7-23-2014

Puzzle-Based Learning for Cyber Security Education

Sanjib Kumar Saha

PUZZLE-BASED LEARNING FOR CYBER SECURITY EDUCATION

by

Sanjib Kumar Saha

A Thesis

Submitted in Partial Fulfillment of the

Requirement for the Degree of

Master of Science

Major: Computer Science

The University of Memphis

August 2014

ACKNOWLEDGEMENTS

I would like to thank cordially my advisor, Dr. Dipankar Dasgupta, for his unconditional encouragement and support throughout my master's career at the University of Memphis. He guided me through all efforts in this research project. I am very grateful to him as he allowed me to work with him and his team, believing in my work and in me, and advising me like a parent.

I would also like to thank the members of my committee, Dr. Scott Fleming and Dr. Vasile Rus. Their comments and feedback especially helped me to improve the content of this work.

I am greatly thankful to my senior lab-mate Abhijit Nag for his help regarding almost all aspects throughout my entire project. I thank him for his helpful thoughts and ideas regarding this work and for his help editing this write up. It would have been very difficult for me to overcome many obstacles without his help.

I am grateful to all my colleagues in our research group at the University of Memphis. Our meetings and discussions opened my mind to new ideas and thanks to Kul Subedi for helping me in all technical support. I will also like to thank Charles Lancaster and Mustafa Hajeer for their continuous support.

I will always remember my professors and colleagues in the computer science department for their generous support and for guiding me during my years at the University of Memphis.

Finally, I thank my mother Alpana Saha, my father Sontosh Saha, my brother Sudip and my wife Aparajita who have been my greatest supporters. Without their unconditional encouragement, love and support, I would have never started this life-changing journey. You have my sincerest thanks.

ABSTRACT

Saha, Sanjib Kumar. M.S. in Computer Science. The University of Memphis. August 2014. Puzzle-based Learning for Cyber Security Education. Major Professor: Dipankar Dasgupta, Ph.D.

Puzzle-based learning has proven to result in a better STEM learning environment in mathematics, physics, and computer science. However, no significant work has been done in computer and cyber security, only the idea of using puzzles to teach cyber security has only been introduced very recently. We introduce two different puzzle designs, truth table based and decision tree based. In both cases participants have to make decisions according to their knowledge and scenario. We conducted some informal surveys and believe that such interactive learning will help students to understand complex cyber-attack paths and countermeasures for fraud detection, cybercrime, and advanced persistent threats (APTs). Participants will learn not only to protect a specific system but also an entire class of systems with different hardware/software components and architectures, providing similar service. The survey result shows that the puzzle-based learning method has been beneficial for the students towards their learning.

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Page**

1. Introduction

Most of the modern functioning systems that operate utilities like water, electricity, gas, and telecommunication systems are connected and mostly operated through the Internet or some sort of network. This makes these systems prone to network attacks. Many security events occur on a daily basis. According to McAfee, they had discovered more than 25 million new Malware instances in the last quarter of 2013 [1]. Over the past year, the Internet and business populations have faced security issues such as malware (in general and for mobiles), ransom ware, network threats, web threats, spam messages, cybercrime, and hacktivism [1] [2]. Failure to protect data in large companies may result in disasters. Recently, massive attacks on the point-of-sale system at Target© compromised about 110 million customers' credit card data [3]. Moreover, targeted attacks on specific systems or institutions are increasing and so are the mobile device vulnerabilities with the increase of mobile device usage. New spearfishing attacks (e.g. Watering hole) are discovered [4]. The data of millions of users has been compromised from reputed organizations like Evernote, LivingSocial, Ubisoft, Ubuntu forum and NASDAQ community forum in 2013 [5]. Existing threats like malware, network and web threats, spam mail, cyber-crime, botnets, etc. are continuing to disrupt the functionalities of systems.

The security of any computer or information system is ultimately the responsibility of the users who interact or control the computer system. Modern computer systems are composed of a number of software and hardware

components, interacting with each other in a complex way. Any improper handling of these systems may eventually lead to compromising the system and data. Users of these systems need to know about vulnerabilities and they should try to safeguard their systems from the waves of attacks.

It is education and training that will prepare a person's knowledge base, analytical skills and thinking ability to defend their systems from attackers. Even though security protocols for network and computer systems are regularly updated to defend against zero day attacks, it is still very difficult to develop routine exercises or course materials to teach the cyber security issues or to defend against these zero-day attacks [6]. Developing a profound understanding is very important to produce a defensive strategy from the users' own knowledge.

Solving puzzles is an interesting and effective way of learning complex logic and abstract concepts. It encourages the solver to use his/her knowledge on that topic and to think 'outside the box' using his/her skills and expertise. In cyber security education, extensive use of puzzles and their benefits to students are yet to be explored and examined in a classroom environment [2].

The idea of using puzzles for the learning process is based on the high level of stimulation of the human mind while encountering challenges. The human mind is stimulated the most when it encounters a scenario or challenge to solve. Any person will have a better understanding of a topic if he/she faces a challenge and then tries to solve it using his/her knowledge base.

We will discuss the definition and categories of puzzles with the use of puzzles in different sectors of education in the next chapter. Afterwards, we will

focus on the current cyber security problems/issues and the need for puzzle-based learning for cyber security education in chapter 3. We will then present two approaches for puzzle design and explain those approaches in chapter 4. Chapter 5 will show the results of some informal surveys with test implementations of this puzzle-based learning approach and conclude with some suggestions for future works.

2. Literature

Puzzles

Puzzles represent problems that encourage the solvers to use their awareness or knowledge base on the topic and think thoroughly and beyond to solve the problem. Most of the time, the solver has to put the existing pieces of the problem together to get the full picture and only then he/she can solve it. Puzzles are defined in Wikipedia in the following way:

'*A Puzzle is a problem or enigma that tests the ingenuity of the solver.*'

The history of puzzles can be traced back to 1760, when one of the basic forms of puzzles 'Jigsaw puzzle' is first created by John Spilsbury [7]. It became very popular and is still being used as a teaching aid [8]. Until then, different kinds of puzzle have been designed; some for entertainment purposes and others for educational reasons. There are different categories of puzzles. Some of the broad categories are explained below:

1) Jigsaw puzzle: This is a tiling puzzle where numerous small pieces can be arranged (significantly, only one-way) to form a complete picture.
2) Chess puzzle: This is a puzzle using chess pieces on a chessboard where the solver needs to achieve a particular task with the chess pieces.
3) Mathematical problem: Mostly used for educational purposes and to demonstrate complex scenarios. To solve a mathematical puzzle, the solver has to find a solution that satisfies the given constraints. There are

many forms of mathematical puzzle; like logical puzzle, Seven Bridges of Königsberg problem etc.

4) Combination puzzle: A Rubik's cube is a famous example for this category of puzzles. These puzzles consist of a set of pieces that can be manipulated in different ways. The solver has to achieve a particular combination from any random combination.
5) Transport puzzle: These puzzles ask solvers to transport objects from one point to another on a given layout. No object is ever added or lost from the layout and solver has to follow certain rules.
6) Rearrangement puzzle: To solve these puzzles, the solver has to achieve a specific arrangement of objects with a given number of moves or specific number of objects.
7) Situation puzzles: These puzzles have associative storylines for the puzzle scenario. The solver or the user has to provide feedbacks whenever he/she faces a challenge or question. Depending upon the settings, level of difficulty and explanations, his/her answer may be considered acceptable. The puzzle is solved when the solver is able to understand whatever aspect of the initial scenario was puzzling. These puzzles are inexact and many puzzle statements may have more than one 'fitting' answer. It requires critical and literal thinking, logical reasoning to solve these kinds of puzzles.

There are other categories and sub-categories of puzzles used for both education and entertainment purposes. Z. Michalewicz [2] suggested that a puzzle is considered good if it has the following four characteristics:

a. Generality: Puzzles should explain some universal problem solving principles. These general strategies would allow for solving new, yet unknown problems in the future.
b. Simplicity: Puzzles should be easy to state and easy to remember. Easy-to-remember puzzles increase the chance that not just the solution method is remembered.
c. Eureka factor: The problem-solver may feel a sense of satisfaction at their cleverness for eventually solving the puzzle. The Eureka factor also implies that educational puzzles should have solutions that are not obvious.
d. Entertainment factor: Educational puzzles should be entertaining. Entertainment is often a side effect of simplicity, frustration, the Eureka factor, and an ‘interesting’ setting (e.g. a casino environment).

Different forms of puzzles may not have all these characteristics but do have most of the characteristics from the list above. As noted by Michalewicz and Michalewicz, generality is a characteristic of problems, not just puzzles and not all puzzles meet the simplicity criterion. However, the other two criteria are critical for good puzzle design [2].

Puzzles are used extensively for education and classroom settings in modern day teaching methodologies. Whisenand and Dunphy [9] showed effective use of

crossword puzzles to present information system terminology for introductory business information systems students. They proposed the crossword puzzles as a vehicle for accelerating learning vocabulary terms for their future classes. The authors also used picture puzzles in upper level information systems courses and showed that puzzles can be successfully used for teamwork building [10]. Berry and Miller [11] conducted a study with athletes where they found crossword puzzles and computer based trivia activities motivated learning, increased confidence and promoted growth in cognitive knowledge of the students.

Gloria et al. [12] studied extensively to figure out the effects of puzzle-based instructional strategies on primary school students in social studies. They focused on the effectiveness of the use of different kinds of puzzles on the primary school students for educational purposes and found almost similar effectiveness from all different kinds of puzzles.

There is interesting work using the game theoretic approach to defend Denial of Service attack using multi-layered puzzle-based defense architecture [13]. The authors introduced techniques such as puzzle auctions and congestion puzzle and embedded them into both end-to-end and IP-layer services for authentication. Authors demonstrated the effectiveness of proposed techniques in DoS threat mitigation to IP, TCP and application protocols maintaining interoperability with legacy systems and supporting incremental deployment.

Crossword puzzles have been also used for medication purposes. Researchers have shown that crossword puzzle participation at baseline could

delay the onset of accelerated memory decline by more than 2 years in the preclinical stages of dementia [14].

Use of Puzzles in Education

According to Falkner et al., puzzle-based teaching addresses two issues [15]:

1) Emphasizes critical thinking skill rather than simply covering content,

2) Promotes mathematical and logical reasoning among students.

Puzzles help the solver to understand the meaning of topic and to correlate their knowledge base for that topic to propose and apply their solution to solve the puzzle. That enhances the comprehension of their knowledge on the topic (figure 1).

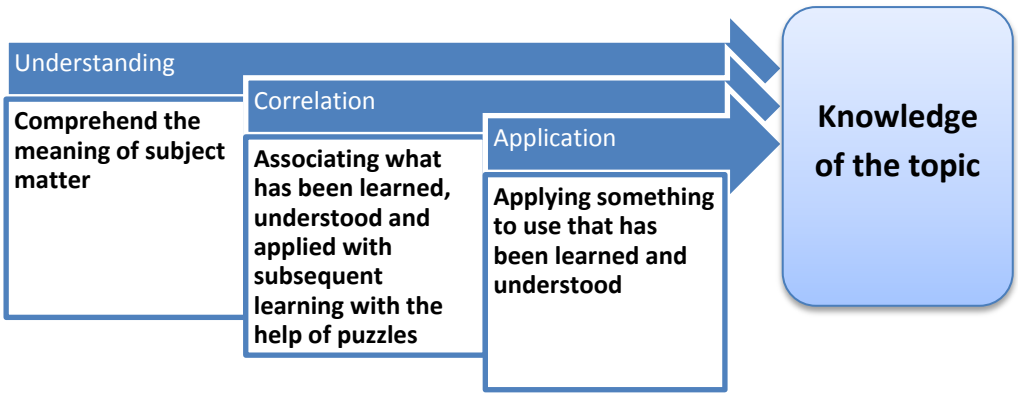

Figure 1: Stages of learning

Many institutions and instructors are using puzzles extensively specially for the STEM curriculums. Specifically, the University of Adelaide offers a Computer

Science course for Puzzle-Based Learning [16]. The course focuses on the fundamentals of framing and solving unstructured problems. This puzzle-based learning course proved developing proficiency in the appropriate use of contemporary technology among the students. Many of the puzzles the class focus on, consist of general mathematical problems, simplistic puzzles that are easy to state and remember, eureka puzzles that often frustrate the solver, and puzzles that have a high entertaining factor. The logical awareness and problem-solving skills of a student are increased by discussing and providing variety of problems in the form of puzzles to the students.

Albright College offers a problem-solving class for their first-year seminar students [17]. The goal of the course was to get students to frame and solve unstructured problems by motivating the students to seek solutions. This course helped the students to develop general problem solving strategies with the aid of a range of challenges and brainteasers.

The University of Technology Sydney offers a seminar on the use of puzzle-based learning to address the gap in the educational curriculum for first year students [18]. The invited lecturer, Zbigniew Michalewicz, presented the idea of using puzzles to improve learning of students in a course at the University of Adelaide. The focus of this course was to increase a student's mathematical awareness and problem-solving skills by covering a variety of puzzles.

The University of Adelaide and The Carnegie Mellon University thoroughly compared the use of puzzles as a teaching tool with the traditional teaching system. The outcome showed the puzzle as a more effective teaching tool over

the traditional teaching methodology [19]. Their work was awarded as the 2010 DSI Instructional Innovation Award Competition Finalist by the Decision Science Institute [20].

The Stanford University Newsletter on Teaching covered a story in reference to problem-based learning [21]. Authors discussed about the concept of problem-based learning and the approach of the problem-based learning in classroom setting. For a successful problem-based learning model, authors assumed that learning to be an active, integrated and constructive process influenced by contextual features. The authors mentioned in their literature review that, a student-centered approach combined with open-ended problems serve as primary incentives for learning for the students [21].

The Centre for Learning and Academic Development (CLAD) at the University of Birmingham funded a project to study the merits of puzzle-based learning in Science, Technology, Engineering, and Math (STEM). The goal of this study is to develop an efficient model for puzzle-based learning to be incorporated in STEM teaching [22].

Authors defined puzzles as perplexing problems that require considerable ingenuity to solve, possibly a lateral thinking solution [23]. The solution may even be unexpected, counter-intuitive or apparently paradoxical. Authors suggested that solving the puzzle should result in a ‘Eureka’ moment or be very satisfying for the solver and the solving process should be both frustrating and entertaining. Additionally, the application of ingenuity should extend beyond writing down correct models.

Melero et al. [24] proposed a conceptual model for designing puzzle-based games to facilitate active learning for students. They proposed two models: generalizing the design of puzzle-based games by integrating puzzle pieces for different learning activities and emphasizing the functional relationship between components of puzzle-based game design. Authors used examples to highlight the concept of puzzle-based games to facilitate the use of their proposed conceptual modal to increase interest in the Information and Communication Technology (ICT) field among students.

Merrick's study [25] conducted a two-year study on the effectiveness on the incorporation of puzzle-based learning into computer science curriculum at the University of New South Wales, Australian Defense Force Academy (UNSW@ADFA). Author compared the responses of her course with other courses that did not use the puzzle-based teaching method on 12 categories including effectiveness of course material, students' perception of course content, development of students' analytical skill etc. The results of the study indicate increment of students' interest and scope for active participation in the course and development of students' critical thinking and problem-solving skills.

Use of Puzzles in Cyber Security Education

Surprisingly, there are very few attempts of using puzzles in cyber security education. Among them, some initiatives are worth mentioning that use puzzles for cyber security education. Gondree et al. suggested some tabletop card and

board games to expose fresh audiences to cyber security via informal learning [26]. The existing cyber security games (e.g. Capture the flag) sacrifice many freedoms of play due to technical reality or simulation. The authors tried to present the idea of informal, social, dynamic, challenging, attractive and rewarding games for the cyber security education that is simple to learn and do not require any special equipment. To be successful as a learning tool, these games should introduce the audience to new ideas and stimulate continued study.

Dasgupta et al. [27] presented the idea of using puzzle for the cyber security education. They have suggested the use of an interactive learning process for cyber security learning will help the students to comprehend the topics and use their knowledge to defend against unexpected attack situations. After that, Dasgupta and Saha presented the idea of using decision trees for designing puzzles for cyber security learning in their work [28].

3. Cyber Security Issues

Modern offices and institutions are moving towards paperless environments for both environmental and efficiency purpose. Nowadays, most of the official documents are saved electronically and official communications are done using electronic media (e.g. email). Complex industry machineries are controlled by large network of computers. Both centralized and de-centralized utility distribution systems use large meshes of networks for efficient operation. Any person, who operates or uses these systems, may become a victim of due to cyber vulnerabilities. The person may be an online customer, IT employee, network/system administrator or security staff. Therefore, all personnel, who use any device that connects with a network, require different levels of cyber security education and training according to their exposure to the network and the value of their work. Users need to know about the security breaches and data compromises associated with identity theft and should learn how to protect them from these attacks and vulnerabilities.

There are incidents where the negligence of one employee resulted in a massive data breach for the institution. In 2011, RSA employee was tricked into retrieving a junk mail message by a well-crafted message containing a virus. RSA experienced a security breach as that virus lead to a sophisticated attack on the company's information systems [29]. In January 2013, Facebook experienced an attack when malware was installed on some employees' laptops. The employees visited a compromised mobile developer's website and the malware

was installed on laptops via the exploit that was hosted on that website. Later, Facebook found that the site was using a previously unseen, zero-day exploit to bypass the Java sandbox (built-in protections) to install the malware [30].

The cyber world has recently experienced some catastrophic exploitation of cyber network security. Five major retailers' networks were attacked using Random Access Memory scraping technique during the 2013 holiday shopping season and compromised customer data [3]. More than 40 million users' credit information was compromised in the Target© Point-Of-Sale attack between November 27 and December 15 of 2013.

'Heartbleed' is a security bug in the OpenSSL cryptography, resulted from a missing bound check in the handling of the Transport Layer Security (TLS) [31], exposing millions of users data to be compromised. It was believed to be the worst vulnerability in the computer science history since commercial Internet service has started [32], compromising the security of more than half million '*secure*' web servers that were certified by trusted authorities, allowing the theft of the private keys of the servers and user session cookies and passwords [33].

Attackers are getting more expert and using sophisticated technologies to exploit the systems than ever before (Figure 2). The differences between emails and social networking, PCs and tablets/smartphones are also going blurred with time. Attackers are changing their attack trends and patterns. For example, attackers are designing threats to take advantage of the user email information regardless of the device used to access email. Cybercriminals identified an exploitable design flaw in email defenses that allowed a 'point-of-click' attack to

occur, where the embedded link in an email points to an infected destination. Attackers exploit the fact that the email links are not evaluated until the email is accepted by an organization's email system. Therefore, cybercriminals infect the link's destination after email gets past security defenses and before recipient clicks the link. According to the threat report for the last quarter of 2013, almost one in every four emails contains malware as URL [4].

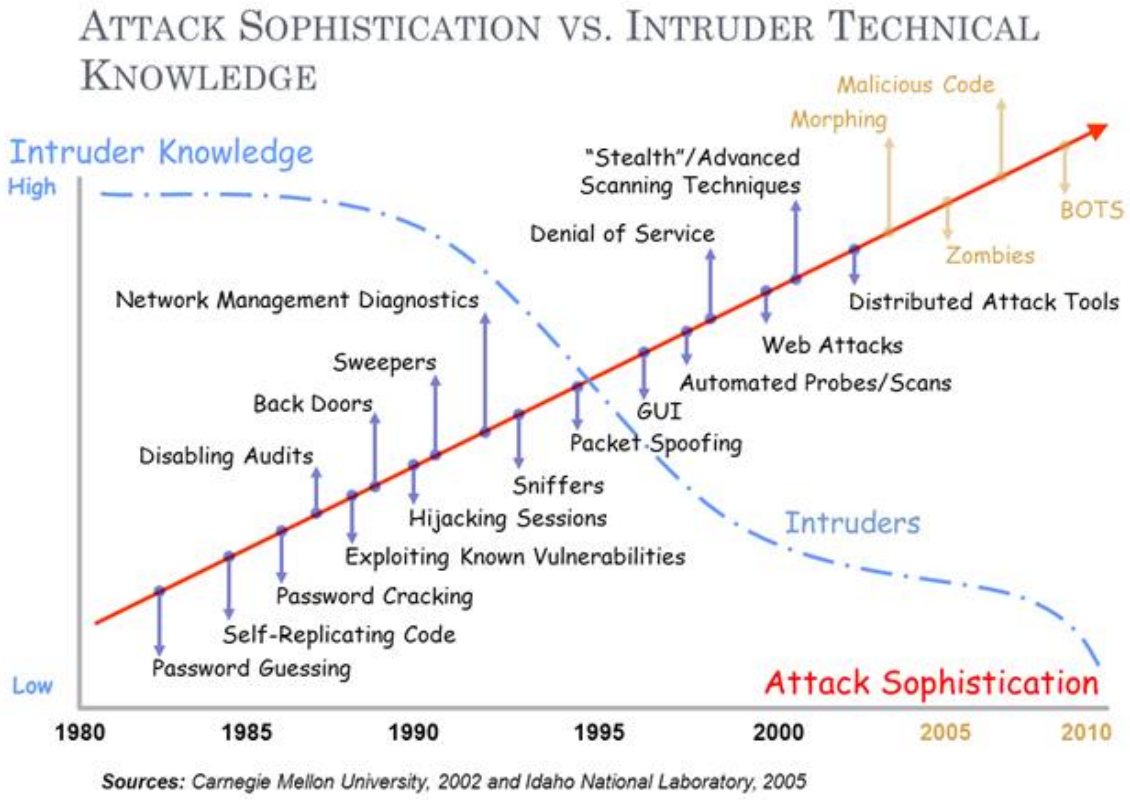

Figure 2: Trend of attack sophistication with timeline

Attackers are using malware to steal sensitive and confidential information from organizations for around for a decade. Attackers maintain relatively low profile for these targeted attacks to remain below the radar of security technology. Attackers use malwares aimed at a specific user or group of users within a targeted organization and may deliver through spear-phishing emails, or a form of drive-by download known as a watering-hole attack [4]. These attacks are designed to be low in volume, often with malicious components used exclusively in one attack to remain undetected. Their ultimate goal is to provide a backdoor for the attacker to breach the targeted organization (Figure 3).

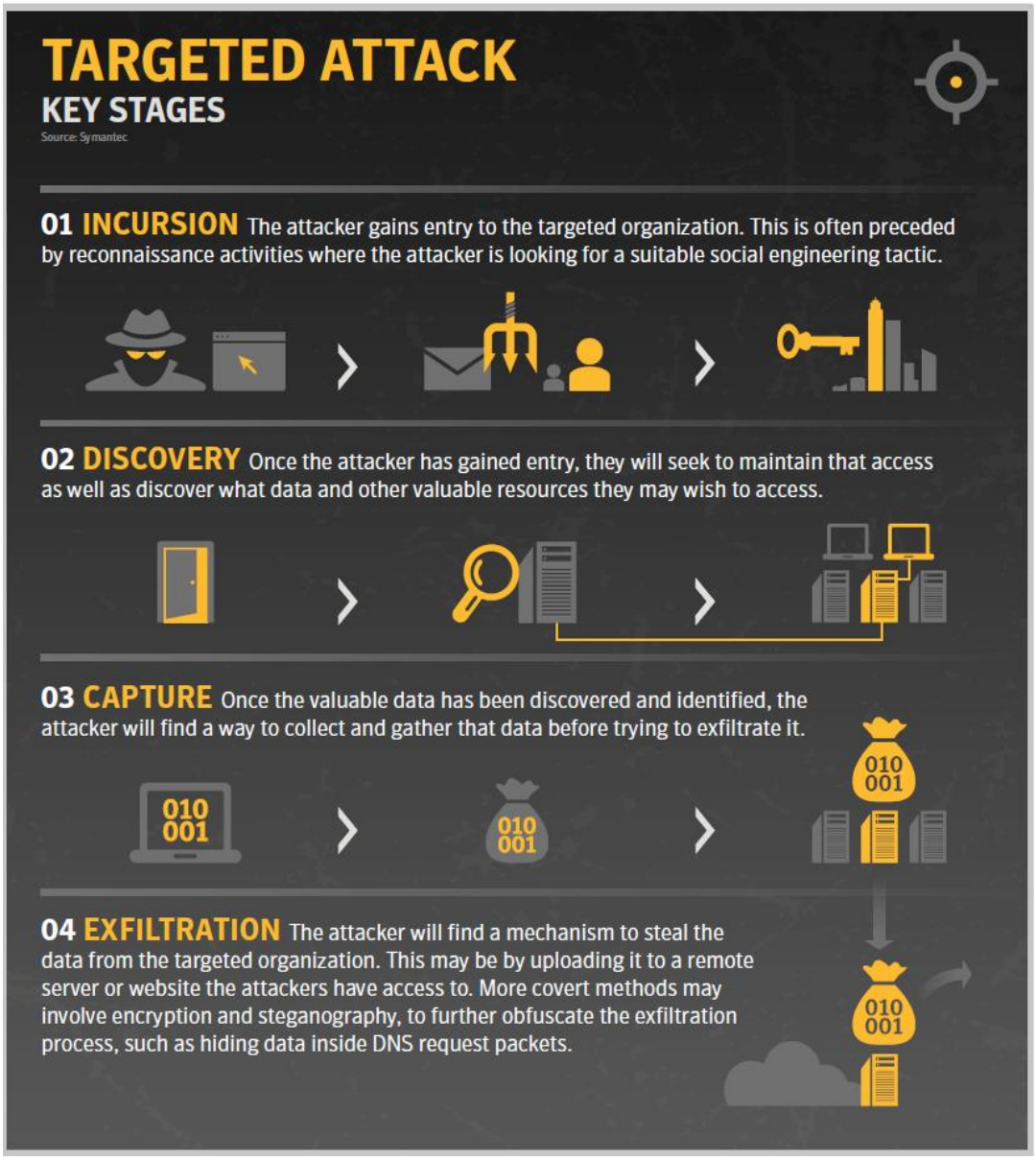

Figure 3: Key Stages of Targeted attacks [4]

Attackers no longer rely only on spear-phishing attacks in order to penetrate an organization's defenses. Rather than, they have expanded their tactics to include watering-hole attacks, which are legitimate websites, compromised for installing targeted malware onto the victim's computer. These attacks rely mostly

on zero-day vulnerabilities for client-side exploits. In order to remain undetected, attackers keep switching the vulnerability used for exploitation, as the vulnerabilities, they are using, has been published. Attackers are more interested towards the targeted attacks because one successful attack will result in a large set of compromised data with large financial implication. From Figure 4, attackers are targeting almost all sectors of business keeping government networks at the top.

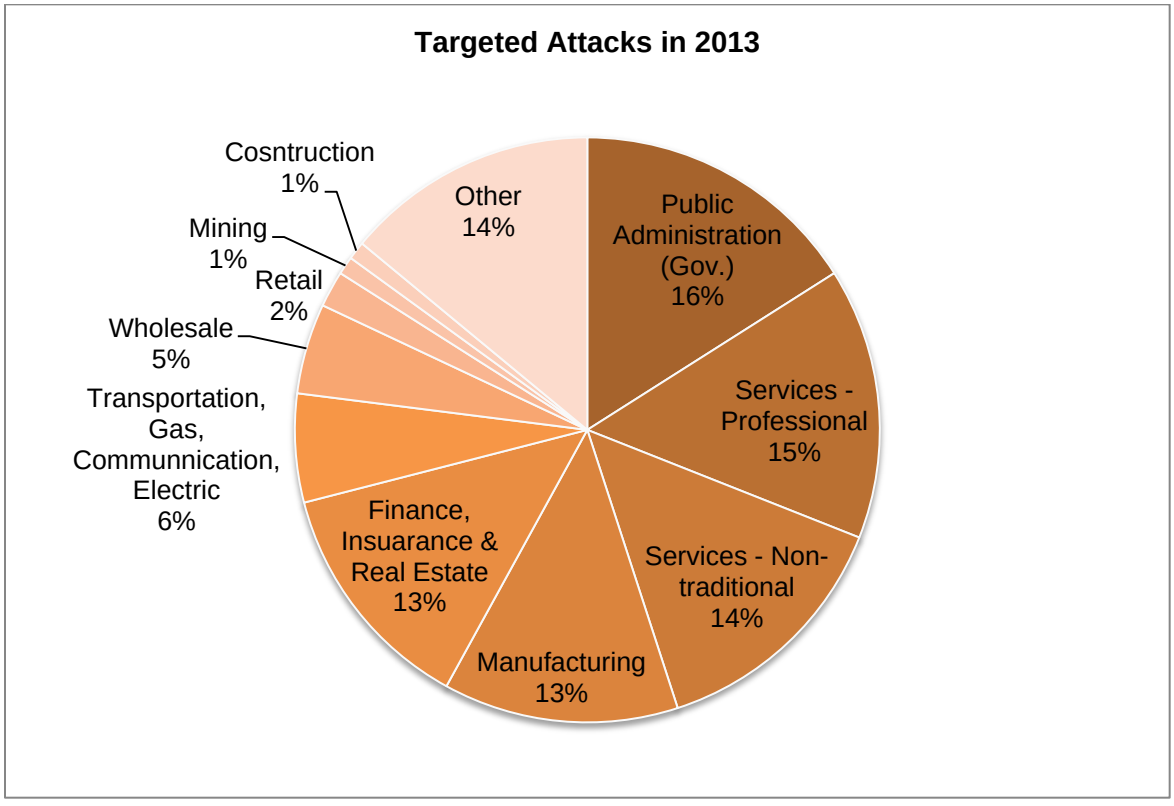

Figure 4: The distribution of Targeted attacks to various Industries

Why improvement is needed

With the increased use of credit cards, online transactions and virtual money, even the sole user lives at the edge to compromise his/her money or even identity. Many of the mobile phone and social network applications, web site memberships and other applications require the use of credit cards for verification purpose. Online banking and online shopping are getting more popular to users to save money and time. These modern life trends also carry the risk of losing the information that may cause financial losses and identity theft. Almost 552 million identities were exposed in 2013 alone [4]. About 66% of the emails delivered every day are spams. More than 3,200 Android malwares were detected and more than 56,000 new malicious web domains were found only in 2013 [4]. In this situation, nothing other than knowledge is the key for the users to defend against these vulnerabilities and attacks.

Cyber security education is already an established area of study in most educational institutions. New attacks evolved every day and security policies are updated to defend against the new attacks. Attackers continue to deliver sophisticated and innovative approaches to bypass the security defenses and the cycle continues. To cope with the ever-evolving area, cyber security curriculum needs to withstand the changes.

Various approaches are used for cybersecurity education purposes. The methodical classroom settings are used almost everywhere with basic contents to convey the knowledge to the students. Lab setup is also used to create the network environment to simulate the role of attackers and defenders using the

vulnerability databases [34]. Projects are also used to provide students thorough understanding of the systems and complex relation between machine and networks. Cyber security competitions (e.g. Capture the flag) are also arranged to inspire innovative ideas.

In his work, Eagle discussed the current trend and issues on the cyber security education [6]. He focused on the issues with teaching methods ignoring the constantly developing fundamentally new kinds of attacks. He also argued about the advantages of the security competitions over the stand-alone exercises for the cyber security education and pointed on the deficiencies of the current competition systems. He suggested scope of improvements in competition values that might help to achieve higher rate of success for the cyber security competitions.

Folkner et al. [15] has discussed about the learning methods that can be used to develop the problem solving skills among students. Traditional problem-based learning helps acquisition of domain specific knowledge for the students. Project-based learning, depicting problems most relevant to real world situation, trains the students with to deal with uncertainty and changing conditions. On the other hand, puzzle-based learning stimulates student's critical thinking and logical reasoning capability and helps the students to grasp abstract reasoning (Figure 5).

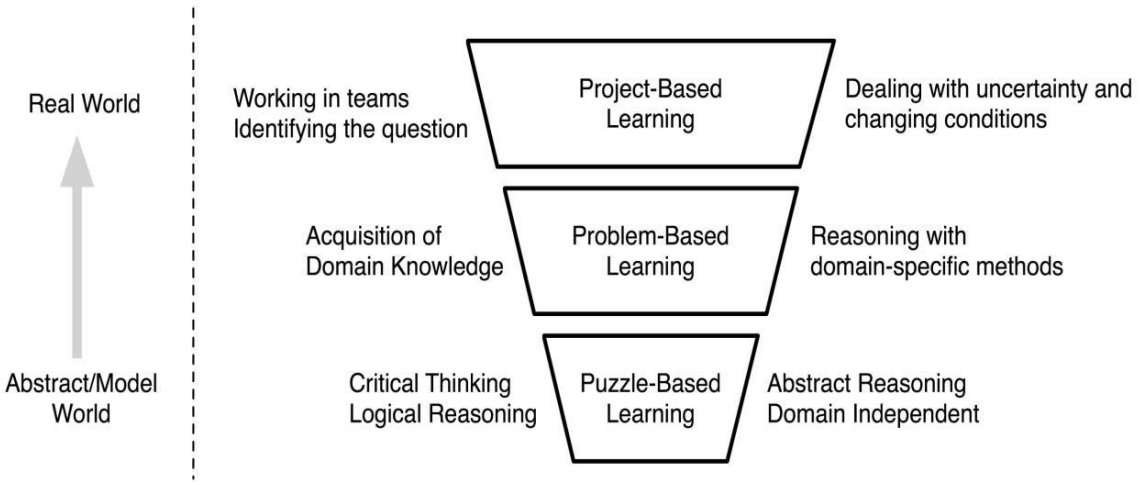

Figure 5: Variety of learning and skills needed for problem solving in real world

With the ever changing situation in the cyber security domain, users need to develop their own reasoning and thinking ability. As discussed by Eagle [6], methodical classroom setting or problem-based learning does not prepare the participants to defend against unseen zero-day attacks. There will be no pre-defined patterns of cyber security threats and vulnerabilities. Therefore, it is important that the learning methods develop a clear understanding of the scenario among the participants and they can produce effective defense strategy for any new attack from their own perception.

4. Puzzle-Based Learning for Cyber Security Education

The introduction of puzzles in the learning process will help the participants to realize and evaluate the cyber security concepts while solving puzzles related to cyber security problems. Different types of puzzles are needed to cover various knowledge domains and complexity levels according to the need of different user domains. There should be levels of puzzles to test the ability of the solvers at different difficulty level. Level-one puzzles may constitute of only very basic operations regarding computers and networks and covering only one knowledge unit. Next level puzzles may deal with different kinds of exploitations and vulnerabilities. These puzzles may cover more than one knowledge units. Level-three puzzles may have problems regarding cross-linking exploitation, code injection attacks and may cover 3 – 4 knowledge units. Higher-level puzzles will cover complex real life events, regarding social apps, secure server penetration, web browser security etc. and will cover many knowledge units. An example for a high-level puzzle scenario is shown in figure 6, where the participant has to consider different application and server modules along with a range of vulnerabilities.

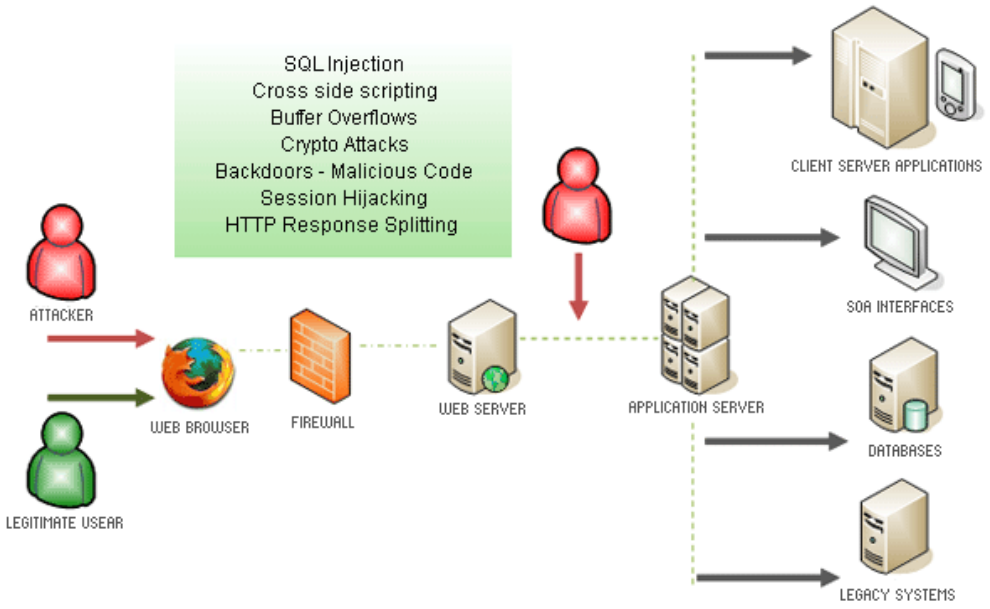

Figure 6: Plot for high-level puzzles

We introduced some ground principles for developing cyber security puzzles:

1) Puzzles should have different levels of difficulty like some popular games for different target groups. Entry-level puzzles cover one knowledge unit (KU) such as existing vulnerabilities, common errors in user interaction etc. Higher-level puzzles encompass bigger scenarios, real life events and cover more knowledge units and attack surface regarding cross-linking complex exploitation, code injection attacks, which may originate in social apps, secure server penetration, web browser security etc. Such attacks may not follow predefined exploitation paths; similarly, our puzzles follow non-trivial solutions.
2) Puzzles may not have unique solutions rather most likelihood outcome. Since a security puzzle cannot describe all real world environment setting

so there may not have unique solution/decision, which is correct. In addition, interactive puzzles should provide hints to guide the learner in finding a most likelihood solution based on the assumptions made. Accordingly, a difficult puzzle (with more ambiguous options) should incorporate many hints as it may come across different attacks/solution.

3) Puzzles should be open-ended (if possible) and may have inter-connected paths or branches. For example, in the higher level puzzles, someone may start with one puzzle and can move around multiple knowledge units with the flow of the scenario.
4) A good security puzzle must have out-of-the-box attack/solution component of knowledge units. All puzzles should be in-line with the emerging technology to provide up-to-date knowledge.

We developed an interactive environment, where the participants can take their own decision based on the available options. We created some scenarios based on the real life events depicting some possible attacks. Every event has a corresponding state that can be safe, suspicious or compromised. Participants start from a safe state and then asked to perform certain tasks or to take decision regarding to a situation. Their actions can lead to different states so to realize whether their response lead to any exposed state or data breaches. Participants have to perform their tasks or take their decisions in a manner such that, they always remain in safe states. In this way, the participants will know the consequences of their actions and decision that may lead to possible breaches. Therefore, participants can have an experience of the real world operation

scenario beforehand without actually exposing any system in the risk of real compromise. During the decision making, participants get feedback from the puzzle scenarios about their responses. These feedbacks explain why any participants' choice is good or how their choice can expose the system towards some vulnerability. These analyses help the participants to build their mental model for the scenarios and assist them to grasp the knowledge more efficiently.

In our puzzle scenarios, the participant will have to play the role of a character in a story line. The person also needs to make decisions based on the current situation of the scenario. While taking any decision, the participant has to consider the present situation and the future outcome of the decision so that his/her decision does not lead to any weakness or vulnerability of the system, which may expose the entire organization to any attack. The puzzles are designed in such a way that they do not have unique solution with most likelihood outcome. Hence, participants will face different challenges based on their prior responses.

These puzzles are supposed to be used in physical classrooms as well as virtual classrooms. These puzzle scenarios are designed to be interactive and self-explanatory, so that, participants can use these scenarios without any previous walkthrough or external help. Still, it will be a good idea to include some introductory slides to demonstrate the navigation through the puzzle scenarios.

These puzzles are designed in a way so that the participants face variation of challenges based on their prior knowledge and based on their responses on prior puzzles. Two kinds of puzzles are proposed. One kind of puzzles uses truth

tables to formulate attack vectors. The variables of these truth tables are different network layers or components and functions are the combination of some vulnerabilities and weaknesses of those network layers. Participants will be given a scenario and they will be put into a situation where they will have to face some attacks based on the weaknesses exposed by them so far. The use of structured truth tables with network components and corresponding vulnerabilities help to build attack functions using network weaknesses as parameters.

Other kinds of puzzles are based on logical decision trees. At the end of running through the puzzle scenario, the result will show the participants whether their actions and decisions make them a victim of vulnerabilities or save them from exploitation.

Truth Table (T-T) based puzzle

Truth tables are used to breakdown a logic function by showing all possible values the function can attain. A truth table lists all possible combinations of values of variables and corresponding function outputs. Thus, a truth table can be used to find out the required states of the variables for a desired state of the function.

We use truth tables for vulnerabilities and attacks. There are certain components for any network architecture, and a weakness may exist in some or any of the components of the architecture. In T-T based approach, we expressed

the vulnerabilities and attacks as functions of these different network layer weaknesses.

The vulnerabilities and attacks are expressed as functions of these different network layer weaknesses. For an example, we considered the layered addressing model of network traffic flow (Figure 7). Any inbound traffic arrives at application layer has the DNS address. The corresponding IP address is resolved by the DNS server and after that destination MAC address is translated from the IP address to deliver inbound traffic. For outbound traffic, the reverse path is usually followed. We considered only ARP, IP and DNS service components for this example. Any of these components can have weaknesses: either functional or in implementation. Any of the weaknesses may expose the system to various kinds of vulnerabilities and attacks depending of the particular component weakness.

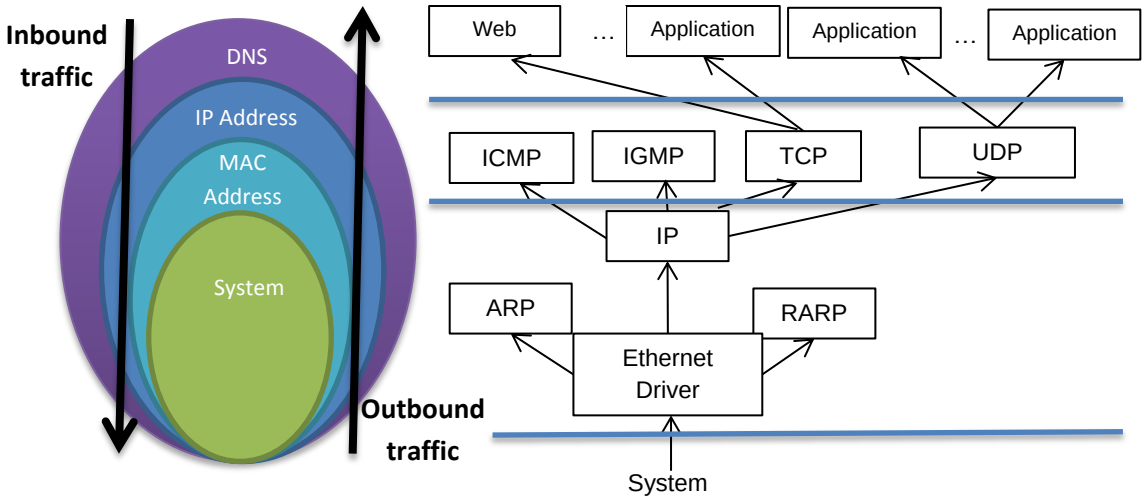

Figure 7: Illustration of layered addressing (in traffic header) and corresponding network protocols associated with addressing.

The relationship among the attacks and the addressing component vulnerabilities is expressed with a truth table. For example, we took three components of the TCP/IP packet retrieval process and prepared a truth table (table 1) for ‘man in the middle’ and ‘DNS spoofing’ attacks. Table 1 shows the relationship among the attacks and component vulnerabilities. We took ARP, IP and DNS as the components for the vulnerabilities and they are the variables for the truth table. Any cell in components columns with value ‘0’ denotes no vulnerability is present and ‘1’ denotes some kind of vulnerability in present in the corresponding component. A value of ‘1’ in the attack column denotes the attack is possible for the corresponding combination of vulnerabilities and ‘0’ denotes a safe state from the attack. The combination of the vulnerabilities can be denoted as a vector of truth-values. For example, the third row of the table can be

expressed as a vector of variables like <0, 1, 0> and these values of the vector are mapped to the table variables ARP, IP and DNS accordingly. The <0, 1, 0> vector denotes no vulnerability exists in ARP and DNS component, but some vulnerability exits in IP component. For the <0, 1, 0> combination in table 1, we have '1' in 'man in the middle' attack and '0' in DNS spoofing attack column. It denotes that, for this combination of vulnerabilities in the corresponding components, the given system is prone to a 'man in the middle' attack but apparently safe to a 'DNS spoofing' attack.

Table 1: The truth table for ARP, IP and DNS layer weaknesses and attacks.

Components			Attack	
ARP	IP	DNS	Man in the middle attack	DNS spoofing
0	0	0	0	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Using this table 1, we formulated logic functions for any specific attack using the component vulnerabilities as variables. Function minimization tools (ex. K-

map) can also be used in this process. From table 1, the function we come up with the following logic functions for the attacks.

f (Man in the middle) = IP + DNS …… (1)

f (DNS spoofing) = DNS ……. ……... (2)

Therefore, function (1) denotes a ‘man in the middle’ attack can be launched if there is some vulnerability in either IP or DNS components. It can also be expressed as a vector of table variables as <X, 1, X>, <X, X, 1>, symbolizing two possible scenarios for ‘man in the middle’ attack, where any IP component vulnerability or any DNS component vulnerability is providing enough scopes for the attack.

We propose another format for the T-T based puzzles, where the vulnerabilities will be considered as variables for some specific attacks as functions. We follow the same structure as table 1 to prepare these truth tables, where 0 in the variable columns will denote absence and 1 will denote the presence of the vulnerability specified in the column header. Also for function columns, 0 denotes a safe state and 1 denotes an attack possibility for the attack specified in the column header. For example, we consider two vulnerabilities

from both IP layer and DNS layer. Then we prepared a truth table for ‘Worm propagation’ and ‘Man in the middle’ attacks.

Using data in table 2 and function minimization tools, we can derive the attack formula for ‘Worm propagation’ and ‘Man in the middle’ attacks. The functions for the functions will be following:

f (Worm propagation) = (Access Control List Vulnerability) + (MS DNS Server Misconfiguration) …… …… (3)

f (Man in the middle) = (DoS MAC Entries Vulnerability) + (Access Control List Vulnerability) ……..…….. (4)

Here, function (3) denotes a ‘Worm propagation’ attack can be launched if either of ‘Access Control List Vulnerability’ or ‘MS DNS Server Misconfiguration’ vulnerability exists. It can also be expressed as a vector of table 2 variables as <X, X, 1, X>, <X, X, X, 1>, symbolizing 2 possible scenarios for ‘Worm propagation’ attack. Similarly, the ‘Man in the middle’ attack will have vector as <X, 1, X, X>, <X, X, 1, X> of table 2 variables.

Table 2: Truth table for IP vulnerability and DNS vulnerability with corresponding attacks

IP layer vulnerability		DNS vulnerability		Attack	
Ping flooding	DoS MAC Entries	Access Control List Vulnerability	MS DNS server misconfiguration	Worm propagation	Man in the middle
0	0	0	0	0	0
0	0	0	1	1	0
0	0	1	0	1	1
0	0	1	1	1	1
0	1	0	0	0	1
0	1	0	1	1	1
0	1	1	0	1	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	1	1	0
1	0	1	0	1	1
1	0	1	1	1	1
1	1	0	0	0	1
1	1	0	1	1	1
1	1	1	0	1	1
1	1	1	1	1	1

We termed these vectors as '*Attack vectors*' for the corresponding attacks. Analyzing attack vectors of two or more attacks, we can find any relationship between these attacks. For example, we can see from the attack vectors of 'Worm propagation' and 'Man in the middle' attacks that, a 'Worm propagation' attack may also lead to a 'Man in the middle' attack in certain circumstances.

Matrix Representation of Relationship between Vulnerabilities and Applications

The relationships among applications with their corresponding vulnerabilities are represented in matrix format. Every type of application has a two-dimensional matrix to store the relationship among the vulnerabilities and the applications. In these matrixes, vulnerabilities are arranged row-wise and applications are presented in columns. A value of 1 denotes that the vulnerability is applicable in the corresponding application (column header) and a value of 0 denotes that the vulnerability is not applicable for the corresponding application (Tables 3, 4 and 5). These two dimensional matrixes are combined and represented by a three-dimensional matrix.

Table 3: Vulnerability Matrix for Operating Systems

	Windows XP SP2	Windows 7	Mac OS X	Linux	Android 4.0.0
CVE-2013-6666	1	1	1	1	0
CVE-2014-0497	1	1	1	0	0
CVE-2014-0521	1	1	1	0	0
CVE-2014-0502	1	1	1	1	0
CVE-2012-2036	1	1	1	1	0
CVE-2014-0515	1	1	1	0	0

	Windows XP SP2	Windows 7	Mac OS X	Linux	Android 4.0.0
CVE-2013-1729	0	0	1	0	0
CVE-2014-1732	0	0	0	1	0
CVE-2014-1735	0	0	0	1	0

Table 4: Vulnerability Matrix for Browsers

	Google Chrome 34.0.1847.131	Google Chrome 33.0.1750.116	Mozilla 24.0	Mozilla 19.0
CVE-2013-6666	0	1	0	0
CVE-2014-0497	0	0	0	0
CVE-2014-0521	0	0	0	0
CVE-2014-0502	0	0	0	0
CVE-2012-2036	0	0	0	0
CVE-2014-0515	0	0	0	0
CVE-2013-1729	0	0	0	1
CVE-2014-1732	1	1	0	0
CVE-2014-1735	1	1	0	0

Table 5: Vulnerability Matrix for applications

	Adode Reader 10.1.9	Adobe Acrobat 11.0.06	Adobe Reader 9.5.2	WordPress 3.7.1	WordPress 3.8.1	WordPress 3.0.1	Sea Monkey 2.16
CVE-2013-6666	0	0	0	0	0	0	0
CVE-2014-0497	0	0	0	0	0	0	0
CVE-2014-0521	1	1	1	0	0	0	0
CVE-2014-0502	0	0	0	0	0	0	0
CVE-2012-2036	0	0	0	0	0	0	0
CVE-2014-0515	0	0	0	0	0	0	0
CVE-2013-1729	0	0	0	0	0	0	0
CVE-2014-1732	0	0	0	0	0	0	0
CVE-2014-1735	0	0	0	0	0	0	0

For any specific configuration, the corresponding values are extracted from the relational matrix to prepare the dependency matrix. A dependency matrix is created for every application from the configuration. For example, we consider the following configuration of a computer system:

- OS: Mac OS X
- Browser:
    - Mozilla 19.0
    - Google Chrome 34.0.1847.131
- Application:
    - Adobe Acrobat 11.0.06
- Considered vulnerabilities:
    - CVE-2013-1729

Dependency matrixes are created for each kind of application using the data from the vulnerability matrixes. The effect row for each matrix is calculated by performing AND operations for the values in each column. The result value for each matrix is created by performing OR operation for the values of the effect row.

Table 6: Dependency Matrix for Operating Systems

	Windows XP SP2	Windows 7	Mac OS X	Linux	Android 4.0.0
Browser application running on OS	0	0	1	0	0
CVE-2013-1729	0	0	1	0	0
Effect Row	0	0	1	0	0

The result value of the dependency matrix for operating systems, Result1 is calculated as (0 OR 0 OR 1 OR 0 OR 0) = 1 (table 6). Similarly, the result value of the dependency matrix for browsers, Result2 is calculated as (0 OR 0 OR 0 OR 1) = 1 (table 7) and for applications, Result3 is calculated as (0 OR 0 OR 0 OR 0 OR 0 OR 0 OR 0) = 0 (table 8).

Table 7: Dependency Matrix for Browsers

	Google Chrome 34.0.1847.131	Google Chrome 33.0.1750.116	Mozilla 24.0	Mozilla 19.0
Browser application used	1	0	0	1
CVE-2013-1729	0	0	0	1
Effect Row	0	0	0	1

Table 8: Dependency Matrix for Applications

	Adode Reader 10.1.9	Adobe Acrobat 11.0.06	Adobe Reader 9.5.2	WordPress 3.7.1	WordPress 3.8.1	WordPress 3.0.1	Sea Monkey 2.16
Application Running	0	1	0	0	0	0	0
CVE-2013-1729	0	0	0	0	0	0	0
Effect Row	0	0	0	0	0	0	0

Browsers and applications both run on top of Operating System (OS). But browsers and applications can run independently. So result 2 (browsers) and result 1 (OS) are logically AND to check if the considered vulnerability creates any risk for this specific combination of operating system and browser application. This process is repeated for every combination of dependent applications. For the considered example:

- R1 = result 2 AND result 1 = 1 AND 1 = 1
- R2 = result 3 AND result 1 = 0 AND 1 = 0

As browsers on OS and applications on OS runs independently, so these two results (R1, R2) are logically OR-ed to determine the effect of the considered vulnerability on the given system configuration. For this example, the final result R is calculated as (1 OR 0) = 1. The value of R as 1 (one) denotes the current configuration is not safe for vulnerability CVE-2013-1729. If we get 0 (zero) as the value of the final result R: then we can conclude that the given configuration is safe for the considered vulnerability.

Decision Tree (D-T) based puzzle

We also use a decision tree to model attack scenarios. This decision tree can also be termed as an attack graph or attack tree. Nodes in the tree denote different states in the puzzle scenario. An edge exists between two nodes ‘a’ and ‘b’ if there is any action from the user from state ‘a’ leads to state ‘b’ (as shown in

Figure 8). These states are divided into different network planes based on their functions. States are converged to some destination goals, possibly a state where user is exploited to some attack or a state where the user is safe. States in different planes are connected as consequences of the user actions. Figure 8 shows how the consequence of user actions will result in user states in different planes.

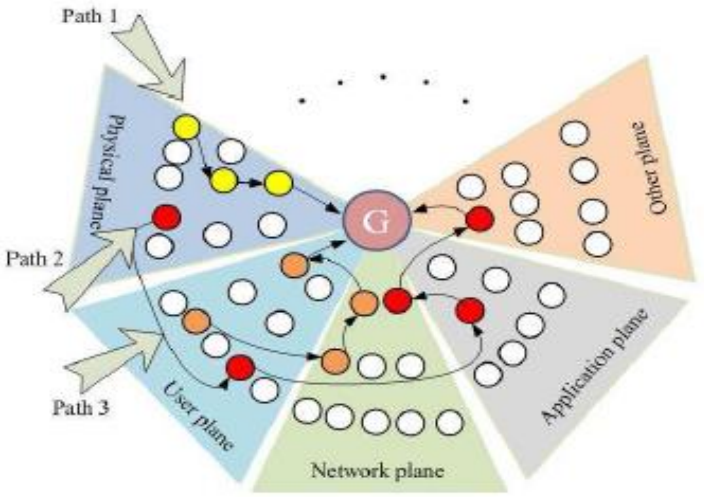

Figure 8: Connection of events among attack planes [35]

Figure 8 demonstrates how complex attacks can be launched from any plane to exploit a system and the consequences of any inappropriate user action from any plane may lead to the exploitation of some other plane. We showed another example of possible attack scenarios for online social networks in Figure 9.

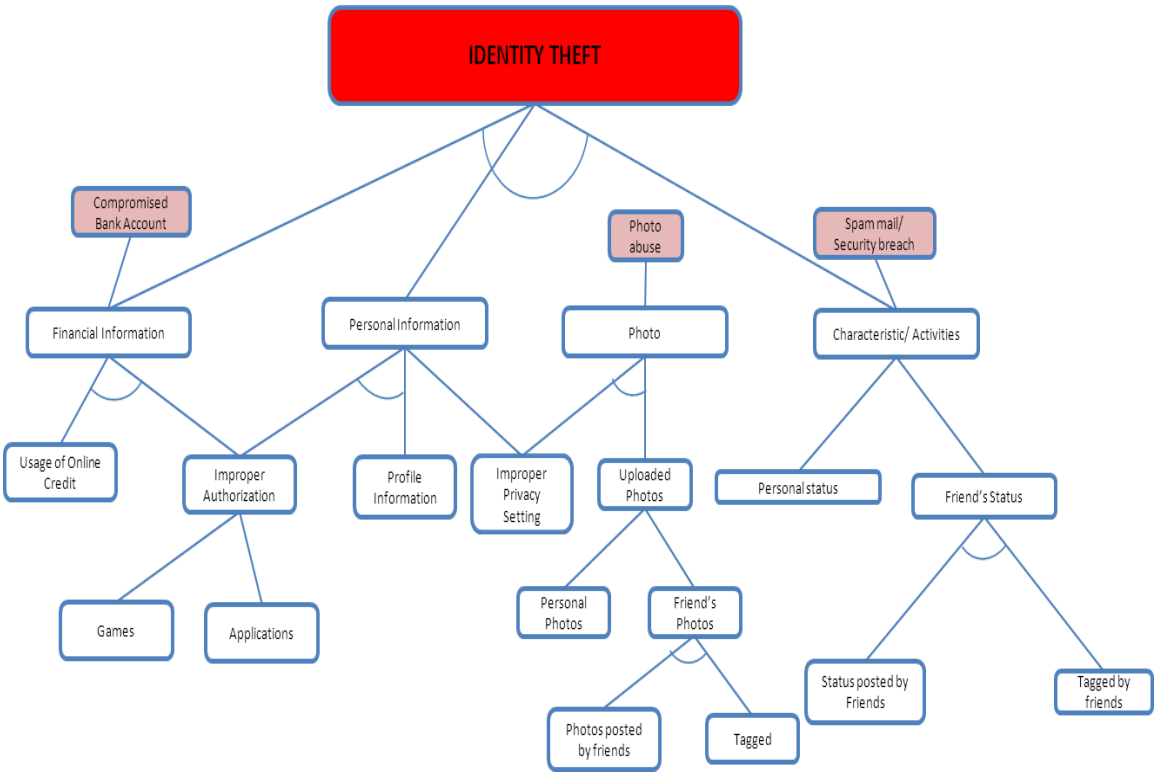

Figure 9: Decision tree depicting the consequences of user action in different states

In Figure 9, the relationship between different states and consequences are shown in a tree structure. As shown in the graph (Figure 10), a goal or final state can be reached in more than a single way. We use this ideology in our decision tree (D-T) based puzzle design using formulated decision trees as the backend logic of the simulation of the puzzle scenarios. For example (Figure 10), two different action sequences are shown in a decision tree (or attack graph) that can lead to the same final state of a compromised bank account.

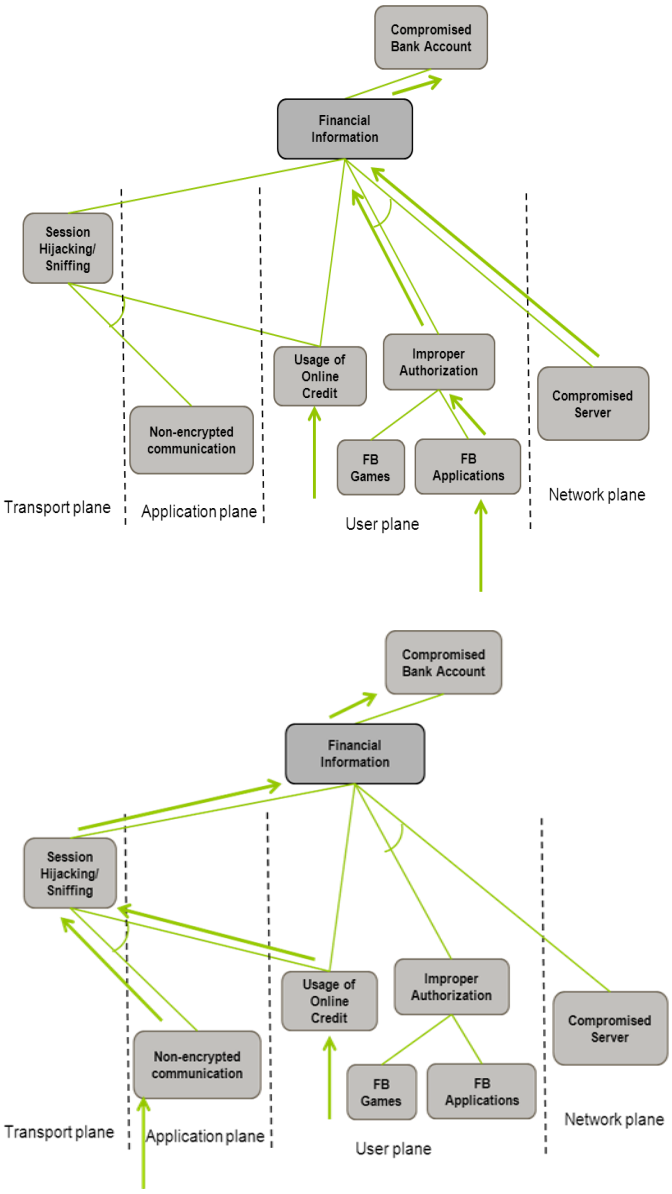

Figure 10: Different traversal of the decision tree using different network planes

Advance Persistent Threats (APTs) are emerging for the last couple of years. From the figures 8, 9 and 10, it can be shown that attacks are no more confined to any specific vulnerability. Any loophole can result into complete compromise of

the systems. Specifically, with the APTs in sight, we should check all communications (emails, links) and executables running in a machine. Any apparently innocent link in a mail or an executable (running in any plane) can create the channel for attacks for other planes. Therefore, it is very important for the users of the system to have proper knowledge about system functionalities to detect any kind of intrusion or attack.

Implementation

We have used Articulate Storyline® to simulate virtual environments to implement our puzzle scenarios. Participants will find themselves in a virtual environment with many options to choose. Their actions or choice of option will lead them to different situation (state) or may expose them to a new problem. Therefore, depending on their course of actions, a participant may experience different outcomes in different simulations. We present some examples of our implemented puzzle scenarios.

Puzzle example 1

This is an example of a basic level 1 puzzle designed using a decision tree (D-T) model. In this scenario, participants are asked to check his/her online banking account on a virtual bank. The scenario starts from choosing the device they want to use (Figure 11). In the course of action, the participants need to decide among different options according to their prior decisions (Figure 12).

Figure 11: Choosing device (Example 1)

Figure 12: Login window (Example 1)

Participants are provided various feedbacks in the middle of the simulation depending on their feedbacks and decisions. At the end of the simulation, Participants will be provided with the evaluation of their actions (Figure 13) and they will be showed the possible vulnerabilities they were exposed during the simulation in the form of an attack graph in the decision tree (Figure 14). The evaluation and attack graphs will be generated according to the actions of the participants.

Figure 13: User evaluation (Example 1)

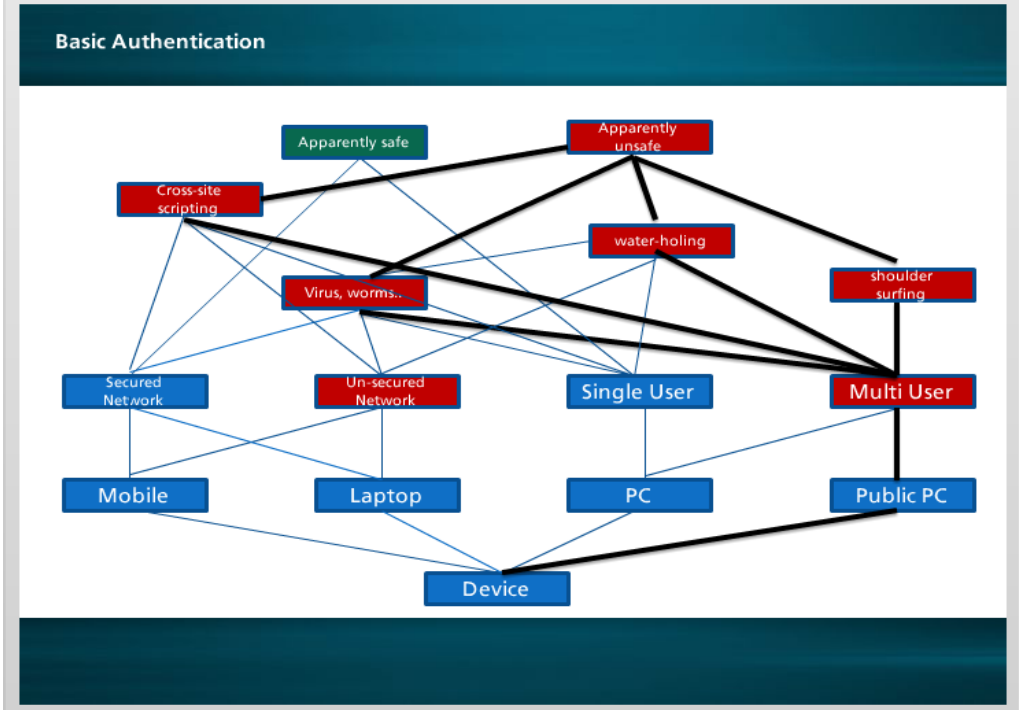

Figure 14: Generated attack graph in the decision tree (Example 1)

The generated attack graph (Figure 14) will show the possible vulnerabilities the participants may be exposed to, according to the actions they have taken during the puzzle scenario. In figure 14, a sample generated attack graph is presented. Here the dark lines resemble the paths the participant has taken according to their decision and also the possible attacks and final goal. In this example, the participant has selected to use a public pc. So that is used by multiple users, and thus he/she may be exposed to virus, worms, and watering-hole attacks. Also using computers in public space carries a risk of shoulder surfing. Therefore, the participant is apparently unsafe in the browsing session.

Puzzle example 2

This is an example of a level 2 puzzle, where the participant has to take the role of a network administrator in an office. This puzzle is also designed using a decision tree (D-T) model. In this scenario, participants are made aware of the current network security situation of the office (Figure 15). Then participants have to train their staffs and need to decide some IT policies for the office infrastructure (Figure 16).

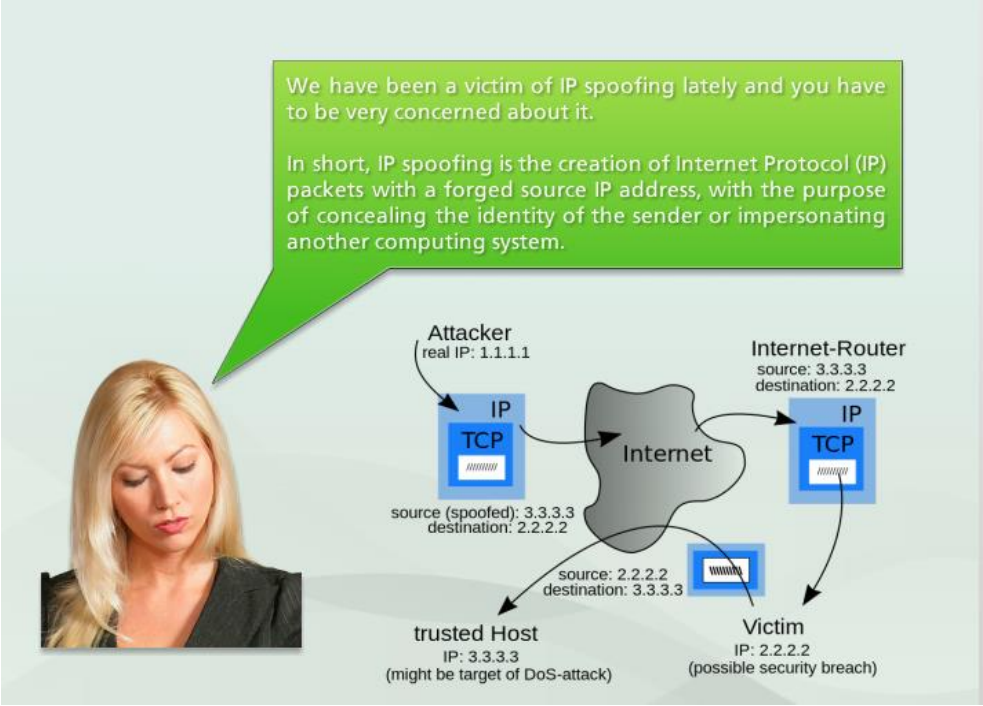

Figure 15: Introduction to office network vulnerability (Example 2)

Figure 16: IT policy decision making (Example 2)

Participants get various feedbacks during the simulation. At the end, participants will know whether their policies and decision are successful enough to defend the office network from some specific threats.

Puzzle example 3

This is a high-level puzzle example designed using a truth table (T-T) based puzzle design model. Participants need to have thorough knowledge about network component functionalities and vulnerability to answer these puzzles.

Participants are presented with a network setup for testing purpose (Figure 17). They are asked questions regarding to the network with some vulnerabilities marked to specific nodes (Figure 18). Participants have to choose from the options to solve these problems.

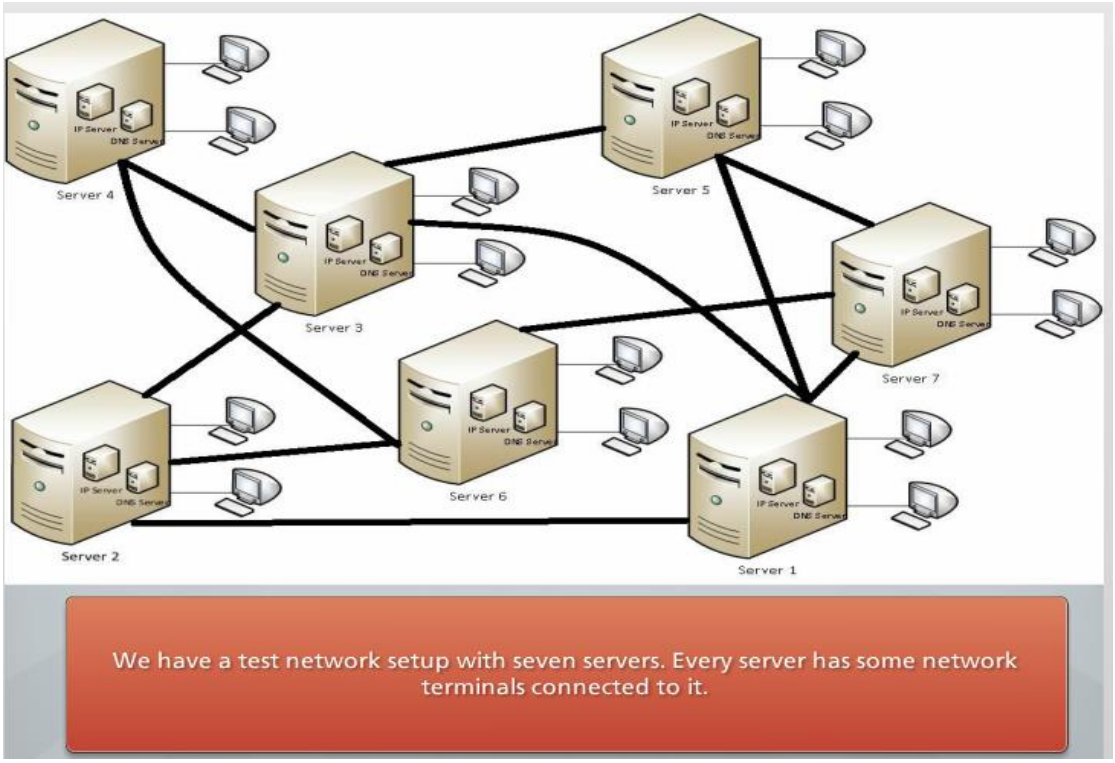

Figure 17: Network setup (Example 3)

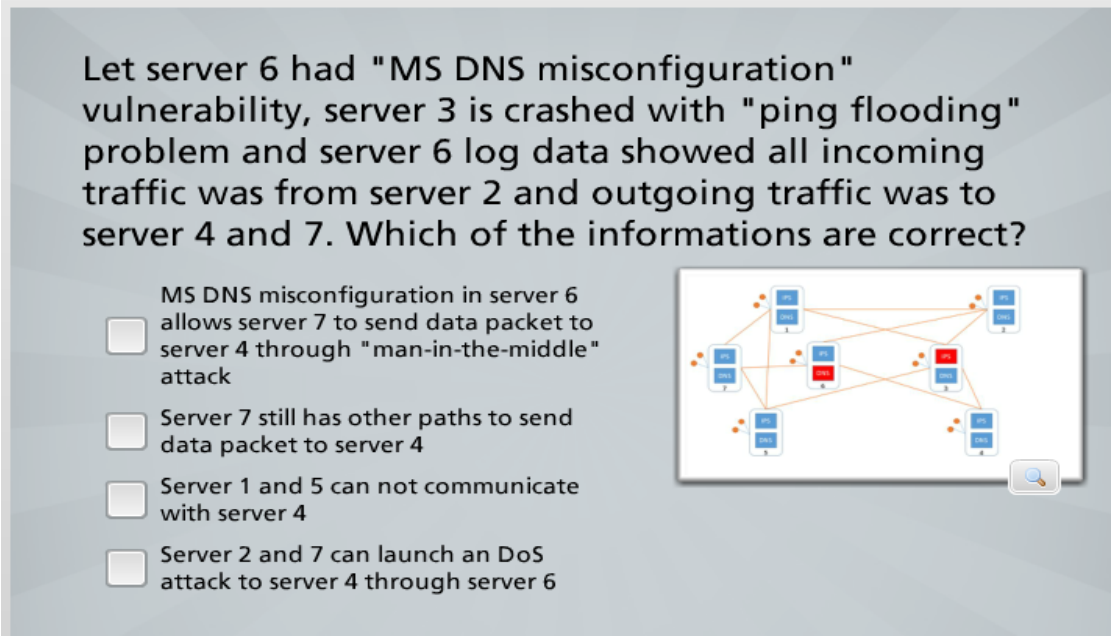

Figure 18: Questions with network nodes marked for vulnerabilities (Example 3)

Participants are notified about the correctness of their responses after they have submitted their answers. Responses are evaluated and marked and at the end of the scenario, participants are declared ‘pass’ or ‘fail’ according to their solutions for the network problems (Figure 19). Participants can review their answers after the result is declared.

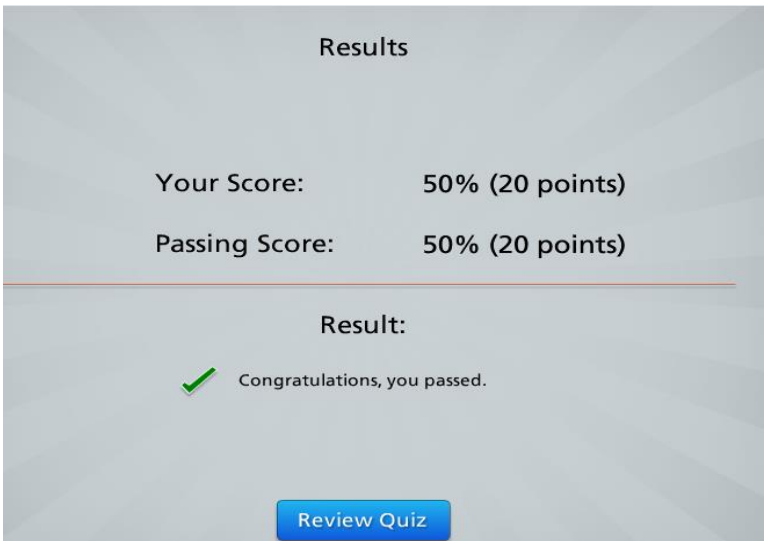

Figure 19: Evaluation of the performance of the participant (Example 3)

5. Evaluation

Effectiveness of Puzzles in Learning Environment

We conducted an informal survey with 28 students to find the effectiveness of the use of puzzles for learning purpose. The students were not aware about the survey beforehand so that the result of the survey remains unbiased.

At first, an introductory lecture was presented to the students about two new topics. Then two questions were asked about the lecture topics to the students. After that, some puzzle questions were asked to the students and all answer sheets were collected. Later, the same questions (the two questions that were asked at the beginning) were paraphrased and asked again to the students.

We compared then the answers of the topic questions that were asked before and after the puzzle questions. After analyzing their answers, we found that 82% of the students had either corrected or improved their previous answers. Among them, 50% of the students corrected their answers which were wrong in their first attempt. Also 39% of the student expanded or improved their answers in the second attempt. This result is showed in Figure 20.

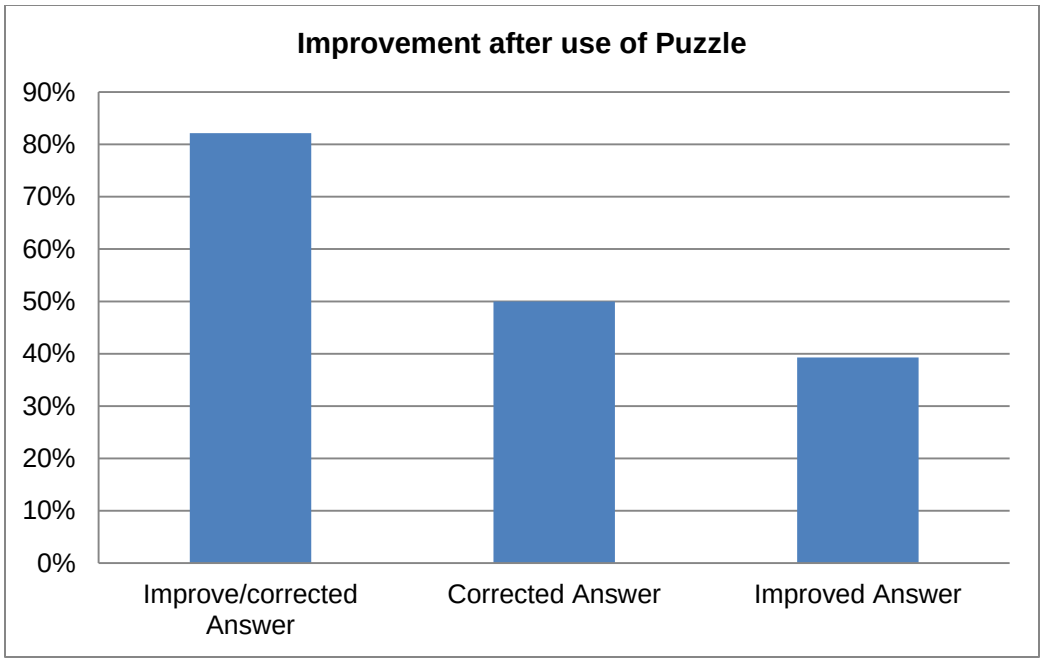

Figure 20: Improvement of answer quality after the students solved the puzzle questions

Among the 28 students, 50% of the students have correctly answered both questions before they answered the puzzle questions. After the puzzle questions were used, 81% of the students answered all question correctly (Figure 21). This result indicates the usefulness and benefit of using puzzles as an education tool.

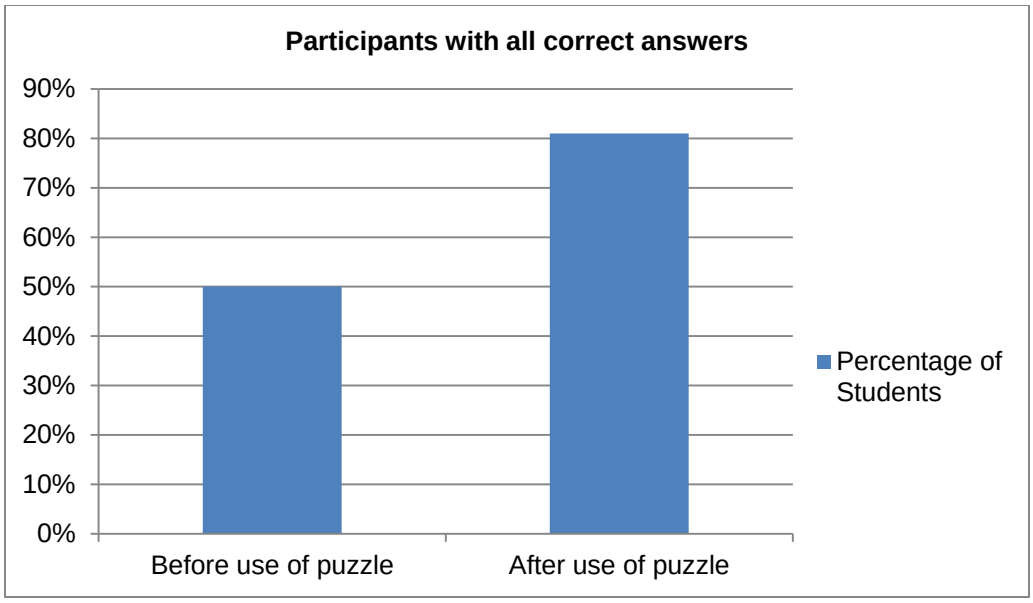

Figure 21: Percentage of the participants with at least one wrong answer before and after use of the puzzles

Figure 22 shows the comparison between the percentage of correct answers before and after the use of puzzles question with the students. It shows that the percentage of wrong answers reduced significantly and most of the answers were correct after puzzles questions were solved by the students. An interesting fact is, though most of the students did not correctly solve the puzzles, but still they were able to answer the follow up questions correctly.

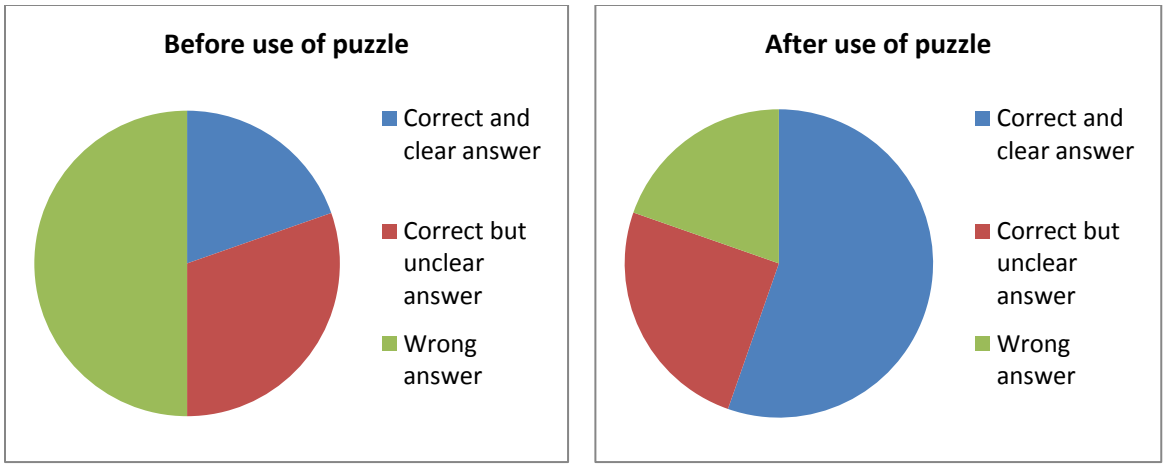

Figure 22: Category of answers received from the students before and after the use of puzzles

Qualitative Merit of Puzzles

Two informal surveys were conducted for the qualitative study of this puzzle-based approach. These surveys were conducted with graduate students as they already have some in depth knowledge on their relative fields and they can provide some insightful thoughts on these implementations. First survey was conducted with nine persons. They were given three different implementations of puzzles with different difficulty levels (discussed in examples 1, 2 and 3) and they were asked to submit their response in a survey website (Survey Monkey) to make this survey anonymous. One puzzle shows the participant the traversed path in the decision tree as the result, another showed the future consequences and the result of their decisions and the other one graded their answers for every question and showed the participants if their performances are above or below

the cutoff margin. All participants successfully completed all three-puzzle scenarios.

Another survey was conducted with six persons to determine the quality of the puzzle-based method. The students were randomly given one of the three puzzle scenarios discussed in examples to interact with, so that they can focus their feedbacks on only one implementation of the puzzle. Their responses were also collected using that particular website to keep the survey anonymous.

All participants were asked to evaluate the ideology and implementation of the puzzle-based approach. Their feedbacks are summarized in table 9.

Table 9: Summary of the findings of the qualitative study on the puzzle-based approach for cyber security learning

Question	Answers
Positive points	• Story based scenario and accompanying pictures • Easy to interact framework • Use of practical scenario. • Use of Decision tree as the background logic. • Interesting questions • Additional information learned while interacting with the puzzle scenarios
Shortcomings	• Some puzzles are too technical for the some participants. • Requirement of computer science background. • No options to correct previous answers.
Difficulties:	• They had no problem to navigate through the puzzles. Participants mentioned the puzzles scenarios as self-explaining and easy for the participants to interact. Every participant was able to complete all the three puzzles.

Question	Answers
Review:	• Learned new stuffs through the survey • Useful to learn useful information regarding the security issues • Good initiative
Suggestions:	• Inclusion of initial lecture slides or reading materials • Additional questions may be necessary for each puzzle to make more valid result • Use of hints • Refinement of ambiguous questions and scenarios

The approach of using puzzles for the cyber security education can be supported from the analysis of experimental studies as very inspiring results are found from the surveys. This method showed significant improvement of the understanding of the knowledge on the students as depicted in the first survey. Feedbacks from the students also show good qualitative merit of the proposed method.

6. Conclusion

The notion of security, especially the field of information technology, continues to be more vulnerable with the invention of new innovative and complex systems. Attackers are growing more sophisticated and equipped. Therefore, the traditional case based learning is not enough anymore. It is very essential for the security personnel to have appropriate knowledge and training to evaluate their security measures and to defend against the ever-growing smarter and innovative attackers.

Different forms of puzzles are in existence for people to think, expand knowledge and stimulate their cognitive ability. We proposed some guiding principles for creating cyber security puzzles, and introduced two new approaches to develop interactive puzzle-based scenarios for teaching different aspects of computing, networking, and information security to help students in better understanding and critical thinking to defend against increasing complex cyber-attacks.

Puzzle-based learning provokes the thinking process of the participant by providing challenges to them. The reward of satisfaction of overcome a challenge in the form of puzzles makes it more interesting to the participants. The interactive process allows them the participants to seek all possible solutions to a security problem, and can better realize the risks of their actions in cyber space, without disrupting any real world setup, which makes the learning process enjoyable to them.

7. Future Work

An interesting idea will be to combine the decision tree based approach and the truth table based approach together. In this combined approach, a decision tree will be used to generate the attack tree where possible vulnerabilities and attacks will be considered using the truth table rows specified by the states from the decision tree.

Inclusion of automatic question generation with these models will be a good idea. Puzzle creation process will expedite if puzzle questions can be auto-generated from a descriptive paragraph.

Larger databases of vulnerabilities with their relationship to various attacks and network components need to be constructed. A smaller part of these large databases can be used to create basic level puzzles where a larger portion can be used to design complex higher-level puzzles.

More experiments with control groups need to be carried out to test the effectiveness of the puzzle-based education. The use of control groups in the studies will eliminate the effects of external variable over the final outcome.

As seen from the informal surveys, this puzzle-based approach for cyber security learning has a good potential as a learning tool for the students. To reach a conclusive state, we need formal studies comparing this puzzle-based approach with other existing learning approaches involving larger group of students.

BIBLIOGRAPHY

[1] McAfee, "McAfee Labs Threats Report, Fourth Quarter 2013," 2014. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf. [Accessed 25 April 2014].

[2] Z. Michalewicz and M. Michalewicz, Puzzle-Based Learning: An Introduction to Critical Thinking, Mathematics, and Problem Solving, Melbourne: Melbourne Victoria Australia: Hybrid Publishers, 2008.

[3] S. Scheferman , "The Target POS Attack - Attack Attributes, PCI Compliance, and Going Beyond," Sentek Global, 2014.

[4] Symantec, "Internet Security Threat Report 2014 Volume 19," Symantec, April 2014.

[5] A. Jean-Phillippe, "Password Hashing: The Future is Now," 11 July 2013. [Online]. Available: https://media.blackhat.com/us-13/US-13-Aumasson-Password-Hashing-the-Future-is-Now-WP.pdf. [Accessed 25 April 2014].

[6] C. Eagle, "Computer Security Competitions: Expanding Educational Outcomes," *IEEE Security & Privacy,* vol. 11, no. 4, pp. 69-71, 2013.

[7] Wikipedia, "Puzzle," Wikipedia, 23 April 2014. [Online]. Available: http://en.wikipedia.org/wiki/Puzzles. [Accessed 25 April 2014].

[8] D. McAdam, "History of Jigsaw Puzzle," American Jigsaw Puzzle Society, [Online]. Available: http://www.jigsaw-puzzle.org/jigsaw-puzzle-history.html. [Accessed 25 April 2014].

[9] T. G. Whisenand and S. M. Dunphy, "Teaching Tip Accelerating Student Learning of Technology Terms: The Crossword Puzzle Exercise," *Journal of Information Systems Education,* vol. 21, no. 2, pp. 141-148, 2010.

[10] S. M. Dunphy and T. G. Whisenand, "Building Camaraderie Through Information Processing: The Wuzzle Picture Puzzle Exercise," *The Journal of Information Systems Education,* vol. 17, no. 1, pp. 11-16, 2006.

[11] D. C. Berry and M. G. Miller, "Crossword Puzzles as a Tool to Enhance Athletic Training Student Learning: Part 2," *Athletic Therapy Today,* vol. 13, no. 1, pp. 32-34, 2008.

[12] A. Gloria, A. James and A. A. K., "Effects of two puzzle-based instructional strategies on primary school pupils' learning outcomes in social studies in Ondo State, Nigeria," *African Educational Research Journal,* vol. 1, no. 2, pp. 58-63, 2013.

[13] H. Narasimhan, V. Varadarajan and P. Rangan, "Game Theoretic Resistance to Denial of Service Attacks Using Hidden Difficulty Puzzles," in *Proceedings of 6th International Conference IPSEC*, Seoul, Korea, 2010.

[14] J. A. Pillai, C. B. Hall, D. W. Dickson, H. Buschke, R. B. Lipton and J.

Verghese, "Association of Crossword Puzzle Participation with Memory Decline in Persons Who Develop Dementia," *Journal of the International Neuropsychological Society,* no. 06, pp. 1006-1013, 2011.

[15] N. Falkner, R. Sooriamurthi and Z. Michalewicz, "Teaching Puzzle-based Learning: Development of Basic Concepts.," in *Teaching Mathematics and Computer Sciences*, 2012, pp. 183-204.

[16] the University of Adelaide, "School of Computer Science | COMP SCI 1013 Puzzle Based Learning," 13 July 2010. [Online]. Available: https://cs.adelaide.edu.au/users/first/pbl/. [Accessed 25 April 2014].

[17] Albright college, 2011. [Online]. Available: http://www.albright.edu/academics/freshmen-seminars.pdf. [Accessed 25 April 2014].

[18] University of Technology, Sydney, "UTS: Seminar: Puzzle based learning," March 2009. [Online]. Available: http://cfsites1.uts.edu.au/qcis/news-events/seminars-detail.cfm?ItemId=18283. [Accessed 25 April 2014].

[19] Z. Michalewicz, N. Falkner and R. Sooriamurthi, "Puzzle-Based Learning: An Introduction to Critical Thinking and Problem Solving," *Decision Line,* vol. 42, no. 5, pp. 6-9, 2011.

[20] Decision Science Institute, "Decision Science Institute," 2010. [Online]. Available: http://www.decisionsciences.org/DecisionLine/Vol42/42_5/dsi-

dl42_5_instructinno.asp. [Accessed 25 April 2014].

[21] Stanford University Newsletter on Teaching, "Speaking of Teaching: Problem-Based learning," Standford University, Standford, 2001.

[22] M. Badger, C. J. Sangwin, E. Ventura-Medina and C. R. Thomas, "A Guide to Puzzle-Based Learning in STEM Subjects," University of Birmingham, 2012.

[23] E. de Bono, "New Think: The Use of Lateral Thinking," Jonathon Cape, 1967.

[24] "Towards the Support of Scaffolding in Customizable Puzzle-based Learning Games," in *International Conference on Computational Science and Its Applications, ICCSA*, Santander, Spain, 2011.

[25] K. E. Merrick, "An Empirical Evaluation of Puzzle-Based Learning as an Interest Approach for Teaching Introductory Computer Science," *IEEE Transaction on Education,* vol. 53, no. 4, pp. 677-680, November, 2010.

[26] M. Gondree, Z. N. Peterson and T. Denning, "Security through play," *IEEE Security & Privacy,* vol. 11, no. 3, pp. 64-67, 2013.

[27] D. Dasgupta, D. M. Ferebee and Z. Michalewicz, "Applying Puzzle-Based Learning to Cyber-Security Education," in *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*,

Kennesaw, GA, USA, 2013.

[28] D. Dasgupta and S. K. Saha, "Puzzle-Based Learning for Cybersecurity," in *4th Annual NICE workshop, NIST*, Gaithersburg, MD, USA, 2013.

[29] E. Chabrow, "'Tricked' RSA Worker Opened Backdoor to APT Attack," 4 April 2011. [Online]. Available: http://www.govinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504. [Accessed 25 April 2014].

[30] E. Chabrow, "Examining How Facebook Got Hacked," 13 February 2013. [Online]. Available: http://www.govinfosecurity.com/examining-how-facebook-got-hacked-a-5518?rf=2013-02-18-g&elq=018e0428373442d7bb41edbce0eddb39&elqCampaignId=5887. [Accessed 25 April 2014].

[31] Cyberoam, "Cyberoam Knowledge Base," 26 April 2014. [Online]. Available: http://kb.cyberoam.com/default.asp?id=2909&Lang=1. [Accessed 30 April 2014].

[32] Forbes, "Massive Internet Security Vulnerability -- Here's What You Need To Do," 10 April 2014. [Online]. Available: http://www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do/. [Accessed 30 April 2014].

[33] Netcraft, "Half a million widely trusted websites vulnerable to Heartbleed

bug," 8 April 2014. [Online]. Available: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html. [Accessed 30 April 2014].

[34] National Institute of Standards and Technology, "NVD - Home," NIST, [Online]. Available: http://nvd.nist.gov/. [Accessed 30 April 2014].

[35] F. B. Schneider, "Cybersecurity Education in Universities," *Editorial, IEEE Security & Privacy,* pp. 3-4, July/August 2013.