Hello World: Bootstrapping Cybersecurity Education In Indian Rural High Schools

Vipin Pavithran*, Arvind S Raj*, Prema S Nedungadi† and Krishnashree Achuthan*
*Amrita Center for Cybersecurity Systems and Networks
†Amrita Center for Research in Advanced Technologies for Education
Amrita School of Engineering, Amritapuri
Amrita Vishwa Vidyapeetham, Amrita University, India
{vipinp,arvindsraj}@am.amrita.edu, {prema,krishna}@amrita.edu

***Abstract*—Cybersecurity is increasingly becoming relevant in India. In recent years, the Indian government has been incentivizing cashless transactions and few villages have been completely digitized. A major concerns of digitization is the rising cyber crimes such as malware infections, cyberbullying and other online financial frauds. Nearly 70% of India lives in villages. Channelising the young minds in villages towards informed use of technology and information security awareness can greatly benefit the cyber safety of the country. In this paper, we describe a game-based training model for imparting cybersecurity education and awareness for village students in India. We conducted pilot workshops in two different villages in Andhra Pradesh, a southern state in India. We blended constructivist pedagogy along with game based learning and collaboration. The training involved theory classes along with practical and game based learning sessions that introduce the basic fundamentals of cybersecurity and programming. We also perform a detailed analysis based on surveys and present the workshop outcome.**

***Index Terms*—cybersecurity awareness; cybersecurity training; rural education; game based learning, collaboration, constructivist pedagogy**

I. Introduction

There has been an exponential increase in the number of internet users in India during the past 10 years due to development of infrastructure, smart phone adoption and cheaper internet. It is currently estimated by the Internet and Mobile Association of India and market research firm IMRB International that there are about 465 million internet users in India. The overall internet penetration in India is estimated at 31%. Currently India is ranked 2nd in the world in terms of total number of internet users. There is a major push for Digital India - an initiative by the Government of India to provide all citizens access to government services via internet. The Indian government is providing incentives for cashless transactions and few villages have been completely digitized. However, there are major concerns against digitization due to rising malware infections, financial frauds and cyber crimes. There has been a 350% rise, from 2011 to 2015, in the number of cyber crimes registered in India under the IT Act 2000.

We believe that the exponential rise in cyber crimes is due to two reasons. One is the lack of trained manpower [1]. Indias National Association of Software and Services Companies (NASSCOM) estimates there will be a shortage of 1.5 million cybersecurity professionals by 2019. The other is a lack of awareness amongst internet users about online scams and attacks.

Studies have indicated that young people in the age group 18 - 22 are more susceptible to email scams and phishing attacks [2]. An understanding of the mechanics and modus operandi of these internet scams can greatly reduce their occurrence. Currently, school and college curriculums do not have cybersecurity or cyber safety as courses. Hence, students have very less exposure to cybersecurity as a branch of study.

Since 70% of India lives in villages, we decided to focus on imparting cybersecurity awareness and training in the village high schools. In this paper, we present an experimental method to impart cybersecurity education to school students. This is based on our experience training students in two different villages in Andhra Pradesh, a southern state in India. We partnered with the Andhra Pradesh State Skill Development Corporation (APSSDC) for a pilot training program. In June 2016, we conducted training for 200 students from 9th to 12th grade (age group of 14 to 17). We used a combination of constructivist pedagogy, game based learning and collaboration in the training. Constructivist pedagogy is focused on students experientially discovering learning via exploration [3]. Game based learning uses elements of game mechanics such as levels, theme, scoring, competition and teams. Since the workshop attendees were students in 9th grade or above, we knew that students were familiar with basic mathematical concepts such as algebra and number system. They also have basic experience of working with computers.

Initial survey of career interests among students in these two schools indicated that over 75% of the students prefer the medical profession. None wanted to choose computer science related job. We believe this is because of the lack of knowledge or exposure to these areas.

We designed and developed content for a workshop that achieved the following

- **Creating awareness**: Tests conducted after the training revealed that the students understood about the common online cyber crimes and scams that happens via SMS and email.
- **Imparting knowledge**: Students were able to implement basic decryption routine.

978-1-5090-5920-1/17/$31.00 ©2017 IEEE

- **Inspiring them to explore the field**: At the end of the workshop, another survey was conducted to see how many students would be interested in software or cybersecurity related jobs. About 64% students expressed interest.

We believe the model described here can serve as a starting point for developing a training model for imparting cybersecurity education to high school students in a rural setting with minimal exposure to computers and internet.

The rest of the paper is structured as follows: Section II describes some of the the existing training done in rural areas and how ours is different. Section III discusses the background information needed to understand the rest of the paper. In Section IV we describe in detail about the workshop. Section V we discuss about our major observations during the workshop and conclude the paper in Section VI.

II. Related Work

Kam et al [4] made an effort to educate students of rural India using e-learning games. They built on principles described in the book What Video Games Have to Teach Us About Learning and Literacy [5]. Their work involved conducting a study on how students respond to digital games with western influences and concluded that students were not motivated to play these games. They then came up with traditional digital games which incorporate familiar game mechanics from everyday village games will be more culturally meaningful to rural children. The aim of these e-learning games was offering English as a Second Language (ESL). In comparison, our work categorically aims at developing the cybersecurity skills of the children.

Situation analysis in Indian schools suggested that students from urban and private schools preferred Computer Science as a subject while state school standards primarily had ICT literacy [6].

Nedungadi et al [7] explain another initiative to improve the quality of education in rural areas. The work is about decreasing absenteeism of both teachers and using a combination of Android monitoring apps & WhatsApp communication.

The role of ICT and games for learning skills, providing awareness and bringing about change in social behavior has been substantiated by previous efforts in rural and tribal communities by previous research. Unnikrishnan et al. [8] discuss the use of a tangible game interface for teaching programming concepts and computational thinking to communities in Gujarat and Himachal Pradesh. Their approach was applied to school going as well as children who have dropped out of the school system with documented success.

III. Background

A. APSSDC

Andhra Pradesh State Skill Development Corporation (APSSDC) is an organization to promote skill-development and entrepreneurship in the state of Andhra Pradesh (AP). The AP government has also set up what are called as model schools throughout rural areas in AP. The goal is to set up one rural school per block (geographic unit). The medium of instruction in these schools is English and the schools are also equipped with 8-10 desktop computers. They also have a mandate to innovate with the curriculum and pedagogy. APSSDC provided us with 40 laptops and a projector additionally.

TABLE I
Student statistics

District	School	Total Students	Female Students
Guntur	AP Model School, Krosuru	110	48
Krishna	AP Model School, Peda Komera	90	34

B. Cybersecurity Basics

Cybersecurity broadly refers to the technology, processes and protection mechanisms against unauthorized use of electronic data and networks of computers that make up the internet. There are different aspects of cybersecurity such as cybersecurity awareness, secure coding, web security, cyber forensics, cryptography and mobile security. We decided to focus on cryptography and cybersecurity awareness with a brief discussion on forensics and ethics.

By cybersecurity awareness, we mean making students aware of the dos and dont's while using the internet. Some examples of this include choosing good passwords, not sharing personal information online, not chatting with strangers, usage of fake profiles on social media etc.

Cryptography is the science of creating (encryption) and breaking (decryption) secure communication. We motivated the need for secure communication and covered some basic concepts. Cyber forensics is the application of investigation and analysis techniques to gather and preserve evidence from a computing device. We demonstrated how to hide messages within images and audio and how to recover them.

IV. Workshop Details

Our audience consisted of students from classes 9 to 12, aged 14 to 17 years. It was conducted in two AP Model schools in Krosuru and Peda Komera villages of Guntur and Krishna district respectively of Andhra Pradesh.

Based on our past experience with training students, we found that a mentor to student ratio of 1:10 is ideal to keep the students engaged and motivated. Additionally, we included two mentors who were fluent in the local language(Telugu).

The schools were equipped with 8 desktop computers. APSSDC provided 40 laptops, projectors and all other infrastructure needed for this training.

A. Pre-Assessment

A pre assessment survey was conducted to find out about awareness about computers and cybersecurity amongst students and their professional aspirations. Over 75% were interested in pursuing a career in medical science. We believe this is because the village lacks sufficient healthcare facilities and

thus faced several hardships when requiring medical attention. None of the students wanted to become an engineer or pursue a career in computer science. The reamining students (about 20%) were interested in agriculture or joining the army.

B. Curriculum

Based on the pre assessment, we modified the curriculum to describe how computers can play a role in improving the society and help villages develop. We believed this would help them relate to computers and get them excited. The major topics of the curriculum are described below.

1) **Motivation**: Role of computers in enhancing quality of life in villages: How computers help human beings. How automation is helping societies to progress and the role of computers in automation. How are computers helping humans in various fields such as medicine, remote sensing, agriculture, transportation, communications etc.
2) **Basic understanding of computers**: Help students understand what is a computer and its different parts. Most students thought the computer is just a black box. We wanted students to understand that computers are there in cell phones, calculators, cars, airplanes etc. We wanted students to understand the difference between hardware and software and what is an operating system. Help students to understand binary number system and how numbers are stored in a computer.
3) **Computational thinking**: Learn basic computational thinking by designing a game using MIT Scratch [9]
4) **User awareness**: Cybersecurity and cyber safety awareness related to common internet scams.
5) **Cryptography**: Need for secret communication and security. Understand encryption and decryption using gamification.
6) **Automation**: Learn to automate encryption and decryption of large text using programming. We used Python as the choice of programming language as it is easy to understand.
7) **Career Opportunities**: Exposure to various career opportunities in the area of cybersecurity.

C. Constructivist and Collaborative Learning

We found the rural students to be highly active in class and very curious. We needed to actively involve them in the learning and keep them motivated and engaged throughout the training. Hence we adopted well known approaches such as Constructivist Pedagogy, problem based learning, game based learning and collaboration which helps in active learning.

Constructivist methodology is student centric based approach to learning. The teacher is only a knowledge facilitator. There are no lectures or step by step guidance. Students use information they already know to acquire new knowledge.

Problem based learning is a methodology under the constructivist pedagogy where students are given problems to solve based on existing knowledge and they are able to construct new knowledge by solving the problem Game based learning uses various game mechanics such as different levels, elements of chance, a theme, competition and scoring

In game based learning, game mechanics and elements of game play are used to help impart a concept. This has been found to help encourage engagement and interest of students [10].

The students were familiar with the decimal number system. In order to help them understand how numbers are stored in a computer using the binary system we posed a question: ”How will you count if there are only two numbers that are allowed?” Students were discussing in groups and over 90% of the students could come up with the binary system.

We used a game based approach to teach students the importance and need for secure and private communication and to help understand the concept of encryption. The students were divided into batches of 12 students in a batch. Within each batch, teams consisting of 4 students were formed. The first team of 4 students was the sender team, the next set of 4 students were the receiver team and the last 4 were the eavesdropper team. The game begins when a mentor verbally conveys a secret message to the sender team. The objective of the sender team was to communicate this secret message in a written form to the receiver team via the eavesdropper team, without letting the secret message be known to the eavesdropper team. Once the eavesdropper team received the message from the sender team, they create a copy of the message and then pass the original message to the receiver team.

The objective of the game was explained to all the teams and the sender and receiver team were given 10 minutes to decide a strategy to come up with a way they could achieve this. At the end of the game, we found that all the sender receiver pairs came up with custom substitution cipher schemes. The sender and receiver team had decided upon the substitution and was successful in transmitting the message without the eavesdropper team being able to break it.

At the end of the game, students felt they understood the need for encryption during secret communication.

The next step was to help students understand the importance of automation. The encryption of a small piece of message took some time for the students. What if the message was bigger ? How could this be done faster ? How could an eavesdropper break the secret message faster? This was the motivation for them to learn programming. Basics of Python was taught and the students were made to do simple programs that performs mathematical operations and outputting text. The mentors wrote a program to encrypt a given text file using a simple substitution cipher. The program was explained and then the students wrote the program and tried this on their computer. The students were then asked to write a program which would decrypt an encrypted text. With some help from the mentors, about 80% of the students were able to complete the program.

Fig. 1. Mentoring

TABLE II
CAREER INTERESTS

School	Areas of Interest	Pre-Assessment	Post-Assessment
Krosuru	CS	0	48
	Security	0	17
	Medical	79	21
	Others	21	14
Peda Komera	CS	0	41
	Security	0	21
	Medical	76	23
	Others	24	15

V. DISCUSSION

During the pre-assessment, we found that most students had little knowledge about computers. The students, though lacking in hands-on experience with computers, had a good analytical thought process. We believe this helped them to understand the workings of programming language with little effort. Though the medium of instruction in the schools was English, students were able to understand better when the sessions were led in local language(Telugu).

During the game based learning of secret communication all the student teams came up with different forms of substitution cipher, in which an alphabet is substituted for using another. We expected the students to come up with this scheme as this is the most logical and easiest approach to encryption.

Table II shows the results of career interests of students both pre-assessment and post-assessment. We can see that the number of students interested in CS job or security were zero during the pre-assessment. However, post-assessment results indicate an increase of 44.5% students interested in CS Job. Also, there is an increase of 19% for students who were interested in cybersecurity jobs. Post-assessment results also show a decline of 55.5% of students who were interested in medical jobs. This is represented in the Figure 2.

We used a problem-based learning learning where we provided motivational examples of how computers can solve day-to-day problems with a special focus on health-care. Our survey shows many students found the role of computers in health-care, such as remote patient monitoring, robotic surgery and heart-rate monitors, fascinating. We believe this is the reason for the increase of 89 students interested in CS jobs, post training.

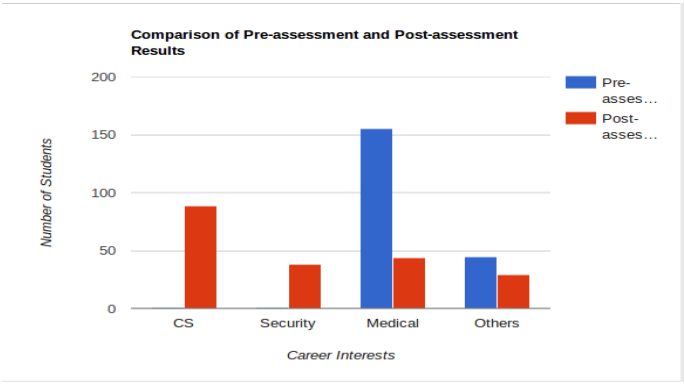

Fig. 2. Pre-assessment Vs Post-assessment

Although only 19% of students were interested for a career in security, we believe this is a good start in making them aware of cybersecurity and relevant areas.

In spite of the long commute and the workshop being scheduled during school vacation, the fact that 200 students attended demonstrates how much potential the state has.

With a teacher-student ratio of 1:10 and the use of game-based learning, we identified that students were interested in learning by doing and keen to work on new challenges. We believe our teaching model can serve as a basis for cybersecurity training activities in other parts of India.

VI. CONCLUSION

In this paper, we describe a game based training model for imparting cybersecurity training to village students. We started with basic programming and computational thinking concepts to lay a foundation for discussing fundamental security concepts like encryption and decryption through game based activities. At the end of the training program, more than 80% of the students were able to write computer programs in Python language. Surveys conducted to determine career interests indicate an increase of nearly 64% interest in studying computer science and pursuing cybersecurity related jobs. This clearly indicates that the training model developed interest and enthusiasm among students to study cybersecurity. We plan to train 50 trainers who will travel 400 village schools across the state of Andhra Pradesh and train the high school students.

ACKNOWLEDGMENT

We would like to thank Shri Mata Amritanandamayi Devi (Amma), Amrita University's Chancellor and a humanitarian leader, for inspiring and encouraging us to work with villages. We would like to thank APSSDC for funding this initiative and AMMACHI Labs and Amrita e-Learning Research Labs of Amrita University for facilitating this workshop. We would like to thank the student volunteers from FOSS club and team bi0s of Amrita University, Amritapuri campus for helping run the workshop.

REFERENCES

[1] Standing Committee on Information Technology, MeitY, Govt of India, "Report on 'cyber crime, cyber security and right to privacy'," 2013.

[2] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 373–382, ACM, 2010.

[3] C. T. Fosnot and R. S. Perry, "Constructivism: A psychological theory of learning," *Constructivism: Theory, perspectives, and practice*, vol. 2, pp. 8–33, 1996.

[4] M. Kam, A. Mathur, A. Kumar, and J. Canny, "Designing digital games for rural children: a study of traditional village games in india," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 31–40, ACM, 2009.

[5] J. P. Gee, "What video games have to teach us about learning and literacy," *Computers in Entertainment (CIE)*, vol. 1, no. 1, pp. 20–20, 2003.

[6] R. Raman, S. Venkatasubramanian, K. Achuthan, and P. Nedungadi, "Computer science (cs) education in indian schools: Situation analysis using darmstadt model," *ACM Transactions on Computing Education (TOCE)*, vol. 15, no. 2, p. 7, 2015.

[7] P. Nedungadi, K. Mulki, and R. Raman, "Improving educational outcomes & reducing absenteeism at remote villages with mobile technology and whatsapp: Findings from rural india," *Education and Information Technologies*, pp. 1–15, 2017.

[8] R. Unnikrishnan, N. Amrita, A. Muir, and B. Rao, "Of elephants and nested loops: How to introduce computing to youth in rural india," in *Proceedings of the The 15th International Conference on Interaction Design and Children*, pp. 137–146, ACM, 2016.

[9] MIT Media Lab, "http://scratch.mit.edu/."

[10] G. Mehta, X. Luo, N. Parde, K. Patel, B. Rodgers, and A. K. Sistla, "Untangled-an interactive mapping game for engineering education," in *Microelectronic Systems Education (MSE), 2013 IEEE International Conference on*, pp. 40–43, IEEE, 2013.