CapTech

A Password-less Future with Passkeys

CAPTECH TRENDS PODCAST | EPISODE 34

Vinnie

Welcome back to CapTech Trends. Really excited about today's episode. At Apple's WWDC they announced Passkeys and I was right away excited to talk about it and to learn more. Today, I've got two guests. Andrew Levy is a Senior Consultant out of our DC office, and Mark Badger, a Fellow at CapTech, and also a Creative Director for our CX practice. Andrew, Mark, welcome.

Andrew

Thanks.

Mark

Excited to be here.

Vinnie

So Passkeys may be a new concept for a lot of people, or maybe they've heard of it because they watched the conference, and like any new technology, there's lots of different ways to look at it or think about it. From both a technology perspective and a creative design perspective, I'd like to hear how you guys think of Passkeys and we'll get into more detail about how they can be implemented and some of the details. But from a high-level definition, educate me on what Passkeys are and we'll go with you first, Andrew.

Andrew

Sure. Passkeys are a frictionless and secure alternative to passwords that have been standardized by large companies like Google, Apple, and Microsoft, to provide a consistent login experience for users across different platforms and devices and at a high level, it's the first big step towards a passwordless future.

Vinnie

Great, and I'm glad you said frictionless. If you've been listening to the previous podcast, specifically the ones on virtual and augmented reality, both of which I enjoy and have multiple headsets for, there's so much friction to having to put something in your head, clear out space around you. And whereas CapTech sees a lot of these trends going is to have more and more technology involved in our lives and throughout our daily tasks, but realizing it less, seeing it less, feeling it less. It just becomes more natural. Steps are removed. Augmented and virtual reality adds steps to add immersion. But this is a technology that reduces friction and reduces steps. I think that's one of the things that gets me excited about it and it's a perfect lead in, Mark, for you to talk about the user experience.

Mark

I think maybe we'll talk in a little bit in terms of implementation and how it actually plays out. I think the idea of friction and frictionless is interesting when it comes to issues around convenience and security. I'm sure we'll get into some of those topics, but I think the shortest way to talk about Passkeys is like Andrew said, it's meant to obviate the need for passwords altogether. There's a lot of challenges with security when it comes to passwords. We know how users, people, how they deal with passwords. They will repeat them all the time across sites. I myself do it. They will write them down sometimes. They will use easy-to-remember words, just because you have so many things you want to be able to log into and authenticate. All the security provisions that various companies have done in various industries to try and make things secure often contribute to the problem. Things like automatic sign-outs after a certain delay, just ways that it makes it hard for people to maintain that security while also maintaining the convenience. Then there's all these other structures, like third-party password managers. Google and Apple have their own frameworks, which we'll probably talk about a bit too, because they do intersect with Passkeys. As Andrew said, Passkeys are intended to basically be the next gen altogether. Some of that framework we will still need for the foreseeable future for years probably. But the vision for it, and when it works, it does work really well like this. You don't need a password. And it's easy. It's as easy as unlocking your phone. I want to talk about that a little bit later in terms of the customer experience as well, because there's some downsides to that actually. When you talk about awareness of what's going on and you talk about the friction you have with technology, sometimes that friction is good, because you want to be reminded of what's going on. You don't have to understand what's actually happening underneath the hood. But you want to be reminded for example, oh, actually one nice thing about two 2FA and MFA, that's two factor authentication, which is just a subset of multi-factor authentication, is you are very much reminded I am going through a secure experience, because I'm being prompted to provide other ways of validating who I am. When you unlock with just your thumbprint, it's easy to forget.

Vinnie

Yep. It's a good point. You hit on a couple of things in there, the multifactor authentication, the pass phrases. I know it seems silly, but as you get older and you need readers, and you're on an airplane, and your readers aren't available, and you try to type in 37 characters, and you can't see, you're going to make a mistake. It's going to become frustrating. That's a high-friction experience. I use one password as a password manager and I know I've got well over a hundred passwords in there, which is crazy to think about. Then it alerts you when you're using the same passwords in multiple areas. So now, I've got a hundred different things in there. It alerts you when sites have been compromised and you need to go change your password, which happens more often than you would think. We're at a point in time where we have a technology with really no downside other than implementation details, which we'll get into. But it is more secure, not less secure, has far less

friction, and improves the user experience. There's no downside academically to this.

Andrew

It's a very rare technology that when something does something like that, it improves UX and adds security.

Mark

As Andrew mentioned also, it's one of those things that I think we as consumers and as technology implementers for the work that we do, the more that we can have these foundational technologies where the largest companies in the world agree on a standard, it makes everything so much easier. I'm sure y'all have done things with smart homes and trying to figure out how to get a home kit to work with Google's version of that. It's a nightmare. The upcoming, I think, is it Matter? I'm trying to remember now, because they've had a couple different standards. There's Thread and Matter, but these standards where we can all kind of, "Okay, all our devices will talk to each other on a shared understanding," it makes our lives easier. This is the same idea. There's just so many ways right now that we're trying to keep our lives secure. The frictionless, passwordless future is definitely ideal.

Vinnie

Definitely, the password is a big, big deal.

Mark

I don't know how much you want to go into it, but some of the details about how authentication works, there's three basic principles. There's the something you know, something you have and something you are. Something you are is biometrics are common. Something you have could be something like your device or even in a way, a third party Apple…

Vinnie

An authentication app giving you a code.

Mark

Exactly. And there's something, it's like your password or passphrase, or the old-fashioned security questions about, they're really hard to find out. Mother's maiden name, that is really hard to dig up, your birthday, all these things that nobody ever knows.

Vinnie

Well, and people on Facebook will tell the world who your childhood best friend was.

Mark

Exactly. Or where I went to primary school, whatever it is. One of the things about Passkeys is the part of the, relying on something you know, which is the most fragile part of password security, disappears, because it's not based on something. Andrew can talk, I'm sure, more about all the

details about how that works, because it's definitely out of my wheelhouse. But that's an interesting part of it.

Vinnie

Well, something you have and something you are become one thing, because you have the phone that's biometrically identifying you.

Mark

Well, the part about the secure layer of it is this is one of those, I think, again, there're some trade-offs, but in terms of the ease of use from a customer experience perspective, all the complexity is taken care of behind the scenes. It's just your thumbprint or your face kind of thing. So yes it is…

Vinnie

It feels like one step.

Mark

It feels like one step, exactly. But the behind-the-scene stuff is, I mean, this is secure authentication that goes beyond again, what I can talk about with any kind of confidence.

Vinnie

Let me go back into the defining part of it. You guys did a good job of defining it, but I want people to get a visual image in their brain of what this looks like and behaves like. Let's say I already have a passkey set up. We'll get into how it gets set up. So I go to my phone. Let's say I go into my banking app and it just does a face ID and I'm in.

Andrew

It depends on the platform. It's implemented a little bit differently based on Android, iOS, and web. I'll take iOS for example. When you get into an app, you're presented with a login screen usually. If you click on the username field and focus on it, it will auto suggest any passkeys that you have for that given app and associated with that username. As soon as you click that you want to use that passkey, your biometrics modal will pop up, just like you're used to, like signing into your iPhone, and you're automatically logged in.

Vinnie

On the Mac it would be your fingerprint on the keyboard.

Andrew

Correct.

Mark

If you have that.

Andrew

That's a big thing. Passkeys are only supported for those devices that support biometric support as well.

Vinnie

Well, you have the QR code potential as well.

Mark

There's some workarounds. QR code is one of them. Your PIN can be that. But when you're navigating Passkeys on desktop and web experiences in particular, or I guess, it might be apps as well, but you need that workaround potentially if you don't have the biometric authentication available.

Vinnie

I'm going to give three examples. One, I pick up my iPhone. I launch the app. I just touch the ID field and it suggests my passkey. And I say, "Yeah, I want to use my passkey, face ID." Same flow for my desktop Mac with my fingerprint on the correct keyboard. Now, I'm visiting my parents who have a PC, hypothetically, I made them get rid of PCs a long time ago. I'm not supporting you anymore. You're out of service. But hypothetically, I'm on their PC. Or you know what? I've got a gaming PC that I use for VR, so I'm on that. And I want to log in something that has an Apple Passkey. What happens then?

Andrew

On the web experience, you can choose the option to share a passkey or use it on a different device. It'll pop up a QR code. Then you take out your device that has the passkey installed on it, and then you use your camera app to scan the QR code. Boom, you're in.

Vinnie

So my PC would have to have a camera.

Andrew

Yep.

Mark

Also, I think it has to have Bluetooth enabled as well.

Andrew

Actually, it doesn't need to have a camera. You scan the phone camera on the QR code. Then biometrics pops up on your phone and it communicates to the-

Vinnie

Gotcha, and using Bluetooth low energy.

Mark

The Bluetooth layer is there to validate proximity, right?

Vinnie

Yes. That makes total sense. These are implementation details, but what's important here, this is where things explode. Because you could say, "Wow, it's biometric. And even when it's not biometric, I'm just pointing my phone at a QR code. This is awesome." Now, you get into edge cases, where Bluetooth is disabled on a device or not available on a device. Now we have to handle that from a user experience perspective and it gets more complicated.

Mark

I've been trying to imagine what the true future, 5 years out, 10 years out, I don't know.

Andrew

When passwords are gone.

Mark

When passwords are gone and when it's all about the passkeys, what that really looks like, because we've been living with passwords since the dawn of computers pretty much, since we had authenticated things, even if it was just a password and wasn't username at the time.

Vinnie

We had passwords before computers. To get into a speakeasy you had to have a password.

Mark

I'm sure y'all done this too. When you dig into the history of authentication and you talk about keys as a concept, of course, you have keys and locks, which at a philosophical level are no different than a public and private key exchange that we have going on. If you've used a key to enter your house, which most of us do, that is at some very basic level –

Vinnie

We're so used to the abstraction, we forgot the origin.

Mark

Exactly, right. It's not this velvet rope club. The in between now and that 5 to 10-year future, what we've been talking a lot internally is what are the best practices around mitigating the messiness of it, I guess, in particular around the user experience of it, because that's really where it's going to play out. Last night I went through and for those that are curious, I can't remember the URL or app, but one password actually maintains a directory of currently available passkey experiences that you can use online.

Vinnie

I didn't know that. I'll look that up.

Mark

I can tell you. Because I tried all the ones for which I had an account, eBay, Kayak Shop, Best Buy, those are the ones. I think I tried another one or two, but I tried them all and they were all different. The passkey layer, once you get there, is the same. The getting there is different. Not intuitive. Sometimes I had to dig for it, which shocked me because actually if you're looking for a good intro to passkeys and what the prospect is, New York Times did an article back in January about the RIP password, here come passkeys kind of thing. You can look it up and it tells you a lot of this stuff in very accessible terms.

Vinnie

What was the publication again?

Mark

New York Times, which is actually how I found the directory in the first place, actually. With Best Buy, I had to dig. I was expecting actually because they've been noted as one of the retailers that was first to market for this thing. That's something we should probably talk about too. What are the brand advantages to embracing Passkeys now as opposed to waiting? I was expecting a really best-in-class implementation and I have to say, it was rougher than I thought. It didn't prompt me immediately to, do you want create a passkey? Once I created one, I think I actually was only on the app finally able to ever use a passkey. It's still wanted me to use my 2FA, which I had set up previously.

Vinnie

It brings up a good question. I'm company X and I want to implement Passkeys. What's my responsibility for educating my customers on what a passkey is? Do I assume that people who want to use them know what they are? Do I obfuscate it entirely? Not even call it a passkey and make it, this is a fast pass. How do companies meet their customers with this technology in a way that we don't have to overeducate or over explain?

Mark

I'll go backwards on that. I don't see an advantage to trying to create your own cute marketing term around what this is. Call it a passkey. It's meant to be a generic word like password. It's not meant to be Passkey TM trademark. It's meant to be a common way that we refer to this going forward, period. The best thing you can do from a brand perspective is to lean into that, because you're going to then leverage everybody else's adoption of this passkey concept. You're not going to have to work upstream to create your own quick pass, one-time only, whatever it is kind of thing. I don't know what you would call it. From a branding perspective and the effort you would need to lift to

educate your customers, go ahead and use everything that's available, including client passkey. Start with that. But I think for the foreseeable future, we would recommend that brands do some amount of, certainly a lot of edge case testing to look at all the flows that would likely come from this, including, does the user already have 2FA set up? Does the user already have some other form of multi-factor authentication set up? What does it look like to them? Once they've enabled a passkey, you should basically opt them out of these other ones so that they can have this more frictionless experience.

Vinnie

There's going to be a sun setting of-

Mark

It will take some time. But to your question about educating the customer, I don't think they have to do the heavy lifting about certainly all the technology behind it. But I think there's some education that a brand will want to do. I think it'll be to their benefit to do it. We haven't really talked about this yet, but in discussing why a brand would want to do this now when it feels, and reality is like it's not bleeding edge. It's not cutting edge. But it is your early adopter type stuff. There's going to be a lot of fumbling. This vision though feels very real. Nothing that has come before has really had the promise that this does. When it actually works, it feels like it lives up to it. It truly does. If you're a brand where security is really crucial to, I mean, for most brands it is, but when you're talking about things like financial services, healthcare, where you've got PII and PHI and other things that users find, whether by regulation or just by desire to be really private information, I think it's to your benefit to go into security now, to push for this. Then I think you do have some responsibility, some education, but I think you can do it in a way that's got a marketing edge to it. So no, it's not creating a cute term, but it is lean into, "We are here for you in terms of protecting your information."

Vinnie

Well, there's a nuance there that I think I want to call out. A, it is more secure. A CISO in an organization would want to do this, because it's less complex and more secure. But then from a marketing branding perspective, being thought of as a security conscious organization, like Apple is quite frankly, famously not even sharing phone data with the FBI when it could solve a crime. There's nothing they're going to do to do that. I think that helps the marketing and brand. Andrew, I want to switch to you. You've been involved internally in creating a proof of concept. There's going to be a link to the blog right after this in the description of this podcast. If anybody wants to see, I don't know if it's going to be images or a short movie or –

Andrew

We could probably have a screen recording of –

Vinnie

We'll walk you through that. Maybe a voiceover or something, so you could see it. But tell us what that was like to create a demo. Here's what I'm thinking. If I'm an organization and I've got 47 different assets, whether it's mobile sites, or websites, or whatever else. Maybe it's 20. I don't know, maybe it's a hundred. What does it look like to roll this out across not one asset, but all these assets?

Andrew

We wanted to start with a real life scenario, a real client scenario. We started with a normal, traditional password login experience and then add on passkeys to see what that level of effort would be.

Vinnie

Right, and that surprised me, because I thought the demo was going to be, "Hey, here's Passkeys working as passkeys." And what I saw was, "Oh, here's an organization that's been using passwords and MFA for years and now they're adopting passkeys," which I think was the right way to do it. I just wasn't expecting that.

Andrew

Because we assume that most people who are going to implement Passkeys, they're not going to be a greenfield project. It's going to be an add-on. We wanted to see what the level of effort was for that. So we started with the traditional login flow and we incrementally added on different features like autofill. That's when you focus on the username field, you get suggested. Your passkey is on that device. We ran into a lot of issues with documentation considering how new this is. So we got about halfway through and we realized that the API for Android doesn't even exist yet. That came out about three weeks, or two weeks ago.

Vinnie

It's available now.

Andrew

It's available now, yes. At the time, it did not. But iOS, I mean, there's documentation out there and the same for web, but there are are no real concrete examples that we can work off of. There is now. So we were making it up as we went along.

Vinnie

And it's ours and you can find it in the blog. It's not written yet.

Andrew

It was definitely a good learning experience. The result that we came up with is, it's pretty easy to add on. It's a nice add-on to an existing app. It integrates well with existing login flows, which is nice. There's really not much rework that you need to do above your current, even if you have a third-party authenticator, it can just be added on and you have Passkeys.

Vinnie

Right. And it's backward compatible with FIDO2, WebAuthn.

Andrew

Correct. Yes.

Vinnie

What's interesting here is it seems like it's not a super heavy lift, correct?

Andrew

Yeah.

Vinnie

Okay, so not a super heavy lift. But if you have a bunch of assets, are you repeating this process from a code perspective across all those assets? Or does it sit behind, that they can all share some common implementation?

Andrew

There is rework. We can leverage technologies like React Native, for example, that can output to iOS, Android, and the web. There's something in the works right now. We're going to experiment with that a little bit. But as of right now, for each platform, we're implementing it from scratch.

Vinnie

Great. So if we did something in React Native then, and put that in a repository somewhere, that everyone on the implementation teams could just pull that down.

Andrew

Yeah, it can be a reusable module that you just pull down. It's not specific to React Native. It can be another multi-platform app.

Vinnie

Sure. Gotcha. Then two questions related to that. One, what would have to be true for this not to be easy? Do you have something that's a 20-year-old legacy system that's not compliant with WebAuthn? Give me a situation where this is harder.

Andrew

One thing we discussed was device support. If you are still supporting iOS 11 and an iPhone 4, you're probably not going to be able to add it as easily. You can edit for devices that are running iOS 16 and up, but how are they going to get the benefit of that? So there are some restrictions on device support. Do you know any other things that would make this hard to implement?

Mark

On the back end or the front end?

Andrew

On the front end.

Mark

I think the front end, it's all about technology adoption and how fast people upgrade.

Vinnie

Which honestly, is faster on iOS than Android.

Mark

Historically, yeah, for sure.

Vinnie

Well, it's forced more. It's pushed more. It's a focus. I've had a thought, and I don't know if this is true and I want to whiteboard it out at some point, but a lot of the companies I work with and do high-level IT strategy type work, getting down to single sign-on or a single entry point and into all the services that a company offers is a big deal, because a lot of these companies grow through acquisition. They're doing a lot of work in the background to try to make it seem like it's one password. Seems to me that this could be almost a workaround to that, where if all I have to do is look at my phone and it reauthenticates me for the next thing, it's so frictionless. If that was a pass for a different pass phrase for everything I had to type in, that would be unacceptable. You'd want to push towards single sign on. But if all I have to do is look at my phone and I'm already looking at my phone, that doesn't feel like something I necessarily have as much reason to solve for.

Mark

I'd love your thoughts on this, Andrew, because I've been focusing mostly on the impacts to users and how it plays out. But I was wondering similar things. Recently, in addition to the third-party tools, like Author, Google Authenticator, Microsoft Authenticator, in the past five years, Facebook has their centralized login. Apple, Microsoft all have invested in this. As far as I can tell, and this is where I rely on you guys. You're much more conversant in technology than I am in terms of the underpinnings. It seems like from a security perspective, having a trusted third-party that isn't necessarily all that different. I mean, it's different for the user. That's part of what I would want to talk with brands about its managing. Okay, al of a sudden you could have a login experience that has username, password, sign in with Apple, sign in with Microsoft, sign it with Facebook, sign in with Google, sign in with Passkeys. It becomes insane. But on the backend, when you're talking about these trusted security providers, is it that different? I think it gets to your point, Vinnie, if I'm an enterprise thinking about this, why would I choose Passkeys over a Microsoft or an Apple-based solution?

Andrew

At first glance, when you see Passkeys, you might think that it's a third-party authenticator killer, but it's actually not. There's one problem that Passkeys solve currently, which is if you create a passkey on your iOS device and you try to do the QR code thing that we discussed earlier on Google Chrome, on your laptop, that won't necessarily work, because they're different cloud storage providers. So you have your Google Cloud and your iCloud, and those don't communicate with each other. That's a huge gap right now. But something is in the works with third-party authenticators, like OnePass or Microsoft Authenticator to bridge that gap and act as a middleman so that you can store them in their cloud storage and share them across different platforms.

Vinnie

It's going to be a passkey broker?

Andrew

I believe so. I think OnePass is leading the charge on this. I saw something the other day for a few others as well.

Mark

One of the things we haven't talked about actually is, you just alluded to that, if you're inside an ecosystem, it really is painless. I mean, Apple has been doing this for a long time. In a way, I don't know if they had this vision in the future, but some of the behaviors that they've been doing through either software or hardware have really trained us to be ready for Passkeys, so having biometrics widely available on keyboards and our mobile devices. But also the iCloud shared keychain, Passkeys just leans right into that. This was one of the things that is really, really nice about it once it's set up. You create your passkey on your laptop and it's just there on your phone. As long as you're logged in and you have an Apple ID account and you're logged in, that gets shared pretty much, it feels automatic. I didn't have to wait. I was able to use that passkey right away. I feel like that worked even better than it has with passwords. I've had things where I'll reset a password and it still has my old password on my other device. I'm like, "This makes no sense." I think the other thing we haven't talked about that's really an enabling technology is this cloud storage, which again, we've been getting trained as users to rely on companies like Apple and Google to share all my stuff across all my stuff, make it easy for me. The advantage is now you add that layer of security and everybody's ready for it.

Vinnie

I have a naive question for you. I wish I knew the answer to this so I didn't have to ask on a podcast. If I'm a company and I'm implementing Passkeys, do I have to choose whether I'm working with Apple only, Microsoft only, or Google only? Or because I'm using Passkeys, can my customers use whatever passkey storage they want to use?

Andrew

Right, as a company, you don't need to have that responsibility of choosing. That's on the user, depending on what their device is, which is actually nice because it gives them the freedom to use whatever device and it will just work that way. If you do eventually incorporate this with the password manager or a third-party authenticator, then that would bridge the gap like we were talking about earlier, between platforms.

Vinnie

One thing then, and it relates to that, and we've chatted about this before the podcast, one of the only downsides I can see then in this is you need to trust not one of these companies, but you need to trust all companies. So it's like, "Do you feel good that Apple and Google and Microsoft have this information?" Now, make me feel better about that. It's super encrypted. They can't do anything with it. What are the details? It's not open text, things they can look at and copy and reuse.

Andrew

Right. The thing that we're trusting these companies with is this private key. When you create a passkey, you create a public key, private key pair. We don't have to get too technical. But the private key is stored on the device, and that's what we're entrusting Apple and Google with. It's not like a readable thing. It's not like a password or anything. But if it does get compromised, then all your passkeys are compromised. A lot of people currently use these password managers heavily. I know I use it on my iPhone for all my passwords. So whenever you store a password with these password managers, you're already entrusting them with less secured data.

Vinnie

Okay, so it's a moot point. Well, it's funny because you read publications and it's like, "Well, that's one of the risks." It's like, "Well, okay, but if you've ever said yes to remember this ID on an app or a web interface, then you're already doing this and you're already doing it in a less secure manner."

Andrew

Yes.

Mark

As you're saying, we're trusting companies with access to our private data or access credentials anyway, a lot. The difference going forward though is the brute force hacking or social engineering backed hacking, where you see these data breaches. Huge batches of passwords and usernames have been leaked out. One of the things that that Passkeys says is-

Vinnie

That goes away.

Mark

... it goes completely away. From that attack vector, it's really eliminated as an issue, because a hacker can't actually make use of all those passkeys.

Andrew

It might be advantageous if I explain that a little bit of how traditional passwords work. When you log into an app using a username and password, sending that data, the username and password that they input into those fields across the wire, sending it to our backend service, storing it somehow-

Vinnie

Across the wire, it's encrypted with-

Andrew

Encrypted in some way. Even though it's encrypted, once it gets to our backend service, we're still having to store that, so that on subsequent logins, we're comparing, the password every time. With Passkeys, all of that goes away, because we're not sending any personal information or sensitive information. We're sending a signed signature from the private key on the device. It's like an imprint of the private key that says, "I was the private key that signed this." And we can verify that because I used my biometrics. Then once that signature gets over to the backend, we use the public key to unlock that message. If the public key that replaces the password, that can be breached, if the public key gets out, nothing happens. There's nothing that can be compromised.

Vinnie

Right, because you have to have all the private keys that are on all the local devices.

Andrew

Exactly. Right.

Mark

That thing that happens now, we all probably experience this at some point where you hear about one of the services that you use has a data breach and nothing happens. But then you have a security issue that shows up on some other place that you have an authenticated relationship. What's probably happened is that dump has gone to some farm of hackers or automated systems that are just trying all those username and passwords against any number of sites hoping for a hit. But once you have the computational power cheaply available to just do these brute force strategies, why not? You'll get a hit every now and then. You can't do it with passkeys.

Vinnie

Right. When you talk about phishing, that goes away.

Mark

Bye-bye. Gone.

Vinnie

Gone. Malware, that can't work that way. To use your phrase, there's several attack vectors that go away.

Mark

Yeah. I think the other thing we haven't talked about, so we talked a little bit obviously, about the consumer or customer advantages, a little about the brand advantages, both from a PR and actual obviously security perspective. The other thing we haven't talked about yet, is the operational costs involved with the current authentication scheme. How many calls are made to call centers for password resets? I forgot my... That won't go away, especially in the interim so we shouldn't be naive about that either.

Vinnie

But once passwords go away, that goes away.

Mark

Yeah, because actually, the call center can't do anything about that.

Andrew

There will be a new set of problems that will have our own frequently asked questions, documents that we'll have to go through, but the old set of problems will go away.

Vinnie

I think the new problems will be less costly.

Andrew

I agree.

Vinnie

Because there'll be less humans involved.

Andrew

Definitely.

Vinnie

And that's the long pole in that tent. Before we wrapped up, I wanted to get into, what are the first steps someone should do, a client should do? You're a motivated smart developer or creative CX person in an organization. What are the first couple things you do to dig deeper into this within your organization, either to learn about it, or get adoption, or get excitement?

Andrew

Do you want to start with this one?

Mark

Yeah, so I mean, just a plug. As you mentioned, we'll have at least one or two blog posts after this that will lay this out in detail.

Vinnie

So more to come.

Mark

Right. So there'll be some things there. I mentioned the Times article from January. That's a decent place. Fidoalliance.org has all of this stuff in detail, probably more detail than you want. But they have some videos and demos that when you're looking to understand the concept and the underpinning, especially if you're on the implementation side, whether that's the design or the technology side, it's a great place to go. Apple does have some great stuff as well. In terms of base understanding, those are the ones I would initially recommend. They were actually much easier to consume than I thought. Especially FIDO Alliance, they make it easy.

Andrew

Yep. We're definitely going to be putting out a technical and a non-technical blog. If you're interested in the public key cryptography stuff, the technical one's for you, just to learn a little bit more about how this is actually working under the hood.

Mark

I would say also, I mean, there's a couple articles, two or three articles, from Forrester in the last year that have talked about this, some directly in terms of literally about FIDO authentication and Passkeys. Others, just about the trends around consumer authentication. But I would note, actually, one of the things that are pointed in there, so this was a year ago, but they did research around customer behavior. It said, "38 of adult US smartphone users have no intention of changing their behavior around authentication."

Vinnie

30%.

Mark

38%, so not a majority, but certainly a notable plurality of people that have no intention of changing their behavior. We also haven't talked about this. This probably isn't a ground swell type thing. It's going to have to come from companies adopting this and then pushing it, just like they did with 2FM and [inaudible 00:34:37].

Vinnie

I would argue of that 38% that are planning to do nothing, 99.5% of them don't know what a

passkey is.

Andrew

Yeah.

Mark

Right.

Vinnie

It's like saying, before the iPhone came out, how many people intend to use their phone as a movie studio? 0%.

Mark

Right. That's fair.

Vinnie

I think some of this goes back to the education I was saying and getting people excited about it. Internal to an organization, I'm trying to decide where I would go. Do I go to IT, because it says technical problem? Do I go to the CISO, because it's a security problem? Do I go to the head of marketing and brand, because that's what it is? Is it talking to all of them? Where do I go to be the, "Oh, my gosh, guys, you got to come see this. This is great"?

Mark

I mean, I don't want to go into the consulting. It depends.

Vinnie

Right, so you're going to strike that. So you can't say.

Mark

But having not said that, if your company's budgets... So if your customer experience is centralized, whether that's through the CMO or chief experience officer, that's likely the place to start. Because I'm imagining in that scenario, your company's set up in a structure, however it's meant, structured for software delivery life cycle, the budgets are probably managed across the customer experience. This is really, yes, a security play, but I mean, it's hand-in-glove. It's a customer experience play. The brand play is also there, so enhancing the posture and positioning of the company as security focused, as privacy focused. I think if your company is leading from an experience perspective, that's where you start. I think it's an attractive conversation. You watch a couple of these demos and you try it out, and like I said, when it works well, it's amazing. It feels magical. It's one of those technologies that actually when it works well, feels great.

Vinnie

There was a comedy bit one time about someone getting on an airplane when WiFi on the airplane

was first available, early on. The flight attendant said, "Sorry, WiFi's not available." And the guy was like, "Oh, this is unreal..." Getting mad. I don't want to obviously repeat the words. It was, how quickly do you become so self-entitled to have a technology that just came out? But that's me. Because when I now have to log to my corporate systems and I have to type a passkey in, a pass phrase in, I'm sorry, pass phrase in. And then a box comes up and I got to put my finger on the keyboard and another box comes up that I got to take my phone out of my pocket, launch an authentication app, and then take that number and type that number into a browser, I am getting angrier and anger every time I have to do that. This problem is now solved. It's just a matter of being patient enough until it's implemented across all the devices and services that we want to use. Great. Is there anything else that you guys wanted to touch on before we wrap?

Mark

I think one of the other angles, this supports what we were talking about before from a customer perspective and also the brand responsibility for the user experience, is I was looking at, does this fall into the technology adoption curve that everybody knows about or some other kind of change behavior or curve? And the one that I actually, that I liked a lot, which it doesn't help with passkeys, it's just in general when you're asking people to make changes to how they do life kind of thing, BJ Fogg has a good model for this. He talks about motivation versus ability, which is basically ease of use and then triggers. There's a great chart for this. Once you're on the upper right corner of this chart, change is likely to happen. When you're below this curve, change won't happen. So motivation matters quite a bit. Am I motivated to make this change? So when you look at the research around authentication and user behavior and adoption, people that have been hacked are highly motivated to secure their stuff. It makes sense. But it also falls along industry lines. People don't care as much about certain relationships, maybe their local retailer, even if there's logging in experience, than they do with their banks. I absolutely want 2FA, MFA, whatever passkeys with my bank relationship. But ease of use is a critical factor in that, because we're all inherently lazy. We want easy ways out. So even if the motivation is high, if you make this an onerous experience, and again, it's going to be some stuff that the company will have to take responsibility for, for the next few years to make this transition to Passkeys, make it easy to use, and then you'll get the change that you want out of the user's behavior. But if you don't make it easy, it's like Apple Pay or Samsung Pay, Google Pay, all of these touchless payment schemes, they're super easy. But if they're not made easy during the process, so if I have to wonder at any given-

Vinnie

Every time I use Apple Pay, I'm studying the interface to say, "Will this device support it?"

Mark

This is the thing. You walk into your local grocery store and if it says on there, you see the Apple

logo, you see the Google logo, you see something, you're like, "Great," that's referred to in his framework as a trigger. So I know at that point, "Oh, this is great. I'm just going to tap my phone or my watch, whatever. I'm done." But the moment none of that is there, I'm like, "Can I use my..." All of a sudden, what used to be actually, and we talked about this with the touchless adoption in the first place, how hard is it really to use a credit card? It's not that hard.

Vinnie

Well, this goes back to the frictionless trend we're seeing. It goes back to me being increasingly irritated with pass phrases. These are long-running problems. Passwords have been a problem forever. Another thing that's been a problem forever, and maybe just for people like me who are hyper urgent, A, if I'm at a restaurant and a check is dropped off, I'm ready. I got my credit card. Don't walk away. But they walk away and now you're sitting there for another four or five minutes while they have a very busy job to do to then come back and take it. And then they walk away again. The ending of the meal is artificially lengthened by a lot. So now, if I get a bill that has a QR code on it and I can just use my phone and Apple Pay, I'm choosing those restaurants over ones that make me sit and wait. Just like you said, I choose locations where I can use Apple Pay instead of... It seems like a minor thing, but it adds up.

Mark

It does. It also plays into another experience concept. It's like peak and end theory. The experiences that you have, and digital are no different, the ones that you remember are the highs and the lows, the highest point and the lowest point, obviously of something that's really horrible or something that was really great. But also, importantly, the end. The last interaction you have as part of a chain of interactions in this, whatever you're doing with a company brand or restaurant-

Andrew

You remember it more.

Mark

You remember it more.

Vinnie

It's beginning and ends, and you-

Mark

Yeah, you want to end well.

Vinnie

Right. You can test this with a friend. If you give someone a string of numbers, 14, 21, 8, 9, 12, 32, 10, what was the first one? 14. What was the last one? 10.

Mark

32 and 10.

Vinnie

Right. What are the ones in the middle? No idea. You can list 10 numbers out fast and most people will get the end. A lot of people will get the first. And almost no one's going to get the stuff in the middle, just the way our brains work.

Mark

The main thing I just want to reinforce is that I think there's a real advantage to brands, especially those for whom a security and privacy posture plays strongly into their brand and the brand messaging and how they convey trust to their customers. They need to take on, to an early point you made, a little bit of the lift of educating what is a passkey. And then taking the time to make sure that transitional experience where we have to from a security posture and because of technology not being evenly distributed in terms of available to use passkeys, is going to be a little bit of messiness. The companies that make it easy, I think, are going to benefit. But it will take some effort. It will.

Andrew

It really comes down to the way we market it and the way Apple markets it, because we're not going to teach the average person what a public key, private key pair is. You don't need to know that to know that it works. I showed you the demo earlier and I was one click, biometrics and I'm in. And it just felt like magic. So that's the thing we have to sell.

Mark

Correct.

Vinnie

Well, Andrew, Mark, thank you for joining me.

Andrew

Thanks for having us.

Vinnie

Great discussion. Again, there'll be a blog linked in the description. And I wanted to end with I guess a thought, which is part of my job and a team that supports me in that is to look at trends, what's going to hit, what's not going to hit, where to invest, where not to invest. A lot of that comes down to the engineering discipline and rigor behind something, which is a really important aspect to it. The other part is the user experience part of that, how it improves upon the user experience. So some things I say, "No, I'm not believing the hype cycle." And some things I'm like, "Okay, I don't see why this wouldn't happen." And this fits in that camp rather squarely it.

It's strong technology. It's backwards compatible to all the standards. All the major cloud vendors are in. It improves the user experience. It improves security. I don't see a downside of this. The only thing I see as a risk moving forward is the hype cycle hasn't hit this yet. Apple had a big launch on it and a big push. You don't hear… I don't think that we're getting the press on this that we should be getting.

Andrew

Most people don't know they exist yet.

Vinnie

Correct. Death of the password is a huge, huge, huge deal. I'm hoping that this gains that steam and momentum. I think that's going to be led by the early adopters, who get out there and do it first.

Mark

I think the hard part is early adopters means a couple different things. It's brands and companies as well as end users. I think it'll be interesting to see, Andrew mentioned before, Google just two weeks ago came out, finally certified their standard around how they're doing this. I think, is Microsoft's out yet?

Andrew

I don't know, actually. But the APIs that matter are really iOS and Android and the web.

Vinnie

Yeah, so that's the last point. Start with mobile.

Mark

Well that, absolutely. But the reason I mentioned it is because we have Google iO coming up. We have the Worldwide Developer Conference this year. So it'll be interesting to see how much press comes out of this, because last year, as we keep talking about Apple led the way last June by announcing this. Then there has been some steam in the tech press in the fall now coming in. But now, with the big conferences coming out, we can imagine an additional push. So I'm hoping that the hype cycle is actually coming.

Vinnie

Great. Well, again, thank you both for joining. Great discussion. If you guys want to learn more, earlier on Mark referenced some sites to go check out. Obviously, the blog I've mentioned a couple times. Play with it yourself. There's going to be a technical blog coming out as well that will walk you through how to do some of this in your own organizations. Just start playing with it. It's not a huge technical lift, but there's a ton of value. Thanks again for listening to our podcast. We'll be back with another episode pretty soon.