Blending Bloom's Taxonomy and Serious Game Design

L. Buchanan[1], **F. Wolanczyk**[1], **and F. Zinghini**[1]
[1]Secure Decisions Division, Applied Visions, Northport, NY, USA

Abstract - *Using serious games and interactive exercises can provide a safe and effective practice environment for computer network defenders, but development of these games must blend subject matter content, instructional design learning objectives and engaging game design to encourage learners to practice and develop their skills. As part of a program to develop an interactive training platform for the next generation computer network defender, we developed several Flash-based, casual games designed to target different levels of learning objectives as defined by Bloom's Taxonomy, for various skills, subject matter knowledge and tools. This paper lays out a working hypothesis based on that experience: some types of games are actually better suited to certain learning objectives.*

Keywords: cybersecurity education, security, Bloom's Taxonomy, learning objectives, serious games

1 Introduction

The need for skilled computer network defenders is rapidly growing, both in the commercial sector and in government. Training the next generation of computer network defenders who understand both the tools and the processes of Information Security and Information Assurance (IA) is a challenge being addressed in many different ways.

In most branches of the US Department of Defense (DoD), military personnel with little or no knowledge of computer security or even computer networks rotate into a duty position on a watch floor that handles incident response activities. Personnel generally spend a few weeks or months in a basic IA boot camp designed to teach the very basics of network defense, and they spend the next year learning to do the job with the tools, techniques and procedures used by that service. By the time personnel start to develop relevant skills and knowledge, they are ready to rotate out to the next duty station. Like most enterprises, the DoD needs to train its personnel faster, more effectively and in a more cost efficient manner.

SimBLEND[1] is a research program to develop a platform to assist in training the next generation of computer network defenders by combining traditional computer based training ("CBT") with visually-intense training aids like serious games and exercises. Much of the entry-level subject matter for computer network defenders, such as ports and services and IP networking, is relatively dull and can be difficult to master. By providing an interesting, engaging and interactive opportunity to immediately review and practice the material covered in a CBT, learners are encouraged to improve their knowledge and skills. SimBLEND uses a traditional learning management system (LMS) to deliver both the CBT and the games, and supplements the LMS with an integrated performance analyzer that evaluates recorded metrics of learner performance in each game or exercise. These metrics are combined with grades from the traditional CBT material such as quizzes to determine an overall grade for the learner that is recorded by the LMS.

2 Interactive Cyber Security Training

To understand the issues with training entry-level computer network defenders in the DoD environment, we visited both the Vermont Air National Guard, Information Operations and the United States Air Force 39th IO Squadron at Hurlburt Field in Florida to observe the training for entry-level computer network defenders provided by live instructors at those schoolhouses. The courses begin with fundamental networking concepts, such as ports and services, and IP addressing and subnetting, then covers baseline tools to enumerate a network such as *ping* and *dig*, and culminates in network enumeration and vulnerability scanning tools such as *nmap*.

Based on our observation of these different environments, we developed a sample entry-level curriculum. We did not want to address issues of strategy or managing cyber security processes, but focused on hands-on skills. Tools to be covered in the individual classes of this sample curriculum included *whois*, *nslookup*, *dig*, and various DNS and network enumeration and vulnerability scanning tools such as *nmap*. Individual classes were intentionally scoped to cover smaller, very focused topic areas, providing "just in time" training. We developed a demonstration scenario using this curriculum that would highlight the progression of an entry-level computer network defender just starting with basic knowledge acquisition. We considered how to use games to scaffold the learner's progression through low-level network tools that require applying that knowledge, then moving on to active problem solving that would allow the learner to

[1] SimBLEND was developed under Air Force Research Laboratory (AFRL) Phase II SBIR contract FA8650-08-C6858. SBIR Data Rights (DFARS 252.227-7018 (June 1995)) apply.

demonstrate mastery of a variety of basic tools and techniques.

2.1 Serious Games for Cyber Security

Having identified the specific types of subject matter to be addressed, we began researching available games and interactive exercises for these low-level cyber security concepts and tools, in particular, web-based games that could be delivered from within an LMS and that allow metrics to be integrated into the automated sequencing and scoring. We also planned to demonstrate SimBLEND with a game that would function as a capstone exercise for the curriculum, a hand-on "final exam," requiring the learner to draw upon the various concepts and tools covered during the classes.

We discovered that in 2009, there were very few serious games publicly available for cyber security training, particularly games that focus on specific, hands-on skill acquisition. Games such as CyberCIEGE [1] and CyberOps [2] are strategy-based games that focus on higher-level best practices and procedures for managing cyber security, not the use of actual tools: the player needs to know to buy a firewall for general protection against threats, but does not need to know how to actually set up a specific firewall to defend against specific threats. In addition, none of the serious games that we found were browser-based, they all required a client-side install, which complicated integration of the game with the LMS that was to deliver both the traditional course material and serious game as part of the CBT.

As we considered the nature of game play and interaction in the service of learning about cyber security, we realized we did not want a web lab, or a graphical simulation of a tool's interface that taught the tool interface. We needed interesting games that would help learners with the core concepts involved with using the tool: how to achieve the best results with a given tool in a specific situation, or even knowing when to use a specific tool. In addition, we wanted games that would create excitement in the learners while using the core subject matter concepts at the heart of the games.

It quickly became evident that not every game type is suited to every learning objective: 3-D games or simulations with avatars are just not well suited to basic knowledge acquisition, which was where we began in the process of cyber security game development. Consider CyberCiege, which is a 3-D game using storytelling of activity in an office environment; the learner makes strategic choices to demonstration comprehension of best practice and higher-level concepts. Although 3D games represent state-of-the art technology, using this type of game to assist in memorizing ports and services was too complex, and not very fun for the learner. Using 3D did not seem to actually enhance any of the basic game concepts we developed, which led us to consider a wider variety of game types.

2.1.1 Casual Games

We needed appropriate games to demonstrate the larger effort of the SimBLEND integrated training platform, so we leveraged our experience in developing training games for domains [3], and worked with an outside game studio to create our own serious games for demonstrating SimBLEND. We decided to create a series of short, Flash-based games, known as "casual games" in the professional game world. Casual games are ideal for this purpose, as they have simple rules and are easy to use. The player does not have to worry about learning basic controls and game mechanics; the learner would not have to be a "gamer" to succeed at casual games. Casual games are also typically short in duration, removing the time commitment required by more complex games.

Serious games require some effort to develop, even casual serious games. Defining the subject matter, how the knowledge or skill is used, what a tool's interface looks like, when is the tool useful, how individual commands are used, what can go wrong – these all need to be understood to develop an effective serious game. In addition, an entertaining concept is needed that makes the player *want* to play the game: an engaging storyline or interaction device [3]. In the course of developing the game interaction and progression, the instructor or subject matter expert can discover that the game essentially teaches the wrong behavior, or that the game behaves differently than the tool or the progression of a real-world scenario. At the start of designing a serious game, however, the instructor and the game designer both need to understand the core purpose of a game in a specific learning process: is it to help a learner memorize something as a part of basic knowledge acquisition, or should the game help the learner understand how to interpret results from a tool?

We began by identifying what cyber security concepts and subject matter would be used in each CBT and accompanying game, as well as the learning objectives for each class. Having selected different CND concepts, we looked for a game concept that would be something fun to do when the subject content is boring, while still maintaining some connection to the subject matter and would not get the user stuck trying to figure out the game mechanics. Memorizing ports and services is really boring, but a puzzle game where the learner must match items that belong together seemed like a natural fit for this memorization process.

3 Hypothesis

This led us to the hypothesis that different types of games are actually better suited for certain kinds of learning objectives, based on the type of interaction inherent in the game type. For example, in first person shooter games, the player must decide what to shoot, and in some instances, which weapon to use. This requires the player to understand the environment and tools available. Puzzle games often have an interaction that requires matching of concepts and the ability to recall information. From this understanding of the

interaction inherent in each type of game, it may be possible to determine what type of learning objective may be most readily served by a particular type of game.

3.1 Bloom's Taxonomy

After developing our idea of the learner's progression from low-level knowledge acquisition through understanding how a tool works and then to analysis of when to use each tool, we discovered that this matched existing pedagogical constructs and there was language to talk about this idea. Bloom's Taxonomy[2] is a classification of different levels of cognitive learning objectives that educators set for students. These "learning objectives" in the Taxonomy describe six progressive levels of learning, from the foundation to the pinnacle: knowledge, comprehension, application, analysis, synthesis, and evaluation.

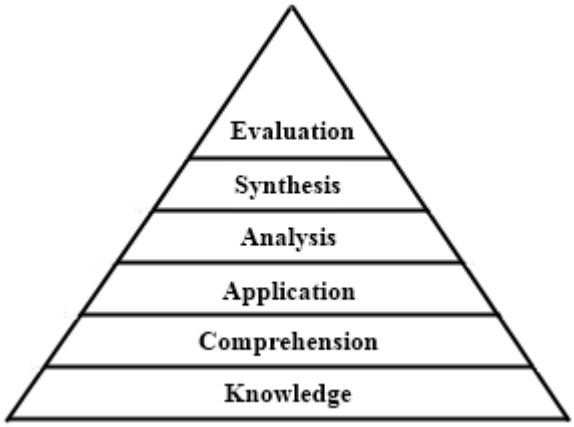

Figure 1. Learning Objectives from Bloom's Taxonomy

Subject matter experts and instructors may understand what the learning objective is for a particular lesson or course, but interaction and game designers generally do not. Having a clear concept of the specific learning objective desired for the game can assist the game designer during initial concept development. Our continued development of demonstration games for SimBLEND was informed by this concept of learning objectives and Bloom's Taxonomy.

3.2 Serious Game Classification

Games are classified by genre or game mechanic, such as first-person shooter, adventure, sports game, driving games, horror, puzzles, and simulations [4, 5]. Different types of game taxonomies exist for serious games such as those based on genre or game mechanics, or the presentation platform or educational purpose [6, 7], but none of the taxonomies we identified address the issue of game design and instructional goals, learning objectives or Bloom's taxonomy.

Serious games design is a relatively new subject for academic research. Much of the existing literature about developing serious games focuses on elements of game design and how to make learning fun, such as interaction development and escalation, like the MDA framework cited earlier. When we began our project, the literature of serious game design had little focus on integrating pedagogical concepts such as Bloom's Taxonomy or learning objectives. Clark [8] mentions pedagogical elements, but refers to elements that appear in the simulation as scaffolding to help the learner, not as part of the underlying design question about what cognitive learning objectives the game needs to teach in addition to the specific subject matter.

The need for a formal design approach that brings together game design and instructional design has been articulated, and frameworks proposed [9, 10]. In these frameworks, integrating learning objectives as part of the early game design consideration ranges from a mere suggestion to a core principle of the framework's design approach. The frameworks do not address game taxonomies, nor do they hint at a potential connection between the type of interaction inherent in a specific game type or genre and learning objectives.

Bloom's Taxonomy did not originally incorporate the psychomotor domain, although this has since been addressed by others. For games designed to increase skills, psychomotor objectives may be very relevant when paired with Bloom's original cognitive learning objectives. A review of the key words describing the various objective levels in the psychomotor domain suggests that there may be a way to connect game interaction and learning objective level. For example, the initial psychomotor learning objective, *perception*, uses keywords such as: chooses, describes, detects, differentiates, distinguishes, identifies, isolates, relates, selects.[3] This list could also read as a set of game mechanic operations.

3.3 Cyber Security Learning Objectives

We did not address every level of Bloom's Taxonomy in our game development, but we have explored the range of objectives, considering what type of game interaction would support the basic learning objectives for a given set of skills and tools. The sections below describe how each layer of

[2] B. S. Bloom (Ed.). *Taxonomy of Educational Objectives: The Classification of Educational Goals*; pp. 201–207. Susan Fauer Company, Inc. 1956.

[3] E. J. Simpson. *The Classification of Educational Objectives in the Psychomotor Domain.* Washington, DC: Gryphon House. 1972. As quoted at http://www.nwlink.com/~donclark/hrd/bloom.html.

Bloom's Taxonomy was blended with game interaction during the design process.

3.3.1 Knowledge

The initial level of Bloom's Taxonomy is the acquisition of basic, foundational *knowledge*. In this stage, the learner should be able to remember ideas and information.

One of the fundamentals of networking and network defense is a thorough knowledge of ports and services. Learning even the most common Well-Known Ports which range from 0 to 1024 and the service associated with each port, is a dull exercise, requiring a lot of rote memorization of pairs. To assist in this learning objective, we designed a matching *puzzle game* around the idea of "connecting the dots." Learners must manipulate tiles to connect a pathway between a numbered port and the corresponding service. The basic manipulation is extremely simple – the focus for the learner is which port and service belong together. The game is timed, and points are acquired for each successful connection. Each progressive level of the game adds more pairs that need to be connected, and while the most common ports are used in the beginning level of the game, less common ports are introduced at more advanced levels of the game.

As a Flash-based game, the ports and services pair data is stored in an XML file, which makes it quite simple to create customized variations of the game. An advanced version adds Registered Ports (1024 – 49151) into the mix, extending the learner's familiarity with a wider range of ports and services. Another version uses common business applications and ports that need to be open or closed in corporate firewalls, and an "evil genius" version includes common malware ports, assisting the learner in learning what activity or configuration issues to look for inside the firewalls.

3.3.2 Comprehension

This level moves beyond surface understanding; a learner should be able to interpret, discuss, compare concepts in terms of similarities or differences, or explain the subject in their own words.

To assist in the comprehension of the network scanning tool *nmap*, we developed a game that is very loose variation of the *first person shooter* type, using missiles rather than guns. In first person shooter (FPS) games, the player must try to take down various targets, typically by shooting a gun; variations on FPS games may provide different weapon types that yield a variety of results and scores.

Nmap has a wide variety of command line switches that are used to control the scanning parameter, and it is critical that the operation of the switches is correctly understood as a malformed scan could cause a network disruption, potentially performing an unintended denial of service attack. By using the FPS concept and making the computers and networks the target, the learner can explore the different command line switches in *nmap* and comprehend how the different switches work (or don't work) with various computer operating systems. The goal of the game is to stop the missiles from falling on U.S. soil; if a missile hits the U.S., the game is over. To stop a missile, the learner must successfully scan (shoot) the computer layers of the missile by selecting the optimal command line switch from a range of choices, however, the learner does not know in advance the operating system or any other characteristics of the computer that is being scanned. The game is timed and different switches cause the scan to run faster or slower as they would in real life. Once the scan is complete, the game displays the nmap output formatted just like the command line tool. The player must also be able to correctly understand the scan results in order to answer questions related to the tool or the computer that was scanned.

A similar FPS concept could be used for any subject matter where the learner needs to understand the action and subsequent reaction and/or consequence. For cyber security, another obvious candidate for this concept would be "shooting down" intrusion detection alerts that are not false positives but represent actual attacks and for the game network.

3.3.3 Application

At this intermediate level in the Taxonomy, the learner should be apple to *apply* a concept, solving a problem by using or examining knowledge and understanding in some manner.

The definition of this learning objective reveals a promising game type: puzzles and problem solving. In the nmap missile game described above, the learner must apply their knowledge of ports and services to answer questions about the scan results, such as identifying the computer's OS or function based on ports reported open by the nmap tool. The learner must also apply their knowledge of the nmap switches to determine what available command line switch options would help "avoid detection" by generating less activity on the network and test different strategies for using some of the most common nmap switches under timed circumstances.

3.3.4 Analysis

The learner can *analyze* the topic or material, and both distinguish between the parts and make connections at this level of the Taxonomy.

Our capstone exercise focused on the higher cognitive levels of Bloom's Taxonomy. The goal of the game is to ensure that the network supporting a logistics convoy is secure

from attack while the convoy travels to its destination. Through the Flash game, the learner gets a feel for what it might be like to sit on the watch floor of a network or security operations center and evaluate alerts that may represent actual attacks. Provided with information about the network to be defended (network topology, device roles, typical activity for devices, relevant firewall rules) the learner must decide if each new alert is a false positive or real potential attack, and take prompt action. The game interface is divided into several areas: a view of the network devices and their current activity levels; a window with incoming alerts; a view of the convoy and its progress over its route, and a window that simulates a window for command line activity. The learner must use information from these multiple sources, and from tools such as *whois* and *nmap* in the simulated command line window to analyze the potential vulnerability of a device for the attack indicated by the incoming alert.

This simulation game uses the narrative devices of supporting the convoy mission and a defined network to get the learner involved and set the stage for further activity. While scenarios were a part of the other two games, they acted as bookends at the beginning and end of the game. The scenario of defending the convoy network is at the heart of this game. It also cultivates in the learner an understanding that computer network defense is not an abstract thing, but that both business operations and physical (kinetic) missions depend on the network. Using a simulated command line interface restricts the learner to a narrow set of options, which greatly reduces the effort to build the game.

3.3.5 Synthesis

Similar to *application*, but on a more sophisticated level, *synthesis* requires a complete understanding of a topic. The learner is able to explain their rationale for choices.

We believe that narrative genre games, particularly the "choose your own adventure" variations, are well suited to the synthesis learning objective. We extended the learning objectives for the capstone exercise described above to address synthesis as well as analysis. After determining if the alert represents a viable attack or a false positive, the learner must also explain the rational for their decision and indicate why each alert was dismissed or was sent on to a handler for further investigation. To assist learners in achieving this learning objective, in this game a false positive incorrectly determined to be a viable attack is acceptable with no penalty, but true attacks incorrectly identified as false positives incur penalties that increase at an exponential rate.

Another game concept we explored but did not develop involved having the learner determine the priority for patching specific systems in a defined network. This would have involved synthesis of vulnerability information, vulnerability scan tool results, and information about other security settings in the network.

3.3.6 Evaluate

At the pinnacle of Bloom's Taxonomy, learners are able to *evaluate* and put together disparate elements to create something new that is a coherent or functional whole.

We considered an extension to our network defense capstone exercise that would address this final learning objective. After successful completion of the capstone exercise, learners would be asked to develop their own set of alerts for the network environment used in the game. The data set would need to include both false positive alerts and true alerts, and learners would need to provide data supporting the evaluation of the alert as false or true. The data could then be loaded into the game and the learner could play against their own data set, testing the accuracy of their data.

4 Conclusions

An interesting discovery was that, unlike simulations, casual games allow the tool interfaces to be abstracted away. They allow the novice learner to focus on the general concepts and skills of the subject matter, and not become distracted by a tool's user interface. This may be useful in areas where there are multiple tools that are based on the same core concept and perform the same function, such as vulnerability scanning tools.

Ideas for future research in this area include development of a different kind of serious game taxonomy, one that specifies which game types are well suited to deliver individual learning objectives at a particular level of Bloom's Taxonomy. We have already begun this work as part of a modification to the SimBLEND project. We are developing *ShortCut*, a tool intended to streamline the creation of visually-intensive training aids such as serious games by facilitating collaboration between subject matter experts and interaction or game designers, using an interactive, web-based knowledge elicitation**.** The knowledge elicitation in ShortCut is designed to allow the instructor or subject matter expert to describe not just the subject matter, but with special consideration for information that would be needed by interaction and game designers. We have begun to collect meta data on other existing cyber security games and will identify the intended learning objective types and correlate them with the type of game or game mechanic used to further extend our taxonomy and evaluate our hypothesis.

There can be serious game design considerations that go beyond the learning objectives of Bloom's Taxonomy. For example, speed may be important to the learning objective and subject matter. It may be critical that the learner gain immediate recall of the knowledge or be able to perform the task very quickly, such as identifying the type of activity that is indicated by port numbers recorded in log data from firewalls or intrusion detection systems. In other cases, correctness and accuracy in the learner's understanding of the skill or tool may be more important than speed. This was true

for the nmap missile game: correctness and accuracy of the switches and flags in the command line string are more important than speed, because an incorrect switch may adversely affect the tool's operation. As a result, while the game is timed, selecting the switch that yields the most information under the circumstances is the most important factor. The game allows enough time to select another switch, but the player does not receive as many points as making the correct selection first. We have incorporated these additional serious game design considerations into the knowledge elicitation used in our ShortCut tool. The goal is to provide the subject matter expert with the ability to describe the fullest complement of game and interaction characteristics.

It would be desirable to test the effectiveness of different game types over the same training material and using the same data set in the different game types. The results of this research could prove or alter our hypothesis, and assist in the further development of serious game design frameworks that blend subject matter content, instructional design and game design. We welcome a discussion of this hypothesis and hope that others become involved in working towards improving the quality of cyber security education at all levels through the use of serious games.

5 References

[1] Cynthia E. Irvine, Michael Thompson and Ken Allen. "CyberCIEGE: An Extensible Tool for Information Assurance Education"; 9th Colloquium for Information Systems Security Education, 130-138, June 2005.

[2] Brian Duffy. "Network Defense Training through CyberOps Network Simulations"; Modeling Simulation and Gaming Student Capstone Conference 2008, 2008.

[3] Markus Lacay and Joe Casey: "Serious Games: Fun vs. Reality", SISO Spring SIW 2011 Conference, No. 11S-SIW-012, April 2011.

[4] Wendy Despain. "Writing for Video Game Genres: From FPS to RPG". A K Peters, Ltd., 2009.

[5] Craig Lindley. *"*Game Taxonomies: A High Level Framework for Game Analysis and Design*";* October 3, 2003. http://www.gamasutra.com/features/20031003/lindley_01.shtml

[6] Ben Sawyer and Peter Smith. "Serious Games Taxonomy"; Serious Games Initiatives, February 2008.

[7] Clark Aldrich. "Learning Online with Games, Simulations and Virtual Worlds". Jossey-Bass, 2009.

[8] Clark Aldrich. "The Complete Guide to Simulations & Serious Games". Pfeiffer, 2009.

[9] Brian Winn. "The Design, Play, and Experience Framework"; Handbook of Research on Effective Electronic Gaming in Education (Information Science Reference), Volume III, July 2008.

[10] G. Gunter, R. Kenny and E. Vick. "A case for a formal design paradigm for serious games"; The Journal of the International Digital Media and Arts Association, Volume 3, 93-105. 2006.