The Future of Authentication

Dirk Balfanz | Google
Richard Chow | Palo Alto Research Center
Ori Eisen | 41st Parameter
Markus Jakobsson | PayPal
Steve Kirsch | OneID
Scott Matsumoto | Cigital
Jesus Molina | Independent Consultant
Paul van Oorschot | Carleton University

As part of this special issue on authentication, guest editors Richard Chow, Markus Jakobsson, and Jesus Molina put together a roundtable discussion with leaders in the field, who discuss here their views on the biggest problems in authentication, potential solutions, and the direction in which the field is moving.

Markus Jakobsson: What's the greatest problem with current authentication approaches, and what's needed to overcome these problems?

Dirk Balfanz: I think the biggest problem with authentication today is theft of credentials, which comes in different flavors. It could mean that you get phished and hand your password to a phisher, or it could mean that you share passwords across different sites, and one of those sites gets compromised.

Overcoming this problem means making it harder to steal those credentials. We could, for example, add additional second factors to passwords that are unpredictable, so that even the users don't know what they are, making it harder to give them away to phishers. Or maybe we could change the nature of credentials from bearer tokens—secrets passed from Web browser to server—to using more cryptography. With cryptography, we can design authentication protocols that are not susceptible to phishing, but the challenge is to package them up in an easy-to-use way.

Scott Matsumoto: I think the greatest problem is people—they're the most unreliable devices on the planet [laughs]. Credentials are a very important piece of the authentication problem, but I think that we put too much weight on them. My concern is that when we start looking at other approaches, such as different kinds of tokens or more crypto, we make systems harder to use. The net effect is that we just drive people to create more insecure approaches for handling all of the things that we've tried to do in order to increase security. To me, this is the biggest problem.

Paul van Oorschot: The greatest problem from the user's perspective is "too many." When we talk about Internet authentication today, for the vast majority, we're still talking about passwords, so the "too many" is too many password-account pairings for each person to remember. That's a scalability problem for users. A lot of these passwords are forced on users but don't serve a true security purpose—many sites employ password-based login when the service they deliver doesn't actually need a strong password. Often, what they really want is an email address, for example, to market products to the user in the future. This confuses people when they're actually asked for passwords that are important [for security], and we get the problem of users not

1540-7993/12/$31.00 © 2012 IEEE

distinguishing low- and high-end passwords. Of course, from the security viewpoint, passwords themselves fall short, and static passwords are replayable.

Ori Eisen: I think the greatest problem is that we're mixing authentication approaches for the current Internet with the same methods we might need for high-fidelity transactions. I'm sure nobody who reads this magazine would let a stranger walk into their house because he claims to be a certain person. But on the Internet, crooks can become me or you very easily, because nobody validates who is who. It might be good for free services, if you just want to go read something and you can claim to be anybody. But if we need authentication to move money, if we need authentication to vote, I don't think that the same authentication mechanism should be used. We need to look at better ways to actually know who's on the other end before we give them credentials for high-fidelity transactions.

Steve Kirsch: I think the biggest problem is that today's means of authenticating are insecure and cumbersome to use. I have 352 usernames and passwords, and that number grows every single day. Facebook has 600,000 attempted compromises every single day. I'm seeing emails from spammers who phished my friends' email accounts at least once a week now.

If I had to give our current method a letter grade, it would probably be a D. We need to come up with new approaches, and we're not going to see any significant improvement without a big paradigm shift. What we are doing at OneID is an example of one such shift. [OneID is a single set of credentials for both low- and high-assurance transactions.] The bottom line is this: if we want to solve the authentication problem, we have to think differently than we have in the past. It's time to abandon the traditional username/password metaphor and move the world to a more secure paradigm.

Eisen: I think we need to leave the current Internet with what it was intended for originally—the sharing of information. If we want to also have a network for high-fidelity transactions, we need to separate them. The first separation is visually, so you know which network you are on, very similar to why you see a padlock in an HTTPS session. You don't give the checker at the grocery store your Social Security number because there's no need to do it, and you don't need to go through a high level of security to read the news.

Matsumoto: I don't think we're using a whole slew of different methods; we're using one method, which is the username and password, the least common denominator approach. I think that having a single identity for all the different purposes that you need to conduct your life on the Internet is really an act in futility in terms of protecting all the things you need to protect.

Kirsch: My opinion is you can have a single identity, but the identity has to allow for multiple levels of assurance, which can be achieved by adding requirements to obtain digital approval, such as a PIN code or out-of-band approval. I think that's what users want. They don't want to have to manage different identity systems. It's much easier if they have a single identity that's flexible enough to accommodate the security needs of both users and service providers.

Richard Chow: A couple of you mentioned that users are the problem. For example, we tell people not to reuse their passwords and how to make a strong one, but these sorts of guidelines historically haven't been too effective. What should be done about that?

Balfanz: I'm not sure I would phrase it that way, that users are the problem. Users are what they are. Instead of telling them that they're doing it wrong, over and over, with no apparent positive outcome, I think we should just study how people behave and build our systems around that. If it turns out that the only thing the user can really handle is a password, then that's what we're going to have to deal with and that's how we're going to have to build our systems.

But if we do get guidelines out, we as professionals in the field should speak with one voice. The guidelines that we have today are confusing and contradictory. A reasonable guideline might be, "stop reusing passwords across different sites." We sometimes overemphasize recommendations about picking very complex passwords, though they're certainly more effective than trivially guessable ones. At any rate, we should come to a common understanding of what those guidelines are, instead of different people giving different—and often conflicting—advice.

Matsumoto: I agree with Dirk. You have to assume that the credential—username and password—is what it is. Users are going to use the same one across sites, their "best" password, so the systems that we have are going to have to compensate for that.

I don't think that the answer is a different kind of credential or some other token-based scheme. Again, I think we have to start thinking of the credential as the first time that we interact with the user. That's one type of interaction. By seeing the user's interaction with the system on an ongoing basis, during and across sessions, we can do a better job of authenticating. It's too simple to think that we can have just one interaction and validate that someone is indeed who they say they are.

van Oorschot: We need to remember that users are the customer—they're the design constraint, not the problem. If we don't want people to choose poor passwords, then we should use something other than plain old text passwords. The user has very few tools at hand. The back-end system puts rules in place, and it messes up everyone's life by asking them to choose one more password—a classic tragedy of the commons, everyone drawing from one resource pool, the user's capacity to create and remember one more password. We have to move past what we have been doing for the past 25 years and not expect things to magically become better at the same time that we're giving users 10 times as many passwords. We need better tools to help users manage the passwords that are unavoidable and also to deploy authentication approaches that are stronger but not a usability disaster.

Eisen: I know for a fact that you can't tell millions of users to do one thing and they will all do it. As security practitioners, we need to factor that into the equation. If we tell them a million times to have longer, more secure passwords, the bottom line is that people are people, and they want to have an easy-to-use password. Therefore, we need to find solutions that do not require users to be security experts.

Kirsch: I agree that the right thing is to design systems that accommodate the way users want to operate. You should allow people to pick the password they want—and the system should assume that it will be phished. You just need to design the system so it's unbreakable, even if the password is phished or keylogged. You can provide guidelines for proper behavior, but people aren't going to follow them most of the time. But it's a good thing to provide guidelines anyway, to help them along.

Jesus Molina: Who should care about authentication for things to change for the better?

Balfanz: We at Google do think it is, in fact, our responsibility to care and worry about the strength of authentication that we give to our users. We even go a step further: instead of just worrying about what authentication between the user and Google looks like, we have projects trying to strengthen security on the Web as a whole. For example, we have the Safe Browsing Initiative, we put special protections into Google Chrome, we call out malware and phishing sites in our search results, we contribute to security-related open source projects, and so forth.

About authentication in particular, we recently launched two-factor authentication for Google accounts. I'm also working on a project that's trying to move us away from using cookies and other bearer tokens as a means of authentication and adding in public-key cryptography to make things harder to steal.

Eisen: Everybody who is part of the network needs to care about it. But if everybody cares about it, nobody cares about it because there's no leadership. The Internet really doesn't belong to anybody. It was one of the greatest things that ever happened to the world, but at the end of the day, the people who need the Internet to survive—Google, Amazon, eBay, Microsoft, financial institutions, and the government—should care about it. Private industry would be the best place to start because in order to keep security and keep innovation going, you need to keep it funded. It's not a situation where we can forget about it: we have the adversarial problem of people trying to infiltrate the network and bring it down or conduct crimes in it.

Kirsch: Everybody cares about authentication. Banks have FFIEC [Federal Financial Institutions Examination Council] requirements; the government has FICAM [Federal Identity, Credential and Access Management] and HSPD-12 [Homeland Security Presidential Directive 12] requirements. But if we are to advance the ball here, we have to have these parties buy into a vision of taking a risk and trying something different that has a chance of working. One of the things that gets in the way is that a lot of these requirements are written with existing authentication paradigms in mind. Having service providers be flexible in terms of what they're willing to require is extremely helpful.

Essentially, we need to stay focused on the goal of better authentication. I find that a lot of sites are loath to make any changes at all, even if it's something that's potentially better because they don't want to have any kind of drop-off on conversion ratios. You have to find service providers who are willing to take a risk and try something new. That's the only way we're going to get ahead, service providers being willing to try innovative solutions.

van Oorschot: I agree we need sites and service providers to be flexible, but we also need cooperation and coordination. The whole system has a limited capacity to try new things. If somehow we could get the major players together to agree on one or two approaches to promote, rather than five or six new ones, we have a chance to move out of our current state of low-security authentication [passwords] that we've been stuck in for 20 plus years. We need one or two new approaches to authentication rather than 10 or 15.

Jakobsson: There's a movement among authentication vendors away from just a binary-type authentication toward a back-end authentication score, using multiple factors and contextual data to establish an authentication assessment. What do you think of this? And is this the future for authentication?

Balfanz: I think this is a good idea. I was speaking earlier about how credential theft is in my opinion the biggest problem, and adding different kinds of contextual data to the authentication process is sort of like a second factor. It makes the complete user credential—which now basically consists of a password plus whatever extra contextual data is added—harder to steal or phish. I see this actually happening across the Web, so it's not so much the future of authentication as much as it's already, in fact, happening.

By seeing the user's interaction with the system on an ongoing basis, during and across sessions, we can do a better job authenticating. —Scott Matsumoto

Matsumoto: We do see this happening, but the other interesting aspect is that one of the factors can be time. You make a decision and then over time, you see the validity of that decision because of another decision. The two decisions might be contradictory, because of something like geography, so now you have to invalidate one or both of those decisions.

van Oorschot: I agree that the idea of multiple factors going into decisions makes sense. Of course, whether we call it a score or something else at the back end, the front-door requirement is almost always to map it to one of two choices: you either let someone in or not. Whatever factors we base this binary decision on, the more, the better, as long as they are invisible and don't further burden users beyond their capacity. Innovative multifactor approaches are promising, but let's admit that we usually underestimate deployability challenges.

Eisen: The more layers, the better. No binary decision on its own will ever be good. It might result at the end of the binary decision of letting you in or challenging you, but there can always be mitigating factors. Let's say they're traveling, so they're coming from a network you've never seen but still at an hour of the day that makes sense to you and a device that you've known. So even though we're taking multiple factors into account that may change the score, it ends up being a binary decision of letting [the user] in or not. But the decision itself is not binary.

Kirsch: I think scores are fine, and whether and how the relying party uses a numerical score is really up to the relying party. If I've already authenticated, for example, but my risk factor is high based on a particular transaction that I'm doing, then the relying party will either completely deny this transaction or ask for additional assurances, such as PIN codes, that are commensurate with the risk level. The risk can be based on many factors. It's probably easiest if we have a standard risk score, such as the probability that the transaction is legitimate.

Matsumoto: We also have to realize that other people in the organization will need to know what decisions were made when a user is not granted access. For example, the help desk needs to help the user unwind the history of decisions when we start putting these systems in place.

Chow: What about biometrics? Is it going to become more important as a factor or less important?

van Oorschot: We need to clarify the question in terms of what biometrics are used for. If we're talking about authentication of end users to sites on the Internet, then biometrics are a nonstarter for high-end security, because you need a trusted computing base, actually a trusted path from input all the way to the far end. The strengths of biometrics, for example, involving high-end equipment and a security guard overseeing the input, don't follow for an untrusted remote client. Attacks that don't work against supervised input are all of a sudden possible. So we need to frame the question and the application of use—for remote applications, it's a bit of a stretch from where we currently are.

Chow: And for local authentication?

van Oorschot: Well, for local authentication, we already have laptops with fingerprint readers and that sort of thing, but I think people mix up the application of use. That's still an unsupervised application, and it's not the scenario that biometrics are strongest in.

Eisen: Biometrics could be useful as yet another factor in a plurality of activities to authenticate. I don't think we should rule it out from usage. But I agree: if it's unsupervised, it cannot be the sole input to the decision. We should use as many layers as we can.

Kirsch: For the right application, biometrics can be a really good thing. But for remote applications, biometrics are less likely to be used. Biometrics have been expensive and inconvenient. If you want the false reject rate to be low, it means your false accept rate is going to be relatively high. Maybe you can weed out 95 out of 100 attempts using biometrics; that's good, not great.

But that's really not the level of security that you need if you want something really secure, so you don't get a huge gain for the amount of inconvenience that you have to put the user through. I love iris authentication and verification. I wish it were done at airports today, because I have to wait 30 minutes to authenticate.

> **"I know for a fact that you can't tell millions of users to do one thing and they will do it. As security practitioners, we need to factor that into the equation. —Ori Eisen**

Molina: I want to talk about device identification and how it's replacing or could replace identity on mobile devices. How can we authenticate people on mobile devices?

Matsumoto: My concern is that we're seeing a lot of applications use mobile device identity instead of user identity. Device identity has become a more convenient way for organizations to manage mobile devices connecting in [to their network]. I'm hoping that it's only a temporary trend, but device identity is moving in the wrong direction as far as I'm concerned.

van Oorschot: I think you have to ask, "What are you trying to do?" Are you trying to authenticate that there's a device involved in a transaction, or that there's a specific person involved in the transaction? With a credit card, for example, today's systems verify that someone knows the credit card number—I'm ignoring the user profiling done at the back end—but doesn't verify which person is behind it. That's why we have to know a bit more about the objectives in specific applications that want to use mobile devices as a substitute for an identity of a person.

Eisen: I would say that when we make a decision on authentication, we have to take a few components. Is the right user behind the device? The device is really a proxy that helps us have more reason to believe or more reason to think that we have the right user coming from the right device. Clearly, the device itself should never be interchanged as user identity because somebody else could be using my device, not me. But device ID should and is used today in the decision-making. Should we let this transaction go, or should we let this login move on with the next step?

Kirsch: If it's done right, the use of device authentication can be a good thing. Personally, I like having a private key that is person-specific, stored on a device, and then uses a PIN to prove it, which makes it two factor. There are no shared secrets.

Being able to preauthorize your devices is also a good idea that tends to work well and minimizes the impact of either a keylogged or phished password. I think that when you tie things to devices and limit things to devices, it is a good thing for authentication.

Jakobsson: What do you think will happen next?

Balfanz: I think user-visible changes will happen slowly. I don't think we'll all be authenticating with some sort of RFID implant come next year, even though if I close my eyes and try to look maybe 100 years into the future, I have a hard time imagining that people will be typing passwords into things. But I think we will see fairly slow changes.

Under the hood, I think there's a constant arms race going on. The service providers will strengthen the authentication method, and hackers will try to circumvent that. When we, as a service provider, add a second factor to our login, hackers will eventually try to steal cookies instead of passwords. And then if we protect cookies through cryptography, hackers will try to steal the signing key. And then when we protect the signing key, hackers will try to get around that, and so forth. This arms race, I think, will continue. But as an optimist, I think we'll be able to keep the Web a safe place for users.

Matsumoto: You're going to see an integration of event data that currently goes into your security event monitor, influencing authentication decisions. I think that you're going to start seeing these events also going into whether or not you're actually going to change the authorization corresponding to the initial authentication decision.

van Oorschot: We're going to see one of the major players, and by that I mean a Google or Microsoft or Apple or Amazon, take some known technology and weave it seamlessly—including from a user interface perspective—into some widely used service that has a big user base, and that's going to turn the tide. Which underlying security technology will be used? I think that can go one of many different ways, but I expect it will take a big player to make a wise choice and then a commitment to it.

Eisen: We will still have to wait a little bit until there's enough of what I would call catastrophic events, where we just don't like the state of affairs anymore. Then enough forces in the market will come together. The fact that we still, 20 years in, don't have a standard of how to do authentication just shows that we are not all in agreement on what's the best way. But I think in the next five years, it will just take care of itself because the network really isn't ours anymore. The crooks are running it, and we're just trying to patch it up.

Kirsch: The current system is not sustainable, and I think that we have to move to something that's better. It's got to be something that we don't have today, because we already know the stuff today doesn't work.

So what's in our future—and I think it's going to come fast—are some new, clever techniques for solving this problem. I think in the next one to two years, we are going to see a big paradigm shift. One of these new paradigms is going to come out and emerge the leader. I sure hope so, because what we have now is really awful. ■

Dirk Balfanz is a software engineer on Google's Security Team, focusing on strengthening authentication on the Web through the use of public-key cryptography. Balfanz also worked on Google's OpenID and OAuth implementations, and contributed to the OAuth standardization process.

Richard Chow is a research scientist in the security and privacy group at the Palo Alto Research Center. His current research interests include using data mining and applied cryptography to improve privacy, security, and fraud detection. Contact him at rchow@parc.com.

Ori Eisen is the founder, chairman, and chief innovation officer of 41st Parameter. He has spent the past 15 years in the information technology industry, working on preventing e-commerce fraud for such companies as American Express and VeriSign.

Markus Jakobsson is Principal Scientist of Consumer Security at PayPal. His research focuses on phishing, crimeware, spoofing, and authentication, with a focus on defenses and mobile computing. He has written and edited three books relating to applied security and is listed as an inventor on more than 100 patents. Contact him via www.markus-jakobsson.com.

Steve Kirsch is CEO of OneID, a startup company seeking to fix the digital identity problem on the Internet by creating a user-centric Internet-scale digital identity system. He's a serial entrepreneur and has started and run five other ventures: Mouse Systems, Frame Technology, Infoseek, Propel, and Abaca. In 1995, *Newsweek* named him one of the 50 most influential people in cyberspace.

Scott Matsumoto is a principal consultant at Cigital, where he's responsible for the security architecture practice in the company. His prior experience encompasses development of component-based middleware, performance management systems, GUIs, language compilers, database management systems, and operating system kernels. He is a founding member of the Cloud Security Alliance (CSA) and is actively involved in its Trusted Computing Initiative.

Jesus Molina is a researcher, inventor, independent consultant, and occasional artist (when nobody is looking). He currently divides his time between standardization committees aimed at improving the security of emerging infrastructures, such as the smart grid and the cloud, and developing cutting-edge authentication solutions for them. Contact him via www.jesusmolina.com.

Paul van Oorschot is a professor of computer science at Carleton University in Ottawa, where he's Canada Research Chair in Authentication and Computer Security. His research interests include authentication and identity management, security and usability, software security, and computer security. Van Oorschot is on the editorial boards of *IEEE Transactions on Information Forensics and Security* and *IEEE Transactions on Secure and Dependable Computing*.