Technology Fee Proposal

Title: Virtual Environment for Information Security Education and Exploration

Proposer: Joseph N. Wilson, Assistant Professor
CISE Department
Rm. E301 CSE Bldg. 42
Box 116120
Gainesville, FL 32611-6120
jnw@cise.ufl.edu
352-514-2191

Sponsoring Organization: Information and Security Compliance

Purpose and Specific Objectives:

This proposal is aimed at providing a remotely accessible virtual environment (RAVE) for supporting information security education and exploration. This proposal briefly explains what the virtual environment is, why it is needed, how it can be used, who would use it and for what purposes, who would benefit from it, and how it would be sustained.

A remotely accessible virtual environment (RAVE), roughly speaking, is a computer (or collection of computers running code that permits it to simulate the behavior of a network of computers in nearly every respect. One important use of virtualization is to provide a safe and secure environment for testing computer malware, intrusively testing software security, and defending against intrusive network attacks. It is infeasible to perform such tests on actual computer hardware because

i) introducing malware to an actual computer causes improper behavior and leads to the risk of spreading to other computers on connected networks

ii) intrusive attacks involve activity that is usually banned by acceptable use policies and may in fact be filtered by protective software or firewalls, and

iii) provisioning and preparation of hardware required for such testing can be expensive and time consuming.

We have identified a variety of uses to which this RAVE system can be put:

i) We will support classes that deal with cybersecurity topics.

CIS 4930/CIS 6930 *Penetration Testing and Ethical Hacking*. This course is being offered in fall 2013 and is open to all students at the University of Florida who choose to participate. Its current fall enrollment is 53 students. Enrollment is likely to near 80 due to further graduate enrollments over the summer. A new course proposal is being prepared to add this to the course catalog and offer it on a regular basis.

CIS 4930/CIS 6930 *Cybersecurity*. This course was offered in fall 2012 with an enrollment of 38 students. A course proposal is being prepared to add this to the course catalog and offer it on a regular basis.

CNT 5410 *Computer and Network Security*. This course is also being offered in fall 2013. Last fall's enrollment in this course was 45 students.

At least two faculty members (3 courses per year) and from 40 to 100 students per semester would be expected to be involved in such classes.

ii) We will support the supplemental activities of students taking our introductory classes (such as COP 3502 and COP 3504) who are interested in learning about cybersecurity. Over 30 such students have participated in weekly meetings to prepare for the National Cyber League competition to be held in the fall of 2013. Activities supported with the proposed RAVE would include providing hands-on sessions showing how to test the security of computer systems and configure and deploy them properly, preparing for nationwide security competitions such as the National CyberLeague and the national Collegiate Cyber Defense Competition, and hosting cybersecurity competitions both locally and via the internet.

iii) We will provide continuing education opportunities for UF faculty and IT staff in an effort to enhance the security of the growing number of internet-accessible applications and many other UF software development efforts.

Current support for these activities involves either UF-managed computer resources (file, compute, and web-servers) or student-owned laptops and personal computers. While these sorts of resources are well-suited to addressing most course needs and software development activities, they do not provide an effective environment for learning about cyber attacks and defenses. One reason already highlighted above is the problem associated with suspicious or malicious network traffic.

Another critical issue that is addressed by access to a RAVE is satisfying the need for students to have access to a wide variety of operating systems and software to comprise a reasonable environment for attacking and defending. This imposes the need to deploy machines having a variety of operating systems and having a broad mix of specific versions of web, mail, database, and other server software products. As an example, consider a current network environment recommended by the Network Development Group to be used in preparation for the Certified Ethical Hacker (CEH) examination. This network involves the use of eight separate machines, including ones running Windows XP, Windows Server 2003, Windows Server 2008, and Windows 7 and several different linux versions. Most students will not have access to a legal copy of Windows 2003 or Windows 2008. Only those having machines with Windows 7 installed will have access to Windows XP through a special program hosted by Microsoft. Furthermore, to effectively deploy a network like this using conventional hardware on hand in the CISE department would require one CPU per virtual machine, possibly tying up from 2 to eight machines to deploy a single laboratory environment. Furthermore, after each student completes a laboratory assignment, those machines must be restored to their initial states, requiring either significant labor effort or development of custom software. The system we've proposed to acquire here could simultaneously host four VM network pods, each one implementing the described network, assigning one VM per processor; and the NetLab software reinitializes the machine states for each subsequent student's access.

Efforts of UF students to prepare for the National Cyberleague competition are already being hampered as a result of the software licensing and resource problem. It is essentially impossible to satisfy the licensing requirements of such networks without finding a new solution. It is also extremely difficult to maintain networks of such machines with specific software installed. Virtualization and the RAVE solve these problems by providing the network in a box and by requiring licensing for software only by the university, not by each individual student.

Impact/Benefit:

Cybersecurity has become a topic of critical and strategic importance to our nation as demonstrated by the U.S. President's recent executive order aimed at defending the nation's cyber infrastructure. Recent media attention given to malicious activities attributed to the Chinese military's APT 1 team has been nearly ubiquitous. News stories describing the software vulnerabilities of Supervisory Command and Data Acquisition (SCADA) devices used to control power systems, dams, and many other industrial systems are nearly ubiquitous. Most Americans are aware that their computer systems are susceptible to attack, but few of them know how these attacks work and, much less, what to do about them. This proposal is aimed at trying to turn that around for students at UF, primarily engineering students studying software development but also those who have a keen interest in cybersecurity but who are not necessarily pursuing careers in the software industry.

Here at UF, the Florida Institute for National Security (FINS) is an interdisciplinary research institute dedicated to providing a unique research and education consortium for University of Florida students and faculty in the College of Engineering. FINS houses security-related research arising across different engineering settings, and encompasses both theoretical and applied studies. The primary mission of FINS is to assemble research teams that collaborate on complex engineering problems via the exploration of complementary facets of the problem. This institute also provides a setting in which researchers having different backgrounds can determine common themes within their research programs, identify emerging challenges in security-related engineering applications, and address these problems together using state-of-the-art approaches. Students that are a part of the FINS program will earn certificates in security engineering on their way to pursuing Masters or Doctoral degrees within their home departments. Dr. Cole Smith (cole@ise.ufl.edu), the FINS director, has expressed his strong support for this proposal.

In summary, the proposed system will benefit UF students, faculty, and staff, as well as all those whose cybersecurity is improved through their efforts. By acquiring this RAVE system, we would not only have the capability to effectively provide new information security educational opportunities to students, faculty, and staff—allowing people access to our virtual environments from anywhere on the internet—but we would also open up the possibility of increasing UFs reputation nationwide and worldwide by allowing others to participate in events sponsored by UF. (A small number of RAVEs such as that proposed herein have been used to support college and university teams in preparing for the National Cyber League competition.) Such activities are not supported by existing facilities at UF.

I have received a number of letters of support from students, alumni, staff, and industrial contacts with UF. You can find copies of their messages at http://www.cise.ufl.edu/~jnw/RAVEletters.html.

Sustainability:

The proposed equipment shall be sustained by UF IT professionals and configured by faculty and staff. IT personnel from Information and Security Compliance and the CISE Department have agreed to collaborate to provide the necessary labor for installing (approximately 6 labor hours) and maintaining the operation of the system (approximately 20 hours per year). Faculty and TAs teaching specific courses and those staff and students organizing events shall provide the effort necessary to configure and deploy virtual environments on the system (approximately 4 to 12 hours per environment).

The CISE department chair and facilities committee have agreed to have the departmental facilities committee prioritize the provision of maintenance and support fees for the requested systems along with those providing other instructional resources. If, as expected, this item becomes an integral to the offering of CISE security courses, its replacement cost will be factored into future departmental equipment budgets.

Timeline:

As soon as an award is made, the requested hardware will be ordered. Racks, network hardware, and supplies necessary for installation are available on-hand and we would expect to accept delivery within 30 days of placing our orders.

CISE system administration personnel will attend VMWare VSphere training on June 7, June 17-19, and July 12.

During the months of July and August, Dr. J.N. Wilson and Dr. R. Newman will study NDG Netlab documentation and courseware to learn how to effectively deploy laboratory pods on the system and Dr. Wilson will prepare virtual network *pods* for use in the fall *Penetration Testing and Ethical Hacking* course. Dr. Newman will prepare pods for use in the fall *Computer and Network Security* class. As pods to support the fall 2013 National CyberLeague competition are made available online, we will deploy these in preparation for that event.

During the fall semester of 2013, pods for special challenges presented to students interested in extra-curricular security activities will be developed, deployed, and used in more informal settings as well.

Technology Fee Full Proposal Template

Title: Virtual Environment for Information Security Education and Exploration

Proposer's Name: Joseph N. Wilson

BUDGET

2U RackMountPro Server w/32-Core 4 Socket 64GB and Redundant Power Supply	$11,620
NDG NETLAB Academy Edition	$ 6,995
NETLAB Academy Edition Maintenance (3YR)	$ 6,995 (recurring after 3rd year)
Miscellaneous supplies	$ 300
Total Budget	**$25,910**