# Using Video Games to Teach Security

Mario A.M. Guimaraes
College of Information Technology
Zayed University
United Arab Emirates
mario.guimaraes@zu.ac.ae
(on leave from KSU)

Huwida Said
College of Information Technology
Zayed University
United Arab Emirates
huwida.said@zu.ac.ae

Richard Austin
Southern Polytechnic State University
Marietta, GA
raustin2@spsu.edu

## ABSTRACT
This paper describes a project to design educational video games as an aid to teaching security. The first section describes the need to create practical hands on security examples where the student is an active learner. This section explains why video games are a natural fit for educational software, particularly in the field of information security and assurance. The second section examines existing videogame software and provides links to download them. The third section describes the three videogame development environments adopted at our university. In the last section we describe the videogame prototypes developed for teaching security as well as the ones under construction.

## Categories and Subject Descriptors
K.3.2 [**Computer and Information Science Education**]:
*Computer science education, Curriculum*

## General Terms
Security, Videogame

## Keywords
Game Engine, Game Maker, Unity, Forensics, Network, Pedagogy, Phising, SDLC.

## 1. MOTIVATION
Traditional security classes are often professor-centered lectures where students learn basic threats and defense mechanisms, without applying this knowledge. Video games offer the possibility to create simulations that bridge the gap between theory and practice by creating a scenario where the user has to react to a series of events and verify the results within a limited time frame.

## 2. EXISTING VIDEO GAMES
Many existing security-related games are complicated and do not have a friendly user interface [1-2]. Also, most games depend on thrill and suspense to deliver the goals of the game, which may make them unsuitable for all ages. Moreover, these games were designed for advanced users who already have basic knowledge about security.
Most games don't provide awareness about security and how to deal with it. They teach users to be hackers and ignore ethics.


*ITiCSE'11*, June 27–29, 2011, Darmstadt, Germany.
ACM 978-1-4503-0697-3/11/06.

## 3. GAME DEVELOPMENT
Three game development platforms were chosen: Game Maker, Flash and Unity Pro. Game Maker is suitable for quick prototypes. F lash is the natural choice for web-based games and Unity is for serious gamers to develop and deploy their products to a multitude of platforms.

## 4. PROPOSED SYSTEM
The proposed system is being implemented with two levels or type of games. Since we are in the prototyping phase, Gamemaker is used. At level 1, several prototypes are built where students gain background and apply basic security knowledge. At level 2, the system attempts to simulate a r eal world environment with the knowledge gained from level 1.

### 4.1 Level 1
Figure 1 displays the network diagram at the beginning of the game. The user drags the text in yellow to the corresponding image on the diagram.

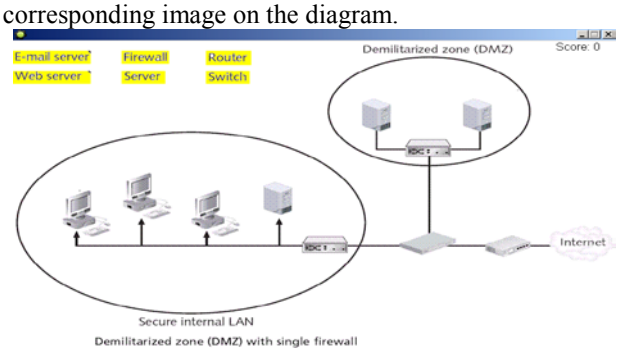


Figure 1 – Network Diagram – Start of Game

### 4.2) Level 2
In level 2, the user must defend his/her system. The goal of the game is to survive the attacks. Every 10 seconds that the user lasts, he receives 50 points. If the user survives all the attacks, the user will advance to the next level. There is a **Help** Menu, an **Accounts** Menu, an **Application** Menu and an **E-Mail** Menu. Level 2 is currently under construction and the first prototype should be concluded and tested prior to May of 2011.

## REFERENCES
[1] Uplink, Retrieved Jan 6, 2011, from http://www.introversion.co.uk/uplink/about.html

[2] Portsign Hacking 2, Retrieved Jan 6, 2011 from http://download.cnet.com/PortSign-Hacking/3000-7551_410728340.html