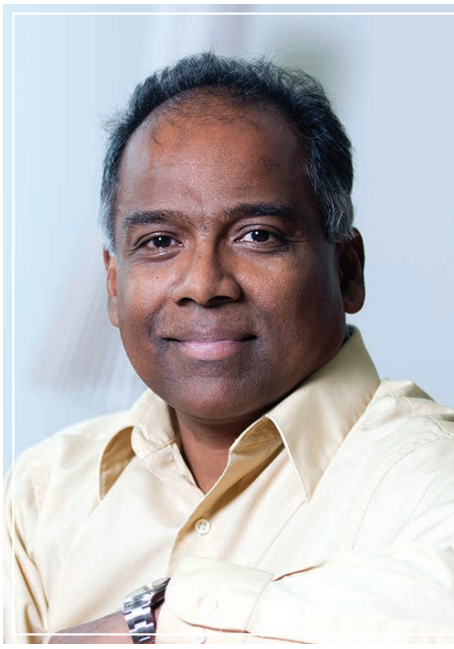
Ethics in Information Security



N. Asokan
Associate Editor in Chief

Our society is undergoing pervasive digitalization. It's not an understatement to say that every facet of human endeavor is being profoundly changed by computing and digital technologies. Naturally, such sweeping changes also bring forth ethical issues that computing professionals must deal with. But are they equipped to deal with them?

Ethical concerns in computing are widely recognized. For example, the recent upsurge in the popularity of applying machine learning techniques to various problems has raised several ethical questions. Biases inherent in training data can render these systems unfair in their decisions (for example, basing hiring decisions on factors, such as distance from workplace, that correlate closely with past performance might also inadvertently correlate with other factors like race[1]). Identifying such sources of unfairness and making machine learning systems accountable are active research topics. Similarly, the rise of autonomous systems has led to questions such as how to deal with the moral aspects of autonomous decision making and how societies can respond to people whose professions might be rendered obsolete by the deployment of such systems.

The information security profession is grappling with its own share of ethical considerations. Among them are privacy concerns about large-scale data collection, the use of end-to-end cryptography in communication systems, wiretapping and large-scale surveillance, and the practice of weaponizing software vulnerabilities as "offensive security."

The latter issue was brought forth in dramatic fashion in early March of this year when WikiLeaks published a collection of documents called Vault 7, which consisted of numerous vulnerabilities in popular software platforms like Android and iOS that could be used to compromise end systems based on these platforms.[2] That national intelligence agencies use such vulnerabilities as offensive weapons didn't surprise anyone except the popular press. But the WikiLeaks revelation led to a flurry of discussion on the ethics of how vulnerabilities should be handled.

Over the years, the information security community has developed best practices for dealing with vulnerabilities. Timely "responsible disclosure" of vulnerabilities to affected vendors is a cornerstone of such practices. Using vulnerabilities for offense is at odds with responsible disclosure. As George Danezis, a well-known information security expert and professor at University College London, put it, "government 'Cyber' doctrine [not only] corrupts directly this practice, by hoarding security bugs and feeding an industry that does not contribute to collective computer security, but it also corrupts the process indirectly."[3]

However, when a government intelligence agency finds a new vulnerability, deciding when to disclose it to the vendors concerned is complex. As another well-known expert and academic, Matt Blaze from the University of Pennsylvania, pointed out, on the one hand, an adversary might rediscover the same vulnerability and use it against innocent people and institutions, which calls for immediate disclosure leading to a timely fix. On the other hand, the same vulnerability can help intelligence agencies thwart adversaries from harming innocent people, which is the rationale to delay disclosure. Blaze reasoned that this decision should be informed by the likelihood of the vulnerability's rediscovery but concluded that, despite several studies, there's insufficient understanding of factors that affect how frequently a vulnerability is likely to be rediscovered.[4]

This brings us back to our original question: Do information security professionals have the right knowledge, tools, and practices to make judgment calls when confronted with such complex ethical issues? Guidelines for computing ethics have existed for decades. For example, the IEEE Computer Society and ACM published a code of ethics for software engineers back in 1999.[5] The ACM Code of Ethics and Professional Conduct was introduced in 1992 and is currently being revised (ethics.acm.org). But to what extent do such codes reach practitioners and inform their work? There

are certainly efforts in this direction. For example, program committees of top information security conferences routinely look for a discussion on "ethical considerations" in submitted research papers dealing with privacy-sensitive data or vulnerabilities in deployed products. They frequently grapple with the dilemma of requiring authors to reveal datasets in the interest of reproducible research without compromising the privacy of the people whose data was collected. Awareness of ethical considerations needs to be fostered systematically at all levels of the profession.

Ethical concerns in information security can't be simply outsourced to philosophers and ethicists, because such considerations will inevitably inform the very nature of our work as information security professionals. For example, several researchers are developing techniques that allow privacy-preserving training and prediction mechanisms for systems based on machine learning. Similarly, as Matt Blaze pointed out, active research is needed to understand the dynamics of vulnerability rediscovery.[4]

Should undergraduate (or even graduate) computer science curricula require exposure to ethics in computing? Where is the right place to add this to the curriculum, given the limited instructional time available? Should university computer science departments host computing ethicists among their ranks? What are the ethical limits of computer scientists working for intelligence agencies on finding vulnerabilities and developing attacks that use them?

Vault 7 had a silver lining: the focus on amassing weaponized vulnerabilities to attack end systems suggests that the increasing adoption of end-to-end encryption by a wide variety of messaging applications has been successful! Passive wiretapping is likely to be much less effective today than it was only a few years ago. Intelligence services are now forced to attack the endpoints, rather than the cryptography. ■

References

1. B. Porten, "Your Hiring Algorithm Might Be Racist," Technical.ly Philly, 12 May 2016; technical.ly/philly/2016/05/12/solon-barocas-hiring-racism-big-data.
2. "Vault 7," WikiLeaks, 7 Mar. 2017; wikileaks.org/ciav7p1.
3. G. Danezis, "What the CIA Hack and Leak Teaches Us about the Bankruptcy of Current 'Cyber' Doctrines," Conspicuous Chatter, 8 Mar. 2017; conspicuouschatter.wordpress.com/2017/03/08/what-the-cia-hack-and-leak-teaches-us-about-the-bankruptcy-of-current-cyber-doctrines.
4. M. Blaze, "When Should the Government Disclose 'Stockpiled' Vulnerabilities?," Exhausted Search blog, 10 Mar. 2017; www.crypto.com/blog/between_immediately_and_never.
5. D. Gotterbarn, K. Miller, and S. Rogerson, "Computer Society and ACM Approve Software Engineering Code of Ethics," Computer Society Connection, *Computer*, Oct. 1999, www.computer.org/cms/Publications/code-of-ethics.pdf.

Erratum

In "Practical Evaluation of Internet Systems' Security Mechanisms," (P. Lubomski and H. Krawczyk, vol. 15, no. 1, 2017), there was an error in the equation that appeared on page 38. The equation should read:

$$STL = \frac{nZ + nL \times 0.6 + nM \times 0.3 + nH \times 0.1}{nT}$$