Helping You Protect You

M. Angela Sasse | University College London
Charles C. Palmer | IBM
Markus Jakobsson | ZapFraud
Sunny Consolvo | Google
Rick Wash | Michigan State University
L. Jean Camp | Indiana University

Guest editors M. Angela Sasse and Charles C. Palmer speak with security practitioners about what companies are doing to keep customers secure, and what users can do to stay safe.

M. Angela Sasse: The theme of this special issue is "protecting you"—what are the biggest risks that your customers face, and how do your companies help customers keep secure?

Markus Jakobsson: Until quite recently, I was principal scientist at PayPal. Malware and spoofing are the two biggest risks for its customers. Mobile malware is becoming a significant threat, with the increased use of financial resources on mobile devices. In terms of spoofing, many people thought that the deployment of DMARC [Domain-Based Message Authentication, Reporting, and Conformance] would mitigate this problem. However, a new, closely related problem, which I call semi-spoofing, bypasses DMARC. Here, attackers don't actually spoof emails but instead use a misleading "friendly" email address—which in many email readers is the only sender information displayed. Therefore, typical users can't determine whether the email is spoofed, and DMARC doesn't address semi-spoofing.

Sunny Consolvo: At Google, we've had some success in blocking automated attempts to gain unauthorized access to users' accounts. Using risk analysis techniques, we saw a 99.7 percent reduction in successful compromises.

More generally, one of the big risks people face is someone logging in as them. If attackers can do that, they can access the user's stuff, take it elsewhere either by making a copy or taking it away from the user, or pose as the user. After compromising accounts, attackers might do anything from embarrassing users—by sending spam to their contacts—to something more serious such as stealing their identity for financial gain. Gaining access to users' accounts is generally cheap because, as hackers know, many people reuse their passwords across different sites, use weak passwords, respond to suspicious requests for personal information, run out-of-date software, and neglect to set up recovery options in case they get locked out of their account.

Sasse: Can you give an example of how Google tries to protect customers against that threat?

Consolvo: I work on the team that provides two-step verification—Google's two-factor authentication feature [www.google.com/2step]—which we made available to all Google users in 2010. Two-step verification provides an additional layer of security for users' Google accounts using something they know—their password—and something they have—a one-time

code that they get on their phone. To make two-step verification more usable, we generally enable them to do it only once on their trusted computers.

One of my favorite things about two-step verification is that if they use our mobile app called Google Authenticator, users don't need Internet or cell connectivity to get their code. The app generates the code locally on their device, which is particularly handy for people who travel internationally or live in an area where they have unreliable access to SMS or voice calls. This one little step makes it significantly harder for a hacker to break into accounts.

Another thing we've done that's more subtle from the user's perspective is to encrypt much of the traffic to our services with SSL. Many companies have added support for SSL since we made it our default for mail and other products; this is really a positive trend for everyone.

Charles C. Palmer: Jakobsson, how is PayPal dealing with the problems you described earlier?

Jakobsson: Again, there is DMARC, which has already been deployed. PayPal has also been strongly involved in the FIDO Alliance [www.fidoalliance.org]—a framework for authenticating people, including using biometrics. These are two initiatives already on the market or in the pipeline.

PayPal is also performing security research. For example, it's made progress in research on improved password strength meters. Traditional thinking on password strength is that the back end counts the number of upper- and lowercase letters, length, and so on, and makes a determination of password security based on these observations. However, a password's actual security depends more on users picking memorable yet unlikely passwords than on their using a certain number of uppercase letters.

By studying the distribution of passwords and password resets, we gain a better understanding of what makes a strong and memorable password—and this allows us to not only block weaker passwords but also identify users with poor security habits.

Sasse: Clearly, service providers are trying to make users safer, but they also have an idea of what the users' responsibility should be. Do you think putting users in that position of responsibility is fair, or do you see some probable improvements service providers could make?

Rich Wash: I think service providers are doing a pretty good job. The division of responsibility changes as capabilities change, and there's been a lot of thinking about how these technologies are evolving. Two-factor authentication technologies have changed significantly, becoming easier and easier. I like Consolvo's example of the Google Authenticator app, which is much easier to use than some of the older two-factor authentication systems out there.

L. Jean Camp: I don't think the carrier responsibilities are particularly well aligned. I think that there's a certain amount of living in a bubble. For example, Xbox One had a great security architecture, but it just assumed that everybody was always on all the time, and that Internet connectivity is completely ubiquitous and reliable. And then if you look at Google's two-factor authentication, a message is sent to your phone, so for example, if you're traveling internationally and T-Mobile isn't working and you're logging in from another computer, you're completely locked out. There is an assumption that your phone will be available if your computer isn't. Sometimes companies make assumptions about availability and reliability of technology that aren't widely applicable.

Consolvo: Google has a few different solutions to that issue. First, the authenticator app that I mentioned requires no Internet or cell coverage, so if you have your phone and it's powered on, you can get a code. You don't need to be able to receive an SMS or a voice call or connect to the Internet. We also allow you to print single-use backup codes, which you can print in advance and use when your phone isn't available. And if you're signing in from your own computer, you won't be asked for a code. We recognize that limitation and are trying to accommodate it.

I also wanted to mention, in line with what Wash was saying, that we ran a study recently asking people who they thought was responsible for keeping hackers out of their accounts [R. Shay et al., "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra: Experiences with Account Hijacking," to be published in *Proc. ACM Conf. Human Factors in Computing Systems*, 2014]. We were pleasantly surprised that, for the most part, they thought users and service providers shared this responsibility: users are responsible for using strong passwords, not reusing their passwords, and so on, and service providers are responsible for keeping hackers out of the databases and encrypting network transactions.

Wash: The challenge with a lot of these online security risks is that there are many different types, and people aren't sure which ones to focus their attention on. Users could perform most available countermeasures, but that would basically take all their time. Almost everyone I've talked to really wants to do something, and I think that resonates with what Consolvo was saying—there is a shared responsibility. People do feel responsible for their

own information and their own protection, but they're not entirely sure what to do. Whenever you're providing advice to users, you should pair instructions with reasoning about not only the threat but also how following the instructions will help protect against that threat.

Jakobsson: Many service providers tell users what not to do or tell them about risks, but their advice isn't actionable. It doesn't tell them what they should do, or as Wash pointed out, why. They say "don't do this." That isn't helpful. It creates a sense of paranoia and fear, which makes some people throw up their hands and say, "there's nothing to be done about security," and then totally ignore it.

Sasse: How do older users cope with user security? What does security looks like for this user group?

Camp: There are two kinds of older users—"older olds" and boomers. Boomers are often much more confident as they age. On the other hand, we need to give older users videos, graphics, less text, and less risk. You need to tell older users, "here is how it's resolved." If you just say, "you're at risk," you put them in a state where they might feel more vulnerable. So, they might heed all your warnings, but it's tremendously disempowering when these warnings pop up all the time.

Palmer: To what extent do service providers think about customer groups such as older users?

Jakobsson: Many service providers don't collect a great amount of demographics about their users, so they don't actually know whether users are elderly. In addition, for privacy reasons, many users don't want to divulge this information. So it's best to design general countermeasures—security measures that are applicable to everybody—and a solution that's invisible and that addresses security pain points. Then, it doesn't matter whether the user is elderly or not.

Take HSTS [HTTP Strict Transport Security], for example. This technology recognizes which websites refuse to connect without an SSL connection. PayPal is HSTS compliant, which means that if you've ever connected to PayPal, your computer will have stored information that will cause it to insist on making SSL connections to PayPal. So, if you go to a cybercafé and connect to PayPal, you will get a secure connection and don't have to worry about hotspot security. This security measure applies to everybody in an unsecure hotspot. Like the best security measures, it's invisible and works for everybody who isn't straight-out negligent.

Sasse: Millions of users around the world have enthusiastically adopted online social networking. Are there particular privacy and security risks emerging from the increased volume of users? How can they protect themselves against these risks, and is this something that should be addressed by mandatory online education?

Camp: It doesn't occur to older groups to lie about their birthday, right? Lying to Facebook is a moral issue for older users. However, once they understand that they've identified their children as such, and their birthday is authenticating information, they might consider lying. The primary controller of information sharing is risk perception. So, if people are aware they're taking a risk, I don't think you should stop them. People have the right to be wrong and silly and everything else we are, but they should only take these risks knowingly.

If you have to sit down and watch an educational video before going online, you're going to be bored. However, feedback at that time you're entering personal information would be more effective. If you lie about your birthday, you might forget the date you used and lose access to your account. If you don't lie about your birthday and you're somebody's mom, you're giving away authenticating information. But by the time you get to the birthday field, you've already indicated your gender, so service providers have some idea about whether you're physically capable of being anybody's mom. Rather than generic education before the fact, I'm a big fan of actionable and timely risk information.

Wash: Timely information is really important. One of the challenges is that security decisions are often made at a very different time from the "what information do I provide?" decisions. For example, I make a single security decision about what my default sharing information is, then two years later, I'm deciding whether or not to contribute this information. These are very disconnected decisions. So, on Facebook, one of the things I did was change my default sharing to something significantly more private, so I have to manually change it each time I share. I don't remember the last time I went with the default, but because I have to change it manually, I'm forced to think about it each time I share, not just when I signed up for the account.

Sasse: Users grumble about passwords and say, "I get by using a piece of software that does everything for me, and I trust it completely," or "I only get by storing all my passwords in my cell phone's Notes app," or something like that. Is there something on the horizon that might replace passwords?

Jakobsson: You could get rid of passwords for everyday use, but you can't really get rid of passwords and similar authenticating methods for special cases. As biometrics take hold, they'll make it much easier for us on a day-to-day basis, but every once in a while, they'll fail. We'll have to log in from a new or different device, or we'll be wearing gloves or have torn our fingerprint. So there's still a need for a knowledge-based identification.

The interesting problem now is that although you may very well be able to remember a password that you use every day or every week, it's much harder to remember a password that you use only every 12 months or so. A new technical problem emerges because the infrequent use of the password introduces a temptation for users to choose a silly password like their name, or they'll write the password down and forget where they wrote it—and then abandon their account.

Consolvo: We really sympathize with people who struggle with these dozens of different passwords for their accounts. Even we at Google have trouble keeping our passwords straight, and our two-step verification feature builds on passwords. But because they're the weakest link in the system, we need to continue strengthening them until there's a better solution.

We're also thinking about longer-term ways to make things easier while building in stronger security. As Jakobsson mentioned, PayPal and Google are both part of a group called the FIDO Alliance that's working on a specification for an authentication solution that works more easily across various platforms and services. This will allow companies to explore new possibilities such as hardware tokens, biometrics, and wearables—any of which can be much stronger than passwords if they're designed in the right manner to offer security and respect user privacy.

Wash: The interesting thing about passwords is that they're extremely flexible and they can be used in all kinds of situations. You can write passwords down or give them to someone else who needs to get into an account that you want to let them into. This type of flexibility is one of the reasons we still use them, and use them in so many places. We won't find a single solution with the same kind of flexibility, but we're seeing many different solutions that work well in particular situations.

Sasse: That fits with the usability philosophy—for different tasks and different contexts, you need different solutions.

Camp: FIDO says you have two choices for authentication—something you have and something you know. You can either afford a device that helps you maintain your privacy, or you can have something you know and something you are—that is, a biometric. So let's say the FIDO vision comes to fruition. Either you have the money to carry around a smart device that provides privacy against government, or you're being identified by the government with a biometric, such as your fingerprint. With private-sector providers, privacy might end up being something you can afford or you can't, and this really troubles me about the future of authentication.

Palmer: I think that's a very thoughtful point to end on. ■

M. Angela Sasse is the professor of human-centered technology in the Department of Computer Science at University College London. Contact her at a.sasse@cs.ucl.ac.uk.

Charles C. Palmer is CTO for security and privacy at IBM. Contact him at ccpalmer@us.ibm.com.

Markus Jakobsson works at ZapFraud and specializes in research on applied security, ranging from mobile malware detection to improved user interfaces. Jakobsson received a PhD in computer science from the University of California at San Diego. Contact him via www.markus-jakobsson.com.

Sunny Consolvo is a user experience researcher on Google's Security team. Her research interests include usable privacy and security, persuasive technology, and supporting health and wellness. Consolvo received a PhD in information science from the University of Washington. Contact her at sconsolvo@google.com.

Rick Wash is an assistant professor at Michigan State University. His research interests include usable security, online communities, and mental models. Wash received a PhD in information from the University of Michigan. Contact him at wash@msu.edu.

L. Jean Camp is a professor at Indiana University. Her research interests are human-centered security and privacy, including incentive alignment, risk communication, and usable security. Contact her at ljcamp@indiana.edu.