Integrating Ethics in Cybersecurity Education

Mohammad Taha Khan, Chris Kanich and Cynthia Taylor
University of Illinois at Chicago and Oberlin College
{mkhan228, ckanich}@uic.edu, cynthia.taylor@oberlin.edu

Introduction

Ethics plays a critical role in cybersecurity and provides the moral distinction between black-hat hackers and cybersecurity professionals. The study of ethics in cybersecurity is a complex matter, and as the need for security professionals grows, educators and employers alike have focused more on raw numbers and technical competency than on ensuring that these professionals understand the ethical underpinnings of their sensitive and important roles within any given organization. Whether dealing with entrusted personal user data, developing a framework to store passwords, or investigating a data breach, all such tasks must be executed ethically which requires training beyond the technical aspects of cybersecurity.

Ethics has long been considered important to Computer Science in general, with the ACM and IEEE model curriculums both including it, and ABET requiring coverage of ethics for accreditation. In 2006 Quinn [1] showed that fifty-five percent of ABET accredited CS departments teach computer science students about ethics through a dedicated course on the social and ethical implications of computing, and argued for the benefits of offering ethics courses taught by Computer Science professors. As cybersecurity itself becomes a highly specialized and in-demand branch of computer science, its adversarial, mission critical role coupled with stewardship over an organization's critical infrastructure and private data necessitates a more specialized ethics curriculum tightly integrated into security-related courses.

Here we outline how to improve the overall instruction of computer science ethics by refining the content of the sole ethics course offered for computer science majors and by

integrating ethics into computer science courses. In addition, we suggest pointers which can be useful in training students from diverse backgrounds for practical situations.

We believe that teaching ethics as an integral component of cybersecurity education will empower future individuals to act responsibly when dealing with sensitive data. These suggestions will also help them better understand the irreversible implications of data breaches and hence promote the adoption of more secure and correct programming practices. Finally, a part of this ethics training, students will also learn how to carry out due diligence in situations of cyber attacks and breaches. The next sections provides details of our proposed ideas.

Suggested Approaches

Teaching The Ethics of Privacy Through Personalized Experiences: Ethics and privacy go hand in hand and a lot of components of ethics for cybersecurity revolve around safeguarding privacy. While the notion of privacy is extensively covered in the traditional computer science ethics course, the descriptions and examples can sometimes be too broad and hence result in a disconnect of the students understanding of privacy in context and it can be hard for individuals to understand the gravity of personal information leakage. However, all college students have personal experience with making their own data available in varying degrees online. By having students take surveys on how they currently share data or discuss the ramifications of having their data made public in various hypothetical situations, instructors can explain the ramifications of privacy policies in a realistic, student-centered way. It is also important that instructors discuss that the ramifications of data becoming public will vary greatly depending on the individual: for example, past dating profiles becoming public may have a very different implication for someone who is gay than for someone who is straight. These activities need to be designed in a meticulous and fine grained manner and require the involvement and overlapping interaction of ethicists and cyber security professionals to sketch out an accurate design.

Including Ethics Components Within Cybersecurity Courses: When ethics is included in the CS curriculum, it is usually taught as a separate course. Even when it is a required course for graduation, it is frequently seen by students as an "easy A" course, and less important than more technical courses. This, combined with the abstract nature of the course frequently results in students not taking much interest, and failing to develop the full practical context of ethics and its importance. Given the importance of ethics to cybersecurity, it's important to add ethics to security courses themselves, as well as covering cybersecurity topics in general ethics courses. This should be done by the including both case studies as well as collaborative exercises. Students should be provided case study readings that pertain to the technical material being covered in class. For instance, while teaching them about SSL and secure web applications, students should have readings about how the Heartbleed bug was committed to the OpenSSL and how it went undetected for years and had catastrophic implications.

Another example of having a more involved activity on ethics can be having students perform an SQL injection (as a part of their assignment) on a sample healthcare database. For submitting solutions, apart from providing malformed queries, students should be asked about their perceptions on how they felt about the data leaked and what possible implications it could have. This will not only allow them to learn the importance of dealing with sensitive data but also provide implicit feedback to the instructor to better evaluate the understanding and perceptions of ethics.

This supplementary approach to teaching ethics will not only strengthen the principles of the students, but will also provide them with real-world examples and implications, which will encourage better programming practices and enable them to realize how as cybersecurity professionals, their design decisions can impact millions of individuals.

Acquiring Industry Feedback: Finally, we also suggest that gaining feedback from senior level cyber security professionals can also helpful and can help develop a more practical curriculum. This can be done in the form of meetings, surveys as well as workshop or panel based interaction where educators can get real insights on what are

the main elements and components of ethics that should be focused on within the courses.

Ethics Within Graduate Security Courses: While the major proposed focus of this idea paper revolves around improving the ethical standards of undergraduate cybersecurity courses, at the same time, it's an important to realize that there should also be continued ethical training for graduate students. This is especially important as students without a US-based undergraduate education are less likely to have been exposed to ethics courses as part of their undergraduate education. Just as students are exposed to more complex computer science problems as graduate students, they should likewise be exposed to more complex and nuanced ethical issues.

Conclusion

Overall, we believe that a more integrated ethical framework is the right step forward in the direction of educating the cybersecurity professionals of tomorrow and will likely avoid situations like the Target breach or Cambridge Analytica. It is our hope that coupling ethics with mainstream technical education will result in better trained cybersecurity professionals.

References

[1] Quinn, Michael J. "On teaching computer ethics within a computer science department." Science and Engineering Ethics 12.2 (2006): 335-343.

Authors Bio

Mohammad Taha Khan is a 4th year PhD student at the University of Illinois at Chicago. His research interests span the domain of security and privacy on the Internet. His focus is on understanding privacy leakage on the Internet, socio-technical aspects of cybercrime and human factors in security. As a lot of his work incorporates insights from empirical analysis, he is particularly interested in developing better teaching methodologies around the ethics of data collection and management. After graduation, Taha plans to pursue teaching based academia.

Chris Kanich is an Assistant Professor at the University of Illinois at Chicago. He conducts research on the socio-technical aspects of cybersecurity. His current work includes analysis of gains and losses due to undesirable activity on the Internet, investigating human factors in effective Internet security mechanisms, and building new technological primitives with the goal of increasing the practical security and privacy of Internet users.

Cynthia Taylor is an Assistant Professor at Oberlin College. Her research interests include Security and Computer Science Education. Her education research interests include active learning, with a focus on peer instruction, and assessment of student learning via concept inventories. Her security research looks at how people use the internet, and its implications for security.