AmigaMCC News
Fort Worth Dallas
August 2011

Your Password Sucks

http://gizmodo.com/5814557/barack-obama-thinks-your-password-sucks

We aren't the only ones who want to see an end to passwords. So does the government. Barack Obama wants to kill your password.

In fact, he's set up a special office just to make that happen. We talked to Jeremy Grant, who runs the program. Here's what he said.

Gizmodo: There have been a lot of really high profile hacks recently that have resulted in the theft and distribution of people's usernames and passwords. Is that becoming more prevalent or are we just more aware of it?

Grant: I think its becoming more prevalent, and in fact, what we're seeing with some hacker groups like LulzSec is that they're actually going out of their way to draw attention to how easy it is to take advantage of insecure password systems—and how embarrassing it can be if people aren't taking proper care with their security.

Gizmodo: Why is that happening so much more now? And why wasn't this going on as much two years ago or three years ago?

Grant: I'm not sure exactly why you weren't seeing some of these things a few years ago. I think part of it now is it's become clear to folks who are doing it—whether attacking for amusement or in some cases looking to do something with more nefarious interest behind it—that password reuse is just a huge problem. And certainly if you talk to the free email providers that are out there, they are all dealing with this problem right now. Every time there's another data breach that occurs, and usernames and passwords come out, people are becoming more and more aware of that they can plug these into Gmail and Yahoo and Microsoft and AOL and other services and see what they find.

Gizmodo: The password reuse issue brings me to your role in this. Tell me a little about the NSTIC and what your mission is.

Grant: Sure. It's the National Strategy for Trusted Identities in Cyberspace, or NSTIC because everything in Washington needs an acronym. The background went back to President Obama's cyberspace policy review in 2009. They essentially did a comprehensive review of US cyberspace policy and came up with ten near-term action items. One of them was specifically focused on creating a cyber-security focused identity management vision, and a strategy that would specifically take into account privacy and civil liberties as well as the security side of things.

Gizmodo: And why is this a government issue? Why does the government care that we have a trusted identity in cyberspace as individual citizens?

Grant: There are several reasons. First of all, we're talking about defending cyberspace. An attack on Americans is an attack on Americans and whether it's an attack on government networks or something that's focused on my mom, it's still very much a concern.

Particularly I would say from the Commerce Department's perspective (since that's where NSTIC is and where I work) our goal is to promote commerce across the country and drive U.S. competitiveness in the global marketplace. So it's in the interest of the government to try and find a way to solve a problem if it is causing an erosion of confidence in activities that are currently online, or if there's an inability to bring additional transactions online. Because 18 years after the old New Yorker cartoon, people still don't know if you're a dog on the Internet. And that's just not acceptable for some kinds of transactions.

Now what's interesting about NSTIC is, unlike some past government efforts in this, the government's not trying to prescribe a specific solution. The government has basically put out our guiding principles: Everything that comes out of the identity ecosystem has to be privacy-enhancing and voluntary, secure and resilient, interoperable and cost-effective and easy to use. It lays out a vision of what this identity ecosystem should look like, but it really leaves it to the private sector to actually come together to come up with the standards and operating rules for it.

Gizmodo: So, you're not just, like, coming up with a secure ID card and saying everybody should use this solution?

Grant: No, no. It seems like most of the other efforts, both in the U.S. and abroad, have been focused on solving this problem by designating a specific technology—like a smart card with a PKI certificate on it. I think clearly that's just not an option that's acceptable in the U.S. We've been through the National ID debate several times, and I don't think anybody wants to go there again. Not everybody wants a smart card. If I'm doing things on a tablet computer, there might not be a place to put it. The form factor may need to change. It can be pretty costly.

The U.S. solution to this has been to accomplish a framework of standards and operating rules, but let's actually not try to specify any one technology. Instead, allow for an identity ecosystem of multiple technologies.

Gizmodo: You use the term identity ecosystem. What is that? Do you have some examples of how an identity ecosystem might work?

Grant: Sure. It's an online environment where individuals and organizations can trust each other because they follow agreed upon standards to obtain and authenticate their digital identities. It's the broader set of technologies that would be out there for identity and authentications, as well as the different parties who would either issue them, use them, or rely on them.

Participants in an ecosystem can include you or me as an individual user. It could include companies, non-profit organizations, or others that would actually want to be an identity provider. It would include all the different relying parties that would actually choose to accept those credentials for different purposes at different levels.

You'd also have a governing structure led by the private sector with stake holders, not just from companies, but also hopefully from advocacy groups, academia, and other interested stake holder groups overseeing it all.

Gizmodo: Can you give me an example of how a login might work? Let's say I'm traveling and I need to use a computer in my hotel to login and make a purchase online. How you envision something like that working in a best case scenario as opposed today?

Grant: It probably wouldn't be that different from stuff that's out there today, but that most people just aren't able to get because most stronger authentication technologies tend to be single use, and that's expensive.

There are companies that are out there, for example, that will let you sign up for what's known as a "PIV-I" credential. The federal government standard for smart cards is PIV-personal identity verification. It's for federal employees and it's also branched out to state local governments, first responders, and other groups that are servicing critical infrastructures like telecom companies, for example.

Now if you're an ordinary citizen, you probably won't be able to get a credential as strong as a PIV. You've got to go through a background check by the federal government in order to get one of these cards. That makes sense for me as a condition of Federal employment, but for someone like my mom, it'd be overkill—and moreover it's not something the government can do or wants to do. But the card itself is pretty secure.

It's a very hardened smart card that basically has D.O.D. (Department of Defense) strength encryption technology in it. So if I as a citizen wanted to have an authentication tool that with that level of strength, could I get something that complies with all those standards? You have companies that will issue you those cards today, that are called "PIV-I" meaning PIV-interoperable.

As for other types of solutions: Google and Microsoft are both offering one time passwords now to users to sign into the free mail applications and other apps. I can go to E-Trade as my stockbroker, and they'll give me an RSA secure ID token with a onetime password generator. But most of what's out there isn't interoperable and tends to be a little cumbersome to use.

Gizmodo: I can envision wanting to purchase something and not have it tied to my identity, somewhat anonymously. Would that still be possible?

Grant: Absolutely. I talked before about one reason for the NSTIC is 18 years after the New Yorker cartoon, nobody knows you're a dog. But the government recognizes there are plenty of times you want to be a dog on the Internet. And the government has no problem with you being a dog! Whether it's surfing on the web or posting comments anonymously on a Gizmodo article after you write something, there's gobs of stuff where identity doesn't really matter or you can operate under a pseudonym.

This is really much more getting to when you actually do care about having a higher level of security or trust or for that matter just having a better technology that you can actually use to protect that pseudonym that you're operating under.

Gizmodo: What would you tell people to do today in terms of solutions that are out there to give themselves a little bit of security in protecting their accounts?

Grant: My personal advice, and this is not a government position, but first as you're doing transactions online where you do have sensitive information, look for solution providers that are out there that offer multiple factors of authentication. There are companies whether it's in the dotcom world or the financial world or the health world or others that do offer solutions and offer you something beyond the password.

My general take is passwords are just outdated and becoming more and more broken each day as a security mechanism. So if you don't have to rely only on a password, don't. And I can say personally I choose some of the firms I do business with based on the ability to offer something a little stronger.

Second, if you are reliant on passwords don't reuse them. Why is LulzSec able to post 62,000 password and say "hey, go test them out and maybe some of them will work?" It's because overwhelmingly, if somebody's signing up for a free email account they're using that exact same password that they used to access that account when they're going onto a bunch of other sites online. If you're using your email as your identifier because that's what your signing in with, at a minimum don't use that password from your email any place else.

Beyond that there's lots of guidelines of what you should have in terms of more complex passwords using multiple characters, uppercase lowercase symbols, numbers. The issue with that is if you've got 25 of them and they're all different it becomes unusable.

And that's actually one of the points that the White House and we have made with NSTIC. If that's the solution, that you've got to carry 25 different, very complex passwords around with you, that's not a very usable solution. One of the things we're focused on is building something that's a little bit better which hopefully can decrease the friction that we're seeing in certain areas of online commerce today.

Gizmodo: Right. I'm a relatively heavy 1password user. And now I find that whenever I get a new device it's pretty much useless to me until I can get 1password installed on there.

Grant: Yeah, and especially so with the move towards mobile devices. I've got, what am I using right now, my Blackberry Torch? Which has got the slide out keyboard. But good lord, trying to put in a complex password on that? It's just not very usable.

One of the things we want to look at is if you deploy in a way where it's secure but nobody likes to use it, then they're not going to use it because it ends up being a pain. Study after study has shown that when you offer more security to people, if it's not also convenient then they're going to find excuses not to use it and go back to the old default of being insecure.

Now how do you change that? First, maybe the attacks get worse and people actually get scared enough that they're willing to put up with inconvenience. We're certainly not rooting for that on our side since that would mean a lot of very bad things have happened. The second is, are there models that are out there that are either more usable or that may offer some other benefits such as the ability to enhance your personal privacy and give you more choices over information that you share that would make it be worth it to take the extra step to do something that's an extra factor of authentication.

The administration's view is let's put a foundation in place in terms of standards and operating rules, but beyond that let the market actually come up with a handful of solutions. We hope it's more than a handful, we hope it's a couple bushels full. At that point let different solutions battle out in the market and may the best one win. If we try to specify one or two solutions we'll probably do the wrong thing and be outdated almost from the start.

August Calendar

August 1 — Amiga-By-The-Loop Chapter
7:30 PM — Main Grand Prairie Library
901 Conover Drive, Grand Prairie

August 1 — Board of Director's Meeting
Approximately 9:15 PM — Location TBD

August 28 — Newsletter Deadline — 7:00 AM

MCCC 4418 Sharpsburg Drive Grand Prairie, Texas 75052
http://www.amigamccc.org