Empathy and Security

Several independent streams of research seem to have converged on the role of empathy in security. Understanding how empathy works and fails—and how it can be harnessed—could be important as we develop security systems that protect people over computer networks.

Bruce Schneier
BT

Mirror neurons are part of a recently discovered brain system that activates both when an individual does something and when that individual observes someone else doing the same thing. They're what allow us to "mirror" the behaviors of others, and they seem to play a major role in language acquisition, theory of mind, and empathy.

Psychologist Simon Baron-Cohen has a new book called *The Science of Evil* (if you live in the US) or *Zero Degrees of Empathy* (if you live in the UK). In it, he postulates that acts of evil are a result of empathy failures. Using a lot of experimental psychology and neuroscience to back it up, he shows that individuals have different amounts of natural empathy, and those on the low end of the scale are sometimes capable of some pretty awful acts against their fellow human beings.

Along the same lines, philosopher David Livingstone Smith has studied dehumanization and the role it plays in inciting otherwise normal people to commit genocide. His book *Less than Human* is a fascinating look at how the process of dehumanization—likening potential victims to vermin or disease, claiming they're somehow subhuman and thus worthy of extermination—serves to dampen our empathy.

These are extreme cases of empathy failure, but we see milder cases on the Internet. Our empathy brain circuitry evolved in a prehistory of face-to-face interactions, and we've evolved, both genetically and socially, a wide variety of social systems designed to enhance empathy and trigger altruism, trust, cooperation, and a broad swath of prosocial behaviors. As our evolved social systems get replaced with deliberately designed sociotechnical systems, these systems work less well. In fact, the entire Internet can act as an empathy-dampening device. For example, it's much easier to insult someone in an Internet chat room than it is to do it to his or her face. Anonymity aside, there's less of a personal connection between the insulter and the insulted, which translates into less empathy. Along the same lines, it's easier to steal money from someone halfway across the continent, whose face you don't see, than it is to commit the same crime in person.

Computer scientist Ross Anderson recently analyzed empathic security and credit cards. Photos were tested as a security device on credit cards in the 1990s, and preliminary data showed that fraud was reduced—but not because merchants used the photos. Anderson's theory is that the photograph was a useful security device because seeing a photograph of the victim on a stolen card triggered the potential thief's empathy and made him less likely to use it.

Researching my own new book, I've been examining the role morals play in providing security. As security professionals, we spend most of our time dealing with attackers for whom morals aren't sufficient to keep them from doing whatever we don't want them to do. But along with intrusion detection systems and harsh criminal penalties for computer crimes, I think we might need to start looking at ways to enhance the natural security systems our species has evolved over the millennia. If adding photographs to bank transfer systems enhances empathy and reduces computer crime, it seems like a smart thing to do. □

Bruce Schneier *is the chief security technology officer of BT. His new book,* Liars and Outliers: How Security Holds Society Together, *will be published in February. He can be found online at www.schneier.com.*

 1540-7993/11/$26.00 © 2011 IEEE