EPISODE 608

[INTRODUCTION]

[0:00:00.3] JM: If you've ever stayed in a short-term rental like an Airbnb or a HomeAway or Couchsurfing, you've probably used the Wi-Fi network at that rental property, and why wouldn't you? It's no different than hopping on an open Wi-Fi network at an airport, or a Starbucks, or your friend's house, right? One major difference, the hardware is easily accessible to previous guests at the short-term rental. Previous guests could tamper with the software on a router and use that tampering to do some malicious surveillant things.

Jeremy Galloway is a security engineer at Atlassian. In today's show, he explains the risk of using Wi-Fi at a short-term rental like an Airbnb, and he includes an explanation of how easy it is to take over a Wi-Fi network as a guest at a rental property. A broader point that we discuss, large attack surfaces are difficult to secure, whether we're talking about Airbnb or another sharing economy app like Uber, or a large corporate network like Atlassian, or even your own personal life. We have lots of big attack surfaces in our life and Jeremy offers some best practices and philosophies for how to respond to the modern world of security.

As always if you have feedback or suggestions on the show or ideas for show topics, send me an e-mail jeff@softwareengineeringdaily.com. I would love to hear from you.

[SPONSOR MESSAGE]

[0:01:36.5] JM: Every team has its own software and every team has specific questions about that internal software. Stack Overflow for Teams is a private secure home for your teams' questions and answers. No more digging through stale wiki's and lost e-mails. Give your team back the time it needs to build better products.

Your engineering team already knows and loves Stack Overflow. They don't need another tool that they won't use. Get everything that 50 million people already love about Stack Overflow in a private secure environment with Stack Overflow for Teams. Try it today with your first 14 days free. Go to s.tk/daily.

Stack Overflow for Teams gives your team the answers they need to be productive, with the same interface that Stack Overflow users are familiar with. Go to s.tk/daily to try it today with your first 14 days free. Thank You Stack Overflow for Teams.

[INTERVIEW]

[0:02:49.7] JM: Jeremy Galloway is a security engineer at Atlassian. Jeremy, welcome to Software Engineering Daily.

[0:02:54.8] JG: Hey, thanks for having me.

[0:02:56.2] JM: You gave this talk at a security conference that I saw, and it caught my eye as I was reading through some of these different talks, and I ended up watching the video of the talk, and it was a little bit alarming, very informative, and it's about how unprotected Wi-Fi can be, a bit like unprotected sexual activity. That was one part of it, but more broadly it's about how to safely stay at short-term rental properties. When I stay at a short-term rental property like an Airbnb, I use the Wi-Fi. What are the risks of using the Wi-Fi at a short-term rental property?

[0:03:41.7] JG: Sure. The risks really vary. When I did the talk I did, make an analogy between using open Wi-Fi and sexual partners, and it seems like a novel, or maybe just alert and silly analogy, but it's really apt, because if you just go, and if you're using rather unknown wireless network, you really don't know anything about the intentions of the network operators, you don't know if they've paid attention to security at all.

Although you might be safe 99% of the time, unless you practice good hygiene and practice good data security, you're not really protecting yourself as much as you could. The risks include things like someone tampering with your traffic, even just your traffic being snooped on, or even things like malicious payloads being delivered back to your machine if the network has been compromised.

[0:04:39.6] JM: Why would a Airbnb host, or a short-term rental host, or a hacker who happens to stay at the short-term rental property and tamper with my Wi-Fi, why would these people want to tamper with the Wi-Fi? What's the incentive?

[0:04:55.4] JG: The number one reason for I would say probably hacking Airbnb is and most hacking in general is for the lulz. When I got the idea to do this talk, it was when I was staying at a vacation rental with some friends, we were in a snowboarding trip, maybe 10 of us in this house, and they're all snowboarding and I thought, “Hey, I've got the place to myself for about an hour. I know what I'll do, I'll go hack the network, mess with a bunch of network settings and just prank my friends.”

Now what I was expecting was I was expecting maybe 20, 30 minutes of messing around, poking around with things, installing tools, and then just another five minutes or so of making some scripts to do silly things like flip their images upside down, what I didn't expect was that I would be able to compromise the network in less than five minutes. The way in which the network was compromised is if you have physical access to the router, well you essentially own the router at that point.

What I came to realize is that wow, if I had traveled back in time a decade and I was 14, or 15 years old, I could have accomplished this very, very same thing. If you spend much time on the internet, 14 and 15-year-olds are just about as into hacking and pranking as anyone else. It really made me realize, you know, hey, if a 13-year-old or 14-year-old kid can compromise your network and completely take it over in a matter of minutes, I mean, that's a real problem. It's a real problem when our lives are this focused online.

[0:06:27.5] JM: It took you how long to tamper with the Wi-Fi? Like five minutes?

[0:06:32.3] JG: Probably less than five minutes, and I would say about two and a half of those minutes were looking for a paperclip, so that I could reset the hardware security.

[0:06:42.7] JM: Yes. Explain the paperclip threat.

[0:06:44.7] JG: Yeah, it's an extraordinarily dangerous tool in security. If you have physical access to a device via network hardware, essentially all you need to do is find a paperclip or a small thin pointy object, and as soon as you have that, and the crucial thing is that you have physical access to the device in this case a router. Imagine like a D-link or a Linksys router. Essentially, you just use the paperclip to reset the router settings back to default. Then what that lets you do is all of a sudden, hey, I can login with admin-admin, or I can login with admin and the hard-coded password that's printed on the back of the router. Really the idea goes back to a pretty fundamental security idea, and that's that if you have physical control of the device, it's basically compromised.

[0:07:35.3] JM: You're a security engineer. You're a security expert. We're doing this interview over audio, but I'm sure if we had video on you would be wearing a hoodie that would be shadowing your face. You would have probably some green numbers and a black background flowing behind you, like all the stock images of security hackers going behind you. Is this something that you need security expertise to be able to do in two and a half minutes? Are you uniquely qualified to hack the Wi-Fi? Or is this something that some naive person staying at a short-term rental that wants the lulz, or wants to more dangerously scrape privacy and fringing, or banking information and fringing traffic. How easy is it to do this?

[0:08:26.1] JG: It's unfortunately incredibly easy. I would say if you don't know anything at all, if you're just barely, you know if you've used Linux maybe once or twice, you could probably get to a point of being able to effectively compromise it, in say an hour, maybe an hour and a half if you're watching the right YouTube videos. Really I mean, how often do you hear stories of teenagers setting up the wireless network for their parents? I mean, this is something that it's a pretty trivial task to set up a new router. I mean, it's meant to be easy. Essentially, all you're really doing is taking over the administrative interface of the router, and then once you have access to the admin settings, it's a matter of just changing things like the DNS server.

It's really scarily easy. That's what I was trying to impress upon the audience when I was giving the presentation is just in fact how easy this is. It's not necessarily some malicious nation-state that's after you, it's probably more likely that there's a bored teenager in your neighborhood that has little else to do but, "Hey, I got a new wireless card. Let me see what wireless networks I can mess with."

[0:09:36.7] JM: Let's go through the steps of this process, either to give a tutorial for somebody who wants to do this thing, actually that's not why we're doing it. We're just doing it, because that information is already out there. If somebody wants to find it, they can find it. We're not telling anybody anything that they don't already know. Of course, Software Engineering Daily listeners are pure individuals and would never do such a thing anyway. Let's start with the router software. Router software; what is a router emulator? How can a router emulator be used in an attack like this?

[0:10:09.9] JG: Basically what a router emulator is, it's not even as fun or as fancy as what it sounds like. There's router emulators posted online from the various vendors like D-link and Linksys. Essentially what it is, it's a contained web app that gives you a page-for-page simulation of the settings that you would find in a particular router. If I own a D-link DIR600 and I'm having trouble configuring it, I can use the router emulator to understand, “Okay, I need to go to this admin page, I need to collect utilities, I need to click DNS, or whatever the setting may be.” Essentially, the router emulator software lets you understand what the admin interface looks like without actually logging in. It's really useful for troubleshooting.

[0:10:59.1] JM: How does that fit into your process of hacking the Wi-Fi? Or maybe you could just tell me what are the steps that you take to hack the Wi-Fi?

[0:11:09.2] JG: Sure. The steps are, I would say step 0, find that paperclip just in case. If you're a guest at a short-term rental, the first thing to do really is find the network hardware. 99% of the time, the network hardware is accessible to you. It's probably underneath the television, or something like that. It's rarely, if ever, in a locked room. The first thing to do is get your hands on it. Pick it up. Can you see an admin password and username printed on the back of it? Are you able to physically put your hands on it? That's really step zero and step one. It's get a paperclip, get your hands on it.

Then the next thing is to authenticate to the network. If you're using wireless, join the network and attempt to browse to the admin interface. Usually a private IP address 192.168.0.1, whatever the address may be, and then you're going to try to log in as the administrator. Unfortunately, admin-admin in 2018 still works really well. Sometimes, you have to look on the

back of the router and type in a hard-coded password that's printed on it, but it might also be the case that the owner has actually set up a password that's not immediately guessable. In which case, that's where the paperclip comes in.

[0:12:25.8] JM: It seems like default credentials are the bane of security these days, whether it's hacking short-term rental properties, or the Mirai botnet.

[0:12:38.7] JG: Yeah. It's a bit depressing that it's still a problem, considering I was reading about the stuff happening in the 80s when I was a teenager and I thought, “Surely, surely we would have this solved a bit better at this point.” It really is the whole point of default passwords is to make administration easy. If I can make – if I'm a router manufacturer, I want my customers to have the easiest experience possible. I mean, I've been frustrated setting up these devices, so I do understand the reasoning why, but from a security/hacker perspective, I mean, it's taking candy from a baby.

It could not be easier. There's enough automation around these things, where even if you don't use admin-admin, if you're using one of the top 1,000 or 10,000 most common passwords, it can be brute forced almost as quickly as it being admin-admin, taking just a matter of seconds.

[0:13:34.8] JM: If we're thinking like a black hat, what is the most malicious thing we can do if we have control over this router?

[0:13:43.1] JG: This really depends on how evil you want to be, and how much time you have. Probably the deepest level of maliciousness that you could do if you had physical access to a router would likely be to upload some altered firmware to the device. Routers aren't commonly updated, but you will occasionally see firmware updates for your devices. If you’re an experienced attacker, or if you were highly motivated, it would be rather trivial to take a firmware download from say Linksys, reverse-engineer it a little bit and add some custom backdoors in there, things that would allow you to record the traffic, send the traffic off to a third party server, do things like man-in-the-middle the traffic.

When you go to visit facebook.com, you're visiting facebook.com, but it’s through a server that I control so I’m mediating the interaction the whole time. Then of course, if I can control what

websites you go to, then I could also do something like serve up and executable to you. “Hey, I see you're using Windows, you're trying to log into Facebook.” I send you a pop-up that says, “Hey, please install this to continue.”

Now to you or I, that sounds silly and suspicious, but it's surprising how often something like that works. If you're able to subvert a router on that low of a level, it's extremely, extremely hard to detect. There is no antivirus for routers.

[SPONSOR MESSAGE]

[0:15:25.2] JM: At Software Engineering Daily, we have user data coming in from so many sources; mobile apps, podcast players, our website, and it's all to provide you our listener with the best possible experience. To do that, we need to answer key questions, like what content our listeners enjoy, what causes listeners to log out, or unsubscribe, or to share a podcast episode with their friends if they liked it? To answer these questions, we want to be able to use a variety of analytics tools, such as Mixpanel, Google Analytics and Optimizely.

If you have ever built a software product that has gone for any length of time, eventually you have to start answering questions around analytics and you start to realize there are a lot of analytics tools.

Segment allows us to gather customer data from anywhere and send that data to any analytics tool. It's the ultimate in analytics middleware. Segment is the customer data infrastructure that has saved us from writing duplicate code across all of the different platforms that we want to analyze.

Software Engineering Daily listeners can try Segment free for 90 days by entering SE Daily into the how-did-you-hear- about-us box at sign-up. If you don't have much customer data to analyze, Segment also has a free developer edition. But if you're looking to fully track and utilize all the customer data across your properties to make important customer-first decisions, definitely take advantage of this 90-day free trial exclusively for Software Engineering Daily listeners.

If you're using cloud apps such as MailChimp, Marketo, Intercom, Nexus, Zendesk, you can integrate with all of these different tools and centralize your customer data in one place with Segment. To get that free 90-day trial, sign up for Segment at segment.com and enter SE Daily in the how-did-you-hear-about- us box during signup.

Thanks again to Segment for sponsoring Software Engineering Daily and for producing a product that we needed.

[INTERVIEW CONTINUED]

[0:17:55.3] JM: If I am staying at a short-term rental and I'm aware of this compromised router threat, is there anything I can do? Are there any countermeasures?

[0:18:08.3] JG: Yeah. With short-term rentals and security in general, there's a right amount to be afraid and there's a right amount to be scared. Being paranoid about every little thing is really not helpful, and it ultimately doesn't make you more secure. The first thing is really to try to have a somewhat balanced objective idea about the actual risk of this. If you go to stay at any particular Airbnb, I wouldn't think that there's a particularly high chance of that particular router being compromised. In security, we need to just do the best practices, so I would say if you're using personal device, if you're just using your personal phone or laptop, you can do something as simple as just using VPN software.

It's pretty much the most foolproof way to not let your network traffic be in the hands of the local network operator, in this case that would be the local router. If you use some VPN software and you have a paid VPN subscription, or maybe it's just a VPN back your home house, or to an Amazon server you have set up, all of your traffic from that device will be encrypted and sent to the VPN. In theory, that really should protect you from almost every single type of attack that could occur as long as that VPN connection is properly set up.

[0:19:33.3] JM: Is there a way to know if a router has been compromised, if I'm staying at a short-term rental?

[0:19:40.0] JG: A similar question is hey, I'm about to download this program. How can I know if this program is secure? It's really hard to tell. A lot of things come down to intention. Now, I wouldn't suggest listeners actually “hack” the routers at short-term rentals, but I don't think it's inappropriate to one, if you're authenticated to the network, just attempt can you browse the admin interface? Is it using default credentials? If it is, well that should probably make you a little bit more nervous. There's really no way that you can truly say, “Hey, I know a 100% my traffic is not being inspected and I know it's not being manipulated.”

[0:20:24.3] JM: Let's say we're Airbnb, or any other short-term rental company. I'm using Airbnb by the way, because Airbnb is the best and the most successful as far as the ones I've used, so I'm simultaneously praising them and making them a victim of our conversation. I love Airbnb and I will still use it and I will probably still use Wi-Fi at the people's houses I stay at. If you were in charge of security at a short-term rental company, what steps would you take to prevent against this thing?

[0:20:52.2] JG: That is a really interesting question, because I'm not entirely convinced it's Airbnb’s responsibility. They have a lot on their plate dealing from insurance, to physical safety, to locks on doors, things that are protecting actual physical assets. I have spent some time thinking about this, and at this point, I really am more convinced that it's the responsibility of the property owner, it's their network, the network is in their name. Airbnb does do some pretty useful things for hosts and guests, like they have a Wi-Fi password sharing feature, which that might not help you if the router is compromised, but they are doing things like trying to enable, or trying to use their app to enable a secure password sharing.

As far as what they're responsible for, I really don't think it goes very far. I would say most of the onus falls on the actual property owner to secure their network, which when you think about that, that's a little scary, because you just went from being a realtor to being a network administrator in one fell swoop.

[0:22:02.5] JM: Okay. Let's say we are a short-term rental owner. As you just said, it's my responsibility. What can we do to mitigate against this?

[0:22:14.0] JG: What you want to do is just practice what I would consider good network hygiene. Step one, change that default password, use something long, don't use your address, don't use something that could be guessed in a few tries. Use a long complex password. The next thing is to actually keep your router up-to-date. Now we can fault the router manufacturers for not releasing quick iterative software updates, but most router software is updated infrequently. Even with it updated infrequently, you should at least check a couple times a year to see if there's an update for your router, something that patches vulnerabilities. Change the password, keep the software up-to-date.

You can also do things like use third-party DNS providers in your router settings. Most routers have really simple configuration to add DNS servers. You can use DNS services provided by CloudFlare. You just type in the IP address 1.1.1.1. Google of course offers DNS services as well. Essentially what that will do is it adds a small layer of protection for anyone else using that network. Now there's also protecting the physical network device itself. If you have the device sitting out where anyone can touch it, there's the huge risk of it being able to be reset.

It's uncommon to stay at a short-term rental or an Airbnb and for there to be locked rooms, or locked doors, usually just a few closets. It of course depends on the layout of the house, but I've been at Airbnbs where they've had the router locked up, and I had to say it really annoyed the hacker part of my brain. I was like, "What? Why won't they give me access to this device?" Even something as simple as putting it in a locked room, or there are some rather inexpensive hardware cages that you can put the router in that won't affect the signal, but that will prevent physical access to the device.

[0:24:12.9] JM: Maybe you could also put glue inside of that paperclip hole.

[0:24:18.9] JG: Yeah, that will definitely keep anyone from resetting it, until they pop the case off and connect up a different way.

[0:24:25.9] JM: Oh, no. Then we have a false sense of security to go with everything else.

[0:24:30.3] JG: Yeah. There are some other options too. Depending on the router hardware that you have, a lot of the slightly higher end routers these days have options for guest networks.

While the security on those is far from perfect, they're actually more robust than you might think. A lot of people have Airbnbs and short term rentals and back houses and casitas behind their house, and it's an option to have a primary router in your residence and maybe a Wi-Fi extender in the rental, and you only give guest network access to the guest network. Most of these guest networks prevent access to the administrative interface. It only gives the users of the guest network plain internet access, which is essentially what you'd want.

[0:25:22.0] JM: There are a number of sharing economy companies. I think short-term rentals are just one of them. The sharing economy platforms have a wide surface area. If we think of them from the point of view of protecting against attacks, whether or not it's within the purview of the sharing economy company owner, like you said it's maybe not an Airbnb's purview to protect against this. Obviously, it's in their interest to protect against this. They would certainly have no motive to not protect against it. Thinking about sharing economy platforms more broadly, are there security vulnerabilities in other sharing economy platforms like Uber, or maybe the TaskRabbit flavor of businesses where you have people come over and help you with stuff. Do you have any principles for protecting against these kinds of attack vectors?

[0:26:21.2] JG: This is a completely disregarding their actual mobile app security, and speaking more to the actual, "Hey, I'm going to take an Uber." What are the risks of taking an Uber or rideshare compared to taking a traditional taxi? Really the thing is we are getting away from a "professional" into just regular people working the gig economy.

What's the difference between the risks of riding in a taxi? Like yeah, you could potentially still get into a car accident, but the people that drive taxis professionally, it's their career, versus someone that's maybe just making a little bit of extra money on the side. You have more regular people carrying out these sorts of jobs. Now that being said, even working in security and being in the hack space for so long, I'm really trusting of people.

There's a site called couchsurfing.com, which the nature of the site is you can just let people stay on your couch for free. It's geared towards world travelers and people that travel a lot. I used to host my couch on the site and I've had all kinds of people stay with me. I remember five, six, seven years ago, I would tell people about Couchsurfing and they would look at me like I'm

crazy. They're like, “What? You just let a stranger from the internet that you don't know come and stay at your house?”

At the time, it seemed far-fetched and people thought, “Wow, you must be really trusting.” Now you fast forward to 2017 and 2018, and they've – Airbnb has essentially made a business model out of it. Very quickly, there's a pace of people who are using various services in the sharing economy, like ride sharing, or Airbnb, or Favor. We're forcing each other to trust each other a lot more. When I stay at an Airbnb, I'm pretty much just as confident staying there as I would be staying at a hotel, even though it's not someone that's necessarily worked in the hospitality industry for decades. There is a broader set of trust. We're all trusting each other a lot more these days.

[0:28:33.8] JM: What about more specific things? Like I hop into an Uber, or even a taxi I think, and if I have a Android phone and I need to charge my Android phone, how big of a risk is it to plug in that nice inviting cable that can refresh my nearly dead phone?

[0:28:56.9] JG: There's been a lot of really fun and interesting research on, “Hey, what happens if I plug my phone, or my device into this USB port?” Potentially, the USB port could be tampered with, and at least with an iPhone, when you plug it in, if the port is attempting to access data, your phone will prompt you and say, “Hey, do you trust this device?” The reality of the situation is that's really interesting research, but it's not something that you really practically see in the wild. As far as things that you want to spend your time worrying about, I wouldn't worry about it.

Even at airports, places where there's a lot of – there's high amounts of traffic, I mean, sure you should think twice before you plug your phone into something, especially if it's asking for a data connection. The reality of the risk is there's a lot more legitimate things to be worried about than having a USB port that could potentially be hacked. It's really, really interesting research, but it's honestly not something that's really seen in the wild very often.

[0:30:08.6] JM: The broader flavor of attack surfaces that we're talking about is attack services that are very wide. You could sit in a room and probably enumerate lots and lots of attacks on a whiteboard that could take place across sharing economy apps. When I'm thinking about wide

attack surfaces, big companies also come to mind. You work at Atlassian. Atlassian is a large company with lots of products. How does a company like Atlassian secure a wide attack surface?

[0:30:39.9] JG: Well, the first thing is we have a pretty incredible security team. Security is something that's taken extremely seriously here. Really the first thing to secure an organization as big as Atlassian is that you have to make it a priority. Even with our security team, we go far beyond that, because no matter how many people you have on your security team, you're going to have less than the amount of people that are attacking you, just by being exposed to the internet.

One of the things that I'm really proud of is that Atlassian is been using a bug bounty program through a company called Bugcrowd. We actually won a best bug bounty program of the year this past year. All right, let me ask are you familiar with bug bounty programs?

[0:31:29.7] JM: Oh, yeah. Of course.

[0:31:30.6] JG: Yeah. Really, that's a way to get the wider security research community to look at our products and to look at what we have out on the internet. Our security team does everything that we can, but we also rely on security researchers reporting things to us. That honestly I think is the best way to get a wide set of coverage hardly anything is a better incentive than offering people a few thousand dollars for finding a bug.

[0:31:58.8] JM: Indeed. At Atlassian, you are in charge of various security practices. You're in charge of responding to incidents. Describe your approach to incident response. When something goes wrong, what's your security methodology?

[0:32:14.8] JG: One of the most important things to incident response is having a plan. You got to know what you're going to do when X, Y, or Z happens. The first thing is to know what your basic procedure is going to be in the event that, let's say hey, we have web server that's running on AWS and we discovered that it's compromised. What we have is basically sets of documentation on hey, this is the alert that we received. We noticed this type of traffic coming out of it, and here's what we're going to do to mitigate it.

In the case of a compromised web server on AWS, the first thing you might likely want to do is get a copy of the disc. Just even something as simple as cloning the compute resource inside EC2 and making sure that you have forensic artifacts.

[0:33:16.6] JM: Okay, we've talked about a few wide attack surfaces, short-term rentals, sharing economy platforms, Atlassian. Another wide attack surface is my life, my personal identity, my personal security. I know you have some strong beliefs about this. What are common mistakes that people make in their personal online security?

[0:33:41.2] JG: If there's one thing that listeners take away from this conversation, please do not reuse passwords. We as a security industry have tried to reiterate this time and time again, but we've really come to a point where password reuse is become very, very dangerous. The most important thing is use a password manager. It does add some complexity to things. I admit it's a lot easier to just log in with the same password to every single site, but the amount of credential reuse that we see basically helps drive a lot of cybercrime, because essentially what happens is hey, company X gets hacked and a million usernames and passwords are dumped to the internet. Every enterprising cyber-criminal grabs that username and password lists, they try it against Netflix, they try it against Atlassian, they try it against Tumblr, and they try these credential lists everywhere they can.

There are credential lists that are literally in the billions, billions of username and password pairs. People will simply try these against every single site possible. If you use a password on one site and that site happens to get compromised, there's a high probability that any other site using that password could also be compromised. Really just the most important thing is use a password manager, try to use unique passwords for any accounts that you care about.

Also, extremely importantly, it’s 2018, passwords are good, but if you care about security and the security of your accounts, you really want to enable two-factor authentication. What I, what I tell my loved ones is you don't have to enable two-factor authentication for every single account that you have. You should only enable it for the ones that you really care about, and that might be things like your e-mail and your banking.

Adding two-factor authentication is probably one of the best things you can do to protect yourself, even in the event that you were reusing a password, if the password is compromised and someone tries to login the two-factor is going to save you from having your account totally compromised.

[SPONSOR MESSAGE]

[0:36:06.4] JM: The octopus, a sea creature known for its intelligence and flexibility. Octopus Deploy, a friendly deployment automation tool for deploying applications like .NET apps, Java apps and more. Ask any developer and they'll tell you that it's never fun pushing code at 5 p.m. on a Friday and then crossing your fingers hoping for the best. We've all been there. We've all done that. That's where Octopus Deploy comes into the picture.

Octopus Deploy is a friendly deployment automation tool taking over where your build or CI server ends. Use Octopus to promote releases on prem or to the cloud. Octopus integrates with your existing build pipeline, TFS and VSTS, Bamboo, Team City and Jenkins. It integrates with AWS, Azure and on-prem environments. You can reliably and repeatedly deploy your .NET and Java apps and more. If you can package it, Octopus can deploy it.

It's quick and easy to install and you can just go to octopus.com to trial Octopus free for 45 days. That's octopus.com, O-C-T-O-P-U-S.com.

[INTERVIEW CONTINUED]

[0:37:38.2] JM: We have done a couple shows with Coinbase about security and the vulnerabilities that can be associated with SMS two-factor authentication. Is that an okay solution for some applications, the SMS as a two-factor, or should people be using apps like Google Authenticator or Authy?

[0:37:58.9] JG: SMS two-factor authentication should not be used really, unless it's the only option. It's even so bad to the point where the US cert, US security organization has published multiple times bulletins asking people to please stop using SMS for two-factor authentication,

because it's insecure. If the US government has – is the one telling you to like, “Hey, this is outdated,” that should be a signal.

Really, there's a lot of options as far as apps. You can use Google's Authy, I use Duo almost every single day. And if you have something like an Apple watch, or a lot of other of these watch devices, it makes using the two-FA really simple. I click one button on my login screen, tap something on my watch and I'm in with minimal complexity and minimal effort. That being said, I do use SMS two-FA for one application, but it's because it's all the app supports. I'll take SMS two-factor authentication over no two factor at all.

[0:39:10.8] JM: Have cryptocurrencies changed how you think about personal security?

[0:39:14.6] JG: Yeah, somewhat there's been an absolutely massive surge in hacking related to cryptocurrencies unsurprisingly. You spend five minutes and browse the headlines and you just see millions and millions and millions of dollars basically gone from simple hacking. It has reignited some motivation for people that might otherwise not really be that interested in hacking, or compromising somebody. When they realize, “Hey, I can possibly get $10,000 of cryptocurrency out of this and maybe in my country $10,000 goes a lot further.” It's a huge motivator for cyber criminals, and I have just seen an absolutely massive spike in hacking attempts related to cryptocurrency and related to cryptocurrency mining.

[0:40:04.8] JM: At enterprises, there is a widely known threat about social engineering. This is you're sitting in your office and you get an e-mail from somebody with a PDF that says open this PDF to learn about the charity event this Saturday. You open the PDF and it installs malware on your computer, and then maybe, and maybe somebody finds your e-mail address through LinkedIn, or through some other vector. Maybe you could describe I mean, since you're at Atlassian, it's a giant enterprise, maybe we could talk briefly about how a social engineering applies to enterprises, then we can talk about social engineering as it applies to individuals.

[0:40:48.8] JG: Yeah. Social engineering is extraordinarily effective. I mean, you can spend maybe hundreds of hours developing a software exploit, honing it, coding it, getting it just right and making the perfect piece of exploit code. Or you could spend five minutes and chat up

Carol at the reception desk and get the same access. There's definitely no confusion as to why social engineering is so popular, but hackers can be really mean.

Their goal is to exploit trust through any means necessary. They'll use everything from emotional cues, to threats of, “Hey, if you don't fill out this PDF by 5:00 EOB, your Medicare benefits are going to be disabled.” They're really, really most of the time going for a gut emotional response to get you to click something, or to install something. Honestly it's much more effective than spending time coding and trying to hone the perfect zero day. It's a lot easier if you can just ask someone to click something.

It's no surprise that we see it done so often. On the enterprise side of things, it takes a lot of training. For a lot of people, especially if you work in human resources, or if you work at the front desk, essentially your job is to open mail and click on links and attachments, which is basically my security nightmare. We do try to train our staff specifically about social engineering.

[0:42:27.7] JM: How does that apply to individuals? How should individuals think about the threat of social engineering?

[0:42:32.9] JG: The first thing is it is really easy to get confused between whether something is an actual legitimate phishing attempt, or if it's a spam e-mail. We do see that users often get confused, which it's not the best that they're confused, but it is good that they're skeptical. One thing is definitely instilling a sense of skepticism. If you get a piece of e-mail that you weren't expecting, or it's from somebody you don't necessarily know, that should raise the first bar of like, “Hmm, this isn't necessarily bad or an attack, but I'm questionable about this. What is this?”

Then you go through gradients of, “Okay, well I'm not expecting this, but it's just a simple message. There's no attachments, there's no links.” If someone sends you a message and there's no attachments and there's no links, well there's a very minimal threat there. When you say, get a message you're not expecting and there's a link in there, you click that link and then hey, all of a sudden you're brought to a Google login form, that's where the next level of skepticism should come up, that's where you should be thinking, “Hey, I wasn't expecting this mail and now it's also asking me for my password.” Now is the time to pause and reflect and think, “Hey, what is going on here?”

[0:43:55.4] JM: Social engineering has gotten much more complex with Facebook, and you see these articles about people getting their entire account copied somehow. Well, not somehow. I mean, you can easily scrape somebody's profile and recreate a profile that's just like them. You could use that profile for all kinds of social engineering attacks, or advertising fraud, or anything. There's even greater looming threats with this deep fakes stuff with being able to mimic somebody through video. What kinds of social engineering attacks do you think are on the horizon, and have you thought about how to protect against them?

[0:44:37.2] JG: It's interesting because as technology becomes more ubiquitous, there becomes more opportunity for social engineering attacks, but at the same time attackers, one of the reason why attackers are so successful is because they keep things simple. It's really hard to be basically just calling somebody, or e-mailing them and asking them to click on a link. Some things will always be one click away from a really bad situation, and that's scary. Things like two-factor authentication can really help mitigate things like that a lot. Really, most of it all comes down to simple awareness.

You don't have to think that you're being targeted, or that someone is out to get you. I really, really believe that that level of paranoia is not helpful. There's a right balance of the of being skeptical and being aware, especially when anyone is asking for sensitive information. If somebody is asking you for a password, that should be the time that you pause and reflect. If somebody is asking you to run code on your computer, or to download and execute something, that's the time you should really start to put the brakes on and think, “Okay, hold on, hold on. I'm not so sure about this.”

In the future, I mean, with social networks already being completely ubiquitous, there's definitely a risk of hey, if you have a thousand friends on Facebook and someone messages you and you maybe only half recognize their name, you should probably think twice before clicking the link that they post, especially if the link is something like, “Hey, did you see this really embarrassing picture of you last night?” That's one of my favorite social engineering pretexts. It's really hard for people to not click on a link like that.

Really the primary thing is just, it's you have to have awareness if you're not expecting something. Turn up the dial on your skepticism and start wondering, “Hey, is this something that I'm expecting?”

[0:46:45.9] JM: I'm a little surprised to hear your words of reassurance and against paranoia. I feel like that's not, maybe not the majority of security experts that I've talked to think in those terms. Do you think you diverge from many security experts in terms of your level of reassurance that you're providing here?

[0:47:09.4] JG: I mean, that's a possibility. As a security professional, we have a couple jobs. One of my job's is to scare the daylights out of users, by letting them know the really, really scary consequences of what can happen if they do click that link, or if they do run that attachment. It's like being a firefighter. There's huge risks if things go wrong, and you should be extremely careful, because the stakes can be very high, especially when you're talking about corporate security.

The reality of the situation is it's tiring. If you're just constantly thinking about and worried about these threats that aren't real, it becomes fatiguing. That's something we've had to learn as the security industry as is how not to fatigue users. Security can be incredibly annoying and I work with it every day and sometimes I'm annoyed by it. There's a balance of staying out of the way, security in a lot of ways is like design. The designer doesn't necessarily want you to know that what you're looking at has been manicured perfectly for you. Security it's the same way. We're trying to stay out of the way. For day-to-day use, I don't think the average person should really be very extremely nervous every time they check their e-mail. It's just no way to interact with technology.

There is a right balance of trying to understand what the real risks are. It is not easy to understand that humans are terrible at predicting risk. It's just really hard for our brains to wrap our heads around, hey, what is actually the risk of being phished? Well the risk of being phished is actually pretty high. What is actually the risk of someone targeting you personally for something? Well, that's probably a lot lower. There is a right balance of how much to think about security, so I do want people to be slightly paranoid, but it shouldn't really – security shouldn't be this onerous annoying tasks that you have to deal with. It shouldn't really be a source of worry,

but it is something like the firefighter scenario, where it's like, “Look. Hey, we don't want you to be overly concerned about this, but we do want to do fire drills. We do want you to have the right training, so that when the situation happens, you're prepared for it.”

[0:49:35.9] JM: It's 2018. Are there any strange, or disturbing new attack vectors that you've seen this year?

[0:49:42.9] JG: There hasn't been anything incredibly new on the practical side of things? Of course, there's always really interesting research coming out about what you theoretically could do, but really it's more the widespread ability for any random person to attack essentially any random company. I mean, even compared to 10 years ago, the amount of assets that are put online from businesses, I mean, it's absolutely exploded. We live in a cloud world these days, Atlassian is a cloud software company, you probably interact with cloud software day-to-day without even realizing it.

Not necessarily any particular techniques that are especially new, or novel, but it's the attack surface has just grown so much. It’s grown so much, because of the efficiencies of cloud computing. It allows anyone to – anyone that has an internet connection can scan and see what resources you have on AWS. It's really just this bigger and more prominent reliance on cloud vendors in general, that if your server is sitting in AWS and it's not sitting inside your data center, you do have less control of it, and that's definitely a risk that we see.

[0:51:10.7] JM: Security professionals that I've talked to seem to have an affinity for Chromebooks. What is the security model of Chromebooks and why is that so appealing?
[0:51:19.0] JG: Yeah, so Chromebook security is not too dissimilar from Apple security. I'm not sure if Google engineers would like me saying that. The idea is you're really limited as to the code that you can run on the machine. If I can't actually run malware.exe, that prevents a lot of attacks. If there is no Windows operating system to exploit, well that wipes out an entire class of hacking attempts. Even just being off of Windows, even still in 2018 being off of Windows and using Linux or using Mac OS, it's sad but true, but that does reduce your risk of attack quite a lot.

If you use a Chromebook, I mean, I did read that they're allowing Linux code. You could run Linux applications on Chromebooks, but you really just don't see malware designed for Chromebooks, because the target – the overall number of Chromebooks, the number of vulnerable users you could have is extraordinarily low. Chromebooks were designed with security in mind. There's minimal code that can be executed. Even if you click on the wrong thing, or you click on something that might be an attack for Windows, well that's obviously not going to affect you on a Chromebook.

[0:52:42.7] JM: Jeremy Galloway, I want to thank you for coming on Software Engineering Daily. It's been really great talking to you about this wide variety of security topics.

[0:52:48.7] JG: Yeah, thank you.

[END OF INTERVIEW]

[0:52:53.1] JM: If you are building a product for software engineers, or you are hiring software engineers, Software Engineering Daily is accepting sponsorships for 2018. Send me an e-mail jeff@softwareengineeringdaily.com if you're interested.

With 23,000 people listening Monday through Friday and the content being fairly selective for a technical listener, Software Engineering Daily is a great way to reach top engineers. I know that the listeners of Software Engineering Daily are great engineers, because I talk to them all the time. I hear from CTOs, CEOs, Directors of engineering who listen to the show regularly. I also hear about many newer, hungry software engineers who are looking to level up quickly and prove themselves.

To find out more about sponsoring the show, you can send me an e-mail or tell your marketing director to send me an e-mail jeff@softwareengineeringdaily.com. If you're a listener to the show, thank you so much for supporting it through your audienceship. That is quite enough, but if you're interested in taking your support of the show to the next level, then look at sponsoring the show through your company.

Send me an e-mail at jeff@softwareengineeringdaily.com. Thank you.

[END]

