Interview with Francisco Artes – Principal Engineer at NSS Labs

Dave: Welcome to the Elegant Workflow Podcast - A member of the Tech Podcast network
Today we are speaking with Francisco Artes – Principal Engineer at NSS Labs
Francisco, welcome to the Podcast.

Francisco: Thank you very much for having me.

Dave: Please tell us a little bit about your background and what led you to your position at NSS Lab.

Francisco: MY background's been a little over 20 years now working within Information Technology and Connection Security specifically primarily focused on the production of intellectual property rather than compliance and regulatory work. So after working for quite a few years I kind of worked it up the totem pole as if it were. I ended up being the head of security for Electronic Arts. And then after working in the computer gaming industry I switched over to Motion Picture industry by hitting up Security for Deluxe Entertainment Services Group as their Vice President for Worldwide Security. After that I went over to NSS Labs where I've been working primarily as their principal engineer in developing testing methodologies, new technologies for them and of course, working through a lot of their reports on so forth on the efficacy and performance capabilities of various security technologies.

Dave: Then, can you tell us a little bit more of what NSS Labs is and what you do for your clients?

Francisco: NSS Labs is actually a independent testing laboratory first and foremost. It has an analyst arm as well as different ways of consuming the empirical data that they put together. So the researchers AKA the analysts themselves, do a lot of research into different avenues of security from market research, very similar to like a Gartner might do to reviewing the empirical data from different technologies and devices as they compare and contrast into each other to help a lot of our customers of reaching everything from purchasing decisions on what might be the best implementation of technology or what might be the best vendor for a particular location within their infrastructure so it's not always just perimeter; to understanding what are the common trends, what are the actors doing on the internet, what are we seeing in modern malware and exploits and so forth, what might those attackers be looking for. So, we work as a research arm and usually like complement security groups.

Dave: I know security is on everybody's mind these days. What are the kinds of things that keep you up at night around security and securing your clients?

Francisco: Really just the the fear that we know for a fact that a lot of the malware riders and exploits riders and so forth are actually using a patched in modern versions of all layers of security from end point protection at the workstation right up to the edge where your IPS, your next GEN firewall might be running. And they're pre-testing their code before they launch it live under the internet as it would be or they sell it to someone else. And then doing this of course, they're just launching out the versions that predominantly can already be bypass certain pieces of technology and there's always that window that exists and unfortunately it's an extremely large window that exists between the time that a new piece of exploit code might come out and when we actually see a definition or capability within security products or even within the applications themselves where there's patches involved to go ahead and remediate that.

Dave: Everybody feels if they have an anti virus or on a corporate level they have a firewall that they're safe, that's not really the case.

Francisco: No. Matter of fact I had a phone call with a new client just last week where the head of security they were speaking to is very fixated on the fact that they were using firewalls and antivirus and that should be the end-all be-all of their security. So a lot of level setting in that particular conversation with that individual to point out the capabilities and the things that a firewall can do and then the limitations that we see even within live information that were actually able to show him. You know that epic scene capability of just antivirus products they're not bullet proof the vendors themselves will tell you they're not bullet proof. It's a work in progress constantly that's why they all have armies of you know coders that are constantly writing signatures or working anew technologies like App Rep systems and cloud based aggregation points and so forth to try and constantly stay ahead of the game. So you know, I have, one of the things you'll hear me say quite often if you watch me speak and so forth is that if you believe in the efficacy of security products that you're running, it's not going to end well for you. In other words, if you install them and you think you now have the most wonderful you know Camelot like experience of a castle that's keeping everybody at bay just simply not the case.

Dave: When you look at a lot of these bright kids that have really been featured in the media these days, Sony or Home Depot, it wasn't like there weren't alerts being sent out. A lot of times the systems that are designed to alert that there's something going on, were sending out alerts but they send out so many alerts at a time that either you don't have yet a full time people analyzing all these data coming in or there's a lot of false positives. What is a good way for a business to protect themselves?

Francisco: Well first and foremost, you know, eyeballs are a commodity especially within the Information Security Group. When you look at even the larger corporations in the world and you say okay great this particular corporation has X thousands of people working for it and then you kind of ask the question of the head of security, how big is your staff? And then you get back to them very quickly, you know, an extremely large information security staff maybe 20, 30 people. Alright so there's 20 or 30 people trying to watch all the infrastructure, applications, log feeds, app feeds, net flow, app flow, you name it from all over these network which is you know probably millions upon millions of transactions per second. It's just not realistic even with other pieces of technology so you do see things like you know, I guess in Target's case, you know, they were using, utilizing Fire Eye and Fire Eye is reporting hey now we actually saw the network communication from the compromised systems but the problem was the signal for noise ratio was just way too high right so they're not noticing what's going on, those eyeballs are an absolute commodity and getting to the point where we utilize and look at technologies and information lately differently maybe the answer. The other answer might also be just to massively increase the size of your security department but that's unrealistic because it's a call center right so you know looking at things like how are we being attacked, what might be the ways that were attacked, how are we using the tools and the resources that are available to us. I have so many people that I speak to that will tell me, hey look we do a quarterly pen test, every 5 months pen test or an annual pen test and we think we do pretty good because sometimes it shows up in the logs and you know, then our people will know to react to it and so forth and I say, hey that's great you're about halfway there. So, you know if you're doing pen testing, pen testing is a fantastic thing but pen testing isn't truly telling you what is and isn't right with your security. It's just, this is how we got happened to get in today. What's more important from that pen test is actually you testing how fast that you people react, how long did it take them to notice that there was a penetration taking place or an attempt taking place and did they follow your practices and procedures and other ways of tuning those practices and procedures to respond to the fact that you are just now being compromised. It's really not intended and never should be intended to point out, well, you know, we had a wonderful pen test. We think our security now is 98%. It doesn't even make any sense but so many corporations will do that. You even see it within the PCI compliance that's like whoa you got to have pen test so therefore we think you're now more secured. That's a full hardy comment to make. It should be you had a pen test that was performed you now at least knew how to react assuming you even noticed it. Al;;right so when you talk to other bigger pen testing groups and their executives we'll say hey I think it's great we have XYZ client that now when we first started working with them it might have taken them a week or two to even realized that we were compromising their systems. Now it's down to like minutes or hours and our phones are ringing within the first hour and they're already blocking us out and their blacklisting things and they're augmenting their security because they've now practiced being attacked and defending that infrastructure. As far as seeing what's going on in your infrastructure, that takes a lot of tuning and unfortunately we see a lot of companies that will buy Sins and other types of aggregating log technologies and what of course they'll wind up doing within is feeding them full of information but then how do you parse all that. We generally don't see them with people that actually know how to write those parsing rules and so forth, there's insufficient staffing to maintain that particular device even if the device is supposed to auto notify you when its seeing certain hits when things correlate with each other. But unfortunately, you know, having a talented individual or probably 2 or 3 individuals that can write those correlating rules not always the case. So, we do see where we have products and technologies and vendors that are trying to address that problem; we see deficiencies quite often in the enterprise side; we see some deficiencies within the product logic it's just not quite there in some cases. But really it comes down to, there needs to be a more consorted effort. The security department is spending a lot of its time worrying about compliance and regulatory checklists and audits. They're probably not focusing all that much or at least as much as they should on actual security.

Dave: You could be 99.9% sure so to speak if anybody ever is to that level but just a .01% if that 1 person gets in there's a lot of damage they can do. It's not about being in a 100% secure but it's also how do you deal with it? How fast can you find it? If someone has gotten in and do you have backup of your data? how quickly can you stop them from doing something, are they on your network for a month or 6 months or a year, just looking around and snooping or do you kind of catch them as they're starting to come in before they can do a lot of damage? Also how you build out your networks too, is it a hard shell that once you're inside it's like a soft cookie?

Do you have various levels within your network of security? Do you have areas that are just walled up completely from the internet? Because there's just no reason for that part of network to even be on the internet. So I think there's a lot of things to think about like you said it's not as simple as just having 200 people just look at logs all day.

Francisco: Yeah. Absolutely. It's also a change in mindset I think you know for the median entertainment industry looking at the Sony compromise which was you know off the scale. This is not your normal type of compromise. This is, you know, in no way shape or form could this be you know dealt with by any other corporation within that marketplace especially. But to look at that and say alright we now have to have a change of perspective. That perspective should be when we get compromised what shall we do? It shouldn't be on the day that something finally happens what should we do. The mindset should be were already compromised. The severity of that compromise we don't know yet. We don't know how bad this is going to blow up so how are we going to redesign our network infrastructure so its not that soft cookie that you mentioned on the inside. I want it to be able to collapse so if one section does get compromised I can literally cut it off as if its cancer and isolate it away or much like you know literally the real meaning of firewalls, it maintains the damage within a certain portion of the building, you know, figuratively speaking, for enough period of time that we can address it and or deal with isolating hat location right. Not necessarily we receive a very large flat internal corporate networks so that once you break through those perimeter pieces or every other ring that you set, everything else on the inside is just one failed swoop. How do you deal with that? You know it's one thing to say I've got 20 people on my staff and were dealing with you know potentially one data center that got affected or one segment of the network that got affected but the corporate infrastructure, the financial infrastructure is all sound and that's great because my people can now focus on a couple 100 or a couple 1000 machines versus tens of thousands machines or just some number that we can't deal with. And I think those mindsets are starting to change, I'm starting to see those changes when I speak to CSOs. I'm starting to see those changes when I see other people presenting at security conferences and that is you have been compromised already full stop. I don't care what company you are. How are you dealing with that? You may not recognize it. You may not see the exploitation of data, it may be sleeping. There may not be any actual damage yet to your corporation. You could be leaking email for all you know but what happens on the day that it does start to explode or that you recognize that they're already there? How can you isolate them to that sandbox? Or do you have a big flat open playground that once they're in that's it they're in. and I think that's what I see with a lot of these corporations is that they're post mortem coming out, whether its Target, its Home Depot, its Sony, whomever it is to look at it and say, okay we have been compromised, were compromised, if we get, when we get compromised not if, but when we get compromised in the future, how can it be different?

Dave: And how do you think is the best way to get employees to buy in around best practices around security because employees want either no security because it's easy for them or they want something like single sign on to all systems including financials systems, hr systems.

Francisco: I agree. I actually even agree on the non federated single sign on. I'm a huge factor of 2 factor authentication and that just means that you could actually do a shared, you know, double As, in other words your authentication in accounting and so forth across the entire enterprise but it’s always a new challenged password that has to be entered into the systems not that it’s one common password and I think really getting away from the whole mentality of passwords is kind of key for security and looking forward. I mean when you look at heart bleed and everything else that took place, you know, large complex passwords aren’t always the answer. First, it makes it very hard, you have an administrative overhead, you have to build systems and put them into place that help people get reminded of their current passwords which is always an actual very easy avenue to leverage in the hacking of something right. So we see a lot of people receive, even a lot of celebrity when they have been compromised, it was their base root email address if you will that got compromised and from that they just simply went to the twitter account of the celebrity or the other social media system and they told to send a new password request because they’ve already taken the central email account so as soon as that new email came in they just click it and follow the instructions like any other person and presto, they took over their social media accounts right. So we have some faults because of course we’ve constantly been trying to look through usability and assisting the end users. I think things like challenged authentication thru 2 factor even you know as simple as using Google authenticator and their technologies that are out there is really key and its better than having people come up with these crazy complex passwords because what you end up doing is creating a barrier for them and security becomes this wall, this obstacle to getting the job done which is bad because at the end of the day, I need all the end users and the corporations to be inculcated into the security mindset and make security part of the culture of the corporation. And to do that I can’t have security constantly being this obstacle. It has to become a facilitator for them getting their work done. We need to be looking at technologies that facilitate people moving in swiftly thru the infrastructure when they’re supposed to whether its authentication because they can just look and type in the correct key or its biometrics or something else not a man, what was the 95 digits special character upper case lower case, you know, using cartoon pieces, what kind of crazy password I had to setup and I had to change every 30 days or 60 days or 90 days. You know that makes it really hard and getting the things we don’t have those obstacles anymore is very important within the security. Clearly we still need to have authentication into things obviously not just for the application security of it but also because we need to be tracking who does what to the data and authenticating gives you that as well.

Dave: the one thing I try to do is not either use a security question I feel nobody would ever know about me or use bogus answers because you can go on my Facebook, you can go on my twitter, you can go on my linked in and you could probably figure out to most of the common security questions. My favorite thing is that people use the same password for every website and it’s just ridiculous. You have things out there like last pass and one password all these great password managers, it’s not the be all end all but at least gives you another level of security where you don’t even know the password, you may know the master password and its easy, if something gets broken into, there’s a breach, I go in I change the password on the website. I don’t have to change my password on every website that I have an account with.

Francisco: Yeah. Especially when you get those systems to generate those heinously long random passwords that they’ll inject into those websites for you. And then you just authenticate into the app and then of course it is handing off the key to everything else. Other things to look at especially more on personal side versus the corporation side you know, if you’re using a lot of the social media like Facebook specifically and Google as well, these all allow you what computers can get into your account right. So you can say hey, this computer can get into my account, if another computer tries to gain access to my account even if it knows my credentials, I want you to send a text message out of band to my phone having me validate thru a pin number or whatever that that computer may access my account so even though they have the user name and the password and that thing to connect to, in this case, Facebook, they still need to have that computer authorized to gain access. These are simple features that can be turned on in the social media sites but they really don't do a huge job in advertising them. You can also go to 2 factor for all of these different websites most especially for all your different Google accounts right. So whether it's your email or your whatever that you're using on Google you know, using authenticator, using all these other systems is absolutely fantastic. And I do like locking things down to the computer it makes it so much nicer plus you also get a an alert when somebody is trying to access your account.

Dave: or even in the case of Google you can go in and lock your account out so only people in the US for example can access your account. If you go and you go into Settings in most of these services have privacy settings or security settings, you really, you do have a lot of control over your security of your account because you're right once they get in to your email or your Facebook sometimes from there there's a lot of other places they can go and it's not the end of the world if its personal unless they get into your bank but even then you have some protections. But as a business, as I understand it on the banking side your liability is so much higher because you don't have the same protections that just a person has involving any type of fraudulent bank activity online.

Francisco: Yeah absolutely at least for US banking there's FDIC insurance for regular like you and me and everybody else who has a savings account but once it's a business account, there is, all the ones for the security of your online banking for business account is absolutely on the business not the bank anymore. So as my personal checking account, it was hacked into and somebody wired transferred out x dollars out of it, I can contact the bank and they'll put x dollars back in. If I'm a private business, and it was my business account and I contact the bank they'll tell me well too bad you should have done something better about your security. And that's just the fun way that our banking laws work.

Dave: As a business, how important do you think it is doing a 3rd part scan of your network and website? Why would you want a 3rd party to actually try to do a penetration test on your security?

Francisco: there's pen testing, there's app testing and then there's scanning the website and I'm actually going to start with the 3rd one which I don't think a lot of corporations stopped to think about until after this has happened to them. Having a corporation, having a 3rd party that can scan your corporate website for example or if you run a blog site or so forth it could be publicly embarrassing because the number thing you need to be protecting is actually your brand management and your identity management within the consumer market. Having somebody scan to make sure that your site doesn't have malware on it is actually a very big deal. We saw I think it was like a year ago or may be even 2 year s ago in NBCs primary websites have been compromised, malware have been put up and I think it was some very large number of malware drops that had taken place from NBCs website before they actually you know, found out about it and can take measures to remove it from the website. That's huge right. That's a massive black eye for them, you know. The next part of course is having somebody go through app testing which is the 2nd item I think I mentioned. In this particular case, I want you to test the application development that I have done on my website is the content management system that I'm using still secured, are there bugs that you can exploit as their cross site scripting? These would be of course the mechanisms that somebody else might have used to inject malware into that website which of course is now then infecting all of my customers and my customer's data is being compromised and then my customers can gain access thru the portal of my website especially if it happens to be one of my admins. Then of course thru that vector I gain access to the whole back end I didn't actually have to compromise the application in that case I just forced it to drop then interject. But in this particular case for the app security, I want somebody to be going from the outside whose expertise it is in finding ways of exploiting those applications that I've put online whether that's a SAS that I'm offering people or just a portal to online banking or into my infrastructure. The last and then we touch a little bit about on this a little bit earlier is the pen testing aspect. Please try and absolutely hack into the system. Tell me what you were able to do, where did we have deficiencies and so forth and that's great and that's usually the final deliverable from a pen tester. You've gotten them yourselves; they're depending on the company that did them for you. Its a couple page brief to a giant D ring sized binder, right, everything that they were able to do and gain access to. Unfortunately, a lot of times it's very hard to trust and that's great that's the final deliverable but really what should be happening out of that pen test is the fact that we are self served learning. What it looks like when we are attacked, how do we recognize that on the systems? What is our response? How did we probably follow the business continuity plan that we have, the plan that we have that we outlined for the operational aspect of our security? How did we react or if we do who did we contact? You know, how did that flow work? Is it efficient? Where can we find more efficiencies in that? Did the chief security officer come to work on Tuesday after the rest of the team noticed the hack on Monday and as he's walking thru the hallway the COO asks him what's going on with the hack and the CSO has no idea that there's a hack going on. So, we work on those aspects. I hate to be the guy in the guy in the hallway when I'm asked how's the hack going and my staff hasn't told me but you know things like this happen. So all those different aspects from having a 3rd party go forth and you know do different testing upon your applications is important. The overlying piece to all of that is extra eyes and extra hands which you generally don't have on your team and its usually very specialized skill sets that you may or may not have in your team as well.

Dave: And there's such demand right now for security professionals and I don't think most teams in smaller companies or mid-sized companies would have people at the level that they need to have. The larger companies, yes, they can afford to do that but I think you mentioned earlier they are understaffed though even if you're lucky to have 20 or 30 people, your corporation maybe 50,000 people with who knows how many possible threat factors into the network and you have these 20 or 30 people trying to do that and do the PCI documentation, listening to all the other departments saying that they want to post holes on this firewall for this application or that application, you know, if they can just sit and watch security all day that would still be a gargantuan tasks let alone the other things that they have to do.

Francisco: And I have to say some of the most fun I've ever had is going to those meetings where people telling me about all the holes they want punched at the end of the firewall. Usually, also right to their desktop right so.

Dave: And they don't want to do any documentation on either like I want this out, what are the security aspects around it, what do you know? I don't know, its really good but I just want it instead of really doing some research or reaching out to the vendor and putting the vendor together with the security group if they're not technical instead I want this, I want this and usually they get their way if we are squeaky enough.

Francisco: That or they can show realistic or fictitious dollars attached to it right.

Dave: What do you think people can do at home to secure their networks and computers? Do you believe in some of the hardware devices out there like the Staros and the Fortinet hardware or personal software firewalls? What do you think would be best for somebody who just wants to have as much security as they can and maybe has a little bit of money to put towards us.

Francisco: I'm a huge proponent and even my own personal website which is a delta from the professional work that I do you'll see me constantly writing blogs and articles on there where I'm talking about being about a more educated, more informed, more engaged home user if you will. Granted, I'm on a, like, the 1% of the 1% of the user market right, nobody makes appliances for me because I want all the capabilities that I can do inside of an enterprise. I want to do outbound rules, inbound rules, massive redirections, multiple static, external IP addresses, I want to be doing proxy filtering, I want to be looking for, you know, malware and exploits in live stream as things come down to my workstations in the house especially for, you know, my wife and my child and so forth. I want to be parsing out certain amount of content from my home that my child doesn't come across adult oriented materials, you know, so I am way beyond. I think where the common consumers but there are many of these aspects that I'm very happy to see that are starting to become more mainstay and those are like the 40s, the 40 nets and so forth of the world who are starting to make smaller, you know, kind of small office, home office/home used appliances. Cisco has some great ones too and these things are fantastic. They allow you to do actual robust inbound and outbound rules, they have proxy technologies built into them, they have spam filtering, they have blacklisting that's automated thru things like snort and so forth to keep you from going to malicious websites. So they're fantastic that I'm starting to see this. I don't think the use of this is going to be very high amongst the common person, they're at least right now, maybe in my son's generation, you know, as they start to become consumers will be much greater in that aspect but you know, when I look at today's common home appliances like I stop by at Best Buy or you know, Target and so forth and I look at what's on the shelf and sometimes you'll see me buy one just to play with it and so forth. And you know, you're talking your standard, you know, half the time my favorite is they munch up networking nomenclature so much that I just want to throw a tantrum when I'm looking at the boxes right so its my WIFI router, you know, or its my home router. Well it should be a firewall not a router, right. It's a state full of inspection device but of course you get to the UI of the thing and it like the only rules you can write or predicted upon are pre-set drop downs. You can't actually write your own and then oh, you can have your one DMZ housed but that’s it. You know, you can't have special rules for this computer and for this one over here. And by the way, all these other things that I’ve been talking about aren’t even options. You can't even like do a transparent proxy to filter things out so on and so forth. We see some kick starters and stuff coming along for new home appliances. I personally run, you know, a microprocessor technology where everything’s solid state like a Socrates box for example. And I’ll run PF sets sitting on top of it which is a pre-VST firewall that’s based on the mono wall project that allows me to do a huge amount of robust data manipulation and security and so forth and a little tiny box that cost a couple hundred dollars and I’m light years ahead of you know, these “routers” you know, which should be firewalls and so forth.

Dave: Oh yeah and some of these home routers personally drive me crazy because you can't even turn off the firewall on some of them. They were built in your cable modem or DSL modem. What I’d like to do is turn it off, put something after that I have more control of. Sometimes I find myself so frustrated that I’m like putting something into a DMZ that I don’t even want on the DMZ just to get it to work.

Francisco: We utilize DSL at my home and of course like you said, they came, they installed. They put this device on the side of my house which you know, the technician described as a, I don’t even know what you called it, router, everybody calls everything a router, it drives me nuts. So he called it a router whatever and then there’s a little “firewall” in my house that they dropped off which is really just an extension of the thing on the outside of the house. And I get into it and this was an upgrade for me I’ve been using them for many, many years in the past with just standard DSL where there’s a DSL modem and then there was my firewall hooked in line with that DSL modem. And of course the DSL modem could be put in bridge mode so while it did at one point have a self contained little quasi baby firewall, you could turn it off right. And you just let everything go forward and then you would proxy or any extra IPs or utilize any more interfaces on your firewall and you can start doing any magic you want. You can put things in real actual DMZs, you could write rules about who could get top those cameras and so forth and that was fantastic but this new device that they brought out doesn’t do bridge mode right. And it drove me absolutely nuts and finally I found in forms somewhere you know or other networking geeks if you will have figured out ways of manipulating and getting certain things to work because it was driving me nuts because I felt like I was typing with mittens on every time I wanted to do something with my network configuration. And I was working around some stuff and there was a setting that I had to have them changed and I called off the particular provider and I said, ‘Hey, you know, these settings need to be changed so I can do this advanced feature with that thing that you bolted on to the side of my house. And the technician, you know, you go through the various wrongs of technicians and you finally get to the one who knew what he was doing or she knows what she’s doing. And I get in there ready to login to it and I go, hold on a minute, I changed the default password on the device, let me go switch it back or just set a temporary password so you can login and the technician says to me, oh don’t worry about that I already reset it back to the default password on your home network right. And you have to stop and think yourself in a minute, wait, wait, what? You did what? And if you start looking at the route rules and what’s really going on with that, they have their own private network that all these devices sit on that allow them to administrate them and get to them and through them they can literally write into your home infrastructure. And a lot of the consumer market I would say probably predominantly set in the 90 percentile of the consumer market has no idea that this is possible and that this can take place and it's actually quite this disconcerting. You know, I would like to trust them but who's to say somebody doesn't pop them and starts hopping onto anybody's house right.

Dave: If it's disconcerting to you and I to the average consumer who change the password, forgets what the password was, they're like, oh thank God you can go in and reset this. It's so funny because when you use something like you use File Vault on the MAC OS so that says you better remember this password. You better put this recovery key somewhere or make a recovery disk or whatever the process is around that and people don't and then they locked themselves out of their computer and later they call Apple and Apple's like, what do you want us to do? Its military grade encryption and there's nothing we can do for you and then they blame Apple. They say, well Apple's terrible or Microsoft's terrible.

Francisco: And I think they're wonderful. They're wonderful for doing that it's not terrible. It's how it should be. I mean they give you plenty of opportunities to save these keys but at the end of the day I want encryption that's running on my devices that makes it so that if I don't give you the password or even if I forget the password, I'm an adult. This is the thing that I'm losing. If I lose the keys to my house I have to call a locksmith to get me back in right. Depending on the types of locks that I have truly secured locks the only answer may be we have to drill it out and replace them all, right. There is no picking at. And that's what I really want on my workstation right so I want if somebody tries to get in and has multiple tries or whatever, that my workstation goes, okay fine, you're obviously not the person who's supposed to be using it, I'm now going to either turn it into a brick or format it, right or in the case of these high level encryptions like you know, iPhones and so forth that have an AES 256 chip in line between the UI and of course the storage on the device it simply destroys the private key held within that key and just rotates it and you will never again decrypt the data on that was there you just have to start over again. Really, that was, it's fun because we bring up Apple and we point to that level of security when even Apple especially during the 4s and 5 development times you would look at their documentation and say, hey this is not intended to be a security feature right. We actually put a chip in place where the capability of you know, reaching out and destroying the private key inside of that key bag so we can “instantly wipe” the device like if you had lost your device or somebody had stolen it and it was actually pushed by enterprises you need to have this feature so we can utilize these devices for enterprise use. In other words, if my CFO is in Manhattan and were getting ready to, you know, release their quarterly numbers, and he leaves his iPad in a taxi cab and in it of course are the discussions and spreadsheets and everything else that were doing on the number that could be horrible insider information to have out there, you know. We want a way that can remotely detonate with one push of a button and instantly have all of that data destroyed well the only way to do that was to just remove the cipher key and this key is the private key in the device and then from then on nobody in the world can gain access to that even you with your password, right. All you can do is format the device and set it up brand new and that was their original intent for that. The fact that it turned into massive security is great but then of course, Apple like every other vendor then has to start fighting with the main consumer based. What makes it more consumable and I, its mean because I always use like my mother as the example on this but what would be better for a consumer like my mother to use if she forgets her password and you know, she hasn't backed the phone up in a year and she has pictures of all her grandkids you know, over the last year whatever on that device that she hasn't backed up she doesn't want that device destroyed because it's the only repository of those children's pictures and so forth. So there is that weird line that they have to fight. I personally am on the standpoint like you which is I'd rather my device just got destroyed than somebody can gain access to it. There shouldn't be a backdoor.

Dave: So I make it a point to back up my devices weekly. I just take it upon myself that I need to, like you said, I need to be an adult. If I leave my iPhone in a cab or lose it or something then it's up to me to know that I have that information and that I've put enough security around where that information is and making sure it's in a safe place and all that. And I think you brought up a lot of good points, what should the industry be doing differently around designing products that are more secured? Because you said it's a fine line between making it easy for the consumer and also making it so that there is some real security in these devices, how do you handle that fine line of making it usable yet making it as secure as possible?

Francisco: I probably would have been more on the fence had you ask me that question a year ago right, but let's talk about 2015 where we are today, right. So, I've recently had to make like 400 trips to the Home Depot because I was trying to do some plumbing on my own and plumbing is not my forte, just FYI. And I wound up, you know, walking some of the aisles and I was looking at some of the new modern locks and so forth for your homes and of course they all now work off of your Smart devices so if your smart device some of them are proximity based right so if you happen to have your phone with you and you start to your purse, the door and the door unlocks. Or you use or utilize an app on the device and you can either unlock the phone from proximity using Bluetooth or through the internet, anywhere that you happen to be with that phone, right. So you're in Bangalore and you decide to unlock the door for like, your cat sitter right, so that can be done. And when you start to look at the fact that these smart devices whether they're tablets or phones or whatever, are now bridging the gap between our digital security and our physical security – that to me takes away the aspect of where I want more consumability I'll call it within the device. I now want the device to be as hardened and as secure as possible because it now literally is the key to my house, right, which is all the physical things and wealth and so forth that I collect in my home and the safety and security of my family right. So, it's more than just, oh you got my device and I'm a celebrity and because I didn't have a pin set and a password in the device, you found all my selfie pictures that I was sending my significant other, right which is embarrassing and launches somebody's career, right. It's like a pop lock right. But at the end of the day, I feel that we should be getting to a point where there no longer is an option to turn a pin on on your device, right, it's just mandatory. That's how the device and the OS sets and there's no way to turn it off. You have to authenticate the device, whatever the authentication means is, I don't care if it's facial recognition in the future of its Star Trek: Next Generation where you have to say your password or whatever phrase and there's a voice recognition piece or it's the thumb being scanned on phones that we have currently which is like a biometric type piece of technology. I don't care what it is but I think we're now reaching a maturity point where if we are putting in the internet of things into everything in our life and the pinnacle for authentication and access to most of these things is now the small micro computers that you're walking around with that make really poor telephone calls, that should be something that we are really starting to secure.

Dave: What are you seeing now that’s like the future of the bad guys, the future for techs, what new technology are you seeing them trying to explore, things that the people should be aware of so that they understand that things are changing and these crackers so to speak because I know, you know, hackers, there's a lot of controversy about what to call somebody who breaks in so I prefer the term cracker rather than hacker because there's this whole hacker movement about just learning how things work and building things on your own. So these crackers, these people who are breaking into your network, or breaking into your devices at home, what are they doing now that’s so different than what they might have done years ago?

Francisco: So yeah, to start with, I follow you on this one and I've been part of the hacker community since I was a teenager which was quite a long time ago. I have a different perception of the word ‘hacker’ and the mentality that goes behind it and I think it’s an extremely healthy thing. So yeah, crackers probably or just criminal, I like the word criminal. So, you know if you have somebody that’s breaking in, we still predominantly see inter-corporations and even into private accounts for individuals and so forth, fishing is still predominantly the way that were seeing like account compromise and you know, level access to your workstation and so forth. We are seeing some things change, right. We are seeing a lot of this was happening in various types of malware in the past. We are seeing more and more of this now happening through exploitation versus malware. This is of course a code that activates instantly by leveraging a vulnerability in an app on your workstation when you connect say a website and so forth where malware of course is you know, files that end up on your workstation whether you execute the files or the files are executed autonomously by the next lines of script in the website they’re at and there's no file delivery when we’re looking at exploitation. And we’re seeing a rise in that actually it’s been steadily rising pretty much all year long since about October of last year. So that is new and different, we do see the response from the different security products that are out there, you know, adding more and more capabilities to detect this type of attack against an individual. You know, home individuals, you lose that, it’s very interesting sometimes to even sit down with security officers and security staff from corporations saying, ‘Great, we’ve invested all these money into layered security and technologies and you finally have enough eyeballs looking at screens and we have the operational capabilities within the company that feel very, very more safe, I wouldn’t say very safe. Then, you know, the vice president of whatever grabs their laptop and goes off to a conference and you know, some beautiful place and they’re using the hotel network all the time, you know, sitting in a coffee shop and so forth or the an airport or even in an airplane these days. What happened when you just remove all those layers of security the only thing left on that laptop is just the end point protection product, you know, that’s running on there. What is your business plan for when that laptop comes back? Did you quarantine it for a while? Did you scan it? Did you build a network infrastructure so that the laptop are on their own subnet behind their own firewalls and their own IPSS and bridge products so that when they do move in and out physically from the perimeter that when they come back again if something’s wrong with them you can contain it within, you know, that level versus the workstations that happen to live all the time in the building or the servers and our protected infrastructure which should be barricaded off from even these with very specific pinholes even on our local area network or our wide area network. For home consumers, some more stuff – we see big trends in all of these. We see a lot of targeting of financial, right; stealing money from people is still very big. We see, believe it or not, online gaming is huge; stealing your account credentials for the online game that you're playing and then logging into that online game and stealing your digital property if you will. And then selling that digital property on the black market, or actually it's even an open market. You can find it on eBay and several different sites that are dedicated to selling things like your magic sword from the fantasy game that you're playing. And were talking real money, it might be a couple hundred dollars, that could be several thousand dollars for all your stuff that they took from you and it took you a year and a half to like collect it all within that can. It's actually a very large section of the world being targeted believe it or not. And then of course, gaining access to things like your media files and then gaining access to your home systems, your home email, we're seeing a lot of different security groups, or I shouldn't call them security groups, different hacker groups and so forth that when did you compromise large corporations that they're putting all the email, you know, from that corporation up and placed it in other places where everybody can go ahead and mine it and learn all the corporate secrets and learn who's been talking to whom and who has been making comments that they shouldn't have been made that's now going to end her career. I don't see it being very long until that's being leveraged so that its, oh this is the, these are the key officers in that company or here are some key individuals, now let's go compromise them individually through their social media, right. I want to see more of this dirt that we can pull up because of course not everybody acts and you shouldn't have to act the way that you do or all the time, right. And then let's get on their personal computers and so here's their personal life, you know, this will ultimately ruin this person. So, we see a lot of leveraging and changing and what's going on mentally that's being used. It's becoming a bit more personal.

Dave: And also sounds like it's a lot more economic like it was 10 or 15 years ago where it was more about, oh I want to break in, I want to fool around and learn and now it's about hey, how do I make money off of this?

Francisco: Yeah, there's a pricelist for everything out there. Do some Google-ing and just for entertainment, there's pricelists for how much money you can get paid for per social security number that you can collect, how much per credit card number that you can collect, how much per email, how much per zombie, my favorite is selling Botnets, right, so you'll see groups that'll go out and all they do is just try and collect as many bots as possible from infected machines that are out there. And they do a lot of reverse lookups and some database manipulation and so forth and they start to say, okay great, I have, you know 40,000 computers in California that I've compromised or better yet I have 5,000 computers inside of corporation X, who wants access to corporation X? You don't even have to hack it anymore. I'll sell you 5,000 compromised computers in that corporation. Of course, through slight elevation of privileged I can even come back and probably give you specific information on whose computers I have compromised. Who wants access to Francisco or Tessa's computer? I have that one compromised, how much would you be willing to pay for this? And that also is beyond the selling of 0 days and you know, exploit code and malware and so forth it's a new vulnerability I should actually say that are out there that we see, we already know it's a cash business, it's been around forever. But the interesting, some interesting aspects of that when we have sequestration in the United States in other words, the government has been told stop spending money, you know, there's a vacuum. These guys still want to sell. They're new exploits in the US government isn't bidding everybody and it's actually a pretty honorable system. They'll buy them and they'll have embargos, like they can't sell it to anybody else for an X amount of time. So we see that vacuum getting, you know, it's there and that space gets filled by other individuals. We do a presentation from NSS where we talk about purchasing all the films that come out as in NATO or UN project, right. Because it would actually wind up financially saving corporations billions upon billions if not trillions of dollars and one of the things that we argue in there is, in order to commit these acts against nation states, right, so cyber warfare, if you will, cyber terrorism and so forth, it used to be that if I wanted to go to war with another country, I have to be another country, right and I have to be able to afford battleships and airplanes and missiles and troops and you know, nobody has that budget. But now, I can write, you know, one weekend worth of codes and take out an entire country or I can take out an entire corporation. I can cost that corporation billions of dollars. I can do all the things that you see in Hollywood to a country and you know, I'm you know, some guy who's living in his mom's basement, right. It's a completely different dynamic. It' the other end of the spectrum I would say, than being a country. So, the world is very much changing, we are getting to the point where, you know, what we've seen in movies in the past, or read in books and talent or tongue and cheek and look at, wow that would be really bad if that could happen but good news, it's probably way too impossible for that to happen because everybody has this great security people and network engineers know what they're doing and app developers never write apps with, you know, bugs in them and so forth so you know, whatever the world is safe. And you know, with the internet of things and with you know, the progression of technology throughout all of our society and so forth, we actually are in quite the opposite spectrum of that, you know, we don't see, you know large network of coders coming in the universities with CS degrees that understand secure, safe computing programming practices, right. And you'll hear that argument from software development companies when they're being asked to, you know, produce better "more secure code" and they look at that and they go, we'd love to, we're spending so much time continuing the education of new programmers when they come in to give them this expertise. We think that should be in the university and the university turns around and says, well they already have that like 800 semester hours taken in the degree, how long do you think they want to be in college to get a BS degree? When am I going to stick it in or what am I going to take in the current curriculum to add that in to the curriculum? So, consequently we work in a world where producing engineers and programmers and so forth and they don't have these other aspects, they don't have them polished enough and that's a very finite number of people that actually do and corporations of course, try to grab them and retain them but you know, they get to go around and write their own paychecks.

Dave: What advice would you have for someone who wants to enter the security field?

Francisco: Be a hacker. You know, when I look at a lot of the upper echelon of the hackers that we see publicly especially speaking at conferences like Black Hat and DefCon and RSA and SANS and derbycon and everything else that's out there, kind of more the rock stars of the security industry if you will, you know. You look at them and by enlarge a lot of them are self taught. Many have degrees the degree maybe something to do with Computer Science, it maybe Microbiology, it doesn’t seem to matter but their true aspect of really understanding how they’re breaking into things comes from tha fact that they are hackers, the true meaning of the word is to hack at something, right. So, how does the MTA work in transmitting mail? How does it interact with DNS? And that’s very interesting but what if I did this other thing, oh look I broke it, or look I just made it do something it wasn’t designed to do, right. The engineer who built it had a task to accomplish, right and the task was accomplished but unfortunately part of the task wasn't synched of all the other ways the world that somebody could possibly use that. We have lots of wonderful conferences where you’ll see some senior people stand up and talk about look you have to have the right mindset to work in the security industry. Part of that mindset has to be you have to look at things differently than everybody else. It’s not something that you can generally put through school to do; a lot of it is art, right. And I Think it was Kemensky who stood up on that stage and used to hold up a one of the metal dollar coins that you get in the casino and of course he had one because we were in Vegas at DefCon. And he would hold it up and say to everybody in the audience, what is this, and of course, everybody starts yelling back, it’s a dollar, right. And then he goes, no, what is it, and then of course the next step of like you know, your big bang theory kind of nerds in the audience starts yelling back, well you know it’s a semi metallic, you know, circular coin.. and they get like, they think the answer is to become more descriptive of what the device is and then he sits up there and says, no you’re all a bunch of idiots. It’s whatever I need it to be. If I happen to be at a restaurant and the table is wobbly, it’s a shim that keeps the table from wobbling, right. If I happen to be in an old home and the fuse is blue, I can jam it into the slot and now it’s a fuse, right. And he goes through all the different things that this object in his hand can be and the point is it’s whatever I need at the time if I can adapt it to do what I need to do. And that really is the main mentality that you’ve come through with. The other aspect is really come with the attitude into the industry that you want to enable, right. I think we saw an entire generation of security coming through, we still see lingering pieces of it where they think their job is to stand and tell people what they shouldn’t do. Don’t do this, you won’t be secured. Unfortunately, business doesn’t react well to that and that you know, we could argue that maybe one reason why business team, you know, business security teams are very big, nobody wants to, the guy that shows up in the operational development meeting and just, you know, profuse everything that’s being brought to the table, right. You know, get involved in the community beyond, I'm going into my job every day, and I run security for XYZ Corporation or work in security for XYZ Corporation. There are so many free and open groups that are out there whether they’re online so you’re doing them virtually and you’re building a rapport and you’re learning and you’re reading people's research papers and so forth, to you know, in your own communities. You have great programs like Bsides for example where we see, you know, these are small micro security conferences often taking place in the same locales and other major security conference but they’re free to attend hence they use the term Bsides so it’s the B side of the record, right. You know, unfortunately, I think a lot of the new people coming in don’t understand records anymore but, so, you know, go to those. They’re free and you actually have really top level presenters coming, you know, I'm not unfamiliar with speaking at Bsides. I love to speak at Bsides. It’s very old school to me. It’s what DefCon used to be back in the day, you know. And you see a lot of really well known, well respected security researchers speaking at this because they want to talk to the people coming through and the people rising through the ranks to help spread some of that knowledge and network with each other which is of as you and I know is super important with whatever your career is. But get involved, this is more than just I do security and I go in and my job is like, you know, comparing firewalls and routers. Getting into this career, it's a career it's a lifestyle and somebody should understand that when they come in.

Dave: I think a lot of it is about loving what you do and having an appetite for just getting as much as you can and learning as much as you can because this is constantly evolving. You have people out there who are very, very smart, who are constantly trying to break these operating systems, break these hardware appliances. If you don't stay on top to this, you will fall behind very quickly.

Francisco: Oh absolutely. Or you'll find the nitch that you absolutely love. It's a passion, you know. Like a huge fan of the different conferences that go on and meeting with the different groups. We even have, I'm in Austin, Texas so we have a particular group that's run by HT Moore and HT created this group, man I don't even know how long ago and its call AHA. and it used to stand for Austin Hackers Anonymous and I'm not sure what the more PC name is that they changed it to but I'm aware that they changed it so if he's listening to this HT can tell me later what it really stands for now but literally it's a once a month and you have little 2600 meetings and other meetings and all different cities that take place where they have similar venues. With this particular one, everybody has to speak at some point. If you come, they'll make you stand up and speak in front of the entire collection of people. And they don't care if you want to get up there for 10 minutes and talk about how much you love World of Warcraft or what is your favorite TV show. But generally speaking most people get up and talk about their security researcher or something they're working on outside of their current job that's very interesting. Because of Austin has this growing InfoSec community. We actually wind up with a lot of very hard hitting security researchers that get up and they're working on their presentation and they're working on the presentation of the material they've been putting together and research and you're actually seeing a preliminary versions of their talks and so forth, that maybe later you'll see at some of these very big conferences like Black Hat where you're going to have to spend several thousand dollars to actually go and attend and watch the final presentation. So just fantastic. The community really does support itself; it also eats itself so you also have to be kind of careful.

Dave: What's your definition of an Elegant Workflow around security?

Francisco: That's tricky though it depends on the context but generally speaking, I think early in my career I thought if you wrote a policy, then everybody should follow the policy and therefore you were then secured. And after I've got hit in the head several times with a brick, you know, I realized process is really worth it and the process is actually what is the business process at first talking about, you know, doing security inside of the corporation. And that is, I don't care what it is. What I have to do is I have to sit down with, you know, a business unit leader and say, great, you make widgets, walk me through how you make widgets from concept of widget to sourcing parts for your widget to building your widget to distribution and sales of your widget and the great part about that is that's actually security when we start talking about because by going through that process I can help them find deficiencies and those deficiencies are of course repeating the process the same way every single time whether that’s digital or physical. And by doing that every single time, I can then write policy based on the actual process not the other way around, right. People used to interpret policy generally showing up and say great I got a peg board filled with circle holes and now you got square pegs, but here’s a pocket knife start twiddling and that doesn’t work. You can't just make everybody readjust their pegs for you. But you can go and learn what their pegs look like by going through that process. Build a policy that goes along with it. Now the great part is actually both enables the business processes to go through and you can disguise security. Now it’s not making people do security I’m just hoping that you have a repeatable process. And then if something steps off the path of that repeatable process we either have an opportunity to update and say, oh there is a variation to process that’s also acceptable or we have a security breach, right. And by doing that its really great because you can also start to understand what are the drivers of the business unit leader that you're speaking to because I can write a new policy for them. I can even help them with procedures but if I’m not actually looking like I’m on their team and I’m helping them do whatever it is that they want to be doing which is generally how are they getting their bonus is what that that translates to for a preferably not doing corporate speak. How can I help them get that bonus that they’re looking for right and that’s speaking everybody’s language, how do I help them with their pocketbook, right. So, from a corporate executive standpoint, that’s usually the position that I will take when I’m starting to look at well how do I get a division more secure or a dysfunction of the company more secure? And that is to really start looking at the processes, what are the driving factors behind what they’re doing, how are people benefiting from this process overall, right. They probably have MBOs that are tied to what it is that they’re doing so if I can facilitate that so that it operates better so that it hit those MBOs all the time and at the same time it’s now built in security, it’s a win all the way around. And it’s not even sugar coating a pill right they don’t even know that they ate it, right, So, at the end of the day you really wind up with really good security at that point or its very easy for you then to audit the security at the location because you know exactly what that process is supposed to be and your policies are based off of the realities of that process, right. So, it’s kind of a long one to ground about way of answering that but really looking at what are the business drivers and going from there.