Preview of Award 0941959 - Final Project Report

Cover
Federal Agency and Organization Element to Which Report is Submitted: 4900

Federal Grant or Other Identifying Number Assigned by Agency: 0941959

Project Title: Incorporating Systems Security and Software Security in Senior Projects

PD/PI Name: Natarajan Meghanathan, Principal Investigator
Hyunju Kim, Co-Principal Investigator
Loretta A Moore, Co-Principal Investigator

Recipient Organization: Jackson State University

Project/Grant Period: 09/15/2010 - 08/31/2014

Reporting Period: 09/01/2013 - 08/31/2014

Submitting Official (if other than PD/PI): N/A

Submission Date: N/A

Signature of Submitting Official (signature shall be submitted in accordance with agency specific instructions) N/A

Accomplishments

* What are the major goals of the project?

The following are the main goals of our project: (i) Develop course modules in the areas of systems security, software security and cryptography, (ii) Integrate and use the course modules in the Software Engineering and Senior Capstone Project courses, (iii) Develop a Virtual Security Lab (VS Lab) making use of as much as possible off-the-shelf currently available equipment at JSU and the lab can be remotely used by other institutions to test the security course modules and the Senior projects at zero cost and (iv) Develop a sequence of two elective courses on Systems Security and Advanced Information Security that will be offered along with the Software Engineering and Senior Project courses respectively.

* What was accomplished under these goals (you must provide information for at least one of the 4 categories below)?

Major Activities: We recruited student research assistants who can work on various aspects of the project such as lab design, development of course modules and lab projects as well as development of website to host the project materials. We published journal papers and book chapters (all peer-reviewed) based on the work conducted in this project.
We have setup a cloud that is a hybrid of a Platform as a Service (PaaS)-Infrastructure as a Service (IaaS) model running on a Dell PowerEdge T620 server (64 GB of memory, 1.8 TB hard disk and Intel Xeon E5-2680 processor - 2.70GHz, 20M Cache, 8.0GT/s). The cloud (with the Xen hypervisor as the virtual machine manager) is used to setup servers (virtual machine-based) and storage for the senior capstone projects, systems and security courses offered at JSU and other interested institutions with limited resources.

The following courses are referred to as TUES-affiliated courses in the BS Computer Science curriculum at JSU. A course is considered TUES-affiliated if one or more of the lecture modules developed under the TUES grant is taught in the course and/or one or more lab projects developed on Systems Security and Software Security are assigned to the students in the course. The semester/year in the parenthesis indicate the time period starting from which the security modules were incorporated in these courses.

- CSC 330 Database Design (since Fall 2011)
- CSC 435 Computer Networks (since Fall 2010)
- CSC 437 Computer Security (since Fall 2013)
- CSC 438 Systems and Software Security (since Fall 2011)
- CSC 439 Advanced Information Security (since Spring 2012)
- CSC 450 Senior Project (since Spring 2011)
- CSC 475 Software Engineering (since Fall 2010)

The security modules developed as part of the above courses were enhanced with desktop recorded videos of the lectures on the slides and a hands-on explanation of the lab projects (demonstrated in class as well as posted in the course website) providing students an evidence-based learning experience. The videos have been prepared for the different modules in the areas of Cryptography, Database Security, Misuse Case Diagrams, Network Security, Operating Systems Security, Software Security, Steganography, Virtualization and Web Security.

Specific Objectives:
When the students in Spring 2013-Fall 2013 and Fall 2013-Spring 2014 capstone project cohorts formed their groups, we advised that students who plan to take one or both of the two elective security courses (CSC 439 Advanced Information Security, Spring 2013; CSC 437 Computer Security, Fall 2013; CSC 438 Systems and Software Security, Spring 2014) to be part of different groups to maximize the chances that each group has at least one student who will have a good amount of background on security-related topics and will serve as the Security Manager for the team. We found that this strategy really worked well. The students were able to use the knowledge and the security lab project modules (like source code analysis, secure coding standards, encryption, network security standards, CAPTCHA, etc) developed as part of the CSC 437, CSC 438 and CSC 439 courses in their senior capstone projects.

Significant Results:
The incorporation of security modules into these courses was primarily evaluated through instructor (faculty) course assessment and self-assessment feedback surveys from students. In the attachment, we present in detail the survey data and their analysis, assessment results on the two elective security courses CSC 437 and CSC 438 (taught in Fall 2013 and Spring 2014 respectively) as well as assessment of the security modules for the CSC 475 and CSC 450 courses. We also list in detail the assessment tools (quizzes, exams and lab projects) used to
evaluate student performance in the CSC 437 and CSC 438 courses and the security aspects in the other TUES-affiliated courses.

In a scale of 1-4 (1 being Poor/Unsatisfactory and 4 being Excellent), students have been observed to have significantly gained on the different security modules and topics taught. The average student rating on their ability to incorporate security-related aspects in software development before taking both CSC 475 and CSC 450 has been observed to be 1.6; after taking CSC 475, but before CSC 450 has been observed to be 2.7; after taking both CSC 475 and CSC 450 has been found to be 3.5. This shows that students realized the importance of incorporating security in all phases of software lifecycle in an iterative manner.

Key outcomes or
Other achievements:

*What opportunities for training and professional development has the project provided?*

Faculty Members

The TUES project has significantly contributed towards enhancing the knowledgebase of the PI in the areas of Computer Systems Security, Software Security and Cryptography. Over the past 3 years, the PI got introduced to several new topics while he was developing and revising the three senior undergraduate-level/graduate-level elective courses (CSC 437 Computer Security, CSC 438 Systems and Software Security and CSC 439 Advanced Information Security). As there was not any single textbook focusing on all the aspects of systems security and software security, the PI had to read several textbooks that covered particular aspects of systems security and software security and then come up with his own lecture slides for the different modules. The PI had developed an exhaustive question bank featuring a total of about 400 questions covering all the security modules, and used in all the TUES-affiliated CSC courses at Jackson State University. Having disseminated all these question banks online through the TUES website, the PI is also receiving several appreciation emails and clarification emails (for appropriate answers) from the academic community on these question banks. The PI has also developed evidence-based modules on software security attacks.

In addition, the PI conducted an international workshop on Secure Software Development, as part of the 8th International Conference on Software Security and Reliability (SERE 2014), San Francisco, June 30-July 2, 2014. The URL for the workshop is: http://143.132.8.23/cms/nmeehanathan/SEESED/index.html. The objective of this workshop is to encourage researchers to propose models and processes to incorporate security in different stages of software development. He also organized a special track on Software Security as part of the 11th International Conference on Information Technology: New Generations (ITNG) at Las Vegas, NV, from April 7-9, 2014. The objective of this track was to bring together researchers, faculty, students and industry professionals who are experts in different domains of computer and information security, but all leading to the design, development, deployment and maintenance of secure software.

For the CSC 450 Senior Project and CSC 475 Software Engineering courses taught in Fall 2013 and Spring 2014, the Co-PI (Hyunju Kim) seamlessly integrated the security modules developed by the PI with the traditional lecture modules for these two courses. This way, the students perceived Software Security as one of the core aspects of a software development process that needs to be considered in all the stages of a software lifecycle. By integrating the lecture modules and delivering them by herself, the Co-PI got exposed to the security topics and was able to broaden her knowledgebase. As documented in the attachment on Research and Educational Activities, systems security, software security and cryptography modules with a total lecture time worth of more than 800 minutes have been integrated and taught by her in the CSC 450 and CSC 475 courses for each of Fall 2013 and Spring 2014.

Overall, during the period of the grant (September 15, 2010 to August 31, 2014), a total of 7 journal articles, 7 conference proceedings papers and 3 book chapters (all peer-reviewed) were published involving the PI, Co-PIs and students as co-authors. In addition, there were a total of 9 abstract presentations (mostly based on the senior capstone projects) in regional conferences.

Graduate Student Research Assistant

We supported a graduate student research assistant (Michael Terrell for Spring 2014). Michael was primarily involved in setting up the cloud of virtual machines that can be run as servers and as a virtual network lab for the different TUES-affiliated courses at JacksonStateUniversity as well as at other institutions. Michael also developed an interactive website through which users of the different security course modules can submit their feedback online through a survey. Overall, the TUES project trained Michael to be a good software analyst, programmer as well as a researcher.

Undergraduate Graduating Seniors for Academic Year 2013-14

The knowledgebase of the undergraduate graduating seniors who took the CSC 475 and CSC 450 courses as well as the CSC 437 Computer Security courses during the 2013-14 academic year increased significantly. On average, in a scale of 1 (Poor) – 4 (Excellent), the students perceived their knowledge in these security topics tripled or higher, i.e., almost from 1 to 3 or above. More detailed feedback from the student surveys can be found in the attachment for Findings from Activities. The undergraduate students got introduced to a secure software lifecycle process that involved the incorporation of the security aspects in every stage of software development. Such training will be very valuable for these students when they get employed in industries as a software engineer. The undergraduate students also got introduced to certain hands-on lab projects on software testing, virtual machines, web and database injection attacks as well as source code analysis, which will definitely add to their repertoire of skill sets when employed in the IT industry. The undergraduate students got trained in developing security code modules featuring aspects such as public-key encryption (RSA), secure key distribution across sockets, CAPTCHA (XSRF attacks) and login scripts with proper sanitization control routines to weed out injection attacks.

* How have the results been disseminated to communities of interest?

TUES Website for Modules, Question Bank and Lab Project Description: Our primary TUES website, hosted at http://143.132.8.23/cms/tues, has all of the information related to our program. The website has links to the security modules, lab projects and question banks posted for the TUES-affiliated courses (CSC 435 Computer Networks, CSC
450 Senior Project, CSC 475 Software Engineering, CSC 437 Computer Security, CSC 438 Systems and Software Security, and CSC 439 Advanced Information Security) in which one or more course outcomes have been revised to reflect the focus on systems security and software security as well as one or more security lecture modules have been covered and lab projects on security-related issues assigned to the students. All of the security modules, lab project descriptions and question banks posted in the website for these courses are open for public and can be downloaded without any access restrictions. This way, our modules and project descriptions are available for use to any interested student and faculty member in the academic community. In addition, a brief description of the different capstone projects and the incorporation of the security aspects in each of these projects have also been posted online.

The modules that have been posted so far can be categorized under the following areas: Cryptography, Database Security, Misuse Case Diagrams, Network Security, Operating System Security, Secure Coding Standards, Source Code Analysis, Software Security, Steganography, Virtualization and Web Security. For each of these areas, several modules, exhaustive question bank, desktop recorded videos and certain lab project descriptions have been posted on specific topics.

**TUES Website for Assessment and Feedback Collection:** We have also developed a website to collect feedback from users of our security modules, question bank and lab project descriptions. The website can be accessed at: [https://sites.google.com/a/students.jsums.edu/cnss-lab/surveys](https://sites.google.com/a/students.jsums.edu/cnss-lab/surveys). We have posted an exhaustive questionnaire for each of our modules and the associated question bank and lab project descriptions. This website is linked to the modules posted in our main TUES website: [http://143.132.8.23/cms/tues](http://143.132.8.23/cms/tues).

### Supporting Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Uploaded By</th>
<th>Uploaded On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Research and Education Activities of the Project.pdf</td>
<td>Details of the Major Research and Education Activities of the Project</td>
<td>Natarajan Meghanathan</td>
<td>11/29/2014</td>
</tr>
<tr>
<td>Project Findings-Details.pdf</td>
<td>Details of the Project Findings</td>
<td>Natarajan Meghanathan</td>
<td>11/29/2014</td>
</tr>
</tbody>
</table>

### Products

#### Books


#### Book Chapters


Conference Papers and Presentations


M. Terrell and N. Meghanathan (2013). Setting up of a Cloud Cyber Infrastructure using Xen Hypervisor. 10th


**Inventions**

**Journals**


**Licenses**

**Other Products**

**Other Publications**

https://reporting.research.gov/rprr-web/rprr?execution=e1s121
Patents

Technologies or Techniques

Thesis/Dissertations


Websites
Computer Network Systems and Security Lab
http://www.jsums.edu/cms/tues

This website hosts all the materials developed with funding from the TUES project. It hosts the course modules, lab project descriptions and question bank. It also hosts materials about the capstone projects that incorporated the security aspects.

Participants/Organizations

What individuals have worked on the project?

<table>
<thead>
<tr>
<th>Name</th>
<th>Most Senior Project Role</th>
<th>Nearest Person Month Worked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meghanathan, Natarajan</td>
<td>PD/PI</td>
<td>3</td>
</tr>
<tr>
<td>Kim, Hyunju</td>
<td>Co PD/PI</td>
<td>2</td>
</tr>
<tr>
<td>Moore, Loretta</td>
<td>Co PD/PI</td>
<td>1</td>
</tr>
<tr>
<td>Terrell, Michael</td>
<td>Graduate Student (research assistant)</td>
<td>2</td>
</tr>
</tbody>
</table>

Full details of individuals who have worked on the project:

Natarajan Meghanathan
Email: natarajan.meghanathan@jsums.edu
Most Senior Project Role: PD/PI
Nearest Person Month Worked: 3

Contribution to the Project: Natarajan Meghanathan was primarily involved in the following activities during Year 4 (September 2013-August 2014): (1) Develop a new course called CSC 437 Computer Security and teach in Fall 2013. Teach the CSC 438 Systems and Software Security course in Spring 2014. The courses were taught for undergraduate seniors and graduate students. (2) Develop new and revise existing lecture modules and lab project descriptions on various topics in Systems Security and Software Security. (3) Develop and revise question bank for each module and integrate them with the courses using these modules. (4) Maintain the TUES project website posting all the modules, lab project descriptions and supporting materials (5) Coordinate with the Co-PI (Hyunju Kim) to integrate the software security modules in the CSC 475 Software Engineering and CSC 450 Senior Project courses. (6) Mentor graduate research assistant towards setting the cloud for the security courses and the lab.

Funding Support: NSF - TUES

International Collaboration: No
International Travel: Yes, India - 0 years, 3 months, 0 days
Hyunju Kim
Email: hyunju.kim@jsums.edu
Most Senior Project Role: Co PD/PI
Nearest Person Month Worked: 2

Contribution to the Project: Hyunju Kim seamlessly integrated the modules in various topics of systems security, software security and cryptography with that of her regular lecture modules and taught the security modules by herself in Fall 2013 and Spring 2014. As the primary instructor, Hyunju Kim guided the students through all the phases of the software lifecycle. She is also the primary instructor who monitored the incorporation of the appropriate security aspects in the capstone projects.

Funding Support: NSF

International Collaboration: No
International Travel: No

Loretta A Moore
Email: loretta.a.moore@jsums.edu
Most Senior Project Role: Co PD/PI
Nearest Person Month Worked: 1

Contribution to the Project: (1) Recruitment of research assistants to work on the project (2) Locating instructors at other institutions who may be interested in adopting the lecture modules on systems security and software security developed as part of the project (3) Co-ordinate with the instructors teaching the Computer Systems and Software Engineering courses towards incorporation of the security modules in their courses.

Funding Support: NSF

International Collaboration: No
International Travel: No

Michael Terrell
Email: vashisnotatree@gmail.com
Most Senior Project Role: Graduate Student (research assistant)
Nearest Person Month Worked: 2

Contribution to the Project: Michael was primarily involved in setting up the cloud of virtual machines that can be run as servers and as a virtual network lab for the different TUES-affiliated courses at Jackson State University as well as at other institutions. Michael also developed an interactive website through which users of the different security course modules can submit their feedback online through a survey.

Funding Support: NSF

International Collaboration: No
International Travel: No

What other organizations have been involved as partners?
Nothing to report.

Have other collaborators or contacts been involved? No
Impacts

What is the impact on the development of the principal discipline(s) of the project?

The major educational contributions of the project during its third year (2013-14) in the undergraduate Computer Science curriculum at Jackson State University are as follows:

[1] Offering of the CSC 437 Computer Security and CSC 438 Systems and Software Security courses as senior-level elective courses for Computer Science majors. The CSC 437 course was offered in Fall 2013 and the CSC 438 course was offered in Spring 2014. The two courses covered various aspects of systems security (including network security, operating system security, database security, web security, etc), software security (misuse case diagrams, risk analysis for secure software design, secure coding, security attacks and solutions, testing for software security, etc), cryptography (symmetric and public-key cryptography, classical ciphers and their cryptanalysis).

[2] Seamless integration of the security modules with the regular lecture modules of the traditional senior capstone project courses such as CSC 475 Software Engineering and CSC 450 Senior Project to educate students on the incorporation the security aspects in different stages of a software lifecycle. This can serve as a good model for other interested schools to revise their software engineering curriculum and embed security in their capstone projects.

The following security modules were incorporated to the CSC 475 course:


*Security Module 2: Risk Analysis for Secure Software Design*

*Security Module 3: Requirements Engineering*

*Security Module 4: Software Security Attacks*

*Security Module 5: Testing for Software Security*

The CSC 475 course outcomes reflect the tight integration of the security modules and topics with the rest of the course modules:

Each student who successfully completes this course should be able to:

**CO1:** Explain software process models and their characteristics and principles and models for software security

**CO2:** Understand issues in project management, including planning for software development and specify software evolution processes and issues in software maintenance

**CO3:** Apply key elements and common methods for elicitation and analysis to produce a set of software requirements, including the appropriate security-related aspects, for the chosen Senior Project

**CO4:** Select and apply appropriate design tools and guidelines in developing software

**CO5:** Specify issues in risk assessment for secure software design and explore different software security attacks
with respect to dependency, user interface, design, and implementation

**CO6**: Test software, including the security aspects using software verification and validation methods

The following security modules were incorporated to the CSC 450 course:

*Security Module 1*: Basics of Cryptography

*Security Module 2*: SQL Injection, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (XSRF) Attacks

*Security Module 3*: Source Code Analysis using the Fortify Suite

The CSC 450 course outcomes reflect the tight integration of the security modules and topics with the rest of the course modules:

Each student who successfully completes this course should be able to:

**CO1**: Work in a team to produce software solutions to information/automated system needs

**CO2**: Update software requirements and project plan according to new findings and changes

**CO3**: Develop and implement different modules, including security-related module(s) depending on the requirement analysis and design

**CO4**: Produce test cases based on testing methods and incorporate testing for security and conduct testing

**CO5**: Communicate software development information in graphical, written, and oral form

Students were also assigned several hands-on lab projects on Source Code Analysis, Java secure coding standards, SQL injection attacks, XSS and XSRF attacks, TOCTTOU attacks and Software testing. Some of these projects have to be conducted in a virtual machine environment.

[3] Development of an exhaustive question bank covering various topics in the following modules: Cryptography, Network Security, Software Security, Web Security, Database Security, Operating Systems Security, Virtualization and Steganography. The question banks are listed along with the slides for the lecture modules and the lab project descriptions in our TUES website: http://143.132.8.23/cms/tues. In addition, videos on selected topics were also recorded offline (in a desktop recording environment) and posted in the TUES website.

The major research and professional contributions of the project to the academic community during its third year (2013-14) are as follows:

Analysis: A Case Study on a Java File Writer Program with Password Validation Features,” published by the PI in *Journal of Software* (JSW), vol. 8, no. 10, pp. 2412-2424, October 2013, illustrate the use of source code analysis to identify and remove the following software security vulnerabilities: (i) Hardcoded Password, (ii) Empty Password Initialization, (iii) Denial of Service, (iv) System Information Leak, (v) Unreleased Resource and (vi) Path Manipulation. We propose one or more solution approaches to remove or at least mitigate each of these vulnerabilities that have the potential to significantly impact the security of software programs if they are left unattended. In this context, we conduct an exhaustive source code analysis of a file writer program, developed in Java, embedded with features for password validation in order to illustrate the Hardcoded password and Empty password initialization vulnerabilities. We also illustrate the occurrence of one or more new vulnerabilities as a result of incorporating a patch (code) to remove an existing vulnerability. Our solution approaches to remove the above vulnerabilities can also be adapted to other high-level programming languages like C/C++. We use the Fortify Source Code Analyzer (SCA) software to conduct the automated source code analysis of the file writer program to test for software security, including both identification and removal of the vulnerabilities.

[2] The book chapter titled "Network Security: Attacks and Controls," Chapter 11, pp. 174-203, *Network Security Technologies: Design and Applications*, ISBN: 1466647892, IGI Global Publishers, Hershey, PA, USA, November 2013, first presents the classical network attacks (such as Session Hijacking, Man-in-the-Middle attack, DNS attacks, Distributed Denial of Service attacks, and other miscellaneous attacks), which have exploited the various vulnerabilities of computer networks in the past, and reviews the solutions that have been implemented since then to mitigate or reduce the chances of these attacks. We then present the different network security controls, including the protocols and standards (such as IPSec, Kerberos, Secure Shell, Transport Layer Security, Virtual Private Networks, Firewalls, and S/MIME) that have been adopted in modern day computer networks to control the incidence of attacks in modern day computer networks.

What is the impact on other disciplines?
Nothing to report.

What is the impact on the development of human resources?

The TUES project during the academic year 2013-14 had a direct impact on a total of 32 undergraduate students who took the CSC 437 Computer Security, CSC 475 Software Engineering and CSC 450 Senior Project courses. The impact was in the form of revision of the course outcomes to embed the security modules as well as the incorporation of the aspects of systems and software security in different stages of the software lifecycle. Since software security is an emerging topic, the undergraduate students who successfully completed the senior capstone projects with the appropriate incorporation of the security aspects will be well ahead of a larger number of software engineers who are still used to the strategy of fixing a software (through appropriate patches) only upon failure or after the incidence of any security attack.

A graduate student was supported through the TUES project. The research assistant had a significant gain in his knowledgebase by working on diverse activities such as setup of cloud cyber infrastructure, design of website for survey data collection, development of course/lecture modules, lab project descriptions, requirements analysis of various project scenarios from a security point of view and etc.

Integration of Research and Education

The TUES project has been providing ample opportunities for the PIs and students to integrate research and education. Examples of the integration are the publication of papers and book chapters on: (1) Identification and Removal of Software Security Vulnerabilities using Source Code Analysis: Case Studies on Java Programs; (2) Virtualization as...
the Catalyst for Cloud Computing; (3) Setting up of a Cloud Cyber Infrastructure using Xen Hypervisor; (4) Network Security: Attacks and Controls. Most of the materials from these papers were also incorporated as lecture slides and sometimes as part of lab projects, in the appropriate modules on systems security and software security.

We strongly believe in integrating research and education to provide students up-to-date information on the subject materials, specifically on those topics that are not yet well documented in textbooks and are mostly available as research publications. For example, the paper on source code analysis and case studies, evolved from the initiative of the PI to develop a lab project on using the Fortify Source Code Analyzer to analyze the security of a file writer program with password validation features. We observed that there is no such paper that formally analyzed the different security vulnerabilities through hands-on source code analysis, and presented appropriate techniques/solution approaches to completely avoid or at least mitigate these vulnerabilities.

Developing and Disseminating New Education Materials

The security modules, lab project description, desktop recorded videos and question bank for the different modules covered in the TUES-affiliated courses (Computer Networks, Software Engineering, Senior Project, Computer Security, Systems and Software Security, and Advanced Information Security) are posted online at the TUES website: http://143.132.8.23/cms/tues. The slides, question bank and the project descriptions can be respectively used as a good teaching material and assignment material at both undergraduate and graduate levels. The security modules have been prepared in such a way that they can be adopted even by instructors from a non-security background and seamlessly integrate with the lecture modules for their traditional systems and software engineering courses.

What is the impact on physical resources that form infrastructure?

The cloud infrastructure setup by the PI and his research team could facilitate users to be able to access the servers located in the Computer Network Systems and Security (CNS) Laboratory at Jackson State University remotely. They will use this access in the cloud to run virtual machines and utilize the powerful server hardware. These virtual machines can either be created from user provided images or operating system images that have been previously stored on the server. In order to allow users to use these virtual machines some type of virtual machine manager is needed. For this project the Xen Hypervisor was chosen to fulfill this need. The hypervisor was installed on a server located in the laboratory and allows users to remotely log in and create their desired machines.

What is the impact on institutional resources that form infrastructure?

The cloud infrastructure could be used for setting up of virtual machine servers for specific courses. Individual accounts could be created for students and they can seamless login (remotely) from any computer and do their project. Also, students can setup a network of virtual machines and perform research projects as well as capstone projects with minimal resource constraints.

What is the impact on information resources that form infrastructure?

The cloud infrastructure can be used to host websites for the courses and all the course materials. Space-consuming lecture video files could be stored in the cloud and made accessible online for students and faculty.

The security modules along with the question bank (for the TUES-affiliated courses) posted at the project website can be used for seamless integration with the traditional modules for software engineering courses as well as in systems courses such as operating systems, database systems and computer networks. The step-by-step lab project descriptions can be adopted by interested instructors in academic institutions for assigning course projects to their students. The exhaustive question bank for each of the modules will be very useful for both instructors and students to test their understanding the subject materials and ensure that they do not miss any important information covered in the modules. The desktop recorded videos can become very informative for students who seek to get better clarification on the classroom lectures on similar topics.
What is the impact on technology transfer?
Nothing to report.

What is the impact on society beyond science and technology?
Nothing to report.

Changes/Problems

Changes in approach and reason for change
Nothing to report.

Actual or Anticipated problems or delays and actions or plans to resolve them
Nothing to report.

Changes that have a significant impact on expenditures
Nothing to report.

Significant changes in use or care of human subjects
Nothing to report.

Significant changes in use or care of vertebrate animals
Nothing to report.

Significant changes in use or care of biohazards
Nothing to report.

Special Requirements

Responses to any special reporting requirements specified in the award terms and conditions, as well as any award specific reporting requirements.
Nothing to report.