State-of-the-art simulation systems for information security education, training and awareness

Vicente Pastor
Electrical and Computer Department
UNED - Spanish University for Distance Education
Madrid, Spain
vicente.pastor@ieee.org

Gabriel Díaz and Manuel Castro
Electrical and Computer Department
UNED - Spanish University for Distance Education
Madrid, Spain
gdiaz@ieec.uned.es, mcastro@ieec.uned.es

Abstract—**This paper describes state-of-the-art simulation systems designed for information security and information assurance education, training and awareness. Being people the weakest link in the implementation of any security policy, it is of paramount importance to strengthen that link before it gets broken. The best way of improving the reactions of any person when security is attempted to be compromised is by providing him/her with better education, attractive practical training and raising the general awareness on information assurance.**

Keywords—information security; information assurance; network simulation; education; training; awareness.

I. INTRODUCTION

Information security has become one of the main priorities for governmental and private institutions. It has been shown in several occasions that a big amount of all security incidents is caused by human errors such as system misconfigurations, security policy breaches and careless systems administration. Since these actions were not done on purpose, most of them could have been avoided by improving the information security education of managers, the training of the system administrators and the general awareness of end users. Simulation systems are of great help for this task since they allow hands-on experience and user interaction. This sentence, attributed to Confucius, and also mentioned in [1], is self explanatory: "I see and I forget, I hear and I remember, I do and I understand".

This paper describes the results of a research on state-of-the-art simulation systems for information security and information assurance education, training and awareness. As first stage of the research, several of those systems have been identified and studied. The second stage makes an initial attempt to construct a taxonomy of the found simulators, following the one proposed by Saunders [1, 2] in which five distinct categories of simulation for information security are defined and described:

1. PacketWars
2. Sniffers + network design tools
3. Canned attack/defend scenarios
4. Management flight simulators
5. Role-playing

The found simulation tools have also been classified attending to their target audience, usability, learning curve required, level of detail, scalability, the possibility of being remotely used, etc.

The rest of the article is structured as follows. In section 2, brief descriptions on the research and on each of the found tools are provided. In section 3, the results of the proposed taxonomy are presented. Finally, the conclusion and possible future research are offered.

II. STATE-OF-THE-ART SIMULATION SYSTEMS

The current research has been performed by looking up different sources such as: IEEE magazines, IEEE Xplore Digital Library, ACM Digital Library, ISI Web of Knowledge, SpringerLINK Book Series, Google Scholar, Scientific Commons, Scirus, RefSeek or Scitopia, among others. Overall, more than one hundred references including journal and magazine articles, conference proceedings, technical reports, thesis reports, book sections, computer programs and web URLs have been obtained, classified and reviewed.

While other state-of-the-art reports on information security simulation focus on different aims of such simulations, the authors have special interest on information assurance and on the activities that allow transmitting the corresponding knowledge to the students. They have experience in both the education and private sectors in subjects directly related to information security. Within the University environment, the educational experience is directly related with grade and post grade subjects in Computer Science Engineering and Industrial Engineering at the Spanish University for Distance Education.

The education on information security subjects at University, when available, is most of the times mainly focused on theoretical issues. However, without an adequate practical teaching of information assurance matters, we are leaving the students with a weak knowledge that is not yet consolidated. The use of a security laboratory and/or a simulated network scenario is very beneficial as a mechanism for supporting active learning strategies such as: learning-by-doing, learning-by-example and learning-by-exploring.

While other forms of getting to the objective of simulating network security situations could also include adaptations, modifications or extensions to generic network simulators, in this article we have chosen to focus on the tools that are

978-1-4244-6571-2/10/$26.00 ©2010 IEEE April 14-16, 2010, Madrid, SPAIN
IEEE EDUCON Education Engineering 2010 – The Future of Global Learning Engineering Education

specifically designed having information security in mind. Nevertheless, some of these generic simulation tools and a description of their use for information security teaching can be found at: OPNET Modeler [3], OPNET IT Guru [4], OMNET++ [5] and ACME Studio [6].

Some of the analyzed tools are not specifically designed for an autonomous learning of information assurance aspects but are anyway included because they can be used to demonstrate certain concepts to the students even when the intervention of the trainer will be required in all cases.

Among all the simulation tools found during the research we are highlighting the following ones:

*A. **CyberProtect**, developed by US DoD's Defense Information Systems Agency (DISA) in conjunction with several entertainment software companies [7].*

CyberProtect is an old product. It has not been revised since July 1999. The product received several awards on its creation year: 1999 NewMedia Gold INVISION Award (Best Overall Design), 1999 NewMedia Gold INVISION Award (Technical Training) and 1999 International Cinema in Industry (CINDY) Competition Silver Award.

In spite of not being modified since 1999, the principles that guided its creation are still valid and the application is still fully functional. CyberProtect version 1.1 can still be obtained on CD from the Information Assurance Support Environment (IASE) of the US DoD's Defense Information Systems Agency (DISA) [7].

CyberProtect was developed as a training aid for novice network security professionals to familiarize them with information systems security terminology, concepts, and policy. It is an interactive computer network defensive exercise that provides the users with the opportunity of configuring network security features and running them against real world network security attacks. The users face a variety of security threats and must make practical decisions for allocating resources using the elements of risk analysis and risk management. CyberProtect simulates a complete fiscal year lifecycle of a simple computer network divided into four sessions. After each session, the user receives feedback on his/her performance. At the end of the last session, users are given a report detailing their cumulative scoring classifying the attacks by origin, type, and effectiveness.

*B. The Military Academy Attack/Defense Network (**MAADNET**) simulation designed by the Department of Electrical Engineering and Computer Science, United States Military Academy [8].*

The aim of this application is to simulate diverse aspects of building and managing an information system and combining them into an information assurance learning environment. MAADNET is built on a client-server architecture using the discrete events simulation (DES) paradigm. The user starts building a network on the client side in accordance with a given scenario that is then submitted to the server which will simulate different events. The user can build the network, enforce policies and employ more administrators. After that, several scenarios can be executed against the designed network in order to see how it behaves when attacked. After the simulation, the built network is evaluated in order to assess how well security was maintained.

The simulator was created for assisting in enhancing the quality of the Information Assurance courses offered to cadets of the US Military Academy. At a certain moment [9], MAADNET designers decided to take the option of collaborating and improve the work already completed by the creators of CyberProtect (see section A above). MAADNET was adopted by the US Defense Information Systems Agency (DISA) as an education tool for user, manager, and technician education.

The tool has been built using an Object Oriented Design with Java applets. It was also foreseen to be utilized as a web based application using Java Web Start technology. The server hosts the simulation engine, the attack scenarios and the evaluation mechanisms. On the other hand, the client hosts a scenario generator tool, a network builder and the simulation viewer. The simulation offered is a high-level one not providing all the details down to the network protocol level. The network is built using different components such as switches, routers, workstations, wireless access points, etc. Each of these components can have one or more traffic generators associated to it.

In order to generate realistic events, the Mean Time Between Failures (MTBF) is one of the parameters that could be configured for each of the entities. Also, the Mean Time To Repair (MTTR) is another parameter that can control the time that takes to put again the component into an operational status.

The defense strategy is static: once that the network has been built, it will not change during the simulation of the selected scenario. On the contrary, the attacks are dynamic in nature based on the specific scenario. The probability of an attack succeeding is a function of the type of attack and the skills of the attacker. Creating reliable and credible attack/defense models of an acceptable quality is the main challenge here. Attack trees and Petri nets have been used to model and represent the attacks within MAADNET. The modeled attacks can be from the Internet (outsiders), from an authenticated user (insiders) or from the wireless infrastructure (both outsiders and insiders).

*C. **CyberOps: NetWarrior**, developed from the above one by US DoD's Defense Information Systems Agency (DISA) [10].*

CyberOps: NetWarrior has been developed from the "Military Academy Attack/Defense Network (MAADNET)" simulation closing the evolution of the product line presented in the two previous sections. The main enhancements introduced are related to the improvement of the interactivity and a web based approach with better graphics.

The tool is an immersive 3D virtual environment, with realistic looking network equipment, similar to an interactive video-game, where the player (student) has to create a network within specific resource constraints. The student selects the security defensive tools and other options that are going to be

used on his/her network and then sequences of computer generated attacks are launched in order to assess the strength or the selected solution.

The evaluation performed by the tool takes into account parameters such as the utilization of specific security hardware and software, the policies and procedures in place, and the impact due to the (un)availability of the specialized information assurance virtual personnel, as well as their training, certifications and experience. Money is limited so the student needs to perform a cost/benefit analysis in order to make right choices when building the network. The students receive feedback that helps them to understand their success or failure in protecting the network. This feedback is dynamic and it is only related to the specific configuration selected by the student.

CyberOps can be used as academic classroom, technical training and computer network defense exercise support tool through a series of security roles such as NetBuilder, NetDefenser, NetAssurer and NetWarrior. Multi-player game has been enabled and students can group in Blue (defenders), Red (attackers) and White (referees) teams in an interconnected exercise.

*D. The cyber DEfense Technology Experimental Research laboratory (**DETERlab**) of the Information Sciences Institute of the University of Southern California [11].*

The DETERlab testbed uses the Emulab cluster testbed software developed by the University of Utah. It is a public facility whose utilization for information security research purposes can be requested by any principal investigator to the Emulab Approval Committee. Using DETERlab, a pool of experimental nodes can be controlled and interconnected in nearly-arbitrary network topologies.

The DETER testbed facility, from its inception in 2004, has not been aimed to be used for teaching objectives for users without a solid background in information assurance but for researches made by a relatively small experimental community. It could be anyway used for educational purposes provided that the target audience has the necessary level of knowledge. The DETERlab testbed has been used as a laboratory by university-level cyber-security classes.

DETERlab possess a model for dynamic federation that enables separate testbed facilities to come together on demand in order to support large-scale, complex, heterogeneous, multi-party experiments. In order to support such complex experiments, a tool has been developed for provide the researchers with the possibility of easily creating, planning and iterating through a large range of experimental scenarios: SEER (Security Experimentation EnviRonment) [12]. SEER comprises several tools for the configuration and execution of experiments and provides a user-friendly interface for the investigators. Some of those tools included in SEER are traffic generation tools, attack tools, network configuration tools, and data collection and presentation tools.

The main DETER aim is to be able to provide support for security experiments that are repeatable. This enables the researcher to repeat the experimental conditions accurately and to modify them only in a controlled manner. Currently the testbed is composed of two linked clusters: one at USC ISI and the other one at UC Berkeley, with around 300 experimental nodes at the moment of writing this article.

*E. **CyberCIEGE** from the Center for Information Systems Security Studies and Research of the US Naval Postgraduate School [13].*

CyberCIEGE is a high-end, commercial-quality video game developed jointly by Rivermind and the Naval Postgraduate School's Center for Information Systems Security Studies and Research [14]. The tool shows a simulation in which the student has to be the decision maker of an IT organization. The aim of the game is to protect the system by using appropriate security measures involving procedures, physical and technical security, while keeping the virtual users productive and pleased.

The number of different scenarios that can be played is unlimited since CyberCIEGE has been designed to be completely extensible. Apart from the simulation engine itself, CyberCIEGE includes a scenario definition language (with the corresponding definition tool - SDT) and a scenario development tool that enable creating completely new situations, and a context-sensitive video encyclopedia that serves as instructional aide.

Some of those new scenarios have also been developed within the Center for Information Systems Security Studies and can be obtained from [15].

CyberCIEGE is available at no cost to agencies of the US Government and there are also educational licenses available at no cost to educational institutions. Finally, there is a free evaluation version that has limited capabilities.

A comparison between the features offered by CyberCIEGE and the ones by CyberOps NetWarrior (see section C above) can be found at [16]

*F. NIST IPSec and IKE Simulation Tool (**NIIST**) [17, 18].*

NIIST is an integrated Internet security simulation framework developed by the National Institute of Standards and Technology (NIST). The tool has been implemented in Java and integrated in the Scalable Simulation Framework (SSF), a discrete, event-driven, scalable modeling framework, and SSF Network Model (SSFNet) [19], a collection of Internet modeling tools for simulating Internet protocols and networks. SSF is mainly focused in scalability and high-performance for large networks simulation.

While the main goal of NIIST is not to serve for the security education or training, but to characterize and study IPSec/IKE performance and its influence on end-to-end protocols such as TCP, it still could be used to teach the fundamentals of the Virtual Private Networks (VPNs) and IPSec.

*G. The Real-time Immersive Network Simulation Environment (**RINSE**) for Network Security Exercises of the Information Trust Institute of the University of Illinois at Urbana-Champaign [20].*

RINSE is a highly extensible simulator designed for large-scale, real-time cyber-security training and exercises. The simulator consists of five components: the iSSFNet network simulator, the Simulator Database Manager, a database, the Database Server, and client-side Network Viewers. The iSSFNet network simulator, which was previously known as DaSSFNet, is the latest implementation of the C++ network simulator based on the Scalable Simulation Framework (SSF) [19] mentioned and referenced in the previous section.

Every simulation entity connects to the Simulator Database Manager, which provides the data from the simulator to the database and delivers control information from the database to the simulator. The Database Server communicates with client applications, such as the Java-based application "Network Viewer", which allows the users to monitor and control the simulated network from the client side. From there, the user can issue several commands in order to influence the model behavior. These commands include five different types: attacks, defenses, diagnostics networking tools, device control, and simulator data.

As other simulators presented in the article, the type of educational target for this tool is aimed at large-scale network exercises. However, it still can be used for smaller security training scenarios in order to teach specific information assurance issues on a network.

RINSE has evolved into a more complex and generic network simulator: PRIME (Parallel Real-time Immersive network Modeling Environment) for large-scale real-time network simulation [21]. PRIME is a project of the Modeling and Networking Systems Research Group within the School of Computing and Information Science of the Florida International University that has also been used for information security studies such as attacks in routing environments [22].

*H. The Reconfigurable Cyber-Exercise Laboratory (**RCEL**) for Information Assurance Education at the Center for Information Systems Security Studies and Research of the US Naval Postgraduate School [23].*

RCEL is the result of a Master's Thesis developed by R. J. Guild within the US Naval Postgraduate School in 2004. The thesis describes the laboratory as a "flexible collection of equipment that can be quickly interconnected and configured" [23] and illustrates six practical scenarios with different learning objectives. These scenarios provide the students with the opportunity of participating in all phases of the security lifecycle: analysis, design, construction and operation. The lab configuration can be quickly changed in order to be used for different activities. In this case, the author proposes the use of Symantec Ghost to create images of pre-configured stations that could then be rapidly deployed when required.

The lab is composed of several stations each of which are specialized in one network function, such as: authentication, domain controllers, DNS server, DHCP server, FTP server, PKI Certification and Registration Authorities, syslog server, e-mail server, web server, database server, disk images storage server, wireless access points, honeynet, vulnerability assessment (VA), switches, routers, firewall, Intrusion Detection System (IDS) and Virtual Private Network (VPN) devices. One lab can be interconnected to another remote one using a public network by means of a VPN. Whether interconnected to another remote lab or not, the main idea for each learning exercise is that part of the LAN (or a complete VLAN) is acting as attacker while other parts act as defenders.

Probably virtualization, while existing, was not so widely spread when this thesis was written. If we would like to build a similar laboratory today we would most likely use virtualization instead of having dedicated specialized stations for each of the network functions. The maturity of virtualization and the processing power of current hardware allow doing so with an acceptable performance as we can see in the system presented in the following section.

*I. **Tele-Lab "IT Security"** from the Hasso-Plattner-Institut für Softwaresystemtechnik GmbH at Postdam, Germany [24].*

Tele-Lab "IT Security" is a web-based tutoring system that introduces students to fundamental IT security concepts and provides an on-line virtual laboratory for them to be able to gain practical experience.

The system leverages virtual machine technology for using a single host system as many different machines at the same time and to assign a remote machine to a student providing him/her with administrator rights without jeopardizing the stability and security of the training system.

Tele-Lab is implemented by using User-Mode Linux. Users manage the virtual machines by means of a connection that uses the Virtual Network Computing (VNC) client application.

*J. The Network Security Simulator (**NeSSi2**) developed at the DAI Laboratory, part of the School of Electrical Engineering and Computer Science of the Berlin Institute of Technology, and sponsored by Deutsche Telekom Laboratories [25, 26, 27].*

NeSSi2 is an open source discrete event network simulator, published under the Apache 2.0 license, incorporating several security-related capabilities that makes it different from the general purpose simulators, such as profile-based automated attack generation, traffic analysis and interface support for the plug-in of detection algorithms. The plug-in concept allows the functionality extension without changing the simulation core itself. Theses extension mechanisms allow three different levels of abstraction: application, network and device level.

NeSSi2 is built on the JIAC framework [28], a service oriented architecture based on agents. Agents are used in NeSSi2 for modeling and implementing the network devices such as routers, clients, and servers. JIAC agent framework provides a rich and flexible basis for the implementation and testing of diverse security configurations and algorithms in NeSSi2 that allows combining the partial knowledge of the

agents residing in the network, in a cooperative approach for identifying and eventually eliminating IP-based threats.

NeSSi2 consists of a simulation back-end, a front-end (Graphical User Interface – GUI) and a database management system hosting the results database. The back-end and the frontend are available for download, for Windows, Linux and Mac OS, at NeSSi2 website [26]. For the database management system, NeSSi2 developers recommend MySQL but SQLite is also supported. The simulator has been built using Java SE 6. The subnets, the network elements and their properties, have been modeled using the Eclipse Modeling Framework (EMF) [29] which also enables automated source code generation and, thus, the model can easily be extended.

*K. **S-vLab**, an experimental environment for teaching Java security developed at the University of Bologna, Italy [30, 31].*

S-vLab is a virtual laboratory for supporting teaching and learning in different domains. Among them, S-vLab can also be applied to the information security area, being one of its main goals helping students in understanding the Java Security Platform.

The tool provides a graphical editor and a set of building blocks that are suitable for designing a simplified version of a system or protocol. In order to test and assess the efficacy and the strength of the proposed solution, students are able to simulate attacks. When playing the attacker role, students improve their knowledge on how to analyze systems for weak points, how to choose designs that prevent these flaws, and how to deploy defenses.

*L. A Windows Attack intRusion Emulator (**AWARE**) from Fairmont State University [32].*

AWARE is an emulator built on Microsoft Windows XP and for Windows XP users. Its main aim is teaching those users to detect potential attacks using the XP included tools and to remediate the effects of those attacks. Some of the XP emulated tools include: the Process List inside the Task Manager, the Registry Editor (regedit), a visual version of netstat (in order to search for unusual port traffic) and a limited version of the Windows Firewall log.

The system also includes built-in tutorials that help the user in understanding the tools, how to use them, how they look like, etc. At the end of the simulation, the user is presented with an evaluation of the results obtained with an indication on how well he/she did.

The emulator tries to change users' passives attitudes and to provide them with the possibility of counteracting future attacks. Previous computer security knowledge is not required.

*M. **RADICL**: A Reconfigurable Attack-Defend Instructional Computing Laboratory from the Department of Computer Science of the University of Idaho [33].*

RADICL is a highly reconfigurable laboratory which main objective is to enable students to understand attack scripts and other malware and to use defensive strategies and tools. It has been designed and developed by senior and graduate students in Computer Science, Computer Engineering, and Mathematics.

The requirements include switching operating systems on each laboratory machine and reconfiguring the network topology in less than four minutes. In twelve minutes, starting from machines without partitions and without operating systems installed, RADICL can be completely configured and ready to run.

The laboratory comprises sixteen workstations with dual NICs and one Xeon server that hosts the OS images. Each of the workstations is partitioned into nineteen segments with the same size in order to provide multi-OS booting. The different networks are separated by using VLANs. Most RADICL activity does not require advanced networking. A KVM switch allows the control of any of the seventeen machines in the laboratory. The central image server consolidates all RADICL capabilities into a single web-based front end making unnecessary moving hardware or unplugging and plugging cables and devices.

Further development has been made in order to extend the capabilities of the original RADICL lab. For example, Team 54 of the Computer Science Department of the University of Idaho has extended the project and renamed it as Vrad LAB [34]. Among other improvements we can find the use of virtualization by means of VMware which enables the possibility of running up to 16 virtual machines concurrently, the central storage of operating system images on a server, the possibility of running multiple isolated experiments and the remote access to the lab.

Not all the analyzed tools are easily accessible; therefore not all of them could be tested, as it was the authors' intention. It appears that it would be a good idea to have more open source, freeware and/or inexpensive developments in this area and specifically individual tools that allow easily good performance training. Within the Electrical and Computer Department of the Industrial Engineering School of UNED (Spanish University for Distance Education) there are several efforts in order to provide such tools not only for the students but also for the general public.

One of those applications is the information security didactical system presented at [35] that comprises two different tools: a network attack simulator and an intrusion detection system, IDS. Both tools share a usable and really friendly interface, and are distributed as a kit that can be easily installed by the student in any computer, since the system is open-source and multi-platform. The system has been developed in Java using Eclipse IDE. The system allows two types of users: the student that wants to explore more in detail the way an IDS works, and the collaborator who would like to extend the system by adding new features, such as new attacks and new signature attacks for the IDS.

Another example is fragSim [36], an interactive simulator for studying the IP fragmentation process that is in the process of being extended to include extra functionality. fragSim is a completely web based network simulator developed for the Adobe Flash framework. This makes possible to have access to

the simulator from almost any imaginable platform with the only pre-requisites of being connected to the Internet and having a web browser with the Adobe Flash plug-in installed. The simulator allows a degree of user interactivity where the user is able to define the desired network topology, the value for the Maximum Transmission Unit (MTU) on each of the links and the size for the telecommunications protocol stack upper layer messages that will be fragmented. The application has also been built to be graphically attractive in order to positively influence the user learning experience while capturing user attention. fragSim has been in use during the academic year 2008/2009 by the students of two subjects within the Industrial Engineering School of UNED (Spanish University for Distance Education): "Industrial Communications" at 5th course of the MSc in Industrial Engineering, and "Industrial Communications Networks" at 3rd course of the BSc in Industrial Engineering. Unfortunately, it is still soon to have enough student evaluations in order to assess their perception when using fragSim, but the tool will continue to be available to the same students on following academic years and it is planned to expand the usage to other computer network and communications courses. It is expected to receive valuable feedback that allows the implementation of improvements and new features.

III. TAXONOMY

Saunders [1, 2] produces a taxonomy by classifying the information security simulators in five distinct categories: PacketWars, Sniffers + network design tools (also named Flexible Network Design in other parts of his document), Canned attack/defend scenarios, Management flight simulators, and Role-playing.

PacketWars refers to a type of simulation that utilizes network attack and defense at a tactical level. Most of the simulators in this category are implemented in real networks with real equipment but not necessarily all of them due to the benefits of simulation and/or virtualization. The network infrastructure used to organize annual Cyber Defense Exercises (CDX) by governmental/military authorities, such as the ones organized by the US National Security Agency (NSA) [37] or the North Atlantic Treaty Organization (NATO) [38], will also fall into this category.

Sniffers + network design tools category comprises the tools that combine the use of Network Modeling and Simulation (NMS) packages with the use of network protocol analyzers (also known as sniffers). In this category, the tools mentioned in the introduction of section 2 [3-6], would be included. In this article, we have also included tools that work as a generic NMS but are specialized in information security modeling.

Canned attack/defend scenarios includes most of the tools analyzed in this article. According to Saunders, here we refer to simulators that are typically standalone and can be used as a game. As we have seen in the previous section, some of them have evolved incorporating the possibility of connecting to other remote "players" or being remotely managed. Therefore, not all of them are completely standalone applications.

Management flight simulators are, according to Saunders, applications built using a System Dynamics or a Discrete Event Simulation (DES) tool. However, in the research, we have not considered the requirement in this statement to be essential and, following [1, 2], the key feature considered for including one of the simulators in this category is the management of resources (money, personnel, devices, etc.) during the simulation, regardless of the tool used to develop the system or its use only by managers or directors.

Role-playing is a type of simulation that does not employ computer-based simulations but, as it can be easily inferred, actors playing different roles within a given scenario. In this area, the Cyber Defense Exercises mentioned before, in their part related to the strategic level decisions, would be included.

Taking into account these descriptions, the simulators analyzed in this article have been classified in Table I:

TABLE I. CLASSIFICATION UNDER SAUNDERS CATEGORIES

Simulator Name	Category
CyberProtect	Canned Attack/Defend Scenarios
MAADNET	PacketWars
CyberOps: NetWarrior	Canned Attack/Defend Scenarios
DETERlab	PacketWars
CyberCIEGE	Management Flight Simulators
NIIST	Not applicable
RINSE	PacketWars
RCEL	PacketWars
Tele-Lab "IT Security"	PacketWars
NeSSi2	Sniffers + Network Design Tools
S-vLab	PacketWars
AWARE	PacketWars
RADICL	PacketWars

As Table I shows, most of the tools analyzed in this article fall under PacketWars category. Saunders' classification was done with the aim of assisting in making a decision about the level of effort that would be needed to get started in the information security simulation world. However, the presented categories do not provide per se the intended knowledge to serve as assistance for making a decision; nevertheless, the required knowledge can be inferred from [1, 2], specially from the categories comparison table included there.

Therefore, in this article, the taxonomy has been broken down into several distinct tables. On the first two (tables II and III), the general technical features of the analyzed tools will be presented while, on the other two (tables IV and V) the focus will be put on the features related to the teaching and didactical capabilities of the tools.

TABLE II. TECHNICAL FEATURES

Simulator Name	Type	Remotely usable	Virtualization
CyberProtect	Simulator	No	No
MAADNET	Simulator	Client/Server Architecture	No
CyberOps: NetWarrior	Simulator	No	No
DETERlab	Laboratory	Yes (using a XMLRPC API)	Yes
CyberCIEGE	Simulator	No	No
NIIST	Simulator	No	No
RINSE	Simulator	It can be interconnected to real-world networks	No
RCEL	Laboratory	It can be connected to external organizations by means of a VPN	No
Tele-Lab "IT Security"	Laboratory	Yes	Yes
NeSSi2	Simulator	Yes (installing the frontend on a different machine)	No
S-vLab	Laboratory	Yes	Yes
AWARE	Emulator on Windows XP	No	No
RADICL	Laboratory	Web interface configuration	Yes

Type indicates the type of analyzed tool. Most of them are simulators, some of them are laboratories and we have an instance of an emulator.

The second column indicates if the tools can be remotely managed/operated.

The third column shows the virtualization capabilities of the tools.

Table II shows how analyzed tools have been classified into three types. Many of them are simulators: computer applications that reproduce the system behavior under certain specific conditions. One of them could be classified as an emulator: a computer application that models a system accurately, mimicking its actions and trying to exactly match the same behavior as the real system. The third type is for computer laboratories: sets of real devices typically separated from the production networks, and which main objective is to perform experiments in a controlled environment.

Regarding the capability of being remotely used, we have found tools that can be managed via web, by means of a custom made client/front-end, using an Application Programming Interface (API), and even connecting to real-world networks, or the ones that do not have any of these possibilities.

Finally, in table II we have classified the tools by indicating which ones use virtualization and which ones not. Virtualization is a technique that allows partitioning a single physical machine into several virtual machines that typically can run different instances of the operating system, not being necessary that those instances are identical or even of the same operating system.

TABLE III. TECHNICAL FEATURES (CONTINUED)

Simulator Name	Standalone	Scalability	License
CyberProtect	Yes	Limited by HW features	Unclassified application available at no cost
MAADNET	No	Limited by HW features	Not available outside USMA
CyberOps: NetWarrior	Yes	Good (by means of new scenarios)	Unclassified application available at no cost
DETERlab	No	Excellent (DETER Federation)	Public use. Projects under a principal investigator previously authorized by Emulab Approval Committee
CyberCIEGE	Yes	Good (by means of new scenarios)	Commercial. No cost for US Government or Education Institutions (also outside US). Free evaluation coy available
NIIST	Yes	Not applicable	Open Source
RINSE	No	Excellent	Open Source (PRIME SSF and PRIME SSFNet)
RCEL	No	Fair (by adding more machines or by interconnecting with other labs)	Not available outside NPS
Tele-Lab "IT Security"	No	Very good	Open Source
NeSSi2	Yes	Excellent	Open Source
S-vLab	No	Unclear	Open Source
AWARE	Yes	Not applicable	Unknown
RADICL	Yes (the network lab is not connected to other networks)	Fair (by adding more machines)	Available only at the University of Idaho

Standalone indicates whether the analyzed tool is/can be installed on a single machine.

The second column gives an indication of the growing capacity of the tool.

The third column expresses the type of license under which is distributed the tool.

In Table III, the tools have been classified as standalone or not. A standalone application is one that can run without a network connection on a single system. Please note that RADICL has been classified as standalone but taking into

account that the whole laboratory itself is not connected to networks other than its internal one.

On the second column, a classification measuring the level of scalability of the solution has been presented. The scalability is the property that allows expressing the growing ability of the tool both in terms of handling increasing amounts of tasks and in terms of being readily enlarged. A scale with values: poor, fair, good, very good and excellent has been used.

The last column on this table indicates the type of license used for the tool distribution, if any. Note that some of the laboratories (MAADNET, RCEL and RADICL) can only be used on the premises where the lab is installed since they also do not have the possibility of being remotely managed.

There are not many tools that are ready to be used for standalone study. This is of paramount importance for the typical student of an Open University. Further development on such tools and/or simulators in-the-cloud would be desirable.

Also, while we found some tools that are open source, for public use or at no cost for educational institutions, it would be worthy to count on further efforts on this area.

Finally, it is necessary to remark that all of the tools found are in English, while it was expected finding some tools completely translated into other widely spread languages, such as Spanish. S-vLab web site and documentation is in Italian.

TABLE IV. DIDACTICAL CAPABILITIES

Simulator Name	Target Audience	Teaching Objectives	Learning Curve
CyberProtect	Novice network security professionals	Generic information security training	Fast
MAADNET	US Military Academy cadets	Generic information security training	Fast
CyberOps: NetWarrior	Information Assurance Students	Generic information security training	Fast
DETERlab	Academic and industrial cybersecurity researchers	Teaching is not the main target. It has been used as a laboratory by university-level cyber-security classes	Slow
CyberCIEGE	Information Assurance Students	Information assurance basics. Risk management. Resource management	Fast
NIIST	Researchers of new and existing intenet security technologies, protocols or	Research and evaluate the dynamic behavior of an interacting suite of security	Slow
	protocol mechanisms	protocols in large scale VPNs	
RINSE	Experienced network security professionals	Large-scale, real-time cyber-security training and exercises	Unclear
RCEL	Information Assurance Students with a profound technical background	Support of an information assurance education program	Moderate
Tele-Lab "IT Security"	Information Assurance Students with minimum previous knowledge	Many different subjects. Basic level	Moderate
NeSSi2	Computer Science students and professionals	Detailed examination and testing of security-related network algorithms, detection units and frameworks	Moderate
S-vLab	Students of 4º course in a 5 years degree	Java Security	Fast
AWARE	Windows XP users	Detect potential attacks and remediate the effects using Windows XP built-in tools	Fast
RADICL	Information Assurance and Computer Engineering Students	Understanding attack scripts and other malware	Moderate

The target audience column shows the expected main "customers" for the tool.

The second column provides a description of the main topics that the tool could be demonstrating to a potential student.

The third column depicts the speed of the learning process from the moment that the tool starts to be used.

In Table IV, as target audience we have mainly found information assurance students within computer science courses/degrees. However, the complexity of the tools makes some of them unreachable for people without a solid background in networking and information security. It is remarkable that there is one tool (AWARE) that is clearly targeted to users with only a basic knowledge on using their personal computers. The authors have tried to obtain the tool from the developers for further assessment without response so far.

The learning objectives cover a wide range of completely different possibilities. While some tools' aims are deliberately high-level, specific ones, due to their focus on large-scale, complex experiments, many of the analyzed tools show

different levels of generic information security training even appropriate to novice students. Those complex ones are not suitable for being used as starting point for teaching information security.

At learning curve column, an indication on the level of effort required for the student to be able to use the tool at an acceptable level of efficiency is shown. The use of the term "steep" has been intentionally avoided since sometimes has different interpretations. The used values are: slow, moderate and fast, being "slow" the one that shows more difficulties in reaching the target and "fast" the one with fewer difficulties.

TABLE V. DIDACTICAL CAPABILITIES (CONTINUED)

Simulator Name	Usability	Level of Detail
CyberProtect	Very good	Fair
MAADNET	Very good	Fair
CyberOps: NetWarrior	Excellent	Good
DETERlab	Good	Excellent
CyberCIEGE	Excellent	Good
NIIST	Fair	Very good
RINSE	Good	Good
RCEL	Good	Excellent
Tele-Lab "IT Security"	Good	Unclear
NeSSi2	Very good	Excellent
S-vLab	Good	Fair
AWARE	Very good	Fair
RADICL	Good	Very good

The usability denotes the ease with which the students can employ the analyzed tools in order to achieve the learning targets.

The second column shows how complex is the tool and how accurately represents the real system.

Finally Table V shows, for the usability, the values poor, fair, good, very good and excellent have been chosen, being "poor" the value that express a condition in which the student hardly can utilize the tool for achieving the objective without a considerable effort, and "excellent" the situation where the student start receiving benefits from the learning action from the very beginning.

The level of detail is related to the didactical capacity since it indicates the fidelity of the abstraction that the tool provides. It has to be noted that the closer to the real system, the higher the level of detail, but also the bigger the effort required. The values are exactly the same as the ones in the previous paragraph with a similar meaning.

As a final point, it can be added that it would be desirable to have more tools for students without previous experience in information assurance issues and covering diverse related aspects.

CONCLUSION

Not all the security simulators found and analyzed in this article are mainly developed having information security education, training and/or awareness in mind. However, most of them can be used in the purpose of illustrating different information assurance concepts and ideas. It would be desirable, anyway, that new tools were developed with a focus on enabling information assurance concepts teaching, not only for university students but also for anyone interested professionally in these subject matters. We think also that these tools must be extremely easy to use and also individualized, allowing a deep understanding of the concepts by doing "experiments" in the students' own environment. In that sense, we are developing an effort to create an integrated toolset of information security training tools, in order to illustrate different aspects of the subject matter and we are also evaluating which of the analyzed tools in this paper could be part of this toolset.

When the tools research was started it was expected not to find many. Even when the number of identified efforts is non negligible, it can be stated that there is still a long way to be followed until finding an acceptable diversity in this kind of tools covering every information assurance aspect that needs to be taught. Therefore, further developments in this area are going to be, for sure, warmly welcomed by the education community.

ACKNOWLEDGMENT

The authors would like to acknowledge to the European Union Socrates the support in the IPLECS Project – Internet-based Performance-centered Learning Environment for Curricula Support Project ERASMUS 141944-LLP-2008-1-ES-ERASMUS-ECDSP as well as in the Project 142788-2008-BG-LEONARDO-LMP mPSS – mobile Performance Support for Vocational Education and Training Project.

REFERENCES

[1] J. H. Saunders, "The Case for Modeling and Simulation of Information Security". National Defense University. Accessed December 2008. http://www.johnsaunders.com/paper/securitysimulation.htm

[2] J. H.Saunders, "Modeling the Silicon Curtain," SANS Institute, 2001.

[3] J. Ryoo, P. Altoona, and T. Oh, "Teaching IP Encryption and Decryption Using the OPNET Modeling and Simulation Tool," Proceedings of the 12th Colloquium for Information Systems Security Education, 2008, p. 113–118.

[4] G. Corral, A. Zaballos, and C. Canet, "Proposal of new challenge labs for the OPNET IT Guru Academic Edition," OPNETWORK'2004, Washington: 2004.

[5] A. Ahman, and S. Hassan, "Network Security Simulation using OMNET++," Proceedings of the Malaysian Government Open Source Software Conference, MyGOSSCON 2008, November 5-6, Putrajaya, Malaysia, 2008. Accessed October 2009. http://mygosscon.oscc.org.my/2008/index.php/papers?task=viewcategory&catid=22

[6] B. Schmerl, S. Butler, and D. Garlan, "Architecture-based Simulation for Security and Performance". School of Computer Science, Carnegie Mellon University, Pittsburgh, USA.

[7] IA Education, Training and Awareness Online Training Catalog of the Information Assurance Support Environment (IASE) of the US DoD's Defense Information Systems Agency (DISA), Accessed October 2009. http://iase.disa.mil/eta/online-catalog.html

[8] J. R. Surdu, J. M. D. Hill, R. Dodge, S. Lathrop, C. A. Carver, "Military Academy Attack/Defense Network Simulation". Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, USA, 2003.

[9] J.M. Hill, J.R. Surdu, S. Lathrop, G. Conti, and C.A. Carver Jr, "MAADNET NetBuilder: A Service/Demand Focused Network Simulator," 2003 International Conference on Simulation and Multimedia in Engineering Education (ICSEE'03), Communication Networks and Distributed Systems Modeling and Simulation (CNDS 2003), part of the Western MultiConference on ComputerSimulation (WMC'03), Orlando, Florida, 2003.

[10] B. Duffy, "Network Defense Training through CyberOps Network Simulations". In Proceedings of the Modeling, Simulation, and Gaming Student Capstone Conference 2008. April 9, 2008, Norfolk, Virginia.

[11] Information Sciences Institute, University of Southern California, "DETERlab Testbed". Accessed August 2009. http://www.isi.edu/deter/

[12] S. Schwab, B. Wilson, C. Ko, and A. Hussain, "SEER: A Security Experimentation Environment for DETER," Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007, USENIX Association, 2007.

[13] C. E. Irvine, M. Thompson, "Teaching Objectives of a Simulation Game for Computer Security". Center for the Information Systems Studies and Research, Naval Postgraduate School, Monterey, USA, 2003.

[14] C. Irvine, M. Thompson, and K. Allen, "CyberCIEGE: Gaming for Information Assurance," IEEE Security and Privacy Magazine, vol. 3, 2005, pp. 61-64.

[15] CyberCIEGE website. Accessed October 2009. http://cisr.nps.edu/projects/cyberciege.html

[16] Note from the Center for the Information Systems Studies and Research of the Naval Postgraduate School on a "Comparison Between CyberCIEGE and CyberOps NetWarrior", dated September 14, 2009. Accessed October 2009. http://cisr.nps.navy.mil/cyberciege/CyberCIEGEvsNetWarrior.pdf

[17] NIST IPSec and IKE Simulation Tool (NIIST). Accessed October 2009. http://www.antd.nist.gov/niist/

[18] O. Kim, D. Montgomery, "Behavioral and Performance Characteristics of IPsec/IKE in Large-Scale VPNs", Advanced Network Technologies Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, USA, 2003.

[19] Scalable Simulation Framework (SSF) and SSF Network Model (SSFNet). Accessed October 2009. http://www.ssfnet.org

[20] M. Liljenstam, J. Liu, D. Nicol, Y. Yuan, G. Yan, and C. Grier, "RINSE: the real-time immersive network simulation environment for network security exercises," Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, IEEE Computer Society, 2005, p. 128.

[21] PRIME Project web site. Accessed October 2009. https://www.primessf.net/bin/view/Public/PRIMEProject

[22] Y. Li, M. Liljenstam, and J. Liu, "Real-time security exercises on a realistic interdomain routing experiment platform," 23rd ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation (PADS'09). Lake Placid, New York, June 22-25, 2009. pp. 54-63.

[23] R. J. Guild, Thesis "Design and Analysis of a Model Reconfigurable Cyber-Exercise Laboratory (RCEL) for Information Assurance Education". Naval Postgraduate School, Monterrey, California, USA, 2004.

[24] J. Hu, C. Meinel, and M. Schmitt, "Tele-lab IT security: an architecture for interactive lessons for security education," Proceedings of the 35th SIGCSE technical symposium on Computer science education, ACM New York, NY, USA, 2004, p. 412–416.

[25] R. Bye, S. Schmidt, K. Luther, and S. Albayrak, "Application-level simulation for network security," Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems, Gent, Belgium: ICST, 2008.

[26] NeSSi2 website. Accessed October 2009. http://www.nessi2.de/

[27] J. Chinnow, R. Bye, S. Schmidt, K. Bsufka, S.A. Camtepe, and S. Albayrak, "An Extensible Simulation Framework for Critical Infrastructure Security," DAI Laboratory, School of Electrical Engineering and Computer Science of the Berlin Institute of Technology, Technical Report: TUB-DAI 09/09-1, September 14, 2009.

[28] S. Fricke, K. Bsufka, J. Keiser, T. Schmidt, R. Sesseler, and S. Albayrak. "Agent-based telematic services and telecom applications". Communications of the ACM, 44(4):43–48, April 2001.

[29] Eclipse Modeling Framework (EMF) website. Accessed October 2009. http://www.eclipse.org/modeling/emf/

[30] A. Riccioni, E. Denti, and R. Laschi, "An experimental environment for teaching Java security," Proceedings of the 6th international symposium on Principles and practice of programming in Java - PPPJ '08, 2008, pp. 13-22.

[31] S-vLab. Website of the course on Information Security, University of Bologna. Accessed October 2009. http://lia.deis.unibo.it/Courses/TecnologieSicurezzaAK/S-vLab.html.

[32] D. L. Tobin Jr., M. S. Ware, "Using A Windows Attack intRusion Emulator (AWARE) to Teach Computer Security Awareness". In Proceedings of the 10th annual SIGCSE conference on Innovation and technology in computer science education, pp. 213-217. 2005, June 27-29, Monte de Caparica, Portugal

[33] S. Caltagirone, P. Ortman, S. Melton, D. Manz, K. King, and P. Oman, "RADICL: A Reconfigurable Attack-Defend Instructional Computing Laboratory," International Conference on Security and Management Las Vegas, NV, USA, June 20-23, 2005.

[34] VRAD Lab Project. Codename: LeapFrog, University of Idaho. Accessed October 2009. http://www2.cs.uidaho.edu/~cs481-54/

[35] H. Menéndez and G. Diaz, "Individualized tools for Information Security Learning: Attack Simulator and Intrusion Detection System", Proceedings of the XI International Symposium on Computers in Education, Coimbra, Portugal, November 2009.

[36] V.J. Pastor Pérez, "Simulador interactivo para el estudio de la fragmentación de datagramas IP," Master's Thesis, ETS de Ingenería Informática, Universidad Nacional de Educación a Distancia (UNED) 2007. Accessed October 2009. http://www.vicentepastor.es/fragSim, http://www.thesis.es/index.php/fragsim

[37] National Security Agency (NSA) Press release, "West Point Takes the NSA Cyber Defense Trophy for the Third Straight Year", Fort George G. Meade, Maryland 20755-6000, April 28, 2009. Accessed October 2009. http://www.nsa.gov/public_info/press_room/2009/cyber_defense_trophy.shtml

[38] Myrli, S. (Norway) Rapporteur, NATO Parliamentary Assembly, Sub-Committee on Future Security and Defence Capabilities, NATO and Cyber Defence, Draft Report, 173 DSCFC 09 E, September 3, 2009, p. 11