Heather (00:04):

Welcome to the Hurricane Labs podcast. I'm Heather. And today we're going to be talking about physical security. I have Tom and Meredith here with me to help talk about some of the issues that surround physical security, as well as some of the things that we can do to help strengthen your physical security status. Let's go ahead and start by defining what we mean by physical security. Are we talking about just being able to get inside a facility by their front or back door?

Tom (00:36):

So I think physical security is wider than that. I think it encompass everything that can be involved with gaining access to something from a non-software perspective. So like whether it is entering a facility, whether it is stealing information physically, whether it's socially engineering people in order to gain physical access somewhere, I think there's a lot of dimensions to it. And we could probably talk about this for hours and hours and keep on coming up with examples of things that are relevant to physical security.

Heather (01:07):

So why do we need to continue to think about physical security beyond, you know, having the lock on the door or, you know, training people, you know, to check badges.

Meredith (01:18):

You know, there's always going to be people who want to get into your office, building your data center, your cars, your works, you know, your work vans, whatever, because there's precious things in there, whether it be data tools, expensive tech, but a lot of companies turn a blind eye once they say, okay, we've got, you know, one security guard or, you know, a case of one security guard on for 24 hours of the day, we've got locks on our doors and we have cameras pointed at our critical things. And they don't realize that they've got a ton of gaps. And as I say, every single time I speak about either physical security or social engineering, your people are always going to your weakest point. One of the easiest ways to get into a building or into a restricted area is merely by tailgating or convincing somebody that, yeah, you do work there or you should be there. You have a right to be there. So some of the easiest things that people can do are go online and look for an advertisement for a security company. See, okay, this is what they're the people on the ads are wearing. I'm going to mimic a shirt similar to this, and we'll walk in and say that I'd like to see your security system. And most people are going to be let in, especially by the security guard, because hey fellow security guy. And you see a lot of that when doing physical pen testing is basically, hey, you try to blend in the best you can, but also make it something that would be considered trusted

Tom (02:54):

Just to get over and up to speed. Let's touch on what tailgating is and some of the ways that that's so, you know, all our listeners are on the same page.

Meredith (03:03):

Yeah, sure. So tailgating is essentially following somebody closely into the building. If you are at a location that has an access card, the easiest way to do that would be if somebody taps their card in to allow them in either you walk in right behind them without tapping your card or in the case of social engineering, along with tailgatingmake sure you have your hands full and ask them to hold the door.

They're usually more than happy to. Going to get the coffee or donuts. People are more likely to help the person bringing in the food.

Tom (03:40):

Yeah, I think that's a, it's a huge social engineering thing. And if you see someone approaching, you can just sit in the parking lot for a while and get a sense of people coming in, how things work. And then time you're walking in carrying something to the point where no one will really bat an eye if you look like you belong there. And likewise kind of what you're saying about researching companies and all that. Looking like you belong, I think is probably one of the biggest ways that you can get physical access. And there's a lot of great examples for that. One that comes to mind is like being a delivery driver. If you act like you're a delivery driver, you suddenly have access to go to basically take things directly to a mail room. A lot of times you might have un-escorted access to that area. And you think about this, this used to be harder actually than it is now because what five, 10 years ago, who was making deliveries, postal service, FedEx, UPS, maybe DHL. So you had companies that drove a big truck that looked like it said ups on there. They had an official ups outfit. You know, all of that. Now you have companies like Amazon where you can't obviously tell that someone is a driver, just how they look a lot of times, especially with like the flex deliveries that they use. So now all of a sudden, some of that, even having to look official like a delivery driver, you could just carry an Amazon box, which I'm sure someone could get one of those and say, "Hey, I have this Amazon delivery." A lot of people are just so used to seeing that they're not going to even bat an eye and think that that's out of the norm. So it's actually gotten harder I think, with the way that delivery is not as controlled by certain companies these days.

Meredith (05:21):

Yeah, I would agree. And one of the easiest things to do nowadays, because all of those delivery companies that you just mentioned have also relaxed their stance on what the uniform is, which in my opinion is a big security risk, but you know, the USPS no longer requires the dress blue shirt, the navy pants and the black shoes. It's some pair of shorts for the summertime and a blue shirt. It has to have the USPS logo on it anywhere, which those can be purchased just about anywhere, including your local post office. And that's all you really need to look like a USPS driver. You know, UPS has got the brown top and bottom. You can easily buy a logo. And then Amazon has their vests apart from, for the people who are in their official trucks. And you can actually buy those on Amazon conveniently for $29 99.

Tom (06:20):

Quite frankly, there's not a good way to vet that a secure or delivery driver is who they say they are. And really, I think the only way to properly handle that is to just be vigilant and have policies and requirements where if someone's bringing packages to the building, they have to be escorted at all times and supervised. Otherwise you're pretty much opening the door to letting you know random, maybe not a delivery driver person into your environment.

Heather (06:45):

So that is about physical security. As far as like getting in the front door to like say they get into say, you know, someone infiltrates, they managed to get in through the front or back door, they're in the building. Are there other physical security means that can help prevent them from doing anything damaging?

Tom (07:04):

So one of the big things that comes to mind once someone gets into a building, they often have to do something or at least hide until they're able to do what they want to do. So a lot of times you get into a building you're not necessarily immediately going to start doing what you want to do. You might want to wait until after hours, for example. So you need a way to get somewhere else or you need at least to be able to get to an authorized or restricted area. And one of the big ways to do that, it's actually elevators from what I understand those are not the most secure systems and because of restrictions around fire code and things like that, they have a lot of security controls that can actually be kind of overwritten due to fire code. That's kind of actually interesting as well.

Meredith (07:52):

I've seen a few buildings where they've added access protection on a level of, you know, on a floor level for an elevator, but then you go take the stairs and because they assume that nobody's going to take the stairs, the door to the stairway is wide open.

Tom (08:09):

As a security person, you see these sorts of things and you just kind of observe what is going on and what you might be able to learn by seeing how some things provisioned.

Heather (08:19):

Meredith. You had a story to share about this, I think.

Meredith (08:22):

So a few years back I was working as a cybersecurity intern for a place that was not Hurricane Labs. And they let me know that they had rolled out this really awesome new feature to all of their doors that had carbon swipes on them. Everybody who was basically at this location had an ID card. You obviously had access provisioned on building by building levels or by room levels in buildings, by floor, however it may be, but each card had its own unique set of licenses you're approved to go. And this company that we used for card management and card swipe management rolled out a new app that they were really excited to talk about. And that app allowed you to remotely unlock a door from your phone, as long as you entered in your card details or your active directory account that linked to the organization. Now from a high-level standpoint, when you look at hotels like Marriott and their bond voice system. And I think it's Sheraton who has the other one where you can unlock your room from your phone, if you're a rewards member and you're right by the door, they were trying to do the same thing. They thought it was cool. It was modern. People would really enjoy it and people wouldn't have to constantly be pulling out their ID card. So from a modern standpoint, it was everything that this company wanted. They wanted it to be cutting edge. They wanted to be seen as awesome, and they wanted to use it as a way to pull more people in. The downside of this was that application was not very secure. And one of the things that it did was if you had an ID card number, you could map multiple cards to that app at one point at one time. So if you got your hands on somebody who had, let's say keys to the kingdom and access to all the doors you yourself had access to all of the doors, or if somebody had a compromised account and left a password on a sticky note, additional physical security pro-tip, don't do that. But if you let your password on a sticky note and somebody else found it, they could log in as you on the app and start using the doors with you. And this app gave very detailed information as to what each door was and where it was. And if there were any default hours of that being unlocked. So not only did you now have access after hours, you knew when it was open and you could technically trigger that app from anywhere as long as it thought you were connected to their network. That meant that for some

people, they had used a VPN essentially to connect to the network and then open doors from cities away as the proof of concept.

Tom (11:17):

But just to kind of go into that a little bit more, what sort of knowledge would someone have to have and what sort of like payload would you use to trigger this sort of thing?

Meredith (11:28):

Funnily enough, minimal and none, because this was all designed as this is all thought of as features for the application. So the knowledge you'd have to going, starting with knowledge the amount of knowledge you would need is little to none as when you first downloaded the app, it gave you a quick tutorial. And how did some of those flaws, as I had said, as features and putting that multiple accounts, linking multiple cards, whatever, maybe that was considered a win. The first time I read through that, to me, that was considered a terrible idea. So as soon as anybody downloaded that app, they had the information on how to use that to their advantage right there. And because of the fact that there was no backdooring or additional exploit needed, there were really no payloads given technically.

Tom (12:25):

Got it. So like you basically just need to have the app and some information and could do this, do whatever.

Meredith (12:31):

Correct. Technically a person walking around this location could have picked up a card that they found on the ground, saw the company name, saw the information on the back of the card that said, "Hey, download this app" and gone have access to the buildings then and there without needing to speak to somebody even.

Tom (12:53):

Got it. So you'd still have to compromise an account, but obviously that's not necessarily that difficult.

Meredith (12:59):

Correct. One of the additional flaws now that I'm thinking about it is if you did have knowledge of account numbers, you could technically brute force your way in as well.

Tom (13:10):

Yeah. Makes sense. And I think a lot of that does come down to like auditing of the process and reviewing activity. And at the scale of some place that's going to have a lot access control. I'm not sure how much of that is practical or done.

Meredith (13:24):

Correct. And for a lot of places, it's hard to create a safe baseline for, is everybody going to be here from nine to five or eight to three, if it's a school and they may see people swiping in off hours all the time to get extra work done, or because they forgot their laptop or, you know, they had a department meeting later or whatever it may be. A lot of companies just say, okay, you know, we've got the access logs if we

need them, but we don't routinely go through and review and check for anomalies or anything odd like one person opening all the doors at one time across 40 different buildings.

Tom (14:07):

Yeah. I think just based on the amount of information a key card can store and the fact that it's basically an IoT device that's being used as a reader, that the security in those systems, even though it is a security system is potentially limited. And I would also say a lot of those systems are probably really old.

Meredith (14:26):

I would certainly not disagree.

Tom (14:28):

And I guess the other thing we're talking about an access systems, but keys still exist. And that's another great factor where it's easy enough to find a key. Or if you find a picture of someone having key, you can make a key based on that. And there's master keys that could unlock entire buildings or entire sets of facilities for that. So that's another consideration at least is how we use it to get a physical key, or replicated physical key and keys are not unique. There are plenty of cases where for different reasons there are standardized keys used for things. I think going back to elevators like fire keys that the fire department would use are in some states or jurisdictions standardized. So the fire department can use the same key in every elevator, for example. Those keys are just like things you can often buy on the internet. If you know what to look for. And there's no like certification to say, "Hey, you, this is only a fire department." Or if they sell it to only like a fire department, someone else sells that key under a different name, that's identical and still works. We have all these different access control systems. And there's plenty of very weak links I think that can be leveraged to get in somewhere, almost to the point where you can pretty much assume if someone wants to try to get in unless, you know, you have other controls, the standard door locks and systems otherwise are not going to be all that effective to keep someone out. People are always going to be your weakest link. Creating a culture of having people security, aware to help at least identify and prevent some of the low hanging fruit type attacks is going to be a pretty big factor, I think. From a pre COVID perspective. We, we definitely tried to teach people physical security where like physical security leaving your laptop unlocked is an example of physical security. But anything that you don't want someone else to be able to do something with, you should always kind of keep an eye on that. So like, I'm overly paranoid about that. Thinking about where's my phone, where's my keys, those sorts of things, just whenever I get it up, because like, if you don't have it in your pocket, it's really easy to lose track of it. This is also even physical security. You have like all these voice enabled things like your iPhone, for example, or, you know, the other NSA listening devices like Siri or those sorts of things. Yeah. Like there's not necessarily any sort of authentication. There's someone saying, you know, so-and-so Siri or so-and-so Google. One of those words that activates it. So like Meredith, haven't some of you been on SOC calls where someone will try to activate someone's device in their room.

Meredith (17:11):

Yeah. That happens quite frequently. Many of us have switched over to using headphones when we're on our normal calls. Just so that people aren't turning our lights on and off. And as you said that I definitely had to mute one of my approved NSA devices for fear of what was going to happen.

Heather (17:32):

I use that as a teacher, when I worked at a school that was very, very strict about students and their devices. And so the school rules were that all of their phones and iPods and everything were to be off during the school day or the school will take them. So I would say, you know, okay, Google or whatever, and try to activate as many phones as I could in the middle of my classroom, it really made students angry. They did not appreciate that.

Meredith (18:02):

I love it. Back one time, I will say a couple of years ago, one of the Splunk team members he was a member of SOC at the time saw my phone sitting on the desk. And we had been recently talking about the latest Apple update that included the wonderful pay she-who-must-not-be-named. And he raised it to send a text to my mother on my own behalf. And my mother was less than pleased receiving said, text.

Tom (18:32):

That's the other thing, the number of people here that I've gotten to turn off a steady texting has, has been impressive. And something to consider, if you have that ability consider what could happen. If someone, someone else is able to do that. And also like mom is a great example. That's someone that's a lot of say a lot of times save that way in contact. So it's easy enough to do that. And then you could even use that to social engineer, someone else. Basically everything, if you think easily, there's so many different ways to take advantage of the things that exist to make things convenient, which is annoying, but that's the world we live in from a security perspective.

Heather (19:15):

So as far as ways that we can help mitigate the risk. So we've talked about security guards and key access. We've talked about lock screens on our devices. What other things can people and companies, you know, what can we have in place to sort of help avoid this risk?

Tom (19:35):

It's like going back to the thing we talked about earlier, deliveries, having training and policies around that, I think is a good starting point, for sure. Whereas like you require every delivery to go to a front desk and you believe we have a place right outside the front desk where packages are left, and that person can't go beyond that point. So like mail room right off of the front lobby, no way to access anything else, always in view of the receptionist, that's a reasonable strategy for that. And if someone is going to random door, you don't let them in. They have to go to the front desk, outside the building. That would be kind of one potential way to do that. But it also relies on people doing the right thing, which is hard to account for. I've worked at companies before, where they had a policy where everyone had to swipe their key card, regardless of if, you know, they knew who they were or anything like that. Everyone you pass the door, you had to do a swipe with your thing. Now that, that the thing that was, I think, not that great about that system is the card reader beep the same way, either way, if it, it would flash a red, if you had an invalid key, but from someone walking around and there was no way to easily tell, Hey, this wasn't allowed or something like that. So I think that, you know, I don't know of a system that does that, but if there's something that does like a different sound or, you know, flags, just red lights or something like that, they have to indicate, Hey, this, this quite wasn't valid because you're still social engineering. If everyone has to do that, and you just have a random RFID thing that looks the same to everyone else, and no one picks up, you could still tailgate. So I think that that's an area that you have to think about what the controls are and how that might be able to be exploited by someone

who understands that the system works, which is often not really hard. Or do you have any thoughts about like what I'm saying about those key things? Does that make sense? Like, have you ever seen anything where there's a different indication if you fail, if the doors, if you let's say you have five people walking in the door, they all are swiping their cards and you know, one person has an invalid one. Like, I don't think there's often a way that you're able to tell that it is a fail.

Meredith (21:53):

Right. It's usually not different enough or loud enough as you were saying. And I mean, the biggest one I can think of is the one that's made the most difference I've seen is ones from my old university they had basically, you know, RFID pads and the pad would have a glowing green ring around it. It stayed black when it wasn't active, it would glow green if you tapped and you were authorized, but that ring would go red if you weren't, but it didn't make any sounds. But if you tapped something red, even if the door had just been opened as a lock would engage, and you could hear the audible click.

Tom (22:38):

Yeah. I still think that's not enough feedback to make it obvious.

Meredith (22:42):

So you essentially want like a wee woo siren rotating light.

Heather (22:46):

Or slam up them up around the door and they're trapped in a cage and then it fills up with water and sharks come in?

Meredith (22:52):

I mean, that being said, man traps are always a good idea.

Heather (22:56):

I like the trap door idea, just drop them down.

Tom (22:59):

And unfortunately the five other people who were walking in at the same time, they're also now trapped.

Meredith (23:06):

Well, that's what you get for associating with somebody you shouldn't.

Tom (23:09):

You actually see that sometimes in certain cases. And I think like a bank, isn't a great example of this, but like some banks actually have physical systems where they'll put up some kind of guard if a robbery happens to protect the tellers. But a lot of kinds of lobby is still going to be open because you don't want to create a situation where you lock innocent people in with someone who could be armed, for example. So it comes down to safety and that sort of thing too, and human life is pretty much always taking priority over the security system. So that's kind of the accepted risk. And obviously that makes

sense, but I mean, from an access card perspective, you know, like if just the key reader made a, you know, a pleasant beep when you touched it and made a, you know, a loud obnoxious access denied type noise that people would notice, you know, and locks may be engaged if you had like a magnetic thing, it would, you know, try to help pull the door shut. I like the red lights around the door too. Cause you got to consider that there's different, you know, sensory impairments that people might have. So if you just have a sound, if you have someone who's deaf, they're not going to hear that. Likewise, if you just have a light, you could have someone who can only really hear and you have the same situation. So you kind of create a situation where everyone can recognize that sort of thing. And it at least becomes apparent that, Hey, there's an issue. And there also needs to be some response to that sort of thing too. Like if someone swipes in a door with an invalid key card and that's activated, do you have a high security environment? You know, how do you prevent that? Now granted if you have a high security environment is probably someone attended at that door. Anyway, that's a security guard and you probably need to have that at every single access point too. So it becomes expensive and complicated, but it really just like anything in security, you can keep throwing money at a problem and get diminishing returns, but still have returns to some degree.

Heather (25:05):

Well, what about having security cameras in place to help monitor entryways?

Tom (25:11):

Meredith you probably would do the same thing, but whenever you are walking around somewhere, you're subconsciously looking for cameras, right.

Meredith (25:18):

Subconsciously, fully consciously. Absolutely.

Tom (25:22):

And I always kind of feel shady doing that. You know, like if you're walking in a store, looking for cameras, clearly you're either a security person or a criminal, but just kind of trying to get a sense of, you know, what is watching you and where it is. But you know, I'll notice that when I'm biking around areas and like, oh, these houses have these security cameras in this area, just kind of that sort of thing too. So it's hard not to kind of notice those sorts of things when you get in the habit of looking for it. But the other thing I think is so many times people think having cameras is a prevention, but it's not a prevention. It really is just there to gain, give you evidence and help with understanding what happens. I don't think cameras really stop things a lot of times, unless they're actively monitored and that's pretty rare.

Meredith (26:11):

Right. And I think that they're officially designed to serve just as that deterrent of something is watching, but is also becoming more and more commonplace now to put up those dummy cameras so that people believe they are being watched. But in reality, in the event that an incident were to occur, nothing is actually being monitored.

Tom (26:33):

And honestly, I don't understand that because the cost difference at this point between a real camera and a fake one, especially when you consider the labor associated with actually putting in place. I mean, assuming that there's wiring there, the wiring is going to be expensive, but like it's not a huge difference. They actually just have real cameras.

Meredith (26:55):

No. And for a lot of the, you know, home automation, special security cameras that can be used at a company or a building now are so cheap. And the risk you have from not having a camera would far outweigh the cost of, you know, that $20 camera with a $12 a year license for unlimited cameras on that system.

Tom (27:19):

And it's also full HD and like, you know, yeah, It's always funny to me where, you know, like someone steals an Amazon package off of a porch and you can like read the license plate of their car and the label on the package from the home security camera and then someone robs a bank and it's like three pixels to the guy's face.

Heather (27:41):

It looks like big foot.

Tom (27:43):

Exactly. Which, you know, granted, maybe there's not the incentive to upgrade those sorts of systems, but still like you think you would think that there would be some more technology that would be put into that given how good cameras have gotten in the past five, 10 years.

Meredith (28:01):

It's interesting that you say that because every time I, well, not every time, I think I've seen one or two policies where they've got physical security access controls listed, and it's actually specifying the quality of the camera or whether or not there's audio involved as well, versus just having a camera. Because I think that quality is something that needs to start to be taking into account at a more widespread level.

Tom (28:29):

Yeah. And there's so many things you can do with lenses and that kind of thing, to be able to get what you want out of the camera. There are cases where cameras can be really effectively used to help protect assets. If the system is well designed and the people using it are well-trained and we didn't talk about the keys freight. Oh, the thing to keep in mind about the ATM key is it doesn't actually get you to the money, but it gets you to the safe of the ATM where you can potentially get in there, or it gets you to the control unit of that. And you know, that technology is really secure.

Heather (29:08):

You know, that list of things that you were saying earlier about things that make you look like you're a criminal, Tom, you should probably add this conversation to that.

Meredith (29:19):

So here to give you a little bit of context. So Tom and I went to Cincinnati and acquired 12 ATMs. They became our diner ATMs for CPTC 2019. And we had one set of keys with them and, you know, we had a large number of ATMs and if we lost, you know, that set of keys, that wouldn't be good. So I started hunting around on eBay and I reached out to a person who was selling keys for the same model and then proceeded to provide me with a list of all of the other ATM models that those keys worked for and then said, well, actually, basically just this type of standard lock, here are the, you know, bicycle key you can get that would fit this. Here are the motorcycle keys you can get that would fit this.

Heather (30:14):

I feel like this is a bad plan for ATM companies.

Meredith (30:18):

It certainly is. And the ATMs we used are widespread no longer in service, but that being said on our way back, we did see one out in the wild.

Tom (30:27):

Well, it was a newer model and I totally wanted to try the key that we just got on that ATM, but I really just didn't want to do that in public with it, like really, you just would walk up to a random ATM in a store and unlock it. That just doesn't seem like right.

Heather (30:43):

Kind of sounds like something you might get arrested for. I feel like it would be.

Tom (30:46):

I think it's, it comes down to permission. If you, if you just ask the person like the manager and say like, I just want to see if this works, is that?

Heather (30:53):

Hello, Mr. Manager, may I unlock your ATM please?

Tom (30:59):

That's all you just need to do is have your ATM, you know, service person. And then the next thing, you know, your ATM technician, right?

Heather (31:11):

All right on that note, that's all for physical security. Next time Tom and Meredith are coming back to talk about single factor authentication. Until next time, stay safe.