Transcript | What Matters Episode 33: Getting to Know Auth with Dan Moore

Voiceover:
Welcome to What Matters, the podcast from the folks at Mattermost. We'll be discussing ChatOps, Open Source, DevOps, and everything that matters most to you. Let's see what we're chatting about this episode.

PJ Hagerty:

Hey everyone, welcome to What Matters, the podcast from the folks here at Mattermost. I'm PJ, your host, as always. For this episode, I'd like to introduce you to my friend Dan Moore of FusionAuth. Dan, tell us a little bit about yourself and what you do.

Dan Moore:

Hi, thanks for having me PJ. I am head of DevRel at FusionAuth, so I am working there. We're an auth provider, something like Auth0 or Keycloak. I am working with our community and our customers and our users to help identify how they can integrate our auth solution or a different auth solution into their applications.

PJ Hagerty:

Awesome. So it seems like the big question right off the top here is, auth authorization is the first line, authentication/authorization, first line of security. Would you agree with that?

Dan Moore:

Yeah, and actually I think it's funny that you kind of stumble over auth in authentication and authorization, because I really wish there was a better way to kind of convey those two interrelated concepts. I would say that they aren't really the first line. I think that there's actually things you could do in front of it to deal with requests that are obviously malicious, but they're absolutely the door, right? So maybe your WAF is your front fence and then Auth authentication/authorization is the door to the house that really keeps the precious stuff safe.

PJ Hagerty:

Right on. So while it's not your first line of defense, it is, I think maybe a better way to say it is, it's the thing that people know about the most. Because I mean, we're living in a world now where there's like lots of APIs, lots of integrations, lots of plug-ins, like Auth has become a huge deal, whereas it was kind of less of a concern before. Do you feel with growth of companies like yours, like FusionAuth, do you think part of the reason for the growth of those companies is there are more malicious attacks? Or we're more aware of them because we weren't worrying about it as much before?

Dan Moore:

Yeah. I think honestly, the codification of OAuth 1.0 and OAuth 2.0 in the early 2010s, and then full credit to Auth0, they really pushed this idea of you can outsource this pretty gnarly undifferentiated problem to other, to a company that can just take care of it for you.

Dan Moore:

And then of course there's a lot of open source options as well, a lot of libraries that have kind of come out. The way I think about it is in the sixties, 1960s, people kind of integrated their data with their application and the seventies and the eighties, the big revolution was the RDBMS, which let you extract that. And I think people are coming that same thing with Auth. So it is definitely more prominent now. I think also, to be frank, a lot of more of our lives are lived online now than they ever were before and we want to protect those.

PJ Hagerty:

Definitely, definitely.

PJ Hagerty:

Right. And I think it's interesting you mentioned the buildup of the relational database and I feel like in some ways that in the eighties and early nineties led to the idea of microservers and I think Auth kind of comes in on that as well. It's like, you don't

have to have such a tightly coupled integration. You can use a service like FusionAuth to kind of off put that and go back to focusing on building your app, which is the thing that you actually care about.

Dan Moore:

Yep, and I'm actually on the OAuth mailing list. And so for members of the community that aren't aware, OAuth is a way to securely delegate authentication/authorization decisions to a third party, whether that's Google or Facebook or Mattermost or something like FusionAuth, that is kind of a first party solution.

Dan Moore:

Anyway, they have been working on this spec for years and years and they have covered so many interesting bases, so many interesting security scenarios. And again, I'm not just pitching FusionAuth, any Auth server that implements the OAuth standard will let you take the benefit of all of those years of frankly, expensive employees that I don't think any one company could put together. The amount of detail and thought that they put into those specification servers is really impressive to me.

PJ Hagerty:

No doubt, no doubt. I'm going to skip around a little bit. What brought you to the world of auth like what, what was your dev journey like? Where did you get started and how did you end up where you are now?

Dan Moore:

Yeah, so I started out and I've actually written a couple auth systems and I've used some open source auth systems. Devise is the big one, obviously in my Rails apps. And I always kind of treated it as something to be kind of gotten through as quickly as possible. I was not the person reading the Devise docs and understanding it, I was the person going through the tutorials and just trying to get it done because I knew it was important. I knew it was kind of scary. I knew it was really kind of getting in the way of me delivering features that customers wanted. And I was kind of on a pause from a job or kind of in between jobs.

Dan Moore:

And I ended up writing some content for FusionAuth and really enjoyed the content and they enjoyed the product I gave, or the product I wrote, and we ended up having discussions and they needed a DevRel; a community person to kind of be out there. And that's how I ended up at FusionAuth. So it wasn't a long-term plan, I definitely... There's a great podcast out there. Am I allowed to pitch other podcasts on your podcast?

PJ Hagerty:

Yeah, sure. Why not?

Dan Moore:

It's called Identity Unlocked, and Vittorio Bertocci, who is just a giant in the authentication world, in the Auth world. He interviews people who work on standards and people who are into different aspects of auth, from Web3 stuff to OIDC and some of these people have very kind of long trailing journeys into auth, started out in the nineties or what not. I just knew that I didn't want to deal with it and then I discovered that it was actually kind of an interesting, rich, richer space than I thought it would be.

PJ Hagerty:

Right on. So let me ask a little bit. If you're looking at auth, is it kind of a situation where you feel like it's an established part where like it's a different part of the community? Or it's like, still part of the general developer community just focusing on a specific problem?

Dan Moore:

Sure. I think that there are definitely devs and admins, I would say, who are kind of really focused on identity and auth authentication and authorization, but for the vast majority of people, or vast majority of devs, I think it's a cross-cutting concern, the same as like logging or security. Right?

Dan Moore:

I don't think you're going to go to very many logging meetups. Right? I'm sure that there are some out there. But the same thing that I found for identity meetups, when I've given a lot of talks at meetups, they're always very interested to hear about JSON web tokens or other auth topics, but they're definitely approaching it from the perspective of, "Hey, this is one of many different things that I need to have some understanding of as a dev".

PJ Hagerty:

Right. That makes sense. That makes sense. You did mention something in your earlier answer, you mentioned Web3. How much, because I know that some people are going to... like there's generally people have a reaction. I won't say whether it's a positive or negative reaction when they hear things like Web3 and blockchain and authorization and authentication.

PJ Hagerty:

How are you seeing that kind of... And I'm not asking you to tell the future, just give us your opinion. How do you see that as coming into play as we see more and more systems saying like, "Hey, it'd be cool if we had like a DAO that's going to handle authentication or handle authorization, or if we could tokenize things like, binary factor", I think is the name of the company that's trying to tokenize authorization so that you can easily just pass a token from place to place. Do you see that as being a big player, or are we still like super nascent and we don't know what that's going to look like?

Dan Moore:

You know, I think that we're pretty nascent. I think that there's definitely some interesting things happening around like the wallet space, but I think honestly that WebAuthn is going to be a bigger effect than Web3, at least for the next 5 or 10 years. And the reason for that is that no one's at least... and I am definitely not in the blockchain space as much as some other friends are, but I have not seen anything that takes it from the geek area. Right? It is very niche right now. You know, it has applications, but I don't see anybody like carrying their wallet. And I mean the Bitcoin ATMs I've seen are very few and far between, I guess.

PJ Hagerty:

Right. So I think that we can kind of extrapolate from that, that the widespread use of blockchain as an auth tool, it's just not there yet.

Dan Moore:

I don't see that being there. And honestly, I'm not sure. I think there'll always be a need for an internal auth situation just because I don't think companies want to share necessarily all their data out in public on the blockchain.

PJ Hagerty:

Right.

Dan Moore:

So even if everybody had a wallet magically, right? Installed with every iPhone. You'd still want to like, take that identity and like tie it to your internal company systems and you'd want to have some way of managing that.

PJ Hagerty:

Interesting. Interesting. I feel like we could really go into like a full on dystopian future about how like, oh, everyone got a free wallet. Cool. It comes on every phone. Oh, who controls it? Well, AppleGoogle does because AppleGoogle runs the government now. We're not going to go down that route.

Dan Moore:

Yeah. Let's keep it happy.

PJ Hagerty:

Totally different podcast. Totally different podcast. So let me... You mentioned some of the tools, but how can people who are really into open source and prefer open source tools, what can they look at when it comes to auth? What are the big hitters?

What are the maybe more secure examples? We don't want to look at things that are like, "Hey, I created this thing and hopefully it works", but like things that are stable, have a good foundation.

Dan Moore:

Yeah, absolutely. So I will say just because I know this is important to your audience, FusionAuth is not open source. We have a free edition that you can use within certain limitations, but we're definitely not open source. The open source options, I kind of break off solutions into two categories.

Dan Moore:

They're libraries, right? Like the afore mentioned Devise that some are more independent, some are more tightly coupled to the applications they're part of. DjangoAuth I would consider to be kind of more tightly coupled. And then there are standalone auth servers.

Dan Moore:

And both of these are great solutions and they're both great open source options for both of them. So it tends to be kind of a winner-take-all market. So I would probably... if I was coding Elixer or Java or whatever, I would probably just Google for "auth solution for Elixer, Java, whatever". As far as auth servers, the big ones I'm aware of that are free as in speech, are Keycloak, which is quite full feature, and you can self host. It actually is the upstream project of Red Hat SSO. So if you actually want to pay someone to run it for you or for support, you can do that with Keycloak. IdentityServer, which is a .NET based one, I've kicked around that a little bit. And then GLUU is another one that I've heard mixed reviews about, but it's been a couple years since I've looked at it seriously and it would probably be worth a review. And that's G-L-U-U.

PJ Hagerty:

Okay. It's not G-L-U-E, G-L-U-U.

Dan Moore:

G-L-U-U. Yep. And those are all as far as I know... I'm not sure the licenses, but I'm pretty sure they're all accepted open source licenses.

PJ Hagerty:

Cool. Very cool. You know, it's interesting because you kind of mentioned if someone's going to use like a specific language they probably have a preferred auth methodology.

PJ Hagerty:

Do you see in your work...I mean, I feel like back in the days there were certain gems you could use with Ruby and Rails specifically for authentication, maybe not authorization, but definitely authentication. Do you think that's something that we might see a comeback for? Or do you think that it's going to more kind of coalesce around having things like FusionAuth available so that we don't have to worry about reinventing the wheel every time a new language comes out or becomes popular?

Dan Moore:

Yeah, it's a great question. I mean, I would say that they're different perspectives, right? When you are early in building your application or you're just trying to get things going, then you really want the simplicity of popping in a library, getting that it's operationally simple to understand, it probably fits nicely with your application.

Dan Moore:

And so I think libraries are always going to be around, but the unfortunate truth is once you get to have a certain size and it doesn't have to be that big of a company, you end up or that big of an organization, you end up with multiple apps. And that could be your office suite, it could be forum software, it could be support software. And we see there, especially when you're looking at kind of having consolidated view of your customers, more and more people want that standalone system that they just hook all their applications into. And maybe it's not quite as seamless or it's not, it's definitely not as easy operationally because now you have this whole other architectural component you have to maintain and care and feed.

PJ Hagerty:

Exactly.

Dan Moore:

You do get this isolation and you get some security benefits. You get some feature benefits because I'll tell you what, let's take Keycloak as an example. If you set up Keycloak, it would be a pain to set up, but once you've set it up once and you have done all of the steps to do it, adding new applications is going to be pretty darn easy as opposed to setting up Devise each time for each Rails application, say nothing to the Data Silo issue.

PJ Hagerty:

Right? So, I mean, in some ways it's kind of like the Elastic Stack. It's like you have an option for free logging and monitoring that's out there and you can use it and you can grab it. But there is that setup cost that you're going to have to be concerned about. So there are services out there that take care of that, but we're not going to get into Logz.io and things like that. But there's always opportunities out there. So I mean, you could kind of, you can choose how much you want to put into that versus how much you just want to say, all right, let me just take this off the shelf and plug it in.

Dan Moore:

Yep, and I think it's a spectrum too, right? I think there's nothing at all wrong with starting out everything entirely integrated and then starting to carve things out as you succeed or grow. I've seen that pattern a lot. One thing, one common thing we see, which I'd like to warn new users against is people rolling their own auth authentication or authorization. Right? They'll like have their own database structure and their own kind of weird role system and they come to us, and I'm sure they're talking to other solutions as well, looking at other solutions. And they're like, "Wow, we really have this mess that we don't want to continue to support that we don't want to have a dev we have to continue to hire, and no dev wants to work on it because it's like not a standardized system.

PJ Hagerty:

Right.

Dan Moore:

So that's one thing I would definitely evaluate libraries or auth servers right now if I was doing greenfield development rather than create my own.

PJ Hagerty:

Right. Don't let it be a second thought, right?

Dan Moore:

Yeah. Yeah. You're going to regret that.

PJ Hagerty:

Yeah, actually it's funny, 'cause as you were saying that I was thinking back to some of the projects that I worked on earlier in my career and how we set up like auth in-roles and things like that and I'm cringing, like you can't see 'cause this is a podcast, but I'm cringing Dan, I'm really cringing. At some of the things I did. We all had those moments as developers that went horribly wrong or shouldn't have been done that we had to do for deadlines or what have you.

Dan Moore:

That's how you learn. That's how you learn.

PJ Hagerty:

Exactly, exactly. I mean like in some ways, I'm happy that I got to work in open source when it was still a little bit "Wild Westy", and you could kind of like, especially with languages like Ruby or Python, where you could kind of definitely bend

the rules, maybe not break them, but you could definitely bend them to your will and make things happen that maybe shouldn't have. There's a beauty to that. And I feel like some languages, especially JavaScript, like you really can't do that. You have to follow the rules. So, pluses and minuses, we learn along the way.

PJ Hagerty:

What are some of the things that maybe over the next couple years in auth or in general standards, what are you looking forward to? What are you hoping to see pop up other than the blockchain taking over everything?

Dan Moore:

The Panopticon. So I mentioned WebAuthn briefly earlier. I think that's something that's really, it's been standardized. If your listeners don't know what WebAuthn is, basically, it's a way to securely authenticate that on websites, on web applications, based on touch ID or face ID or hardware tokens like UV key. I think that is going to be a big deal in the next couple of years, because it solves a lot of problems around registration, around knowing who people are. And it's just, it's got the form factor, it's on your phone.

Dan Moore:

I think that OAuth 2.1 is coming out soon. It's been coming out soon for about a year now, but if they're getting close then that's going to be basically a coalescing of all of the things that have been learned over the last 10 years around OAuth. And I'm excited for that.

Dan Moore:

And the last one is, it's a project called GNAP, which is a re-imagining of OAuth. So it is basically taking the lesson OAuth 2.1 as indicated by the name is really going to be an incremental release. They're not breaking anything, they've purposefully said, "Hey, we'd really like to fix this, but that will break things, so we will not". GNAP is like, "Hey, let's throw it all out and let's take a look at first principles and they got, some of the experts behind OAuth are kind of pushing on that. I'm excited to see where that goes.

PJ Hagerty:

Very cool. Very cool. Is there anything else you would like folks to know before we close up the episode?

Dan Moore:

Yeah, I would say don't roll your own auth. There are lots of options out there. Find one that works for you.

PJ Hagerty:

Awesome. Awesome. And there's lots of open source projects that if you, if you're interested in getting involved, get involved in the project, don't try to build your own, get involved in the projects that already exist. They could probably use your help.

Dan Moore:

Absolutely.

PJ Hagerty:

Awesome. Well, Dan, thank you so much for taking the time to join us for this episode of What Matters. I'm hoping that we can bring you on...and hopefully in the Web3 future, we can bring you on to talk about how everything you said was right or wrong, whichever way it works, but hopefully you'd be willing to come back and chat with us more about authentication authorization and all things that go into it.

Dan Moore:

Absolutely. PJ, thank you so much for having me.

PJ Hagerty:

Absolutely. For those listening, we look forward to bringing you many future episodes of this podcast. Keep listening and feel free to get in touch at "community@mattermost.com" with your questions, comments, or episode and guest ideas.

PJ Hagerty:

You can also find me, PJ.Hagerty at "Community.mattermost.com" anytime you want to talk. Let us know what you think matters most.

Voiceover

You've been listening to the What Matters podcast hosted by PJ Hagerty @aspleenic on Twitter.
Music is "Upbeat Party" by Scott Holmes.
For more information, contact community@mattermost.com. Let us know what matters to you and we'll talk next time on the What Matters podcast.