

Interview

Silver Bullet Talks with Gillian Hayes

GARY MCGRAW
Cigital

Gillian Hayes is an assistant professor in Informatics at the Bren School of Information and Computer Sciences at University of California, Irvine (UCI). She's director of the Social and Technological Action Research Group, otherwise known as "STAR." Hear the full podcast of the interview at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/.

Gary McGraw: The first question is fairly straightforward, but I don't know the answer myself: what exactly is informatics?

Hayes: That is a great question. *Informatics* is actually a really popular term in Europe, and it's gaining some popularity here in the US. It's meant to encompass a variety of studies around technology. So, it's pieces of computer science but also pieces of social science, of the law, economics, all kinds of different things, all around thinking about technology and the impacts on society and how society in turn shapes new computing technologies. That's the rough idea. It's a slightly shorter version of information and computer science.

McGraw: How does the field of informatics relate to security and

privacy and surveillance and all the stuff you've been working on?

Hayes: It's interesting: traditional low-level security, the folks that do new algorithms for encryption and things like that, fits really nicely within computer science. In fact, here at UCI, our security experts who do that kind of work stay in the computer science department. What we do slightly differently in informatics is more of the higher level: how human beings are involved in that loop. So, looking at things like usable security and privacy and what is the impact of new kinds of technologies or these new algorithms that people are creating on how people do their everyday work.

Likewise, in my work, I'm very interested in recordkeeping, and so I am looking at a variety of domains. Obviously, medicine is one place where recordkeeping is incredibly sensitive as well as prolific, so looking at what does it mean to have a digital identity within a medical record, what kinds of things can people learn about you if your medical record is compromised, all of those kinds of things. I look a lot at the everyday kinds of tracking technologies that people use, the kinds of things that maybe aren't as central to core computer science, things like: how do people feel about their cell phones tracking them? How do they feel about creating records of all their

financial transactions through online banking and credit cards and ATMs and those kinds of things?

McGraw: What role does usability play in that work, especially when it comes to security?

Hayes: It's not a surprise that people don't understand the underlying workings of data transference.

McGraw: Do they need to?

Hayes: It's a good question. I think people need to understand a little bit. I often use the metaphor of a car: I understand very little about my car, but I have just enough understanding to know that when I hear a certain kind of noise that means I'd better pull over and call AAA immediately, or if I hear another kind of noise, everything's fine, but maybe I want to get it checked in the next couple of weeks. Little clues like that—you start to learn when you use the technology over an extended period of time, like a car; we're just not at that point yet with computers.

McGraw: What is the best work in usability and security?

Hayes: I've been a great admirer of Jason Hong's work for quite a while now. He does a lot of work in looking at how people can respond to things like phishing attacks and how

About Gillian Hayes



Gillian Hayes is an assistant professor in informatics in the School of Information and Computer Sciences at the University of California, Irvine. Her research interests are in human-computer interaction, ubiquitous computing, assistive and educational technologies, and medical informatics. She's specifically interested in the ways in which people keep records, document their everyday lives, and constitute their identities, clinical, and educational categories through these records. Hayes directs the Social and Technological Action Research (STAR) group, and is affiliated with the Laboratory for

Ubiquitous Computing and Interaction, the Center for Ethnography, the Center for Biomedical Informatics, the Center for Research on Information Technology and Organizations, the California Institute for Telecommunications and Information Technology, and ACE program faculty.

we can teach them what is phishing and what is not. He really focuses on sort of educational interventions and not necessarily developing new algorithms and new techniques for actually locking down these things, but figuring that no matter what we do, hackers and spammers are going to find other ways.

McGraw: It sounds like the stuff that you get excited about is psycho-social in nature?

Hayes: Exactly. Obviously, new technological interventions and new ways of securing things are going to be important in the future. But at the same time, we're constantly racing against the folks on the other side of this battle who also have all kinds of new technologies all the time. We need to make sure to keep the human beings in the loop and help them do the best that they can to make the right decisions and understand the consequences of things.

McGraw: Setting stuff up right. So, obviously, usability must impact the health records field, too, that you mentioned before.

Hayes: Right, and that's actually one of the biggest challenges right now in medicine, and you probably hear in the news all the time that people are really excited about new health IT and the rhetoric of

"this is going to save us tons of money, and we're all going to be much more efficient."

McGraw: What do you think? Will better recordkeeping actually save health care?

Hayes: It will help. There are a couple of big problems. One, of course, is that health care systems are not interoperable in the way that other things are. I often hear people equate the current state of medical records to word processing in the early '90s, where everyone's racing, and they've got their different standards.

McGraw: Yeah, I remember all those function keys at the top of the keyboard in Word Star.

Hayes: Exactly. So we really need some standards there. But the other problem is there is a lot of legislation around healthcare records that has come out with the best intentions and, absolutely, we want to protect people's health records, but in turn it's really made things pretty difficult for those patients and clinicians. If we overlay the technology on top of these current policies, not only is it a really incredibly complex technical system to be giving permission for every different lab test to be shared and all of these other kinds of things, but it's not going to be

able to do all of these things that we think of. We think 'Oh, once it's in the database it's accessible everywhere,' because that's how other kinds of recordkeeping typically will happen. But in health-care, there's so many policy issues surrounding those records that paper or electronic, either way, they're going to be locked down in a variety of ways to make things tricky for people.

McGraw: Jim Routh, who is at JP Morgan Chase, and I wrote an article for *CSO* magazine about what we call "lifestyle hackers," which is, generally speaking, about 20-somethings avoiding security controls to use the productivity tools that they're used to, like AIM, Twitter, and MySpace. The question is, as technology becomes pervasive, how do we evolve our thinking about security and privacy? How is our thinking changing over time, and is there a generational effect there? [For more information on the recent RSA panel on this topic, see the sidebar. —Ed.]

Hayes: I don't know about the generational effect. People ask about this quite a bit, and the tricky thing is that what we know is, of course, the younger you are, the more risk-seeking you are, generally. So it's hard to know for sure whether these 20-somethings will grow out of it as they grow older and become more risk averse like the rest of us old folks, or if, in fact, this is a huge paradigm shift, and they're always going to be incredibly much more open.

McGraw: So we've just got to wait and find out?

Hayes: That's my feeling on it. I think different people feel really passionately on different sides of this. I'm just unsure. But what I do think is interesting is looking at

S&P's RSA Panel: Lifestyle Hacking and Social Networks

How do you balance maximum productivity against tools that may cause productivity loss? Do security controls encourage breaking rules? Is hacking around security controls a gateway drug to more serious cyber crime? These were just a few of the questions asked and answered at this year's S&P-sponsored panel at the RSA Conference held in San Francisco in early March. "Lifestyle Hacking: Social Networks and Gen Y Meet Security & Privacy" was moderated by board member Gary McGraw, and featured this issue's Silver Bullet podcast subject Gillian Hayes as a panelist, along with Kimberly De Vries (California State University, Stanislaus), Avi Rubin (John Hopkins University), and James Routh (JP Morgan Chase).

In addition to kicking off the panel discussion with two skits both titled "The Pursuit of Productivity," McGraw led a discussion on the pros and cons of social networking in the workplace, and on whether blocking access to common sites alienates a new

generation of talented employees who often rely on such technologies to solve real-world problems. Although some argue that social networking on the job affects both security and productivity, the panel's ultimate consensus was that no one solution could address both concerns. Rather, given that the next generation's growing interest in and dependence on such technologies is unlikely to disappear, each organization must assess its own needs to find a reasonable balance.

The panel drew a standing-room-only crowd and inspired articles in *Computerworld*, *Infosecurity*, and Carnegie Mellon's CyLab blog. Attendees' reactions were positive, and S&P got some great comments and feedback throughout the rest of the conference. If you attended RSA and the Lifestyle Hacking panel and have a comment, send feedback to lead editor Kathy Clark-Fisher at kclark-fisher@computer.org, or join our twitter feed at <http://twitter.com/securityprivacy>.

how corporate America in general is having to adjust to this Generation Y set of people. They're very different in terms of their feelings about management and about corporate loyalty and things like that, and they tend to job hop; it's "What have you done for me lately?" kind of behavior.

To be fair, they've seen the tech crash; they've seen a variety of other things—now the banking crash. There are reasons that they're not particularly loyal to corporate America. But what that means is that it's pervading their feelings about technology as well. Couple that with the way that these policies tend to evolve—is it just, "We're not sure about this so we're going to say no you can't use it"? That's not a particularly well-reasoned way for companies to say no to things.

McGraw: It's a pretty stupid reason, actually, and especially if the 20-somethings think, "Gosh, I sure could get a lot more done if I were only allowed to use AIM."

Hayes: Right, and I think you saw the same thing 10 years ago—or maybe even a little bit more—with email, where initially it was like,

"Well you can only email within the company," and then slowly people start to allow you to email outside; some places would let you use external email services; some only your work email. But slowly those things were broken down. Similarly, I think instant messaging followed a sort of path like that. So it may well be that things like Twitter, MySpace, and Facebook are going to follow a similar path, where once the corporations can start to see some value in it, then perhaps they'll let their guard down a little bit.

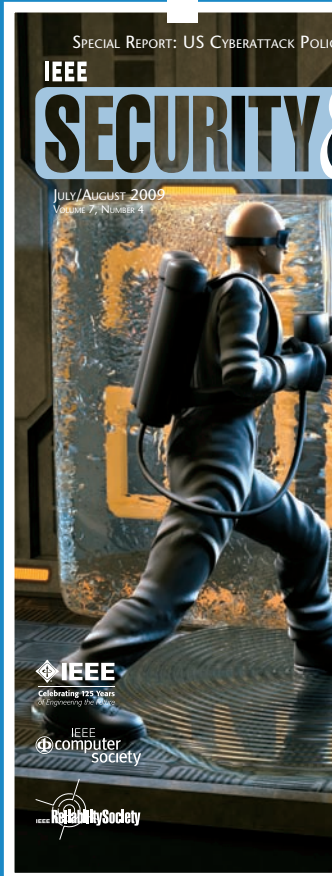
McGraw: Back to informatics. Part of informatics, in my view—and you mentioned this before—involves humanizing technology and technologists. Here's a crazy question: how does having more women in computer science help that agenda or hurt that agenda?

Hayes: It's a funny thing: as it turns out, women are a huge part of the consumer base and, in fact, make more consumption decisions, at least according to most of the marketing folks—than men do. There's this phrase in the technology world that you've probably heard, which is the 'shrink it and

pink it' one—the idea being that if we just make technology smaller, cuter, and pinker, women will buy it. That's fine, it works to a certain degree: I have a pink mouse. These kinds of things are somewhat true. But fundamentally, as technologists and designers, we're always going to bring our own perspective into what we create—that's just natural, and that's just human nature. Having more women in the field will just help to bring more of that perspective to all kinds of different things, so that we're not left with the very simple product solution, which is the shrink it and pink it one. □

See the full text of this interview at www.computer.org/cms/Computer.org/dl/mags/sp/2010/02/extras/msp2010020005s.pdf.

Gary McGraw is Cigital's chief technology officer. He's the author of *Exploiting Online Games* (Addison-Wesley, 2007), *Software Security: Building Security In* (Addison-Wesley, 2006), and seven other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.



■ Subscribe Now!

IEEE Security & Privacy magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.

Watch for these special issues! ■

Mobile Device Security ■ Sharing Sensitive Information ■ S&P of Cloud Computing
Reliability of Embedded and Cyberphysical Systems ■ Engineering Secure Systems

www.computer.org/security