World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:6, No:7, 2012

Cyber Warriors for Cyber Security and Information Assurance- An Academic Perspective

Ronald F. Gonzales, Gordon W. Romney, Pradip Peter Dey, Mohammad Amin, Bhaskar Raj Sinha

***Abstract*—**A virtualized and virtual approach is presented on academically preparing students to successfully engage at a strategic perspective to understand those concerns and measures that are both structured and not structured in the area of cyber security and information assurance. The Master of Science in Cyber Security and Information Assurance (MSCSIA) is a professional degree for those who endeavor through technical and managerial measures to ensure the security, confidentiality, integrity, authenticity, control, availability and utility of the world's computing and information systems infrastructure. The National University Cyber Security and Information Assurance program is offered as a Master's degree. The emphasis of the MSCSIA program uniquely includes hands-on academic instruction using virtual computers. This past year, 2011, the NU facility has become fully operational using system architecture to provide a Virtual Education Laboratory (VEL) accessible to both onsite and online students. The first student cohort completed their MSCSIA training this past March 2, 2012 after fulfilling 12 courses, for a total of 54 units of college credits. The rapid pace scheduling of one course per month is immensely challenging, perpetually changing, and virtually multifaceted. This paper analyses these descriptive terms in consideration of those globalization penetration breaches as present in today's world of cyber security. In addition, we present current NU practices to mitigate risks.

***Keywords*—**Cyber security, information assurance, mitigate risks, virtual machines, strategic perspective.

I. Introduction

THIS paper presents the National University's MSCSIA plan to effectively teach students in a virtual computing environment using virtual machines. Despite the world becoming increasingly connected, there still remain vast vulnerabilities associated with our ability to secure our future. We have seen global cyber security players maliciously attack even the most secure facilities. The public and private sectors are yet more vulnerable with the newest generation of mobile devices [1]. Identifying cyber risks and participating with those standards at both the government and industry level continues to be the basis of establishing a curriculum of learning for the MSCSIA program.

The development of the VEL permits qualified students to pursue high levels of practical cyber skills both with onsite instruction and with online instruction. Student enrollment is organized as classes of 25 that are placed in cohorts.

Ronald F. Gonzales, Gordon W. Romney, Pradip Peter Dey, Mohammad Amin and Bhaskar Raj Sinha are with National University, 3678 Aero Court, San Diego, CA 92123, USA. They are now with the School of Engineering, Technology and Media (phone: 858-309-3412; fax: 858-309-3420; e-mail: rgonzales@nu.edu; gromney@nu.edu; pdey@nu.edu; mamin@nu.edu; bsinha@nu.edu)

The MSCSIA program currently offers 5 start points per year. Three online cohorts and two onsite cohorts represent our current levels of MSCSIA enrollment. Since the beginning of the program in February, 2011 with 22 students, we now have 110 students as of February,. 2012. Enrollment has been successful from students participating from all over the world. We have adopted the motto that, "IP is our campus".

We are committed to increasing our ability to offer additional cohorts and to contribute our share of well-prepared students to fight against cybercrimes. We appropriately call our students, "Cyber Warriors". This paper is a documentation of their successes, the VEL function, curriculum design, asynchronous classroom instruction and testing. The National University, School of Engineering, Technology, and Media (SETM), MSCSIA program is focused on qualifying as a National Security Agency and Department of Homeland Security jointly sponsored Center of Academic Excellence in IA Education (CAE/IAE).

II. Background

The SETM Cloud Infrastructure (SCI) consists of two computing environments operating inside a Palo Alto Firewall that is connected to the Internet, a) the Virtual Education Laboratory (VEL) production environment that provides virtual instruction tools for educational computing lab exercises and projects, and b) a Cyber Security Research environment. The SCI is designed to meet NIST information assurance controls specified in SP 800-53A.

The VEL is a product suite based on VMware virtualization that enables users "on-line" access to virtual classroom and laboratory computing resources that requires two-factor authentication and IPSEC/SSL connectivity from any location with Internet access. The Cyber Security Research environment consists of hardware and software largely contributed by industry collaborators, members of the NU Cyber Security and Information Assurance (CSIA) initiative that makes use of identical VMware virtualization technology when needed for compatibility purposes.

III. Product Description

The VEL is configured to provide academic institutions with the ability to deliver computer science, information technology and cyber security laboratory learning objectives to students participating in classroom or on-line courses.

The VEL has unique capabilities which include:

- Virtualized hardware environment
- State-of-the-art Firewall protection
- Multiple factor authentication protocol support
- State of the Art, Threat Prevention Identification

- URL filtering to ensure institutions are safeguarded from student actions
- Independent Security Zone settings; support for multi-purpose enclaves
- Security Zone – DMZ like enclave for websites and other public facing servers
- Fault Tolerant Administrative Server Configurations
- Windows and Linux Virtual Machines for Students
- Support for multiple ISP internet connections
- Secure sandboxes for class projects
- Simultaneous Support for multiple student cohorts/class strings

IV. Usage Examples For The SETM Cloud Infrastructure- VEL

A. Production Examples

The VEL provides educational institutions the ability to grant secure student access to virtualized computing platforms using VMware ESXi v5.0 in such a way as to provide an on-line computing and networking laboratory experience. Several hundred virtual machines are currently operational and are assigned to faculty and students functioning in both in-classes as well as on-line instruction. This allows students to access multiple computing resources from the convenience of their home, work, or kiosk environment. Cyber security students currently deployed to Bahrain and Iraq regularly access their VM's in the VEL. The VEL functions at a 1Gbps internal bandwidth over public Internet at a minimum of 50Mbps and is the production component of the SCI. Specific examples of the type of academic exercises in the production component that can be set up using this configuration include:

1) Red/Blue team cyber exercises
2) Penetration testing scenarios
3) Simulation of a Multi-Domain / Multi-Corporate WAN/LAN Convergence and the required / recommended Security Posture.

B. SCI Research Examples

The SCI and SCI research were designed to meet the requirements of a) academic research, b) industrial and healthcare research, and c) Department of Defense (DoD) contractor research. The SCI is designed to meet NIST and DoD standards in order to facilitate collaboration with DoD contractors in joint research projects. Security policy is established and a SETM Security Team meets regularly under the direction of a Security Officer. This facility is designed to meet NSA/DHS Center of Academic Excellence in Research designation and is proceeding to so qualify in 2013. Specific examples of research projects currently being pursued are the following:

1) Stealth (Unisys ©) technology, a first for any academic institution, that uses a FIPS 140-2 secure personal authenticator device
2) ITsME personal authentication
3) Red, White and Blue Team interaction data capture

V. Administrative Functions

The VEL uses a combination of VMware, Microsoft Server Products, various Linux distributions such as Debian, Backtrack (Penetration Testing and Security Auditing), Fedora, Open SUSE, RedHat and Ubuntu; and Vyatta virtual routers in conjunction with other hardware/software security applications to provide:

- Institutions with the ability to create multiple Academic Cohorts/Strings and the multiple classes associate with each Cohorts/Strings
- Institutions with the ability to enroll students in each class
- Professors with the ability to create virtual machine templates for each class
- Professors with the ability to set the access rights/privileges for common student resources
- Students with the ability to create virtual machines using the professor designated templates

VI. Information Assurance – NIST Sp 800-53 Compliance

Collaborating with iNetwork, a DoD contractor, the SCI is designed to meet DoD level Information Assurance requirements. The SCI has been designed using DoD Certification and Accreditation process requirements, in order to ensure that it can be easily used to conduct training on topics which concern matters of National Security. Furthermore, this makes it possible to integrate with the research programs of accredited DoD organizations, and assuredly with all industry and academic partners. Specifically, the Information Assurance (IA) controls used in the SCI/VEL are in compliance with the requirements specified in NIST SP 800-54. These, also, are in compliance with ISO/IEC 27000 standards used by many non-governmental entities and several of the project's international collaborators.

VII. Mitigating Risks

Kim Andreasson [2], adviser to the United Nations on e-government, and Managing Director of DAKA advisory AB made the statement that, "people are both the problem and the solution" to ongoing cyber security vulnerabilities.We continue to design, build, and implement better defenses against cyber criminals. The global communities continue to update laws and regulations to keep up with the changing cyber landscape. Managing to identify key risk areas and establish technologies associated with detection and intrusion. Allan Paller [2]. SANS institute made the statement, "It's the people skills that allow one nation to be able to protect it computers versus another nation". Because cyber attacks happen so quickly and attackers can change tactics rapidly, experts say the fight often boils down to people skills - which side has the best trained warriors". Paller further stated [2] that the U.S. is far behind in finding and training talented professional in cyber security and information assurance to protect the country's power grid, defense industry, food chain, and banks.

By one estimate, the United States needs up to 40,000 cybersecurity specialists to protect government and large corporations [3].

A. Global and Interdisciplinary Approach

The word global should be understood as a systemic security framework including political, social, economical, and technical dimensions of cyber security. Clearly, we are all in this together as citizens of the world. Reducing the risk of penetration breaches begin with educating the world population as those practices of malicious intrusion continue to attack our society [4]. In a cybersecurity context, global implies also the necessity to think security in terms of collaboration, cooperation and to understand how-sharing can be a risk. From public awareness to policy makers, a global and schedulable cyber security approach should be available to answer all the various security issues and challenges. We must translate what we now know and practice about personal safety awareness over to technological risk awareness [5]. This is a large undertaking, however, we have the media in place to produce such an awareness.

The political and legal dimension of Information Communication Technology (ICT) is definitely more organized and under those controls by standards and practices [6]. However, we are less aggressive in our overall ability to Plan, Protect, and Respond. Now is not the time to plan for Web 2.0 [7]. It is already here. Our popular interests with iPhones and Androids have put mobile computing in the hands of a large percentage of users. From the perspective of a security expert this large influx of mobile computing has further engaged methods and practices to breach systems.

To reduce risk, organizations need to establish agile policy driven to a point where businesses can collaborate with confidence [8], [9]. This is a closed loop scenario suggesting that confidence becomes a factor of enforceable security [5]. The rapid release of 'next generation' technology products has far accelerated Moore's law suggesting a two year period of upgrade or replacement.

To build security into a super-charged environment suggests we need security everywhere in the network. We need scanning engines that are at the core of firewalls/IPS, a proxy, or an interesting fusion of the two [2], [7]. The trend to offload storage at a remote site with failover capabilities and mirrored backup is rapidly replacing a locally managed network operating center (NOC).

We need to somehow establish a Security Intelligence Operation (SIO) that clears has the 'brains' to identify the good guys from the bad guys [2].One such technology/technique is dubbed the next-generation endpoint. The role of the next-generation endpoint is to reside on a wide variety of devices and make sure all connections coming 'on' or 'off' a device are routed through one of the network-based scanning elements [7].

The line between policy and enforcement must be agile and definitive [10]. As a security person, we would often notice that privileges are first extended to personnel and then qualified by policy. As personnel assume various roles privileges are increased, however, to the contrary, as those various roles do not require privileges they are not likely removed [5]. Hence, a system out of control with personnel involved in computing space they are no longer qualified to access.

Devices can be initiated to make a more robust contextual enforcement decision and produce dynamically updated data sets.

VIII. Conclusion

The traditional process of utilizing asynchronous or online teaching of computer related curriculum as supported through coupled independent applications is not as valid for designing functional bridges of learning representing fully detailed and valid experiences in the virtual machine applications of computing. The high level design of an accessible online computing system accessible as a fully functioning computing system with an embedded layer of security architecture as presented in this paper supports the synergistic relationship among synchronous/on-site learning and practice that becomes self contained within the virtual machine environment using pragmatic components that are designed within the system. Without the architectural properties presented here, an asynchronous computing curriculum designed to practice both the concepts and constructs of cyber security is unlikely to achieve the dimension of qualification superimposed with the virtual computing world. Future practices would include yet additional processing bandwidth.

Acknowledgments

The authors gratefully acknowledge comments, suggestions, help and/or support given by National University administrators, faculty, students, interns and contractors (iNetwork) and individuals who have devoted of their time and subject matter expertise to qualify those dimensions contained within the function of the Virtual Education Laboratory.

References

[1] R. Boyle & R. Panko, *Corporate Computer Security*, Pearson, 2013.
[2] M. Tritschler & W. Mackay, UK Smart Grid Cyber Security, KEMA, June 25th 2011.
[3] K. Pugh, Lean-Agile Acceptance Test-Driven Development, Addison Wesley, 2011.
[4] I. Sommerville, Software Engineering, 9th Edition, Addison Wesley, 2010.
[5] C. Pfleeger & S. Lawrence, Analyzing Computing Security, Prentice Hall, 2012.
[6] A. Whitaker & D. Newman, Penetration Testing and Network Defense, Cisco Press, 2006.
[7] NIST, "Joint Task Force Transformation Initiative, Information Security", February 2012.
[8] W. Stallings, Cryptography and Network Security (5th ed.), Pearson, 2011.
[9] J. Byrnes, Cognitive Development and Learning, Allyn Bacon, 2008.
[10] L. Nelson, C. Wysopal, D. Zovi,, & E. Dustin, The Art of Software Security Testing, Addison Wesley, 2007.

Dr. Ronald Gonzales is a Professor at National University, 3678 Aero Court, San Diego, CA, 92123, USA. He is now the Lead Faculty for the MS in Cyber Security and Information Assurance program, School of Engineering, Technology and Media; and president of DataPoint Consulting. Phone: 858-309-3435; email: rgonzales@nu.edu

Dr. Gordon W. Romney a Professor at National University, 3678 Aero Court, San Diego, CA, 92123, USA. He is the architect of the Cyber Security and Information Assurance Initiative of the School of Engineering, Technology and Media and Senior Research Scientist of the Cyber Security Institute of San Diego. His major research interests are in Information Assurance and Cyber Security, Information Integrity and Confidentiality, 3D Graphics, Anonymization of Data,, Virtual Laboratory, Secure Cloud Infrastructures, Secure Social Networks, and Ruby on Rails. Phone 858-309-3436; email: gromney@nu.edu,

Dr. Pradip Peter Dey is a Professor at National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. He is the Lead Faculty for the MS in Computer Science program, School of Engineering, Technology and Media. His research interests are computational models, mathematical reasoning, visualizations, software engineering, User Interface, education. Phone: 858-309-3421; email: pdey@nu.edu.

Dr. Mohammad Amin is with National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. He is now Professor and Lead Faculty for the Master's degree program for Wireless Communications, School of Engineering, Technology and Media. His major research interests are wireless communications, database, sensors, engineering education. Phone: 858-309-3422; email: mamin@nu.edu.

Dr. Bhaskar Raj Sinha is with National University, 3678 Aero Court Dr., San Diego, CA, 92123, USA. He is the Lead Faculty for the Information Technology Management program, School of Engineering, Technology and Media. Phone: 858-309-3431; email: bsinha@nu.edu