# Design Insider Threat Hands-on Labs

Hongmei Chi, Clement Allen, David Angulo Rubio
Department of Computer and Information Sciences
Florida A&M University
1333 Wahnish Way
Tallahassee, FL 32307
USA
hchi@cis.famu.edu

***Abstract:*** *Insider threat continues to be of serious concern to governmental organizations and private companies. Vulnerabilities of the digital information being shared through mobile devices and Internet clouds increases exponentially due to IT security mechanisms not being capable of controlling what is beyond company network limits. One of the solutions could include providing an effective interactive framework to train future and current Information Technology security professionals and regular employees who need to be aware of these threats in order to avoid being a victim of insider attacks. There are few hands-on labs/modules available for training current students, the future information assurance professionals. This paper will classify the different actors and vectors involved in these attacks focusing specifically on Information Technology (IT) sabotage, theft of intellectual property and insider fraud. Then, we will describe how to design virtual hands-on labs mainly to current or future technology security professionals. The training hands-on labs will enhance trainee's knowledge and practical security skills about how to mitigate insider threat attacks. In addition, the training hands-on labs will be implemented via CyberCIEGE, an innovative video game and tool to educate fundamental concepts for insider threat.*

**Keywords**: Virtual Training, Insider Threats, Hands-on lab, Information Assurance, Active Learning, CyberCIEGE

**Recieved**: 10 January 2015, Revised 8 February 2015, Accepted 15 February 2015

## 1. Introduction

The Insider Threat attacks are concerns to organizations due to its devastating consequences ranging from financial loss, damage of reputation, loss of Intellectual Property, etc. The fact that insiders are in many cases current or former employees, interns, contractors and business partners makes it more difficult to track and determine routine normal behavior from anomalous conduct. This paper will develop hands-on labs based on a 3D virtual SDK so that we can train students and IT professionals to deal or be aware of insider threats. Those modules will show players/students how to detect, prevent and remediate insider threat attacks. An insider threat is generally a person who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems (CERT,n.d.).

Insider threat attacks perpetrated against public and private institutions cost millions of dollars in losses due to theft of intellectual property, destruction and misuse of assets, or stolen valuable information that can undermine the attacked organizations and/or individuals. The way to identify and prevent insider threat attacks is to educate employees in any organization. The Computer Emergency Readiness Team (CERT) Insider Threat Center is a division of Carnegie Mellon University's Software Engineering Institute. They explain that policy enforcement and periodic security training for all employees will greatly reduce insider threat attacks in most organizations. The Intelligence and National Security Alliance (INSA) Cyber Council is a group of executives from the public, private and academic sectors with expertise in cyber security with the mission of improving cyber security policies and practices in the public and private sector. According to INSA, as of September 2013, no standard training program exists that can be used as a valid framework in the private sector to deal effectively with this kind of threat (Cappos et al., 2014,Greitzer **et al., 2013**).

Insider threats are causing serious damages to governmental organizations and also to private companies.  Researchers at CERT Insider Threat Center have developed Enterprise Architecture Patterns that cover people, processes, technology and facilities (CERT, n.d.).. These four elements have to be considered in order to protect and prevent against insiders.Insider threat attacks are disastrous to organizations and there is a vital need to control and mitigate them. Mitigating damages can be successful through use of an effective training module. Training modules designed through CyberCIEGE (Cone **et al., 2007)** are the focus of this study also noted in previous sections. There are four important milestones to focus on in order to build an effective, coherent, and usable training module in CyberCIEGE, those are: how these attacks happen?; why they happen?; the steps that insiders take to perform their attacks; and the inexistent defense mechanisms that the victim organization needs to implement in the form of hardware, software and information security policies. Focus on these milestones will guide the development of the module and training scenarios.

Passive education taught in the traditional classroom does not help students internalize and learn the security concepts taught. The interactive teaching tools are far better than simply power point lectures where students are passively listening and learning by doing is main active learning meth we are adopting in this project (Chi et al., 2013). CyberCIEGE SDKwill use to create hands-on labs. This technology promotes active learning, which has been proved effective in domain-specific knowledge internalization. This will give a higher degree of confidence that the trainee will be effective in applying his security skills in case he is faced with a real insider threat attack. These attacks have three main purposes according to specialists from CERT: (1) destruction, (2) misuse or corruption, and (3) theft of assets. All hands-on labs attempt to show the mechanisms that favor these attacks. These mechanisms can be e.g., the absence of security policies at the workstation or network level. Then the trainee will apply the corrective actions such as the creation and application of security policies to avoid these attacks.

The rest of this paper is organized as following: in Section 2, an introduction to in-depth insider threat training programs and an overview of CyberCIEGE SDK will be provided in detail. Section 3 provides related work. Section 4 will give details of the implementation training modules via CyberCIEGE. Section 5 will discuss a small number of student feedback and lessons we have learned. In Section 6,   conclusions will be outlined.

## 2. Training Tools

CyberCIEGE (http://cisr.nps.edu/cyberciege/ ) covers over 20 game scenarios that address a variety of security concepts. CyberCIEGE is built around the Scenario Definition Language (SDL) that lets the player create and customize the game scenarios. Game designers are responsible for creating the scenarios using the Scenario Development Kit (SDK). After they build them, scenarios are compiled and a SDL is generated. This SDL is the one that will be used by CyberCIEGE game engine (Cone **et al., 2007)**.

There are two principal roles to be filled in the use of the CyberCIEGE tool - a scenario designer and a player. The player is the trainee and the scenario designer is the one designing and developing the training module.

During initial set up of the tool, a lab will be created by a scenario designer. This designer will layout the starting settings in a virtual company. Starting settings are the number and credentials of virtual users, the initial hardware, software, security mechanisms, and policies that are put in place. The initial assets and their correlating values will be determined as well by the scenario designer. The importance of a particular asset to the company determines that asset's value as well as the level of a protection mechanism put in place for said asset. Attackers will almost always go after the most valuable information asset. Another and very important aspect of the set up by the scenario designer is to engineer attack(s) within the module.

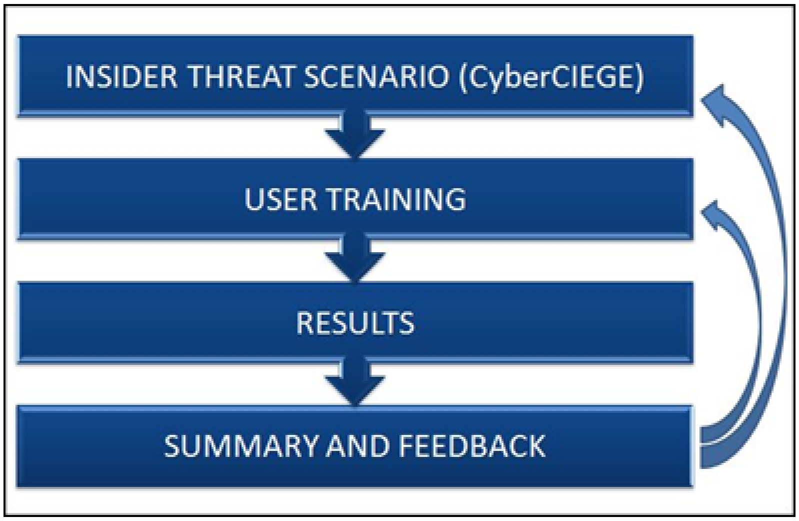


Figure 1. Insider Threat Training Overview

The player (a network security specialist, security manager, etc.) will be in charge of giving virtual users access to assets to keep them productive but also needs to put security mechanisms in place in order to avoid attacks. The player has to keep a balance between productivity and security, and also protect against attacks without overwhelming the users with too many security mechanisms. The player's actions are the ones that will counteract or allow an attack to happen. These actions are: password management, zones and methods of physically protecting assets, network filters, operating system and application patching, basic key management, encryption and PKI, use of SSL and TLS, user identity, mandatory access controls, etc. By the end of a game session a log will be generated detailing the player's actions.

These are some of the capabilities provided by CyberCIEGE and that this study will attempt to use with the purpose of training and educating through this module on how to detect and control insider threat attacks and implement defense mechanisms against them. The intended audiences are mainly information assurance students, cyber security professionals, computer security specialists, and also any user who need training in this area. An overview of this study can be seen in Figure1.

As stated before, the scenario will be built using the 3D gaming-like tool called CyberCIEGE that has been proven very useful in active learning and internalization of knowledge by students and professionals in United States. CyberCIEGE has been used by the U.S. Navy, Army, Air Force, Marines and other Federal Government officers and employees. It has also been used in colleges and schools. CyberCIEGE is similar to Sims, the popular resource management game. In the same fashion as resources are managed in Sims, resources are managed in CyberCIEGE. Where in Sims those resources are city infrastructure, in CyberCIEGE resources are hardware, software, and security policies to be put in place, or reinforced if already existent, with the purpose to detect and eliminate cyber threat attacks. Trainees can play the game as many times as needed until they internalize the knowledge and become acclimated to the scenarios of the game. The aim is to train players so they can use these information security skills in real world scenarios when faced with these threat situations. There are many different pre-programmed scenarios in CyberCIEGE including stop worms, life with macros, identity theft, etc., but there's no pre-existing scenario specifically tailored towards insider threats.

There are multimedia-online tools aimed at teaching cyber security (Du, 2010; Guo et al., 2013). These tools are very different from the traditional classroom setting. For example, one of these tools is the Next Generation Security Game which is an internet based game that has eleven sequential levels that the student or trainee needs to go through. These levels are challenging scenarios presented to the player and he/she needs to solve that challenge in order to reach the next level. There's another tool called CyberProtect, developed by US DoD's Defense Information Systems Agency (DISA) in conjunction with several entertainment software companies. The purpose of these games is to entertain but most importantly teach security concepts to professional workers. Another training program is called Department of Defense Information Assurance Awareness Video (DoDIAA). Both CryberProtect and DoDIAA are for DoD employees. There are studies where comparisons have been made between this online, interactive, 3-dimemsional games and the traditional classroom setup. The conclusions are that these interactive games are better in achieving the purpose of teaching and internalizing the knowledge by the student (Jones **et al.,**

**2010)**. Specifically, a comparison between DoDIAA and CyberCIEGE is studied:  their conclusion was that CyberCIEGE is a more powerful tool to train and teach students in cybersecurity concepts(Jones **et al., 2010)**.

DeterLab (Mirkovic et al., 2012) is an active way of teaching cyber security concepts. DeterLab places the students in cyber threat real world attack where for example the student has to face a SQL injection attack, watch the consequences of this attack (e.g., database corruption) and then solve the problem (e.g., applying Sql store procedures) so this attack cannot happen again. DeterLab also helps students become the next generation cyber researchers or cyber analysts working for the government, military or private companies. There's an open spirit in the DeterLab which means that if a teacher has a suggestion to improve DeterLab. The DeterLab community will use that idea to improve the tool. Deter lab has been evolving all these years also in the direction of the users of this tool, mostly cyber security specialists, constant feedback from the teachers and researches of Deter lab keeps the tool updating its architecture to meet the needs of the users.

As we can see most training tools doesn't include a series lab show to expose and deal Insider Threat attacks, but has all the architecture and purpose that we want to use to achieve the goal of our research project. CyberCIEGE, DeterLab and CyberProtect are great tools that propose interactive learning and training by letting students face simulated real world cyber threat attacks. In this environment by trial and error they will learn the effective methods and techniques to counteract these attacks and by doing this their practical cyber security skills will increase. This paper attempts to build on the foundation presented by these tools and apply it to specifically insider threat attacks because the fact is that there's not a specific standard or model to deal with insiders in the private sector. A standard means that there's not a coherent program or framework that can deal effectively with this malicious kind of threats. This paper attempts to build a module using CyberCIEGE to train cyber security professionals and students to deal effectively with insider threats.

### 3. Related Work

Currently, there are various hands-on labs for information assurance concepts other than insider threat, such as network security ( Tao at el., 2010), secure programming (Chi et al., 2013), secure web-programming, mobile security(Claycomb et al., 2012),Cloud security (Simmons et al., 2012) and applied security(Zeng, 2013).  But is it hard to find few training hands-on labs (for insider threat and how to migrant such threat.  Real-world examples are everywhere, from Manning to Edward Snowden.

According to the Intelligence and National Security Alliance (INSA) and Cyber Council- Insider Threat Task Force report of September 2013, Insider threat programs have been formally established at the federal government agencies level. Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information signed in 2011 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs signed in 2012 are two standard programs working in federal agencies that handle classified information (http://www.insaonline.org ). INSA has also discovered in its report that there are no standards, mandates or benchmarks in the private sector to deal effectively with insider threats. Much of the  nation's technology infrastructure is held by private companies and also private company partner with federal agencies to conduct very sensitive work. Insider threats in the private sector can be very damaging to the nation's well-being. The major findings in this report are that most of the companies have an insider threat program that it is only technology related where they have tools that monitor workstations or networks to detect suspicious traffic activities. However experts conclude that an effective insider threat program should cover technical and non-technical indicators concerning the whole organization. The insider is a person so there needs to be a program that detects anomalous, suspicious, or concerning non-technical behavior as well as technical tools to detect misuse, stealing or destroy of sensitive digital information. Another important finding in this report is that most companies have detection tools but only a few mentioned prevention programs. This introduction is to have a general view of the maturity of insider threat programs in both the private and federal sectors. Based on hundreds of published real-world insider threat incidents, the 13 Essential Elements have been pointed out by INSA.(http://www.insaonline.org/insiderthreat ). More hands-on can be set-up based on those basic elements.

### 4. Design Hands-on Labs

According to the Intelligence and National Security Alliance (INSA)-Cyber Council: Insider Threat Task Force Report of September 2013, the taxonomy of insider threats include: Fraud, Intellectual Property(IP)Theft and insider fraud.

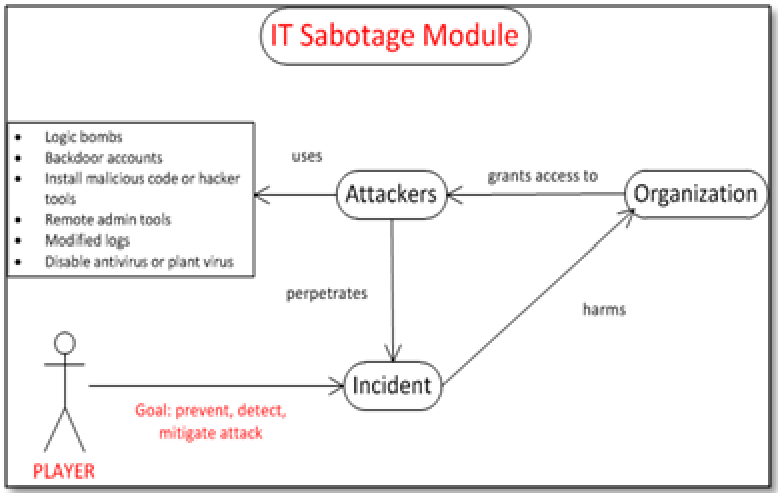


Figure 2. Overview of information technology Sabotage Module

The common vector pattern(s) used by an insider is fundamentally categorized in one of the following categories: printing activity, disable defense tools, use of removable media, changes in employee behavior, and remote access and windows clipboard activity (Crawford et al., 2013). Different mechanisms or tools can be helpful in detecting one of the insider categories, but only one detection tool or technology can't be effective in detecting all of the categories together. For example, network monitoring can be useful for incoming connections from outside the organization but workstation go undetected with network monitoring. Workstation monitoring can give us more clues about what the actives of the employees are. There are also hardware mechanisms that can be compromised and that are most of the time overlook by security employees. One of these devices is Cisco network devices that have a detection capability included which can help detect intruders or malicious traffic, but most of the time Cisco routers are left with the default or factory configuration. Understanding that network devices process all traffic in a network and need to be secured is a must to avoid insider attacks (Young et al. 2013).

This paper attempts to develop a training module for each of these types of insider threat and explain in detail the nature of each one and how to prevent and mitigate them. The goals of these modules are the following:

• Learn about information technology sabotage, insider fraud and IP theft attacks, the consequences of these attacks and the vulnerabilities exploited by the attackers

• Train about security policy creation to avoid the attacks mentioned before.

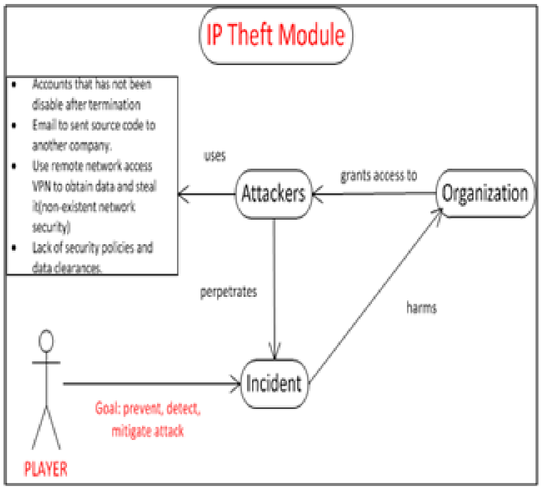

IP Theft Module
Accounts that has not been disable after termination
Email to sent source code to another company.
Use remote network access VPN to obtain data and steal it(non-existent network security)
Lack of security policies and data clearances.
uses
Attackers
grants access to
Organization
perpetrates
harms
Incident
Goal: prevent, detect, mitigate attack
PLAYER

Figure 3. Overview IP Theft module

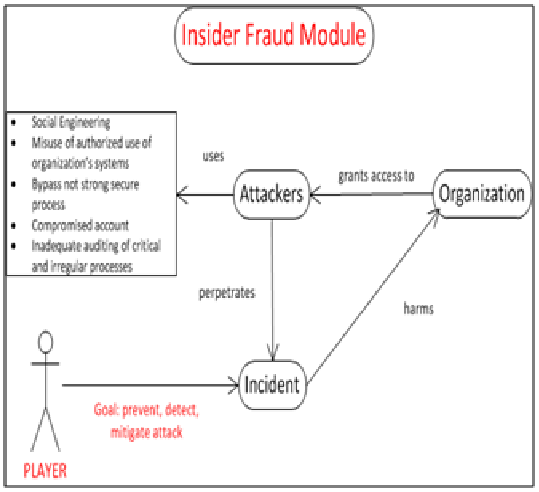

Insider Fraud Module
Social Engineering
Misuse of authorized use of organization's systems
Bypass not strong secure process
Compromised account
Inadequate auditing of critical and irregular processes
uses
Attackers
grants access to
Organization
perpetrates
harms
Incident
Goal: prevent, detect, mitigate attack
PLAYER

Figure 4. Overview Insider Fraud Module

- Train about the effective application of workstation and network security mechanisms
- Internalize and learn concepts that can be applied in real world scenarios of information technology sabotage, insider fraud and IP theft.

Information technology Sabotage is the type of crime committed by a former or current employee, contractor, or business partner who has authorized access to the organization's data, systems or networks. The crime is committed when the insider misused or exceeds the level of access to these assets with the intention to harm a specific individual, the organization's data, reputation, systems or disrupt daily business operations. An overview of the module is presented in Figure 2.

Theftof Intellectual property according the CERT Insider Threat Center is the most damaging and causes the greatest financial losses to organizations suffering from these attacks. As an example from a case from the CERT database of insider threat, an attack where a secret document was stolen cost the victim company almost $ 1 billion in R & D costs. Theft of intellectual property is defined as the means by which an individual steals intellectual property from an organization using information technology means. This includes industrial espionage where an insider steals secret formulas, patents, or documents to take to their next company or to a competitor. In 10 years of investigation CERT has classified insiders who commit IP theft as male in 94% of the cases, scientists/engineers in 44%, and programmers in 10% of the cases.

This module attempts to train and teach the player the following concepts:

- Learn about IP theft vector attacks, the consequences of these attacks and the vulnerabilities exploited by the attackers.
- Understand the common attack pattern of IP theft attacks and the creation of policies to counteract these attacks.
- Train about the effective application of workstation and network security mechanisms
- The CyberCIEGE SDK, the Scenario Development Tool (SDT) and the Scenario Definition Language (SDL) will be used to design the IP theft module. In the design of this module the vector attacks will be presented and the player will experience the consequences of the attacks if in case he didn't take the correct preventive mechanisms.
- The module will end once a successful attack has been committed or when all the vulnerabilities have been addressed by the player successfully. An overview of the module is presented in Figure 3.

Insider fraud is the use of IT for the purpose of modification, addition or deletion of the organization's data (not systems or programs) with the aim of personal gain. It is also the theft of information that leads to an identity crime (identity theft, credit card fraud). Identity crime is the misuse of personal identifiers with the purpose of gain something of value or to facilitate other criminal activities. According to the CERT insider threat center, fraud is the most prevalent crimes in their databases. Fraud crimes do not cover just the financial sector. The primary motivation for fraud is financial gain. All the cases in the CERT database that involved organized crime were related to the fraud cases. In organized fraud cases usually the information is sold to an outsider and it is this person who commits the fraud.

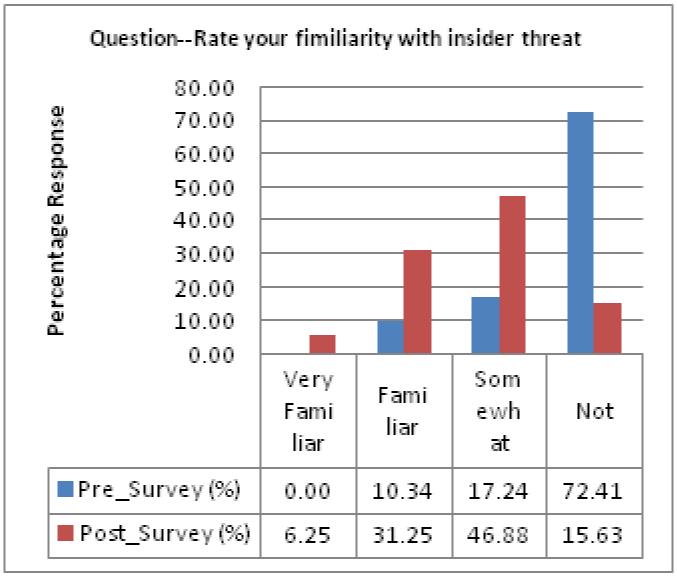
The CyberCIEGE SDK, the Scenario Development Tool (SDT) and the Scenario Definition Language (SDL), is used to design the insider fraud module. In the design of this module the vector attacks is presented and the player experience the consequences of the attacks if in case he didn't take the correct preventive mechanisms.

The module ends once a successful attack has been committed or when all the vulnerabilities have been addressed by the player successfully. An overview of the module is presented in Fig.4.

One lab is built for each insider threat category and more hands-on labs can setup based on different scenarios.

## 5. Student Feedback

Prior to use the training modules, trainees will be asked to complete a pre-survey, and then an introduction of hands-on labswill be presented to the students. CyberCIEGE may be explained briefly to them and how to use and navigate during game time. After each student finishes two hands-on labs a post-survey will be completed by each student. The objective of these surveys is to



| | Very Familiar | Familiar | Somewhat | Not |
|---|---|---|---|---|
| 🟦 Pre_Survey (%) | 0.00 | 10.34 | 17.24 | 72.41 |
| 🟥 Post_Survey (%) | 6.25 | 31.25 | 46.88 | 15.63 |

Figure 5. Survey results from one pre-survey &post-survey question

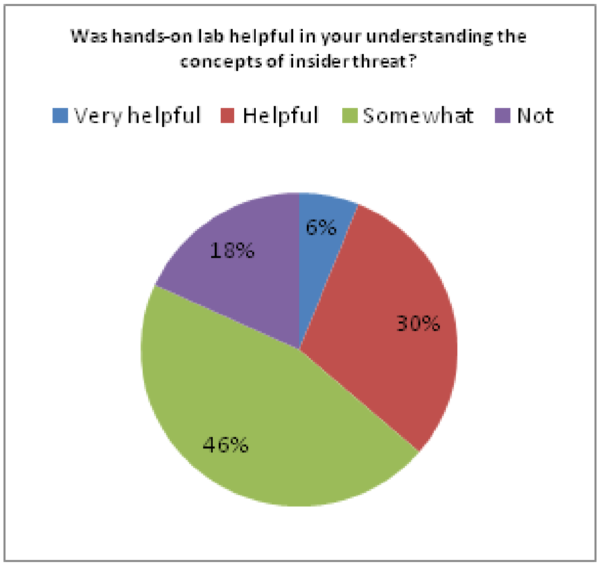


Figure 6. Survey Result from one post-survey question

see the effectiveness of the tool based on the answers from each student. A comparison of the results between the pre-survey and post-survey should indicate the level of knowledge acquired after using those hands-on labs. These labs or scenarios building around the three different areas of insider threats attempts to build in the student an awareness and understanding of Information Assurance (I.A) concepts and the application of these concepts to real world insider threat cases. The pre-survey and post-survey also gave an indication of the usefulness of CyberCIEGE as a training tool for the purposes of this paper. The post-survey is used as a measurement medium to detect how students' knowledge of IA concepts and its real world applications improved after using the module or otherwise.

Since two hands-on labs are first-time to be given one security class for 29 students. A simple pre-survey and post –survey were set for students to answer. Our surveys are included two parts: pre-survey was done before students took any modules and post-surveys were conducted after students completed two hands-on labs. All students are CIS majors.

Figure 5 shows the results when students are asked to rate your awareness with insider threat. Previous before completing the hands-on labs more than seventy percent of students were not familiar insider threat. Post survey results shows that after completing the module students felt more acquainted with insider threat. Figure 6 shows the results when students are asked was the lab helpful in your understanding the concept of insider threat. It was important for hands-on labs to offer a simple approach to convey the importance of insider threat. We knew students wouldn't have a lot of time for a broad topic. The design of those hands-on labs focused on straightforward experience to learn the concepts, so the learning curve was smooth. The majority of CIS students are taught basic security concepts with no or little regard to insider threat issues. Building secure systems requires incorporating concepts of insider threat into security fundamentals. Government and businesses are increasing efforts in this area and so should colleges and universities. The overall evaluation of hands-on labs was positive. A higher percentage of students considered the modules very helpful or somewhat helpful on a topic that they were not familiar with. In addition, the students indicated that the modules helped them understand what and how to handle insider threat issues.

## 6. Conclusions

In this paper, preliminary results are shown and concepts of insider threat are fundamentals of security education. Those hand-on labs are promising and helping students to master those basic insider threat issues. After students completed labs they should understand, remember and know how to apply insider threat concepts. Students exposed to those labs should show increased ability to handle and address specific insider threat issues. This approach can be replicated over time and more empirical evidences will be gained via continuing to insert insider threat concepts into information assurance curriculum. More importantly this paper study provides a theoretical and pragmatic foundation for further basic curriculum in training future employees in identifying cyber threat in early stages, and broadens our ability to protect information systems and cyber-infrastructure against user-centric cyber threats.

It is difficult to detect internal threats within an organization. The trend of "Bring Your Own Device" (BYOD) and the increasing development of cloud computing environments have increased the risks of malice data leakage. Additional hands-on labs based on cloud computing are in demand in real-world as well.

## 7. References

[1] Cappos, J., Weiss, R. (2014, March). Teaching the security mindset with reference monitors. In SIGCSE (p. 523-528).

[2] Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers& security*, 26 (1), 63-72.

[3] Chi, H., Jones, E. L., Brown, J. (2013, October). Teaching Secure Coding Practices to STEM Students. *In*: Proceedings of the 2013 on InfoSecCD'13: *Information Security Curriculum Development Conference* (p. 42). ACM.

[4] Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., Center, C. I. T. (2012). Chronological examination of insider threat sabotage: preliminary observations. Journal of Wireless Mobile Networks, *Ubiquitous Computing, and Dependable Applications*, 3 (4), 4-20.

[5] Crawford, M., Peterson, G. (2013, January). Insider Threat Detection using Virtual Machine Introspection. *In*: System Sciences (HICSS), 2013 46th Hawaii International Conference on (p. 1821-1830). IEEE.

[6] Du, W. (2011). SEED: hands-on lab exercises for computer security education. Security & Privacy, IEEE, 9 (5), 70-73.

[7] Farahmand, F., Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. Information Systems Frontiers, 15(1), 5-15.

[8] Greitzer, F. L., Ferryman, T. A. (2013, May). Methods and Metrics for Evaluating Analytic Insider Threat Tools. In: *Security and Privacy Workshops* (SPW), 2013 IEEE (p. 90-97). IEEE.

[9] Guo, M., Bhattacharya, P., Yang, M., Qian, K., Yang, L. (2013, March). Learning mobile security with android security labware. In Proceeding of the 44th ACM technical symposium on Computer science education (p. 675-680). ACM.

[10] Jones, J., Yuan, X., Carr, E., Yu, H. (2010, March). A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. In IEEE SoutheastCon 2010 (SoutheastCon), *In*: Proceedings of the (p. 176-180). IEEE.

[11] Mirkovic, J., Benzel, T. (2012). Teaching cybersecurity with DeterLab. Security & Privacy, IEEE, 10 (1), 73-76.

[12] Tao, L., Chen, L. C., Lin, C. (2010). Virtual Open-Source Labs for Web Security Education. *In*: Proceedings of the World *Congress on Engineering and Computer Science* (1).

[13] Simmons, M., Chi, H. (2012, October). Designing and implementing cloud-based digital forensics hands-on labs. *In*: Proceedings of the 2012 *Information Security Curriculum Development Conference* (p. 69-74). ACM.

[14] Young, W. T., Goldberg, H. G., Memory, A., Sartain, J. F., Ted, E. (2013). Use of Domain Knowledge to Detect Insider Threats in Computer Activities. In Security and Privacy Workshops (SPW), 2013 IEEE (p. 60-67). IEEE.

[15] Zeng, H. (2013, June). Research on Developing a Lab Environment for Cookie Spoofing Attack and Defense Education. In Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on (p. 1979-1982). IEEE.

[16] CERT Coordination Center (CERT/CC): http://www.cert.org/

## 7. Author biographies

Dr. Hongmei Chi is an Associate Professor of Computer & Information and Sciences at Florida A&M University. She currently teaches graduate and undergraduate courses in Information Security and researches in areas of applied security. Dr. Chi has published articles related to security research and education. Her web page is www.cis.famu.edu/~hchi.

Dr. Allen is an Associate Professor of Computer & Information Sciences at Florida A&M University. He currently teaches graduate and undergraduate courses in Mobile Computing and software security. His research interests are ubiquitous computing, mobile computing, software security and robotics. His web page is www.cis.famu.edu/~allen

Mr. David Rubio is currently pursuing a master degree in computer science at Florida A&M University. He graduated from FAMU with a B.S. in computer science in 2009. His current interests include insider threat detection and mobile security.