In mid-April, I was discussing security engineering with Kristin Esterberg, president of SUNY-Potsdam, one of New York State’s comprehensive universities. A sociologist by training, she’s a passionate advocate for STEAM, not just STEM: programs that incorporate the arts and humanities into science, technology, engineering, and mathematics education.

Esterberg told me how she asked some of her engineering students if art could be relevant to engineering. Their answer: no. So she asked a more targeted question: Is it important for a bridge to be beautiful? Their answer: no; as long as it’s structurally sound, that’s enough. Are you nodding in agreement with the engineers? Think again. As engineers, we often focus only on so-called functional requirements, and only in a very narrow way.

Consider the Brooklyn Bridge, connecting the New York City boroughs of Manhattan and Brooklyn. Completed in 1883, it was designed to carry horse-drawn carriages, railcars, pedestrians, and bicycles. Of course, today it carries automobiles instead of horse-drawn vehicles, and it still moves people using other transportation modes. This bridge functions not just to transport people and vehicles from one side of the East River to the other but also to connect two neighborhoods and the diverse cultures they represent, exposing citizens to different ways of thinking and living. For more than a century, people have been drawn to the bridge by its beauty as well as its amazing engineering—the first steel-wire suspension bridge ever
constructed. Its connective functions and artistic appeal are just as important as its structural integrity.

Interdisciplinary Insights
In the same way, it’s important for us to think about security and privacy broadly so that we understand the context in which our technology will be perceived and used. Nicholas Kristof recently wrote a cogent analysis of the many ways that social sciences can inform our understanding of technology. He noted that “[l]iterature seems to offer lessons in human nature that help us decode the world around us,” and “science depends upon the humanities to shape judgments about ethics, limits, and values.”

In the past, IEEE Security & Privacy’s authors and editors have addressed the value of other disciplines in many articles and special issues. From analyses of the economics of information security to explorations of usability, S&P has emphasized the benefits of multidisciplinary research and thinking. Indeed, it was for these reasons that we introduced the In Our Orbit department when I became editor in chief of this magazine. Department editors Angela Sasse and Alessandro Acquisti have sought input from researchers who work in other disciplines and apply it to security and privacy.

For example, in November/December 2013, sociologist Harvey Molotch described how studying normal routine behavior informs us of the mechanisms through which safety and social order can be maintained. From ethnographic studies of public sites such as the New York subway system, he reports on how to determine whether workers’ routines will fit into official security policies coming from above. From this research, he suggests concrete mechanisms likely to enhance cybersecurity while providing users with the collateral benefits of enhanced efficiency and pleasure.

Similarly, in May/June 2014, Martin Ortlieb provided an anthropologist’s view of privacy, and in November/December 2014, Benjamin Edelman explored the security and privacy implications of online advertising optimization. Fascinating articles like these highlight important advances and insights that come about when we think differently about our technology’s design and use.

In This Issue
Because a multidisciplinary perspective can stimulate new and sometimes groundbreaking understanding, I’ve invited three sets of authors to describe how application of their disciplines’ techniques can lead to important security and privacy insights. In “Big Brother in the Information Age,” sociologists Denise Anthony, Timothy Stablein, and Emily Carian investigate trends in attitudes toward privacy by comparing the results of the US General Social Survey at three points in time when this instrument was administered: 1985, 1996, and 2006. They explore the effects of race, age, education, and income across these time periods and suggest explanations for what they find. In particular, they note the effects of technology diffusion, cultural lag in technology acceptance, and increased government and commercial surveillance capabilities.

In “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” Julie Steinke and her organizational psychology colleagues at George Mason University examine three types of emergency responders—emergency medical technicians, military responders, and nuclear power plant operators—and analyze what makes their teams effective. Then, the authors apply their findings to cybersecurity incident response teams, suggesting how the lessons learned in other response communities can help make our own incident response more effective.

Finally, in “A Sociotechnical Framework for Threat Modeling a Software Supply Chain,” information scientists Bilal Al Sabbagh and Stewart Kowalski apply sociotechnical networking techniques to the problem of modeling threats to a global supply chain. Describing their framework by applying it to a case study, they demonstrate how their techniques can assist in performing a thorough risk analysis.

Multidisciplinary perspectives are becoming more important as our technology becomes more pervasive. In fact, you will see more articles like these in special issues of S&P in 2016, including a special issue on the Internet of Things. Our community is terrific at generating data, and researchers continue to develop and improve techniques for examination, analysis, and prediction. But biologist and naturalist Edmund Osborne Wilson advised caution: “We are drowning in information, while starving for wisdom. The world henceforth will be run by synthesizers, people able to put together the right information at the right time, think critically about it, and make important choices wisely.” At IEEE Security & Privacy, we plan to continue to help provide the right information at the right time.

References

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.