Primary Faculty Name:	Wu He
Department:	Information Technology & Decision Science
Email Address:	whe@odu.edu
Office Phone Number:	757-683-5008
Project Title: (10 words or less)	Using the Workflow Technology to Create Secure Software Engineering Scenario-based Workflows for Information Security Education

Other faculty:

Faculty Name:	Department	Email Address	Office Phone Number
Yaohang	Li	yaohang@cs.odu.edu	757-683-6001x5085

1. Describe the specific teaching and learning issues being addressed by the proposal.

Information security is a serious worldwide concern of governments, industry, and academia. Due to the increased reliance of governmental, military, and financial functions on complex interconnected computer systems and networks, many universities are offering information security courses to both undergraduate and graduate students. ACM/IEEE has also published curriculum guidelines in 2008 for accrediting five computing degree programs: computer engineering (CE), computer science (CS), information systems (IS), software, engineering (SE), and information technology (IT) and recommended all these five programs to include information security as a new focus area because of the emergence of security as a major area of concern.

However, teaching information security courses is technically challenging. An information security course typically requires the use of a series of security analysis and testing services and tools such as source code analysis tools, SQL injection testing tools and web service penetration testing tools. Due to the fact that most of these security services and tools used in information security education are developed by different groups, each of them often has heterogeneous platform requirements and preferences, installation/configuration instructions, user interfaces, and usage parameters. In a security course, students and instructors often end up struggling in low-level and complicated software installation, system setup, service configuration, and data manipulation while losing concentration in learning the important information security principles. Some students without strong technical background often have to give up doing their security exercises or projects due to some technical issues in installation and configuration.

To help students in information security courses learn information security principles more effectively and efficiently, we propose to use the workflow technology to improve teaching and learning in information security courses. The workflow technology provides unified, interactive graphical interfaces for students and allows information security cases or scenarios to be built without the need for low level programming or command-line interactions. The proposed workflow approach will not only save students a lot of time in learning security principles but also help instructor teach security detection and defense techniques using a visual, interactive and intuitive approach.

2. Describe the revised specific teaching and learning issues being addressed by the proposal (if applicable):

3. Describe the development activities involved addressing the learning or teaching issue.

We used the workflow technology (Georgakopoulos et al., 1995) to simulate complex real-life scenarios within a laboratory setting to enhance information security education. The workflow technology provides interactive graphical interfaces to build sophisticated information security cases without the need for low level programming or command-line interactions, and allows collaboration among students with different educational background. Moreover, the workflow technology enables seamless integration of distributed and local services to support composition of complex case studies. The students actually created three cases. After reviewing the three cases developed by students, we finally chose two cases developed by them for

course evaluation. Two complex case studies using the Kepler scientific workflow system (Ilkay et al., 2004) are used in class to show how we create and enact workflows for real-life scenarios. The first case study simulates a scenario of attacking a bank account based on a real security incident described in the Daily Record magazine (Mann, 2012). The second case study models a situation of coordinated attack to compromise an online course management system. The workflows for both case studies were developed by students in Computer Science and were then used to support teaching in Information Technology (IT) security courses. We received IRB approval for this study. Student feedbacks on using the workflow technology in teaching information security principles and techniques are also discussed and analyzed.

4. Describe the learning outcomes attained by the project.

Two finalized workflow-based scenarios were demonstrated to students in four IT courses with small class size (class 1 has 16 students; class 2 has 9 students; class 3 has 7 students, and class 4 has 18 students). After a demonstration of the two case studies, we invited the students to complete a survey on using workflow technology for teaching information security. The survey was approved by the college's institutional review board (IRB). 42 students (26 undergraduates and 16 graduate students) volunteered to complete the survey. The results of the survey are summarized as below.

.

Statement	Strongly agree	Agree	Neither Agree Nor Disagree	Disagree	Strongly disagree
Workflow technology is very useful for learning information security concepts.	12 (28.6%)	21 (50.0%)	7 (16.7%)	0 (0.0%)	2 (4.8%)
I am interested in learning more about using the workflow technology for information security.	9 (21.4%)	20 (47.6%)	11 (26.2%)	1 (2.4%)	1 (2.4%)
I enjoyed learning information security concepts using the workflow technology	8 (19.0%)	25 (59.5%)	8 (19.0%)	0 (0.0%)	1 (2.4%)

Table 1: The survey results of the learning-related statements

The students were asked to rate the degree of their agreement with three learning-related statements. Table 1 shows that the majority of students either agree or strongly agree that using the case studies implemented by the workflow technology is helpful in deepening understanding of the information security concepts and technology.

Students also made some qualitative comments. Some students liked the fact that the workflow break down the scenarios on a step by step basis and make the hacking process

easier to follow. They enjoyed seeing the simulated attacking process behind the SQL injection, denial-of-service, and phishing attacks visually and appreciated the workflow implementation in helping them better understand the concepts. A student even pointed out that the workflow-based scenarios provide an opportunity to conduct practical training without the need of multiple computers or servers. Below are some quotes from the participated students:

- *"I understand the attacks well after seeing the demo."*
- *"It gave me a better understanding of SQL injections."*
- *"Scenario-based workflows look useful in dealing with user requirements."*
- *"Very good. It visually depicts the flow of security attacks and helps improve understanding."*
- *"In the real world, you have to be able to explain security issues to non-technical managers. I think the scenario-based workflows are very important."*
- *"My favorite part is to see codes interpreted graphically."*

The participating students also provided suggestions for improving the workflow-based scenarios. They suggested adding more details to the workflows in order to make the scenarios as similar as possible with real life situations. They also suggested making the GUI of the workflows more user-friendly and engaging. A few students noticed that there were many actors in the workflows and wondered how much time it took to build a complex workflow. Some students expressed interest to learn how to make such workflows because they believed the workflow-based scenarios were useful. Some comments and suggestions from the students participated in the survey are listed as follows:

- *"Make the program mimic more complex workflows based on actual sites."*
- *"Make it a little more realistic. The online banking scenario needs to deal with emails, too."*
- *"I am curious to see the translation from graphical workflow to actual code if possible."*

After in-class demonstration of the two case studies, the instructor asked students to complete the associated learning tasks. For case study I, students in the Web programming course were required to check the programs they developed before and fixed the SQL injection vulnerabilities if they existed. Students were also required to create programs free of SQL injection vulnerabilities in the subsequent assignments and final project. By grading students' assignments and testing their programs, we found that the vast majority of students understood the SQL injection vulnerabilities well and successfully wrote codes to prevent SQL injection. Thus, we were convinced that most students have achieved learning objectives of case study I. For case study II, students in the information security course were required to further research DoS attacks and discuss in class what approaches they could use to detect DoS attacks and mediate the impact of such attacks. Based on their discussion, we clearly found that students had a good understanding of DoS attacks, its consequences, and possible mediation strategies. We did not conduct further testing to assess students' understanding about DoS attacks since our main interest was how students have perceived the workflow-based information security scenarios.

5. Describe unexpected outcomes, if any.

6. Describe the impact of the completed project on your colleagues, department, college, or community.

The two workflow-based scenarios were introduced to students in undergraduate- and graduate-level courses. The evaluation result shows that most students were positive on the effectiveness of using workflow to teach security techniques and concepts. We have submitted a paper to the journal of Information Systems Education. This paper is under review right now and hopefully will be accepted this year.

7. Describe how the project can be a model, template, or prototype for use by other instructors.

Teaching information security skills effectively is difficult without ready access to adequate case studies. Case studies have often been recognized as important tools to illustrate conceptual or complex materials. Oftentimes, a real-life information security situation is complicated, which involves numerous steps. It is often challenging for instructors to describe such complex security situation orally in class. It is also hard for students to understand complex security techniques and concepts without visual examples. In this project, we developed two workflow-based case studies using the Kepler software to simulate real-life scenarios in information security. The two workflow-based scenarios were then introduced to students in undergraduate- and graduate-level courses. The evaluation result shows that most students were positive on the effectiveness of using workflow to teach security techniques and concepts.

Currently, there is a lack of ready-made information security-related case studies available, which makes the application of the case study methods in information security education challenging (He, Yuan & Yang, 2013). We plan to share our developed workflow-based case studies on the Internet. As for our future work, we plan to design guidelines to help interested information security instructors develop workflow-based case studies using the workflow development/management software packages. More workflow-based security case studies are being designed and will be shared with the information security educational community once they are ready.

8. Describe the technology used to help address the issues described in the proposal.

We used an advanced workflow software tool named Kepler to build workflows for three different secure software engineering scenarios used in the PI's security course. Kepler is an open source software tool developed by using Java language. It can be downloaded at https://kepler-project.org/ . Kepler supports Windows, OSX, and Linux operating systems and provides instructional materials and tutorials for learning how to use Kepler to build workflows. Some sample workflows are also provided to help programmers to learn to build workflows using Kepler and programming java language. Overall, Kepler provides a straightforward way to help java programmers build a workflow across a broad range of disciplines such as science, engineering, technology and business.

9. Describe products, if any, that are a result of the project.

We would like to introduce two finalized workflow-based scenarios we developed through this project

.

Case Study I: Complicated Attack Patterns for Illegal Banking Account Transfer

In 2012, a real life security scam involving online bank account balance wire transfer was reported with relatively complicated attack pattern (Mann, 2012). The ultimate goal of the

hacker is to transfer a large amount of money from a compromised customer's banking account to an oversea account. First of all, a hacker breaks into a bank customer's banking account to initiate the money transfer. However, recently, many banks have implemented an anti-fraud policy that unusual activities such as money transfers exceeding certain amount will notify the related customers, mostly via automated phone calls or messages. Warned by the notification messages, the victim banking customer would have a chance to stop the money transfer during a grace period. Therefore, the hacker must prevent the customer from receiving the anti-fraud notification calls or messages. In order to achieve this, the hacker carries out a sequence of denial-of-service attacks by continuously calling the customer's phone. Bothered by numerous strange phone calls, the annoyed customer will likely turn off his/her phone and thereby miss the anti-fraud notifications from the bank. As a consequence, if the above steps in the scam and attack procedure were carried out successfully, the hacker will achieve his goal of transferring money out of the customer's banking account.

This case serves as an ideal in-class example to demonstrate a complicated real-life attack patterns. Using the real-life banking case as the blue print, our first workflow scenario is designed by simulating the above banking case while embedding basic and important information security techniques taught in Information Security classes. First of all, we implemented a module of SQL injection attack to simulate the hacker's process of stealing the user's credentials and personal information from the back-end database by taking advantage of the security holes in the web server. The sub-workflow in SQL injection module serves the educational purpose of showing how a security hole in database can lead to vulnerability of an information technology system. In the denial of service attack module, we developed a sub-workflow to invoke a phone-calling web service to implement consecutive phone call making. During in class demo, we asked a student to volunteer his cell phone to demonstrate the effect of denial of service attack. We also implemented a transaction validator module to reflect the changes of banking accounts in this case study. The learning objectives of this case study include:

- to understand SQL injection attacks in computer programs;
- to describe strategies for avoiding SQL injection attacks;
- to discuss banking anti-fraud policies;
- to analyze computer programs and identify SQL injection vulnerabilities;
- to apply coding techniques to eliminate SQL injection vulnerabilities in computer programs; and
- to create SQL injection free computer programs.

Figure 1 shows the high-level Kepler workflow that implements the banking case study, as well as the relevant screen shots including SQL injection information, banking account status changes, and user notifications, during the workflow execution. The high-level workflow provides a big picture of overall attack pattern in this case study. The execution of the workflow simulates the banking attack case study step by step, which provides students an opportunity to experience a simulated real-life security attack in a lab setting. At the same time, students were inspired to think about the related security techniques and policies to prevent such attacks. For students who were interested in technical details, they can explore the sub-workflow in each module to learn the detailed implementation mechanism. An example of the detailed implementation of the SQL injection sub-workflow is shown in Figure 2.

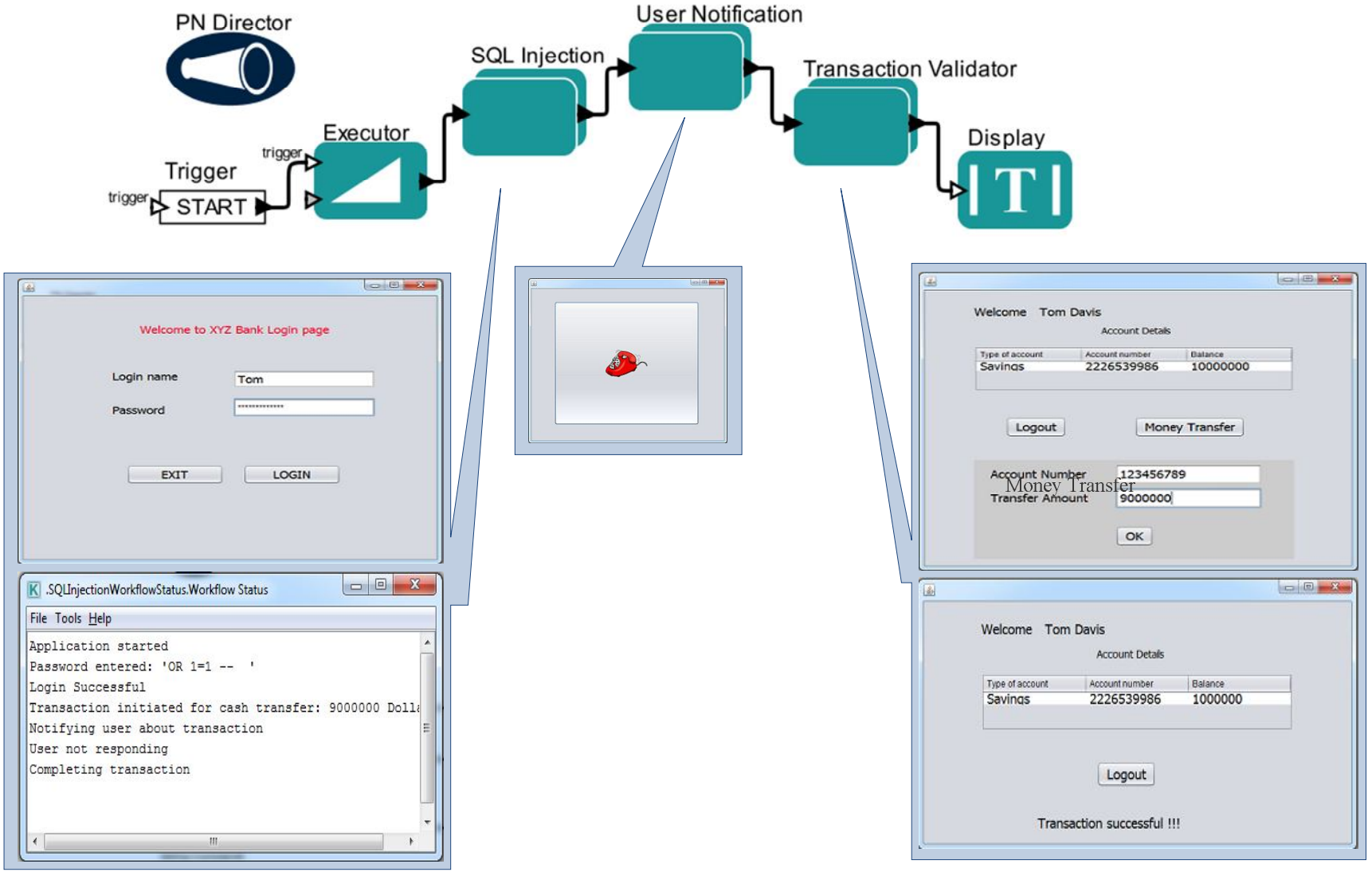


Figure 1: Kepler workflow for Case Study I: Complicated Attack Patterns for Illegal Banking Account Transfer

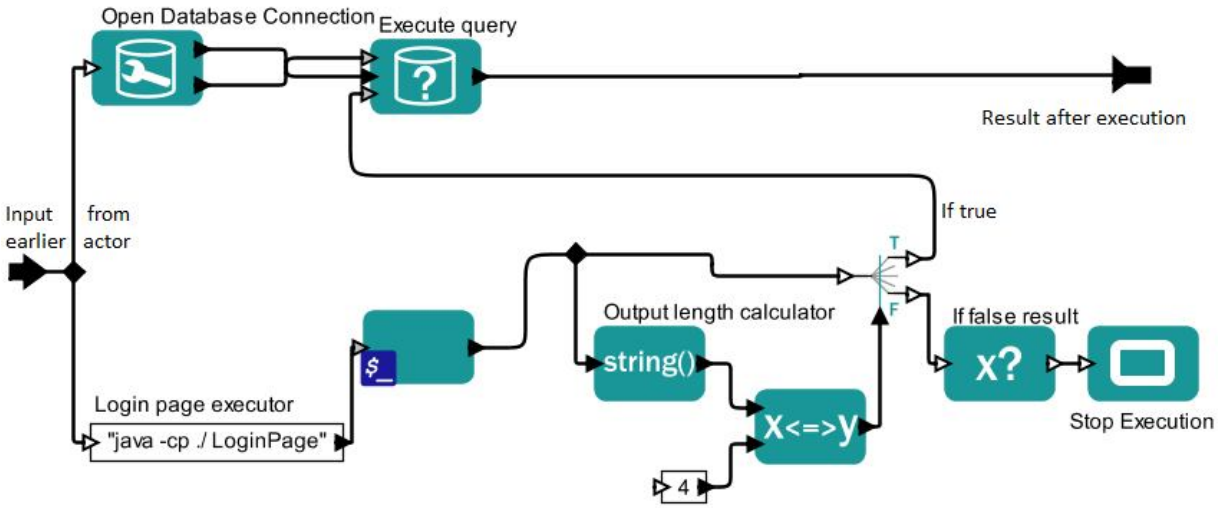


Figure 2: Implementation Detail of the SQL Injection Sub-Workflow

A learning task is associated with this case study to help achieve the learning objectives. Students were asked to evaluate the web scripting programs in the case study workflow for potential SQL injection vulnerabilities and provide solutions to address these security holes. The follow-up programming assignment and project involved creating web scripting programs free of SQL injection vulnerabilities, where the instructor will test and grade their programs against the SQL injection attacks.

Case Study II: Coordinated Attacks on Online Course Management Systems

Online course management systems such as Blackboard and Moodle are widely used in higher education. Many instructors use such systems to teach their online or on campus courses, storing course materials, conducting online discussion, and managing student grades. As the popularity of online course management systems continues to grow, there is increasing interest in attacking online course management systems or other e-learning applications (Schultz, 2013). The design of the second case study is inspired by various recent real-life attempts to break in the online course management systems for grade changing (Carr, 2013). This case study models a situation of coordinated attack to compromise a testbed which is an online course management system based on Moodle. The instructor talked about the ethics guidelines and issues before presenting this case study to students. Several studies discussed ethical hacking and suggested that university information security curriculum must include both “defender” and “attacker” perspectives in order to meet the demand for trained security professionals with attack and defense skills (Bratus, Shubina & Locasto, 2010; Curbelo & Cruz, 2013;Logan & Clarkson, 2005;Pashel, 2006). To reduce possible ethics concerns, we hid the actual programming codes from students.

One way to attack online course management systems is to use the denial-of-service (DoS) attack technique. To launch a DoS attack, an attacker typically sends a very large number of connection requests to flood a target system. When more requests for services than the target system’s handling capability are received, the target system

often stops working or even crashes (Whitman & Mattord, 2011). Once the target system is down, co-ordinately, the hackers can set up a fake system with exactly the same URL and user interface on the Internet for phishing. Phishing is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. When a course instructor tries to login to the fake course management system, his or her account information will be captured by the fake system. Later on, the hackers can use the instructor's account information to visit the legitimate course management system and carry out malicious activities, such as changing grades or stealing exam/quiz questions, at will.

Our second case study implements a workflow-based scenario to simulate the DoS attack and phishing on an online course management system we establish for testing. The learning objectives of this case study are:

- to understand DoS attacks and phishing on computer systems;
- to understand the impact of DoS attacks on network and systems; and
- to identify defense mechanisms to protect against DoS attacks and phishing

Figure 3 shows the designed overall workflow of this case study. The DoS attack sub-workflow initiates the server attack by calling a java application which in turn attempts to establish a large number of connections to the server hosting the on-line course management system. Thereby, when the server's resources are exhausted, it is unable to accept new connections. Figure 4 illustrates the detailed implementation of the DoS attack sub-workflow. Following the DoS attack, a phishing module is used to implement the impersonation of the authentic online course management server. This fake Trojan server has exactly the same user interface appearance as the original system and serves the purpose of phishing the login account information from unsuspecting instructors. The stolen login account information is then used by the hackers to modify student grades.

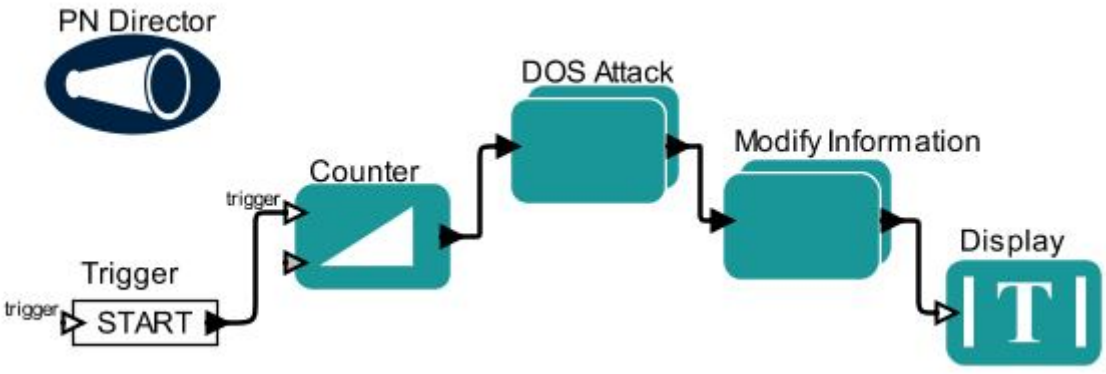


Figure 3: The Kepler Workflow for Case Study II: Coordinate Attacks on an Online Course Management System

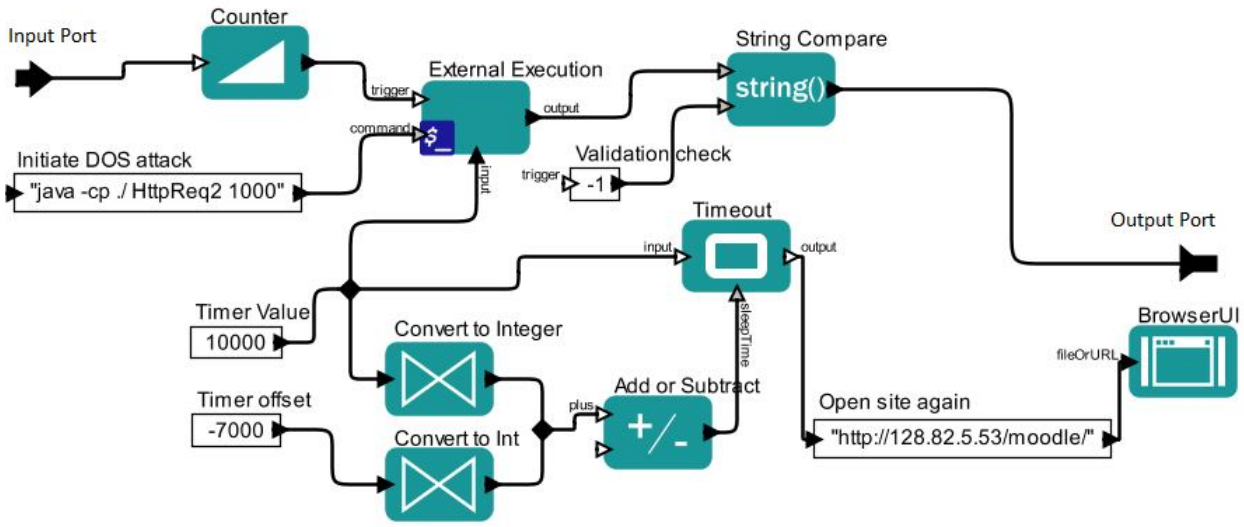
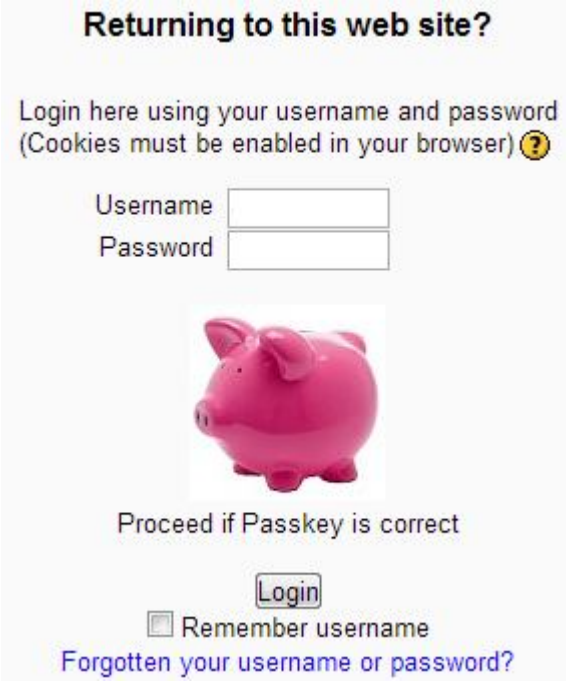


Figure 4: DoS Attack Sub-Workflow with Detailed Implementation of the DoS Attack Mechanism on a Moodle Server

As for the learning objectives associated with this case study, further in-class discussion on possible ways to mediate the DoS attacks can be included to help students further study DoS attacks and techniques that can detect DoS attacks and mediate the impact of such attacks. The example shown in Figure 5 demonstrates the "SiteKey" technique to prevent phishing. By comparing the executions of the Case Study II workflow on the Moodle servers with and without SiteKey protection through the in-class discussion, we can help students get a better understandings on DoS attacks as well as techniques that can prevent phishing.

(a): Moodle Server without SiteKey Protection



(b): Moodle Server with SiteKey Protection
Figure 5: Using SiteKey Protection in the Moodle Server to Prevent Phishing

10. Describe the future plans for this project, if any.
We plan to submit a grant proposal to NSF and other Federal agencies based on the results we gained from this project. We believe that the preliminary data and publications from this project will help us more competitive in applying for grants in the area of information security education.

11. Attach a financial report with updated Budget Plan Matrix.

Final Budget Matrix

			Source of Funds	
Budget Item (equipment, personnel, software, etc.)	**Qty**	**Total Cost**	**Amount from FIG**	**Amount from Other Source**
A student worker	1	$2100	$2100	0