course. The project also includes a pre and post-test to assess the first goal of increasing student knowledge in cybersecurity topics and a pre-and post-survey to assess the second goal of gauging students' interest in cybersecurity in general and as a discipline. In this presentation we share our curriculum and resources as well as challenges we have encountered as we deliver the curriculum. Due to some scheduling constraints we have already administered the post-test for assessing the knowledge gain. We are happy to share that, despite the challenges, a preliminary analysis of students' pre- and post-test scores indicate a significant increase in their knowledge of cybersecurity.

Cyber Criminology, Criminology and Cyber-crime Towards an Academic Discipline

Greg Laidlaw, Charles Wilson

🕓 3:30 PM to 3:45 PM 📍 La Salle C

Cybercrime is a growing global phenomenon that has created a significant paradigm shift in critical areas of the personal life of citizens, and in both the public and private sectors. The negative impact of cybercrime is felt in many diverse areas, such as politics, economics, national security, public safety, and in many critical societal activities related to quality of life. Today, essential online functions are constantly under attack by a growing cadre of sophisticated cybercriminals, organized crime organizations, and nation-state actors. The purpose of this paper is to synthesize current research literature on cybercrime to highlight the scope of the problem; and to suggest a notional concept of criminological theories that can be applied to enhance cybercrime investigation and enforcement efforts. Additionally, the paper proposes the establishment of an academic minor "Cyber criminology" based on an interdisciplinary approach.

Security Lessons From Building A Back-end Service for Real-Time Data Collection

Halmon Lui

🕓 3:50 PM to 4:05 PM 📍 La Salle C

According to the 2018 Symantec Internet Security Threat Report, malware implants grew by 200% and Internet of Things (IoT) attacks grew by 600%. The Edgescan 2018 report found that 20% of all vulnerabilities discovered were either high or critical risk. Enforcing proper preventatives and security assessments can help mitigate those risks. In this paper, we present our security experiences of designing a back-end service for a web application, which was motivated and designed to support real-time data collection for a statistics class in higher education. Our findings are organized into three categories: system software, connection forwarding, and data storage. These categories are main components of the web application and most likely to be targeted by an attacker. These are the main components of the web application and the most likely to be targeted by an attacker. There are three contributions in this paper: (1) The demonstration of building a secure and light-weight back-end service with Node.js, Nginx, and MongoDB, (2) The discussion on the vulnerabilities of a web application from a back-end service perspective, and (3) An explanation of our security measurement to mitigate or prevent attacks on those vulnerabilities. The current findings are promising and we believe they are worth further exploration to help back-end developers create an efficient and secure web service.

A Proposed Model to Unify Cybersecurity Frameworks and Certification Programs using NICE Framework Structure

Justin Smith, Kevin Kim, Dan Kim

🕓 4:10 PM to 4:25 PM 📍 La Salle C

Currently, the cybersecurity industry is seeing a boom workforce participation due to the growing popularity of its services in both commercial and government organizations. Therefore, there is a desire by industry clients and participants alike. This paper will outline the relationships between existing workforce frameworks and propose a single comprehensive and unified model for career progression using the NICE KSA structure.

Cyber Education Outside the Cyberspace

Ngatchu Damen, Leonnel Kwedeu, Divine Anye

🕓 4:30 PM to 4:45 PM 📍 La Salle C

The purpose of this paper is to extend the growing body of research on cyber education, by reporting the experiences of a cyber security department cut-off from Internet access. The value of Cyber education is expressed even beyond the cyberspace.

Diffusion Metrics of the AES Symmetric Cryptosystem

Abdinur Ali, Yen-Hung Hu, Cheryl Hinds, Jonathan Graham

🕓 4:50 PM to 5:05 PM 📍 La Salle C

In this paper we study the diffusion of the AES block modes. When the plaintext is encrypted, the diffusion obscures the redundant arrangements. Therefore, those repeated configurations can be hidden in the cipher text. In this paper we have compared four AES block modes with three key sizes and with five padding modes. First, the original plaintext was modified by changing a random letter in the plain text. Then, in order to study the diffusion metrics of the modification, the percentage of the match between the plain text and the cipher text was calculated. Based on these simulation metrics, the results indicate that CBC block mode with padding ANIS X.923 mode has more diffusion.

The REACH Model: Reinforcing Student Learning Through Abstraction and Distraction

Henry Collier

🕒 5:10 PM to 5:25 PM 📍 La Salle C

Some educators believe it was easier to teach students before the Internet because today, students cannot pay attention to anything longer than a 140-character Tweet. In some respects, this is possibly true, but in others, this belief is certainly false. A student's failure to learn has more to do with how they were taught to learn, than their capacity to learn or how distracted they are.

The No Child Left Behind Act tied federal funding to Adequate Yearly Progress in test scores [1]. The result on the surface was that K-12 teachers were put in a position where they needed their students to do well on the tests, otherwise they risked losing funding for their school and in many cases their own jobs. The pressure applied by the No Child Left Behind Act has led to teachers teaching for the tests, rather than teaching for the student's ability to learn / ability to teach themselves and discover their own learning methods.

A Gaming Platform for Cyber Security Education

Dipankar Dasgupta, Thomas L. Pigg

🕒 5:30 PM to 5:45 PM 📍 La Salle C

Traditional method of cyber-security education and training are not adequate for preparing students to defend against advanced cyber threats, spear phishing, targeted malware and zero day attacks. Education methods need to prepare a person to apprehend his / her knowledge, build analytical skills and thinking ability to defend the sophisticated attacks. This paper highlights an interactive game to teach cryptography concepts and approaches through a gaming platform. In particular, a multi-level game is developed using Unreal Engine for teaching cryptography (encryption / decryption exercises). This NSF-ATE funded project, called puzzle-based learning (PBL) is able to effectively integrate with instructional content and become highly successful for basic cyber-security education.