Raquel Hill - Teaching Statement

Raquel Hill
ralhill@indiana.edu
Associate Professor of Computer Science
School of Informatics and Computing
Indiana University

Teaching Statement

My interest in teaching stems from my experiences as a high school student. While preparing for exams, I often explained calculus problems to my friends. When I reflect on these experiences, I realize that I enjoyed teaching. I also understand that being able to explain the problems to others was just as important for my mastery of the material. Although many years passed before I was able to connect these experiences with my desire to become an educator, they have shaped my overall approach to teaching. I believe that students absorb more information when they actively participate in the learning process. One key ingredient to active learning is to allow students to present their knowledge about a topic. I have found that providing an environment where students can be co-educators increases student interest in the subject matter, increases class participation, and encourages peer involvement. It also enables me to assess student interests and use this feedback to update and refine the course content.

To facilitate active learning and knowledge ownership by all students, I evaluate the backgrounds of the students and create an environment where all feel comfortable participating in the learning process. To this end, during lecture, I often assign students to groups for in class problem solving. I have found that students learn more by actively applying concepts than by listening to a lecture. This has been especially true in my undergraduate courses. In addition to classroom problem solving exercises, at least one assignment per semester allows students to research a topic and present the topic in class. This assignment is usually done in small teams and helps to develop students’ presentation, collaboration and knowledge synthesis skills. This assignment tends to generate much excitement among my undergraduate students. Students not only present on topics that they have researched; they often take the assignment to the next level and implement a piece of software to demonstrate to their peers. I also use similar feedback mechanisms for my graduate course. In the graduate course, I will typically define a real-world problem and the students and I will analyze the problem to determine whether previously studied mechanisms or techniques can be used to address the problem.

Feedback from cooperative learning techniques benefits both the students and me. I have used feedback from group problem solving sessions to identify topics that the students did not understand well. These sessions also helped my students identify areas in which they were weak and motivated them to study those areas more diligently.

1.0 Courses

After joining Indiana University, I developed three new courses: I230 Analytical Foundations of Security, B649 Trusted Computing, B649 Data Protection. I230 has been taught at least once per year for the past eleven years. I have taught two additional undergraduate courses (P438 Introduction to Computer Networks, and H343 Honors Data Structures) and two additional graduate courses (P538 Computer Networks and I520 Security for Networked Systems).
1.1 Courses Developed

In this section, I provide a description of the courses that I have developed.

**I230 ANALYTICAL FOUNDATIONS OF SECURITY**

In this course, students learn the essential functions of computer hardware (CPU, memory, etc) and software (operating system, applications, etc). They also learn how to examine hardware and software processes to identify basic security vulnerabilities, factors that contribute to these vulnerabilities and possible results of these vulnerabilities. Additionally, they learn how the interactions of these components create vulnerabilities and impact the security of the system. Students also analyze the risks to computing systems in various environments (standalone, multi-user, network (wired, wireless, direct access, firewall), etc). In addition, they examine information protection issues that affect our ability to preserve the confidentiality and integrity of data. We use case studies to illuminate the issues of well known security problems and evaluate proposed solutions. The students cover a variety of topics including IP networking, TCP, TCP vulnerabilities and countermeasures, network tapping and design measures to counter tapping. Assignments include problem sets and hands on exercises, such as the PGP lab, that requires students to install, configure and use email encryption software to send confidential email messages.

The target audience for this course is undergraduate students who are interested in understanding the security risks and threats to their computing system. During the course, they also learn how their actions and the actions of malicious users may impact the security of these systems. I230 is an introductory course, and no prior experience with operating systems, computer networks or programming languages is required.

Over the years, the average enrollment has increased from 16 to approximately 120 students. The students tend to enjoy the class and often ask whether I will teach another class in the sequence of security courses that are offered. Below, I quote several unsolicited comments from students that indicate the success of the course: “It has been a very fun and interesting semester. I truly learned a lot. I really enjoyed your class and your teaching”. “I really enjoyed the class and learned a lot”. “I did very well in these interviews because of your class and the vocabulary that I obtained thus far. I received an offer for John Deere to work with encryption and restore points on many different operating systems with their Systems Team”.

**B649 TRUSTED COMPUTING**

A Trusted Computing Platform (TCP) is a device that uses some amount of hardware enhancement to increase trustworthiness. These enhancements often include separate processor and memory that enable the execution of code and storage of data in a protected space. TCPs differ from secure platforms in that TCPs can attest that they are operating as expected, while current secure platforms cannot. The ability to attest operating behavior is of fundamental importance when trying to determine whether Alice can trust the computation that is occurring on Bob’s machine. This question becomes important when considering multi-party computation scenarios that are common to distributed applications. For example, take an online credit card transaction that requires computation on both the client and server. While the Secure Socket Layer (SSL) protocol may be used to authenticate the server and establish a secure communications channel, it cannot ensure that the server application will process and manage the data in the expected manner.
The problem of producing trusted computation becomes more challenging because we are building increasingly more complex applications to carry out some of the most critical tasks in our society. We have long understood that it is essential to validate computers, programs, or pieces of hardware, and we have a myriad of acceptable methods for performing those tasks. However, as we begin composing larger and larger systems out of what may well be individually trusted components, we have introduced a level of vulnerability in the dependencies between these components. Such components include the operating systems, loadable kernel modules, device drivers, application run-time environments, etc. Currently, we do not have a systematic way of understanding all of the dependencies and relationships that may exist within a large software system, and until we develop a holistic, systematic way of understanding these trust dependencies, we can expect to have vulnerabilities in our computing infrastructure.

In this class, students explore current methods for characterizing, establishing and attesting trust of a system. We cover a variety of topics including hardware-based trusted components, trusted identities and identity management, reputation systems, trust negotiation, trust and security metrics, etc. Our goals for the course are to:

- Understand the various issues that require the ability to prove that a computer system can be trusted. The focus will be on the design of trustworthy systems and processes.
- Investigate a trusted computing problem through a semester long research project.

The target audience for this course is graduate students with a background in advanced operating systems and computer networks. Over the years, the average enrollment for the course has increased from 7 to 12 students. Projects from the course have resulted in three publications in prominent peer-reviewed venues [1-3]. Below, I quote an unsolicited comment that indicates the success of the class: “Appreciate your direction in class. Just to give you my personal feedback so far regarding the class. I am learning a lot; to be honest I had never heard about Trusted Computing the way you're teaching it. When I decided to take this class, I thought it was more to do with security cryptography etc. This class has changed my way of thinking and appreciation for Trustworthiness not only in computer systems, but in daily life too. I am also hoping to look into how one can program a TPM to incorporate it into computer system. I believe that is the direction for the next computing platforms and systems. Thank you for your time and input in my career development.”.

**B649 Data Protection**

Big Data is more than the latest buzzword, it is big business. The main revenue stream for many of today’s companies is not the product or service that they are offering, but the data that they collect from the consumer as he or she uses the product/service. Consumer data collection may have begun with retail loyalty cards, but has now exploded with growth in social networks, online advertising, and mobile apps. Recent reports state that most mobile apps collect and share personal user data, including: username/password, phone_id, age, gender, location, phone number, contacts, etc. This data is identifying and can often be used to link de-identified data back to an individual identity. Sharing this data, with third parties makes identifying information more widely available; therefore limiting the effectiveness of current data security and privacy mechanisms. Collecting and owning such customer data is also a liability for businesses, for it makes them targets for attacks that compromise confidentiality and data integrity. The problem is
further complicated when data has been classified as sensitive and access to sensitive data are regulated by legal statutes such as the Health Insurance Portability and Accountability Act.

Trust is central to relationships among people, technologies, and organizations in society. When people provide sensitive information about themselves to organizations, they trust those organizations to protect that information. From an access control infrastructure perspective, people expect that only the appropriate entities will have access to their sensitive information, and that organizations have mechanisms in place to ensure that unauthorized entities cannot gain access. Unfortunately, recent security breaches demonstrate that the level of trust people place in organizations that are responsible for handling their sensitive information can be undeserved. A common theme of these breaches is that compromises to cyberinfrastructure go undetected for extended periods of times. The presence of a compromise indicates that the system is in an untrustworthy state.

In this class, we will explore current proposals for protecting data. We will investigate various methods for protecting the identities of individuals who participate in studies, whether data is maintained by the data owners or by within the cloud. In addition, we will investigate the various risks of storing sensitive data on mobile devices where the threat of access to data by malicious software increases as we download more applications. Our goals for the course are to:

- Understand the types of data that are being collected by businesses or willingly shared via social networking sites, and the associated risks to privacy.
- Evaluate legal requirements for protecting sensitive data
- Perform use case analyses on businesses that collect, maintain, share, and manage access to our sensitive data, and design plans for securing their infrastructure.
- Evaluate proposed best practices for securing data within the context of use cases.
- Understand the various security and privacy requirements for protecting data at rest, in cloud, mobile computing environments.
- Investigate a data protection problem through a semester long research project.

1.2 Summary and Evaluations
The content focus of my teaching has been systems, security, privacy, and courses, such as H343Data Structures that support the development and analysis of systems. During my tenure at IU, 50% of my course offerings were to undergraduate students. I provide my most recent course/instructor ratings from student evaluations in the table below. I include both undergraduate and graduate courses. The student evaluations for undergraduate courses contained questions that were supplied by the department. Indiana University has instituted a new evaluation questionnaire that contains questions supplied by both the university and departments. This new questionnaire was used to evaluate graduate courses. The numeric ratings are the averaged ratings of student responses across all questions for the specified category (e.g, university, and department)

<table>
<thead>
<tr>
<th>Course Type</th>
<th>Course Name</th>
<th>Rating -University</th>
<th>Rating</th>
</tr>
</thead>
</table>

Table 1. Course Evaluations

In addition to student evaluations, Faculty within the School of Informatics and Computing are periodically evaluated by their colleagues. These peer reviews are designed to provide constructive feedback to help improve curriculum and instruction. I’ve provided excerpts from peer evaluations below.

“Professor Hill conducted the session in an informal manner. She demonstrated an excellent rapport with the class, and students were obviously at ease. Professor Hill encouraged students to raise questions, which many of them did. She answered them clearly, making concise notes on the board, providing a useful summary of key points. A well-known difficulty for teaching technical material at this level, for this student population, is the students’ widely varying technical backgrounds and levels of technical interest. This makes it a challenge to engage all students and make the material accessible to them. Professor Hill appeared to be very effective at involving the entire class. Also, I noted that she addressed not only the technical details but also general strategies for problem-solving and building the students’ confidence, which I would expect to be very valuable for those less comfortable with the technical content.” (I230 Analytical Foundations of Security)

“In summary, Raquel is clearly an excellent teach at the level of advanced graduate students: she can expose them to the latest and most advanced technologies without losing them in the details, she guides them to think and ask the right questions, and she shows them how to analyze problems and structure their ideas. Many of these skills are likely to make her an excellent teacher at the level of undergraduates too.” (B649 Trusted Computing)

“Prof. Hill exudes an infectious enthusiasm for the course material and for teaching/learning. It clearly came across to the students and in turn made them

---

1 The rating scale changed from 4.0 to 5.0 in 2012.
Raquel Hill - Teaching Statement

enthusiastic about the material. Prof. Hill successfully used a Socratic style (“what is pervasive computing”) to make the class think and to make them engage. She knew all of the students by name and was interacted with them directly when, e.g., she asked questions in the Socratic manner.” (P534 Pervasive Computing)

“The topic of the day’s lecture was differential privacy. The primary discussion was about, and based upon a research presentation of, a paper written by Dr. Hill on the topic. The students appeared engaged in the lecture and discussion. The presentation was clear and well organized.” (B649 Data Protection)

“I attended late in the semester and thus spent my classroom observation during the student presentation time. This is not a practice I will adopt, in general. However, it did allow me to answer some questions more effectively than observing one or two sessions. In particular the instructor did adapt quite effectively to a range of student performance levels. Secondly, the students clearly had learned what were the major points on the syllabus. Finally, the projects clearly referenced the readings in the course in the new contexts selected by the students for their research.

To be specific, the best students not only showed mastery of the content of the syllabus but also applied the materials to well chosen problems. Prof. Hill interacted with the students appropriately, guiding excellent students to potentially publishable work and asking more tutoring questions to the less excellent students. Questions were probing but not aggressive. Students illustrated clear understanding of the implications of trusted computing in a wide range of applications.” (B649 Trusted Computing)