CS 558
Advance
Computer
Security

Final Project Report

IN-Security (A Cyber Security Educational Game)

Abhishek Kumar
Sohan Sunil Samant
Tanmay Bhatt

Abstract

IT systems in today's world have changed the way companies deliver products and services. It has also changed how people communicate with one another and how organizations make decisions and even the way individuals understand and interact with the world around them. However, just as these shifts have huge organizational impact, the emergence of crime, sponsored attacks and social activism in the digital world is speaking a new reality in which security risks cannot be adequately understood as merely it challenges. These issues can often threaten an organization's brand, intellectual property, sensitive business data and financial resources. To reduce these vulnerabilities, we are trying to help society learn more and learn interactively and in a friendly manner. Today we see many security breaches and these numbers are growing each day and many companies are paying a serious cost. The main goal of this thesis is to represent the security concepts in a playful way which is easy and fun to learn.

I. Introduction

It is predicted that about 50 billion devices will be connected to the Internet in 2020. Out of these devices most of them are not that much protected. Now these many unprotected devices are acting as an open door for many potential doors for hackers to intrude in those devices, into companies, our homes and personal lives. With the increase of networking and connectivity has enabled the organizations to become more efficient, more productive and better informed with what is happening around the world. For every individual, every company data and Information access are key assets. There are important security considerations associated with how technology, and by extension, the world, is changing. Initially computer hacking was a game, hobby for a few curious people and skilled people. With the evolution of the internet these skills became a political or ideological tool in the hands of hacktivist groups. A piece of malware, Trojan or a worm could remain in the system for months before being detected and while it presents it is tapping all the information. Almost every alternate day thousands of gigabytes of technological and strategic data are stolen from thousands of computers of companies. A cyber-attack can cause significant damage at a very large scale and that too for long periods of time and at low costs. To deal with these threats companies don't have enough tools as well. There is also not enough data collection or analyzing techniques to make smart assumptions and decisions if needed. An awareness about the security threats and cyber-attacks is very important among the society. With these security threats there are different ways to meet these challenges and to overcome the shortcomings the industry is facing today. To deal with these threats there is one growing trends which is the use of gaming software with having an element of competition and simple rewards programs to help find security drawbacks and to educate about cybersecurity issues and recruit talent fill the skills gap that is riddling the industry. The intention of the application is to help the player learn about some of the prominent cyber security threats in current world through an interactive game. The main concept is to have players gain some background about cyber security.

II. Gamification's role in raising security awareness

Gamification means use of the game in non-game contexts for increasing user engagement and motivation. This new concept has shown very promising results in creating an engaging and productive learning environment for both education and business. Some research also has shown that gamification and security awareness has created an effective way of learning and have helped in solving some of the critical problems.

The concept of game is not new in cyber security industry. It is mostly used for domain level education and to find talent. In business companies for day to day security practices and procedures are carried out in a traditional way and often considered by an employee as boring and unnecessary activity which can be ignored when in rush to meet a critical deadline. The main contribution for successful data breaches are human error and lack of awareness. Security breaches also happens because many of the staff members don't have enough knowledge and sensitivity in handling data and thus exposing the organization to a huge risk. Teaching cyber-security through a game is becoming more and more popular and an effective way of educating the society. With the help of this new approach we will be able to close the cyber security gap and by using cutting-edge cyber security video games which will help in grabbing the attention of young adults and help them to build a solid foundation of information security knowledge and skills.

Several studies have focused on the advantages of game-based learning and shown that playing games can improve skills, reasoning, and decision-making abilities as well as reduce stress. Few years back, a group created several PlayStation video games with the intention of learning and directed towards actual curriculum-based knowledge to elementary-age children. With the help of the study it was found that children who played a few hours of the games per week outside of class had an increase in 25% in their vocabulary and language skills and a 50% growth in math skills over students who had only classroom sessions. These results show that the benefit of gaming beyond entertainment. Effective gaming strategy will help in understanding the concepts well and it can be fun to play and learn.

III. Cyber Crime

Any illegal activity that uses computer as its primary mode of communication and theft is called as cyber security. Any illegal activity that uses a computer for the storage is also known as cyber-crime. The list of cyber-crimes is growing, and it also includes crimes that have been made by computers. The attach such as network intrusions and the inserting computer viruses, as well as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually it is a crime committed using a computer and the internet to steel a person's identity or sell that information or stalk victims or disrupt operations with small programs. As day by day technology is playing in major role in a person's life and these crimes are increasing day by day. These crimes are now taking in any day to day activity and are using the information collected to earn huge amount of money.

IV. Challenges in Cyber Security

✓ The exponential growth in data

In the age of bigdata, with the volume of data being generated it is very important to manage this data in proper format and with proper security measures. The growth has been exponential and hence the data will also be exponentially growing. There needs to be a proper security mechanism to maintain the confidentiality, integrity and availability of the data.

✓ The extreme and growing shortage of skilled cybersecurity personnel

With this growing data, there needs to be appropriate skilled workforce to deal with this data. This can be achieved by educating the users or the society with all the required information and helping them to resolve the issue.

✓ Industry or Business environment

Business environment for each industry is different. Some of them offer product or service which are exposed to the internet directly. This kind of industry hold critical information about their customer and business partners which needs to be protected. The major challenge here is determining adequate security practices in the enterprise. So, introducing these security practices through a simple game would help to overcome this challenge.

✓ Legal and regulatory requirements

There are various industries such as finance, healthcare, retail and automobile and these industries have a specific regulatory requirement which needs to be followed. So cyber security is a challenge here in this tightly rule bounded industries.

✓ Enterprise IT Architecture

It enterprise have transformed over a period of years in an enterprise by serving the business requirements. Security trend is also a priority here in the large-scale IT enterprise architecture. Legacy systems have increased the security worries across the enterprise. It is very important to have a right security mechanism by preserving the IT security along

V. Attributes for an effective Cyber Security game

✓ Game or the scenarios need to be realistic as possible along with keeping the interest of the person.

✓ Game should stress on the key concepts and skills through repetition and learn from the past.

✓ Game should be engaging and intense but at the same time easy to understand so that player does not abandon it.

✓ Learning objective should be clear and effective.

✓ The game should be fun, engaging and entertaining and the goal should be worthwhile from the eyes of the players.

VI. Key Principles of cyber security

Security is an act of prevent authorized access, use, modification, disruption, inspection and destruction of the information. Cyber security plays a vital role in keeping our data and information safe and secure. Security mainly focuses on three main aspects which are also known as CIA Triad.

□ **Confidentiality**

Information in today’s world has a very high value. Information about bank statement, passwords, credit card details or social security details are very critical. Information which is sensitive should only be shared with a limited number of people. For example, individual’s credit card or social security details should not be shared with anyone and should be confidential. Protecting this information is very critical and is a major part of information security. Confidentiality deals with preventing wrong people from getting access to this sensitive information. One of the important concept in confidentiality is encryption. Encryption ensures that data is accessible only to right people. One of the prominent example of encryption is SSL/TLS; which are the security protocol for communication over the internet.

□ **Integrity**

Integrity means keeping the information from being altered by unauthorized parties. Any kind of tampering with the information can prove very costly. Data must not change when it is being sent and necessary steps must be taken to ensure that data cannot be changed by any unauthorized person. We can have file level permission and user access control to ensure Integrity. There should be versioning of the data to ensure the data integrity. Hashing is one of the common techniques used to ensure data integrity. Checksums and encryptions are integrity verification techniques. If any Malware hits any the computer system, then it can tamper any of the confidential data. So here integrity comes into picture.

□ **Availability**

Availability of information ensures that only authorized people can access the information when needed. Information must available to a correct person at correct time. This ensures that accurate data will be available and accessible all the time to the user. Denying access of information has become very common attack nowadays. Any downtime of resources over the network can prove very costly to the organization. Any natural calamity such as earthquake or floods can lead to loss of data. Availability is related to integrity of the data as well. With the data being stored on cloud servers, availability becomes very critical. One of the better ways to ensure availability is to take regular back up of the data. This can limit the damage caused by the any expected accidents or known attacks. Extra security equipment such as firewall or proxy servers can guard against the downtime and unreachable data due to malicious actions such as Denial of Service attacks.

Often ensuring that the above three phases are an important step in designing security system. Making the user aware of these three factors and making them understand the severity of these three factors is one of the aim of the game which is being developed under this thesis.

VII. Need for cyber security

✓ <u>It is a first line of defense</u>

It is very important to be aware of the different threats to the system. Protecting the data and keeping it safe is very important and that will come if the society is aware of the know threats and attacks. Human errors account to large part of security incidents. Many data breaches occur as a result of an ignorant employee opening a malware infected email attachment or clicking on a link to a malicious site. Instructing the employees or educating them with the security threats and security rules is an important step in cyber security.

✓ Compliance with regulatory requirements
Compliance is very important, and rules and procedures help in increasing the security of the system. Lack of compliance and regulations can result in heavy financial and business consequences. To ensure compliance, each organization should review the regulations and understand how those affect the organization.

✓ Build Trust and Loyalty
Customer trust and loyalty is very important. Without trust and cooperation things will not be as per the requirements. With the help of cyber security, customer start trusting the companies or the service provider and thus increase their loyalty towards that product.

✓ Better culture and Better returns on investment
with knowledge comes power, but this power should be used wisely. People should always be aware of the security threats and that will be possible when you have good source of knowledge. This will help in fostering the relations between the society. Strong culture will cultivate greater sense of understanding and will help in getting better results. Once we start getting better results, the product will be better return on investment.

✓ Be more vigilant and care about the actions
All the organizations care about their employee's actions and their nature at work. Each employee must be always aware of any unknow sources from where the data might get transferred or any unsafe way in which the data might enter into the system. Each action of the employee might have huge impact on the system. So cyber security can help in making employees more vigilant.

VIII. Motivation - Play Safe, Stay Safe and Learn Safe!

□ **Be smart on Internet and share with care**
Internet is a great place to make friends and to gather information, to do any online transactions and have fun. But when all these things are done, it is very important to be smart enough to know what is correct and what is not and to share only what is needed. Good and bad news travels faster and individuals can find themselves in a tricky situation.

- **Be alert on Internet and don't fall for fake traps**
Being safe means being alert as well. This internet giant is one big system where most of the users fall for one or the other fake information. Staying always alert and knowing the difficulties will help the user in protecting their identity. There are many portals on which they ask for personal information. Every user on the internet should be aware of these fake websites which just try to steal the users' personal information and use that information for their own benefit.

□ **Be strong on the internet and keep the space secure**
Personal Privacy and security is very important weather it is online or offline. Securing personal information is one of the most important aspect

of the online world. With being tightly secured, it helps in creating the digital world stronger and secured for the online community. Being strong means, we need to fight against the security threats. There are many scenarios in which we need to be aware of the system and be aware of the loop holes which will help in breaking down these attacks. It is very important not to break down when there is any security breach and try to protect the space from getting tampered.

- **Be Internet brave and when there is any doubt, communicate**

  There is lot of systems which are confusing and questionable across the internet. It is important to feel comfortable while doing any activity on the internet. It is very important to take brave decisions on the internet so that we can keep the online world safe and secure. Effective communication helps in tracking down all the issues and helps in resolving them as well. So, in case of any security breach it is very important to have a proper communication so that everyone is very much aware of the system. Doubts leads to confusion and confusion lead to problem. Hence in case of effective communication it is very important to clear all the doubts.

IX. Story Line of our Game and how we are trying to spread awareness.

With this project, we intend to present an interactive method of learning about topics in the world of security, our aim is to cover some concepts we've learned in CS458 and CS558. Planned topics to include in the game:

DDOS: The game starts with a hacker orchestrating a DDOS attack. The attack type will become clear as the players play on and advance.

Intrusion (weak password by an employee, etc.): The game progresses and the players find that there has been an intrusion through a policeman/avatar.

Intrusion Detection (Malicious code): The players will look for clues within the company headquarters. As they Investigate, they click on the computer to find a virus.

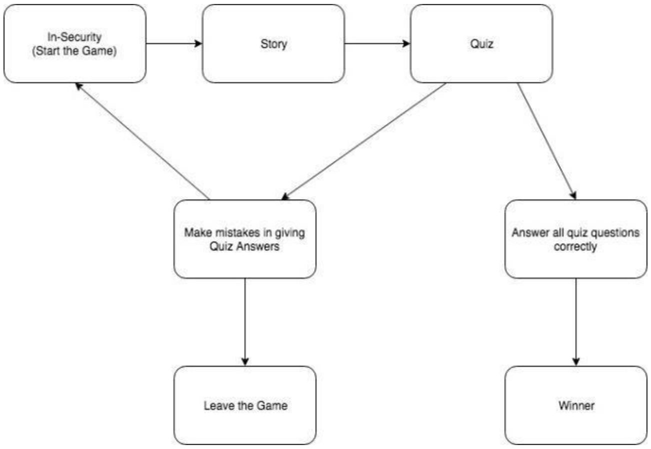
Encrypted clue: Initially when the virus is detected, the players find that harmful activity in the system was caused by it. The intensity of the attack is present in the virus program. Virus reveals a clue which is encrypted.

Decryption: The clue is encrypted in one of the popular encryption techniques. Decrypt the clue to find identity/address of the hacker.

Final showdown: Finally, on decrypting the clue, the players will reach the hacker's area and be able to save the data from getting into the wrong hands.

Educational: Throughout the game, the players will be given vital information about the various forms of security threats in today's world. They will be in the form of:

- **Clues:** the players will find clues which helps them learn about various topics as well as determine which of those topics may have caused this situation.
- **Quiz:** Based on the information found in the clue, the players will be quizzed on what they have learnt, giving correct answers would lead players to advance further in the story. Incorrect answers will not let the players advance. The aim is that even if the players try to skim through information, the quiz will serve as another source of information.


In-Security
(Start the Game)
Story
Quiz
Make mistakes in giving Quiz Answers
Answer all quiz questions correctly
Leave the Game
Winner

In order to make the game more exciting, we have added levels in such a manner that if the player incorrectly answers 2 or more Quiz Questions, he will be prompted that you may lose the game if you keep on playing in the same manner and there is a possibility of the company being attacked more badly. Which encourages the player to perform better in the game.

X. Related Work

To map the current landscape with similar games, a research was conducted to find more information about similar games so that we can have a better understanding of already existing systems.

✓ <u>Tesla Town</u>
Tesla town is an interactive game in which the user must explore electricity generation and delivery. The user is taken to a hydroelectric power plant and can get the actual feel of electricity generation. This game is designed for elementary and middle school kids. It demonstrates the importance of how the current electricity generation is done and how future generation will be done. The information is conveyed from interactive structures and informative photographs.

□ <u>Agent jones</u>
This is a single player game centered on helping secret agent Jones to complete his mission of successfully restoring the electricity in the city. The players will learn about the current power system and future smart grid, as well as the cyber security concerns.

✓ <u>Google’s Interland</u>
The main aim of this game is to educate student and make them understand their responsibility in the digital world. This is an adventure packed game that makes the learning about digital safety interactive and fun. This game helps the kids to understand how hackers can damage your entire system and online world.

XI. Methodology

The objective of our game is to implement game-based scenarios and analyze the effectiveness of this approach in learning cyber security concepts. There are various sub categories in which the game can be functional and useful. We cover different security topics such as DDOS, Intrusion, Intrusion detection, Encryption and decryption.

The game begins with DDOS concept. Here the hacker starts an DDOS attack. The player must understand the attack and then will start getting clues to move ahead. The game plot will start becoming clearer as user starts playing and advances.

Intrusion by weak password is a section in which we try to make the user learn that the password should be strong and easy and weak passwords are easy to crack. The game progresses and the players will understand that the was an intrusion happening. This will be a learning for the user to have a strong password.

Then in the game the user will be made aware of intrusion detection by malicious code. The players here will look for the clues within the headquarters of the company. While they are investigating they try to find the computer to eventually find a virus. In this the users are being educated about the intrusion which happens through a malicious code.

Then in the game, the user will find out something about the encrypted clue. When the virus is detected the user gets aware that there is a harmful activity happening in the system. The intensity of the attack is also presented in the virus program. These viruses are acting as a clue in an encrypted format.

Then once the clue is found which is in encryption technique then the user will reach to a stage where decryption will be of great help.

Once the decryption is done, then there will be a final showdown where the player will reach the area in which hacker is operating. Here the player will try and work towards saving the data from getting into the wrong hands.

Throughout the game there will be vital information given to the user which is a form of learning to the user. This security related information will act as a source of knowledge and this will be a fun to learn as well. The learning will be in the form of clues. These clues will help the players to advance in the game along with educating them to learn about various topics and situations. The players will also be given various quizzes throughout the game which will make the user more knowledgeable about the computer security. Each correct answer in the quiz will lead to next stage in the story line. Incorrect answers will not lead to any further part in the story.

XII. Game Play

This game is developed to make the users or the society aware about different security threats and the importance of the cyber security. In this the story line first begins with the hacker trying to perform the attack on a company and is asking for the keys. The user has to answer some series of the questions and has to move to the next level. There will be an information page given to the player which will look like a quiz. There will be different scenarios which will help in resolving different security related options. With each scenario covering different security options and helping the user to understand in more details about the threats and its effects. The quiz section of the game will be testing various criterion of the players. Each player will be given a different quiz to test upon and help them to understand their capability.

XIII. Technology Stack

Designing a framework for creating game is very important. With the advancement in the technology with respect to web development, this project used pixi.js as its backbone programming framework and was supported by JavaScript, HTML5 and other web technologies.

PixiJS

This is a fast lightweight 2D library which works across all devices. It is a rending library which allows to create rich interactive graphics, cross platform applications and games using WebGL API or deal with browser compatibility. The game is entirely based on this framework. It has full WebGL support which seamlessly falls back to HTML5 canvas if needed. This framework is compatible and has graceful degradation which means there is less work to be done. It helps in polished and refined experience relatively quickly with low level code. It also has sprite sheet support and these sheets can be trimmed or rotated. The user can create WEBGL filter of their own and it can be incorporated with the system to get a seamless application. There are certain older platforms which may not be able to use WEBGL. With PixiJS this worry is reduced and with this system canvas fallback is seamless and automated. With the advance text rendering and beautiful anti-aliased text at native and retina solutions means that Pixi copy is an easy on the eye as it is any other delivery method. Using technologies such as Cordova to rapidly deploy your PixiJS project as an application and this is an advanced technology supported by Pixi. This is the only open WEBGL which is doing that. Spirit sheets, graphics, fonts, animation data all are coming with assets and loaded and handled by PixiJS.

JavaScript

JavaScript is also called as JS and is a high-level programing language. Along with HTML5, JS is one of the three code web development technologies. With the help of JS the interactive webpages are developed and thus it is one of the essential part of web development. With having a multi-programming language, JS supports event drive, functional and imperative programming styles. With the help of API which works for text, arrays, dates, regular expression it works seamlessly with IO functions and networking. Initially it was implemented into client server architecture with JS engine now is used in many other types of host software. It also includes server side in web services and in non-web programs such as word-press and pdf software. In this thesis each step almost has live samples available to play and will help in immediate stages. JavaScript has a universal support library which works across all the browsers. Being structed and imperative JavaScript support structured programming language along with JavaScript makes a distinction between expressions and statements. With JavaScript being completely object oriented we have created a function which can be reused and hence reducing the size of the code. JavaScript comes up with different frameworks such as Node, Angular, Pixi, Backbone, Dojo and many others. Among these framework Node is one of the very prominent and most used frameworks. JavaScript executes in the client system and the use of webserver is less which helps in saving the bandwidth and helps in avoiding the unnecessary security breach. Third party add-ons like Greasemonkey enable JavaScript developers to write small JavaScript which can execute on desired web pages to extend its functionality. If you use a website and require a certain feature to be included, you can write it yourself and use an add-on like Greasemonkey to implement it on the web page. With this kind of flexibility, JavaScript helps in creating an interactive and appealing web applications.

HTML5

HTML5 being the structured mark-up language which is used to present the content on World Wide Web. HTML5 includes detailed processing models which helps in interoperable implementations; it extends, improves and rationalizes the markup available for documents, and introduces markup and application programming interfaces for complex web applications. For the same reasons, HTML5 is also a candidate for cross-platform mobile applications, because it includes features designed with small devices in mind. Currently HTML Canvas 2D context is also being used which helps in rendering the images and 2D content. We can also have a timed media support in HTML 5 which was not present earlier. With the help of offline content API, we can render the screen content offline as well. HTML5 is designed so that old browsers can ignore new HTML5 constructs. In contrast to HTML 4.01, the HTML5 specification gives detailed rules for lexing and parsing, with the intent that compliant browsers will produce the same results when parsing incorrect syntax. According to a report released on 30 September 2011, 34 of the world's top 100 Web sites were using HTML5 – the adoption led by search engines and social network

XIV. Challenges we faced and things we learned.

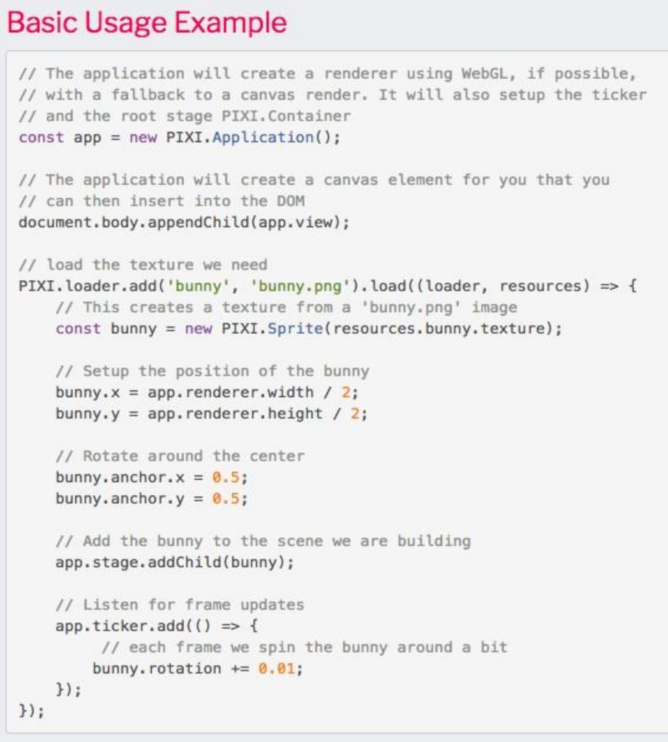
While we had to go through a lot of challenges while learning and implementing the PIXI.js framework and working on WebGL canvas rendering as it is one of the fastest cross platform gaming engines available on the internet today, we also learnt a lot regarding the basic functioning of the game engine and what all components are most important in order to make a perfectly functional game. Some of the important things we learnt are:

- Working with PIXI.js
- Working with WebGL rendering
- Working with photoshop
- Designing the sprites

We are providing a list of very essential features of the PIXI.js framework for those who are making their first games and are getting confused by the huge and confusing documentation given.

1. Working with PIXI:

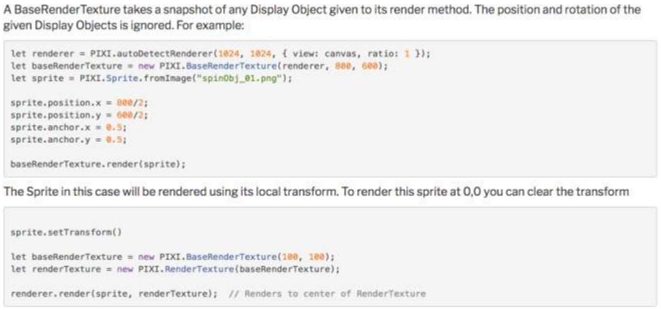
This is the basic structure of the code in a nutshell. In this code we are setting up a stage for our sprites and adding child to the stage so that many different objects can occupy the stage of the game.



Basic Usage Example

```
// The application will create a renderer using WebGL, if possible,
// with a fallback to a canvas render. It will also setup the ticker
// and the root stage PIXI.Container
const app = new PIXI.Application();

// The application will create a canvas element for you that you
// can then insert into the DOM
document.body.appendChild(app.view);

// load the texture we need
PIXI.loader.add('bunny', 'bunny.png').load((loader, resources) => {
    // This creates a texture from a 'bunny.png' image
    const bunny = new PIXI.Sprite(resources.bunny.texture);

    // Setup the position of the bunny
    bunny.x = app.renderer.width / 2;
    bunny.y = app.renderer.height / 2;

    // Rotate around the center
    bunny.anchor.x = 0.5;
    bunny.anchor.y = 0.5;

    // Add the bunny to the scene we are building
    app.stage.addChild(bunny);

    // Listen for frame updates
    app.ticker.add(() => {
         // each frame we spin the bunny around a bit
        bunny.rotation += 0.01;
    });
});
```

2. WebGL Canvas Rendering:



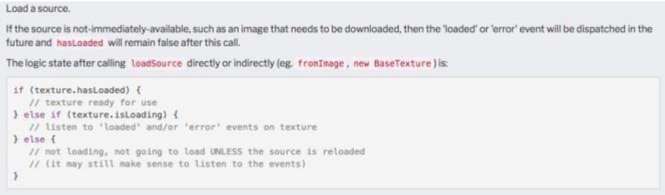
A BaseRenderTexture takes a snapshot of any Display Object given to its render method. The position and rotation of the given Display Objects is ignored. For example:

```
let renderer = PIXI.autoDetectRenderer(1024, 1024, { view: canvas, ratio: 1 });
let baseRenderTexture = new PIXI.BaseRenderTexture(renderer, 800, 600);
let sprite = PIXI.Sprite.fromImage("spinObj_01.png");

sprite.position.x = 800/2;
sprite.position.y = 600/2;
sprite.anchor.x = 0.5;
sprite.anchor.y = 0.5;

baseRenderTexture.render(sprite);
```

The Sprite in this case will be rendered using its local transform. To render this sprite at 0,0 you can clear the transform

```
sprite.setTransform()

let baseRenderTexture = new PIXI.BaseRenderTexture(100, 100);
let renderTexture = new PIXI.RenderTexture(baseRenderTexture);

renderer.render(sprite, renderTexture);  // Renders to center of RenderTexture
```

This is how the WebGL renderer works with PIXI.js in putting everything together for the game engine.



Load a source.

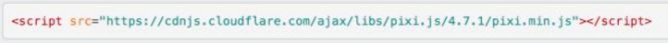
If the source is not-immediately-available, such as an image that needs to be downloaded, then the 'loaded' or 'error' event will be dispatched in the future and `hasLoaded` will remain false after this call.

The logic state after calling `loadSource` directly or indirectly (eg. `fromImage`, `new BaseTexture`) is:

```
if (texture.hasLoaded) {
   // texture ready for use
} else if (texture.isLoading) {
   // listen to 'loaded' and/or 'error' events on texture
} else {
   // not loading, not going to load UNLESS the source is reloaded
   // (it may still make sense to listen to the events)
}
```

This is how we load any source in our renderer for it to run while running the game.

3. Getting it all together:



```
<script src="https://cdnjs.cloudflare.com/ajax/libs/pixi.js/4.7.1/pixi.min.js"></script>
```

This is a very important step in getting it all together. Like even if you are ready with all the scripts of the game but you can’t really make your game function unless you have included this part of code in your code structure. What this part of the code does is it includes all the libraries required for your game to function on any kind of device without throwing any exceptions or crashing.

XV. Results and findings

The main aim of this game was to help user to understand different security threats and their effects on the society. It is very important to analyze these security threats and measure their impact on the organization. By conducting this thesis, it had a very positive impact on the society and this was one of the very effective way of learning. Results indicate this game have positive effects in combination with security awareness and learning.

Firstly, it found that users of the game had a very engaging and fun learning experience. Making people understand the serious issues is difficult with needs some different way to make people understand. With Gamification in raising awareness this above doubt has been resolved and these kinds of issues now no longer persist. This has been a very effective tool for the society.

Secondly, it discovered that user will value the security and its associated threats and vulnerabilities. The society is not aware of the impact of these threats and it is very important to make them realize the severity of these kinds of effects. By using this game, there was a sense of awareness among the society and they understood the impact of these threats. Hence users or the society now began valuing the security related issues and are eventually trying to help and create a better secure system to work with.

Thirdly the result from this thesis was gamification for cyber security has increased the motivation towards security awareness and the ways in which the security threats can be handled. It is very important to learn about the ways in which these threats can be handled. Once we understood the severity of the issue and how these threats are affecting the society, it is important to have a proper defense control mechanism to deal with the security. There was a considerable rise in the way in which these issues were handled.

Fourthly, the results indicated that the game had a positive effect in combination with security awareness and training. Security awareness and training has vast impact in an organization. It is a regulatory compliance to have a periodic training and awareness for the employees.

Fifth, results from the workshops suggests that gamification can increase motivation towards completing training, and potentially improve learning outcomes because of this. Conducting a normal online training will be monotonous and boring. Hence most of the employees try to ignore these kinds of training and thus lose their security awareness.

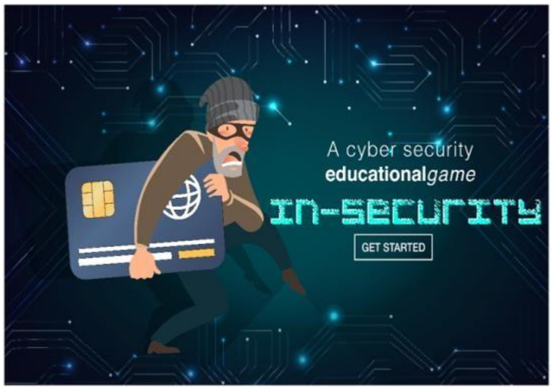
Improved Program metrics also shown tremendous growth. It is generally difficult to calculate the ROI of the program with respect to cyber security. But after conducting the research and finding out the process impact it shown that there was tremendous increase in the ROI and hence it was a very effective technique.

Conclusively, it was indicated that a long-term gamified training program, with use of short and concise exercises, could lead employees to think more about security during the daily work, which in turn suggests a potential for behavior change.

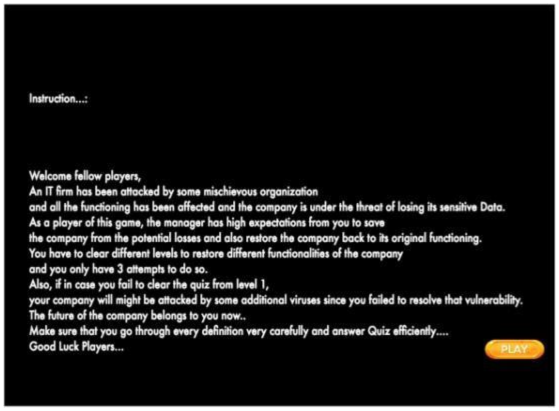
XVI. Screenshots

1. Loading Page

2. Start Page



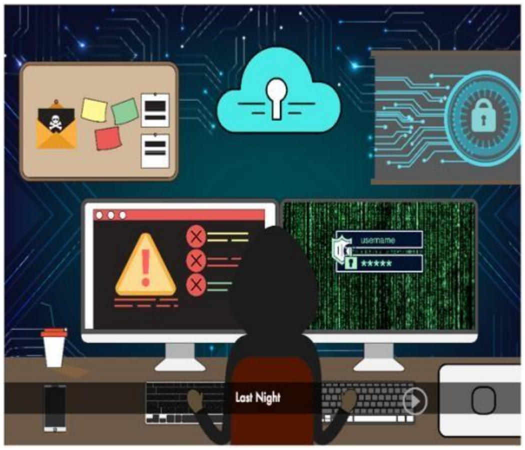
3. Introduction Page

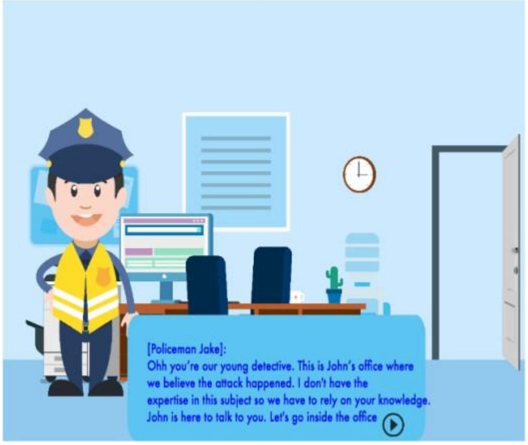


Instruction...:

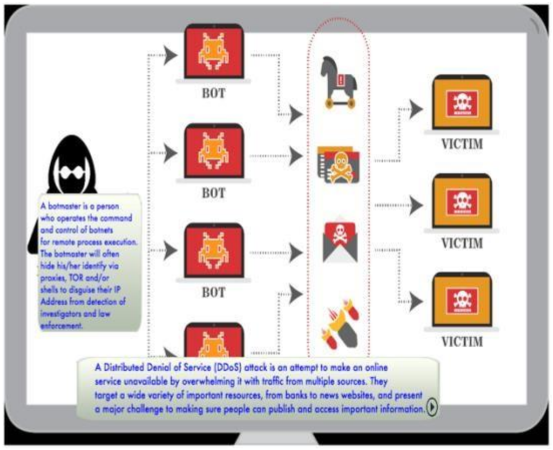
Welcome fellow players,
An IT firm has been attacked by some mischievous organization
and all the functioning has been affected and the company is under the threat of losing its sensitive Data.
As a player of this game, the manager has high expectations from you to save
the company from the potential losses and also restore the company back to its original functioning.
You have to clear different levels to restore different functionalities of the company
and you only have 3 attempts to do so.
Also, if in case you fail to clear the quiz from level 1,
your company will might be attacked by some additional viruses since you failed to resolve that vulnerability.
The future of the company belongs to you now..
Make sure that you go through every definition very carefully and answer Quiz efficiently....
Good Luck Players...

4. Story Pages





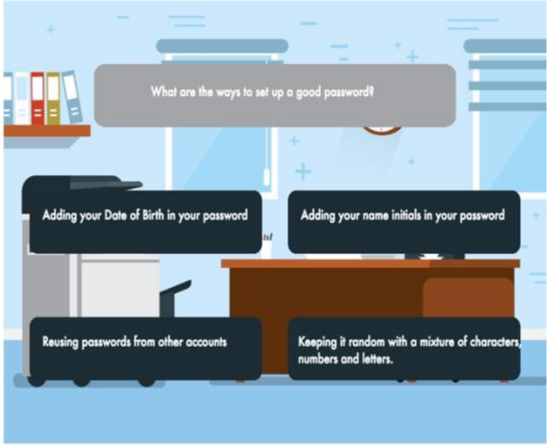
[Policeman Jake]:
Ohh you're our young detective. This is John's office where we believe the attack happened. I don't have the expertise in this subject so we have to rely on your knowledge. John is here to talk to you. Let's go inside the office



A botmaster is a person who operates the command and control of botnets for remote process execution. The botmaster will often hide his/her identify via proxies, TOR and/or shells to disguise their IP Address from detection of investigators and law enforcement.

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

5. Quiz Page



What are the ways to set up a good password?

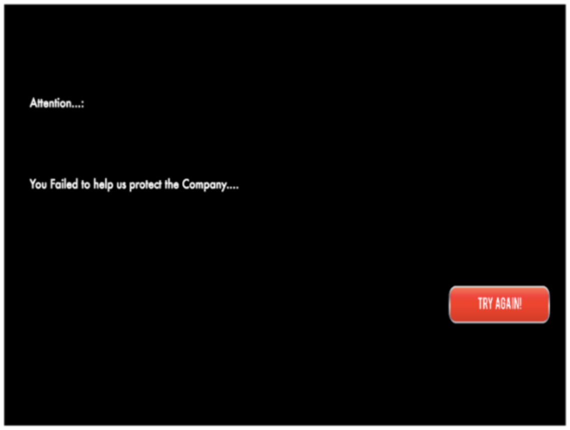
Adding your Date of Birth in your password

Adding your name initials in your password

Reusing passwords from other accounts

Keeping it random with a mixture of characters, numbers and letters.

6. End Page



Attention...:

You Failed to help us protect the Company....

This page appears if the players fail to answer correct Questions.

Hurraayy...:

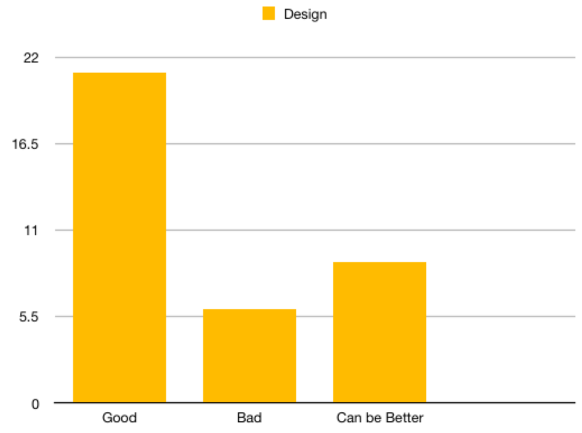
Mission Accomplished ....

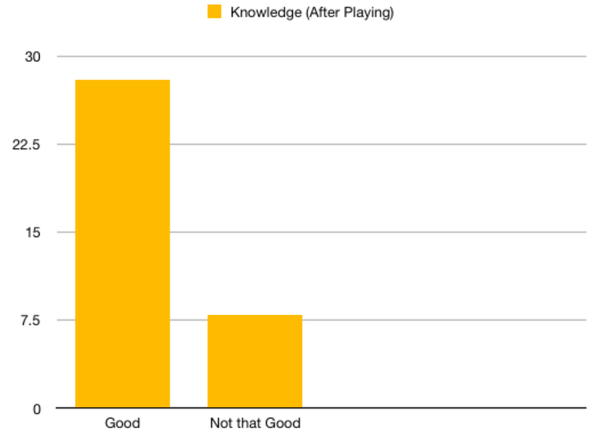
This page appears if the players complete all levels successfully.

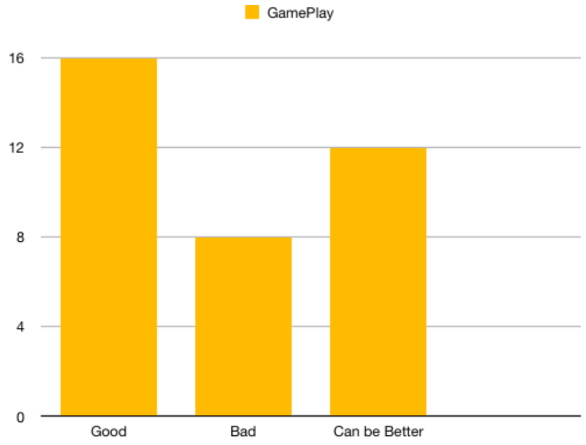
XVII. Feedbacks and Statistics.

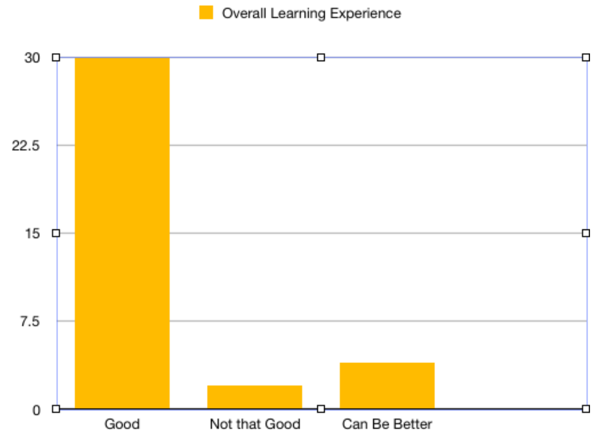
We released our game to our family and friends to play and give us the feedbacks. A total of 36 people played the game excluding us and their feedbacks can be seen in graphs below.

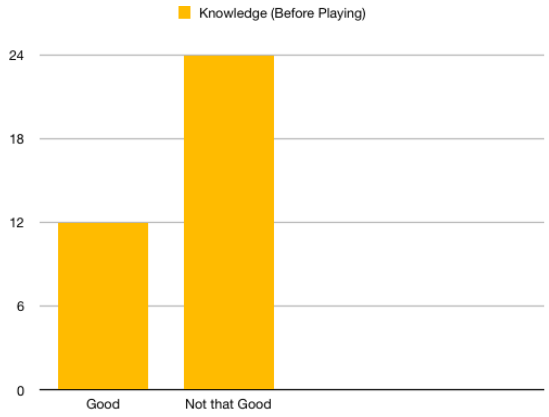
Overall response was good, but a little more development is needed, but since this is the first game we were making, we are satisfied with the feedbacks.











XVIII. Conclusion and Future work

Security awareness and training programs are demanding, and these programs are supposed to create awareness in the field of information security for people with a wide variety of previous knowledge. That includes people with no experience, people who already know a lot—and even people who think they already know a lot. In many ways, the key word here is people, and that is why this study has focused largely on how gamification could and should be used to make security training a little bit better for people.

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions.

The latest and disruptive technologies, along with the new cyber tools and threats and these threats are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. With the help of gamification, the complex and monotonous topics were converted into an interesting and fun learning experience. Different scenarios can be placed very positively and help in making the system more stronger and more effective which can lead towards the betterment of the society.

By using pixi.js as a game engine, it helped in rendering the system very effectively and helped in given an effective representation which makes the game more interesting and more relevant with the todays world. While designing the game we had to cope with numerous interdisciplinary tasks throughout the development and this helped in exercising a broad spectrum of technical skills.

The results which are evaluated also shows that this is an effective way to communicate information and help people and make them aware.

Further Work

The use of gamification in security awareness and training programs is currently a young and unexplored research area. As information security competence is only becoming increasingly important, it is necessary that this research continues. It is therefore necessary to study if gamified training is more effective than regular training. We can have more detailed level of security awareness and can add more levels with respect to the game. We can also create an adaptive game where in each player will get a difficult question with respect to security for every correct action. Awards and recognition can also be presented in this game to give recognition of the players efforts. We can also add multiplayer form in which both players should answer certain set of questions which will help in advancing in the game. This will help in increasing the competition and will help in increase the level of curiosity and awareness among the peers. We can also show a comparison chart which will help in giving a better idea and better results when you are comparing how effective the game was and how efficiently it improved the performance of the player. It can also include the efficient ways of accessing the players current knowledge and explore the ways in which they can adapt to the training that is being obtained from the game.

XIX. References

- Use of Gamification in Security Awareness and Training Programs - https://brage.bibsys.no/xmlui/bitstream/handle/

- BeOne (2016). Mobile learning: BeOne Ubiq app. https://www.beonedevelopment. com/solutions/mobile-learning

- ENISA (2010). The New Users' Guide: How to Raise Information Security Awareness. European Network and Information Security Agency (ENISA). Available at https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

□ https://www.itgovernance.co.uk/blog/95-of-organisations-face-significant-challenges-when-implementing-cyber-security-frameworks/

□ https://deltarisk.com/blog/5-quick-tips-for-implementing-a-cyber-security-program/

□ https://techcrunch.com/2016/03/31/meeting-cybersecurity-challenges-through-gamification/

□ https://arxiv.org/pdf/1804.03567.pdf

□ https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

□ https://www.sogeti.nl/sites/default/files/sogeti-boek-cyber-security-staying-ahead-in-the-cyber-security-game.pdf

- https://www.newscientist.com/article/2150282-online-game-will-spot-if-you-have-hidden-cybersecurity-talents/
- Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors - https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_442344.pdf
- CYBERSECURITY GAMES: BUILDING TOMORROW'S WORKFORCE - https://www.nist.gov/sites/default/files/documents/2017/04/24/cyber_games-_building_future_workforce_final_1031a_lr.pdf

XX. Appendix

Appendix A

```
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <title>In Security</title>
</head>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/pixi.js/4.7.1/pixi.min.js"></script>
<body>
  <script type="text/javascript">
    let type = "WebGL"
    if(!PIXI.utils.isWebGLSupported()){
      type = "canvas"
    }

    PIXI.utils.sayHello(type)



     //Create a Pixi Application
let app = new PIXI.Application({
    width: 1200,
    height:800,
    antialias: true,
    transparent: true,
    resolution: 1,

  }
);
```

Starting the PIXI engine.

Appendix B

```
document.body.appendChild(app.view);

let TextureCache = PIXI.utils.TextureCache;
let Sprite = PIXI.Sprite;
let Text = PIXI.Text,
    Container = PIXI.Container,
    TextStyle = PIXI.TextStyle;

let bg, police,police3,
    op= new Container(),
    s17 = new Container(),
    s1= new Container(),
    s2 = new Container(),
    s3 = new Container(),
    s4 = new Container(),
    s5 = new Container(),
    s6 = new Container(),
    s7 = new Container(),
    s8 = new Container(),
    s9 = new Container(),
    s10 =new Container(),
    s11= new Container(),
    s12= new Container(),
    s13 =new Container(),
    s14= new Container(),
    s15 =new Container(),
    s16 =new Container(),
    q1 =new Container(),
    q2=new Container(),
    bot=new Container(),
    state;

    c =
PIXI.Sprite.fromImage('images/Loading.png');
            c.width=1100;
            c.height=700;
            c.x=150;
            app.stage.addChild(c);



PIXI.loader
  .add("images/S1.json")
  .load(setup)
```

<u>Adding containers and setting up functions.</u>

Appendix C

```
app.stage.addChild(op);

            let bgTexture =
TextureCache["Op.png"];
            bg = new Sprite(bgTexture);
            bg.width=1100;
            bg.x=150;
            bg.height=700;
            op.addChild(bg);


            arrow =
PIXI.Sprite.fromImage('images/Get.png');
            arrow.height=49;
            arrow.width=151;

            arrow.y=422;
            arrow.x=825;


            arrow.interactive = true;

            // Shows hand cursor
            arrow.buttonMode = true;

            // Pointers normalize touch and mouse
            arrow.on('click', onClickone);
            op.addChild(arrow);
            //op.visible= false;
```

<u>Defining Child and assigning functions.</u>

Appendix D

```
function onClickone()
      {
         op.visible=false;
         s17.visible=true;
      }
      function onClickintro()
      {
         s17.visible=false;
         s1.visible=true;
      }
      function onClicktwo () {
            s2.visible=true;
            s1.visible=false;
      }
       function onClickthree () {
            s3.visible=true;
            s2.visible=false;
      }


      function onClickdoor()
      {
        bg = PIXI.Sprite.fromImage('images/door
02.png');
            bg.width=1100;
            bg.x=150;
            bg.height=700;
            s3.addChild(bg);


            police3 = new
Sprite(PIXI.loader.resources["images/S1.json"].
textures["Policeman-05.png"]
            );
            police3.height=500;
            police3.width=300;

            police3.y = 150;
            police3.x=175;
            s3.addChild(police3);


            diag3=
PIXI.Sprite.fromImage('images/diag blue.png'
            );

            diag3.height=200;
            diag3.width=600;

            diag3.y=500;
            diag3.x=400;
            s3.addChild(diag3);


            style = new TextStyle({
            fontFamily: "Futura",
            fontSize: 20,
            fill: "BLUE"
            });
            message3 = new Text("[Policeman
Jake]:\nOhh you're our young detective. This is
John's office where \nwe believe the attack
happened. I don't have the \nexpertise in this
subject so we have to rely on your
knowledge.\nJohn is here to talk to you. Let's go
inside the office", style);
            message3.x = 440;
            message3.y = 540;
            s3.addChild(message3);

          arrow =
PIXI.Sprite.fromImage('images/arrow n.png');
            arrow.height=50;
            arrow.width=60;

            arrow.y=650;
            arrow.x=905;


            arrow.interactive = true;

            // Shows hand cursor
            arrow.buttonMode = true;

            // Pointers normalize touch and mouse
            arrow.on('click', onClickfour);

            s3.addChild(arrow);
```

Assigning Functions to Onclick evnts