Survey of Cybersecurity Education through Gamification

Dr. Chengcheng Li, University of Cincinnati

Dr. Chengcheng Li received his PhD in Computer Science from Texas Tech University. He is currently an asociate professor in the School of IT at the University of Cincinnati. His research and teaching are primarily in the discipline of Cybersecurity.

Mrs. Rucha Kulkarni, University of Cincinnati

Rucha Kulkarni holds MBA degree and has worked in an IT firm. Presently perusing her Masters degree in Information Technology from University of Cincinnati. She is doing her research in Cybersecurity under the guidance of Dr.Li.

Cybersecurity Education through Gamification – the CTF Approach

Chengcheng Li
University of Cincinnati
chengcheng.li@uc.edu

Rucha Kulkarni
University of Cincinnati
kulkarra@uc.edu

Abstract

It is not surprising to see another high profile cyber attack causing thousands of customer accounts stolen or millions of dollar lost. Today, most median and large companies are being constantly probed and attacked. Any weak link in the information defense mechanism can lead to business data breaches. There is a strong need of a larger and professionally prepared cybersecurity workforce to defend IT infrastructure and fight against cybercrimes. It's projected that the US is in an urgent demand of thousands of information security workers. The National Science Foundation has established a number of grants to award projects that promote cybersecurity education and curriculum development. Some of these projects have reported success of teaching hands-on skills through Gamification, a game-like learning environment. CTF (Capture-the-Flag) events are particularly successful in attracting college students, even from non-IT/CS major and high school students into cybersecurity. This paper summarizes the current popular Gamification technologies and the practice of using CTF and competition projects in classroom teaching.

Keywords:

Cybersecurity, Gamification, CTF, Education, Zero-day attack

Background:

The idea of using games as teaching tools is not new but is one of the best ways to teach/learn [19] . Gamification is a very effective way of learning. If competitive elements along with fun are added to the learning Platform, it becomes more enjoyable and brings spirit of learning. Gamification, if integrated properly, can achieve the intended results. There has been a lot of research going on in recent times on the effects of Gamification. It can be identified that Gamification has positive results most of the times [2].

CTF is one such game based learning tool. Today due to the dependency on IT in every walk of our lives, security has become a major issue. In order to face such critical situations where our personal information is at risk, we need to have awareness on what and how of network. Increasing Cybercrime rate suggest that we are not aware of Cyber Security and should start preparing not only ourselves but also the upcoming generation to face Cyber challenges. CTF is a game centered education, which was designed to bring awareness on cybersecurity. If such kinds of games are introduced at early stages of education, we can bring awareness on cybercrime and reduce the crime rate.

Due to lack of knowledge and awareness of cybersecurity, people are becoming victims of cyber crime. Criminals, hackers and people with intention to harm are trying to find new techniques of attack. Though govt is taking interest in this area by conducting cyber awareness events and CTF competitions, encouraging institutions by providing grants for such events, there are still gaps. There have been many events going on to bring cyber awareness particularly among students.

Many educational institutions are now focusing on educating the students on cyber security. CTF events are being conducted at many universities and educational institutions to test the skill set of students and fill the gaps accordingly. These competitions are held with different level of difficulties for students at Middle school, High school, and college level. Efforts are being made to educate the students at elementary level as well. There are also professional levels of CTFs with high level of difficulty such as DEFCON CTF.

Conducting game based events like CTFs in organizations helps in educating the employees and therefore protects Cyber assets of the Organization.

What is CTF

CTF is an attack oriented competition. It can be considered as a measure to what constitutes a computer professional. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft [9]. Success in these competitions depends on the expertise of participants in these areas. CTFs are similar to WAR games which can be considered as best source of practice for CTF. Zero day attacks are a major concern for network security and remain active on an average of 10 months as per a recent study [11]. These attacks are dangerous as they exploit vulnerability with no patches yet.

CTF Competition Events

Many CTF competitions are held worldwide at different locations. These competitions bring together so many teams from worldwide to compete against each other in Cyber Security Challenges. Their efficiency of hacking, detection and protection are tested in these competitions.

Cyber Security Awareness Week is held at different locations to educate young researchers on current Cyber security threats. CTF competitions are held for students during these awareness weeks. Many young researchers are given a chance to prove themselves in these competitions. Cutting edge threats of cyber hacking are discussed and efforts are made to provide pragmatic solutions to them. Many intellectuals come over to view these competitions and discuss on various ethical issues on privacy and security and give their valuable advises to the young competitors. CTF competitions are conducted at college as well as high school level. CTFs are of different types. The most common types of CTFs are:

Jeopardy: In this type of contest, teams have to solve a set of challenges from diverse areas such as Cryptography, Forensics Reverse engineering etc.

Attack-Defense: As the name suggests, this is an attack, Defense game meaning some teams try to attack and the other teams try to defend from attacks.

Mixed Competitions: Change formats.

CTF competitions train the participants to protect their systems from cyber attacks. The challenges are mainly on fixing vulnerabilities in the system and hacking other systems and when a team completes a challenge it gets a **Flag**. The team with more number of flags wins.

Some of the CTF competitions, their uniqueness and specialties are tabulated below. The table also tells about people who can participate in them and also lists the areas of specialization required in each of them.

Table1. A List of Popular CTF Events

1.DEFCON CTF: Largest CTF[9]		
Specialty	Areas Covered	Participants
Attack Defend Type Held once a year For Top Hackers	Reverse Engineering Coding Challenges	Computer Security Prof Journalists Lawyers Hackers
2. PICO CTF		
Uniqueness	Areas Covered	Participants
Story line based Game	Reverse Engineering Hacking, Decryption	Middle schoolers High schoolers Organized by and for Students
3.CYBER PATRIOT		
Specialty	Areas Covered	Sponsors &Participants
Organized by AFA National Youth Program. Held Annually usually starts in October	Vulnerability fixing Forensics Sub-netting, IP addressing Malware Removal	Sponsored by Homeland Security and Dept of Defense Middle & High schoolers Camps are Organized
4. HSCTF		
Specialty	Areas Covered	Participants
International Online Hacking Competition Organized by and for Students	Reverse Engineering Coding Challenges Design Algorithms Internet Skills	Middle schoolers High schoolers
5.CSAW[6]		
Specialty	Areas Covered	Sponsors & Participants
Story line based Game Largest Student-run Cyber Event in Nation Organized by and for Students	DHS quiz Security Challenges CTF	Sponsored by Homeland Security. High school to Doctoral level students. Organizes Cyber Awareness weekly events.
6.MITRE CTF		
Uniqueness	Specialties	Participants
Organized by MITRE Cyber Academy Operates National Cyber Security FFRDC	STEM CTF Competition Works with DHS to secure America	High schoolers and College Students. Provides Job Opportunities to Students.

Cyber awareness at Elementary level

Most of the security breaches occur due to lack of awareness and so cyber education should be included in the academic curriculum [3]. Due to the heavy usage of internet by people of all ages, steps are being taken to educate the students on Cyber Security from elementary level itself. NIST has been working on promoting Math, Science education at elementary and high school level and also calls for the improvement of quality of computer science courses at these levels. Students must have knowledge on how to securely use the ever growing technology.

The president of USA declared October 2015 as National cyber security awareness month and teaching the elementary, middle and high school students about internet safety and security was given special importance during this period [10] [13]. They also have age appropriate resources for kids . AFA has taken a step further to educate students on Cyber Security by organizing activities for students from Elementary level. The ESCEI aims at teaching the students at these levels about the importance of STEM education and careers in an interactive way. They designed different modules for K-3 graders and for 4th to 6th graders.

Cyber Security programs for Non IT Students

Cyber Security programs usually have multi disciplinary approach covering Management, Law, Business, psychology and Technology areas [18]. Though this course is considered ideal for students with strong technical background, Cyber security is not just about Technology. Social Engineering is also a integral part of it. Many Universities are now offering Cyber security related programs for non IT students as well. A program such as Masters in Cyber Security Management does not require students to have extensive technical knowledge [16]. However Knowledge on network and computing skills are required to start with. There are also Digital Forensic and Cyber security Certificate courses available in some Universities [17].

Recommendations on Preparation

CTF events should be considered like a playground where students can succeed or fail at computer defense without fear of consequences [1]. Students who are willing to participate in CTF competitions need to start with a team formation and arranging for the required hardware. Before participating in the competitions, teams need to go through some practice tests to understand the rules of the competition. Many of the CTF organizers provide required training and also help in hardware arrangement. Cyber Patriot is one of them. The hardware requirements of Cyber Patriot are modest and minimum which schools already have with them [8]. If they do not have, CyberPotrait assists them as their main idea is to make this competition available for every interested team.

Attending Cyber camps, participating in practice tests, getting involved in the cyber events can give quite a bit of exposure to Cyber Security. Attending Cyber events also can help in improving awareness on Cyber as many Government security Officers attend these events and share their Cyber related experiences and give their valuable advice to the participants. One of the key factors for student's participation in CTFs is the incentive they receive in the form of cash and gifts and sometimes recognition. Some CTFs are very popular and participating in them is itself a big deal [3].

For students who are new to CTF, Pico CTF is the best way to start with. This competition is based on a unique story line more like a video game. PicoCTF aims at developing interest and excitement among students about computer security. Most of the times, the characters in these games are taken from the fantasy movies, and other such things by which participants can easily connect [4].

You would then want to compete in HSCTF which was started as a follow-up on the success of PicoCTF. These competitions are entirely online. The organizers of these competitions are also high school students. Most of the challenges in this CTF are based on Math and Programming.

MITRE [7], HSCTF conducts CTF for college students as well. There are also international level competitions held which brings together hackers from all over the world. CSAW is the popular of all which is again organized by students and participants come across the world [6].

Fig. 1 Online Competition Environment: www.picoCTF.com

Defcon CTF is considered to be the biggest of all CTFs. Professional hackers come to participate in this competition every year at Las Vegas.

Conclusion

Internet connects us to the whole world but at the same time exposes to many cyber threats. Cyber awareness is as necessary as is Internet. CTF plays an important role in spreading cyber awareness which is needed to protect Nation's Infrastructure.

To stop a hacker, we need to think like one and IT personnel need to be trained for White Hat skill sets in order to secure the systems from hacking [5].

As is said by NICCS [12]," we need a digitally literate workforce that uses technology in a secure manner".

People should be aware of the Cyber crime and also be able to protect themselves from being a victim of it. Govt educates its citizens through different events. NSF offers a number of grants and funds for cyber education [14]. NSA has several early opportunities for students from K-12. It also encourages University students by offering many innovative programs, internships and scholarships [15]. Some of the CTFs such as USCC (US Cyber Challenge), CSAW, and Cyber Patriot are sponsored by Homeland Security to encourage cyber education. More such events should be hosted by the Universities and Schools to educate the student.

REFERENCES

[1]. Author1, Joshi A, Author2, Ramani V, Author3, Murali.H, Author4, Krishnan.R, Author5, Author6, Mithra.Z, Author7, Pavithran .V, "Student centric   design for cyber security knowledge empowerment", Technology Enhanced Education (ICTEE), 2012 IEEE International Conference on, Pages1-4.
[2]. Author1, Juho Hamari, Author2, Jonna Koivisto, Author3, Harri Sarsa, "Does Gamification Work? — A Literature Review of Empirical Studies on Gamification", 47th Hawaii International Conference on System Science 2014.

[3]. Author1, Raghu Raman, Author2, Sherin Sunny, Author3, Vipin Pavithran, Author4, Krishnasree Achuthan, "Framework for Evaluating Capture The Flag (CTF) security competitions" , International Conference for Convergence of Technology – 2014.

[4]. Author1, Kaiyang Zhang, Author2, Shihao Dong, Author3,Guoliang Zhu, Author4,Danielle Corporon, Author5, Tim McMullan, Author6, Salvador Barrera, "picoCTF   2013 - Toaster Wars when interactive storytelling game meets the largest computer security competition", Carnegie Mellon University.

[5]. Author1,Jason Flod, Author2,Mark Denihan, Author3,Anthony Keane, Author4,Fredrick Mtenzi, "Black Hat Training of White Hat Resources: The Future of Security is Gaming", The 7th International Conference for Internet Technology and   Secured Transactions (ICITST-2012)

[6]. Cyber awareness, (n.d), retrieved 11/28/15
   https://csaw.engineering.nyu.edu/

[7]. CTF, (n.d), retrieved 11/12/15
   http://mitrecyberacademy.org/competitions/index.html

[8]. Cyber Camps,(n.d), retrieved 12/5/15
   https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx

[9]. CTF
   https://trailofbits.github.io/ctf/

[10]. US GOVT Cyber Encouragement,(n.d), retrieved 12/9/15
   http://www.cio.com/article/2405474/education/us-agency-releases-cyber-education-plan.html

[11]. Author1,L.Bilge and Author2,T. Dumitras, "Before we knew it: an empirical study of zero-day attacks in the real world", ACM Conference on Computer and Communications Security, Oct. 2012

[12]. Digital Literacy,(n.d),retrieved 10/20/15
   https://niccs.us-cert.gov/education/education-home

[13]. Cyber Awareness,(n.d) retrieved 11/25/15
   http://www.dhs.gov/national-cyber-security-awareness-month

[14]. Funding,(n.d),retrieved 12/2
   http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504984

[15].Cyber Education,(n.d),retrieved11/25/15
   https://www.nsa.gov/acdemia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml

[16]. Non IT Programs, (n.d),retrieved 12/10/15
   http://www.baypath.edu/academics/graduate-programs/cybersecurity-management-ms/

[17]. Non IT Programs,(n.d),retrieved 12/10/15
   http://www.jjay.cuny.edu/digital-forensics-and-cybersecurity-programs

[18]. Non IT Programs,(n.d),retrieved 12/10/15
   http://www.umuc.edu/cybersecurity/academics/masters-degrees.cfm

[19]. Author1, Hee Jung Park and Author 2, Jae Hwan Bae, "Study and Research of Gamification Design", International Journal of Software Engineering and Its Applications Vol.8, No.8 (2014), pp. 19-28.