Crime Still Pays: Winning the Network Security Arms Race

VALERIE ST JOHN: And from the show floor of the 2009 RSA Victory Conference welcome to TechWiseTV. I'm Valerie St John along with Cisco Solutions experts Rob Boyd and Jimmy Ray Purser.

JIMMY RAY PURSER: Hey folks.

VALERIE ST JOHN: We have commandeered the Cisco booth thanks to our gracious hosts although we really didn't give them any option but to be gracious hosts.

ROB BOYD: Ah but they let us in.

VALERIE ST JOHN: And we're talking about -- this is really going to blow your mind.

ROB BOYD: Wait for it.

VALERIE ST JOHN: Are you ready? We're talking about security.

ROB BOYD: Who'd a thunk?

JIMMY RAY PURSER: Ah, who'd of -- yes.

VALERIE ST JOHN: And our specific topic is Crime Still Pays, Winning the Network Security Arms Race. Well guys, there's never a dull moment in security, right?

ROB BOYD: No, there's not.

VALERIE ST JOHN: The threat is always dynamic. I'm going to pass the torch over to you guys but first this question, what do we need to be worried about right now today?

ROB BOYD: Well that's going to be the full focus I think throughout the episode and the thing is, okay, so here's the situation. We always track top 20 vulnerabilities. If there's anything we enjoy doing in security it's making lists and ranking them and then re-ranking them and then comparing our lists. But I mean in all reality when you see some of those things, you can compare the trending. We are seeing a trending for 2009 eclipsing, now just four months into it, anything we've seen in 2008.

JIMMY RAY PURSER: Oh yes, absolutely.

ROB BOYD: But what I'm curious about and let's be fair. I want to make sure anybody who's not familiar with your background both from a security perspective, you're a security knob, can I put it that way? Security researcher...

JIMMY RAY PURSER: Yes, that works, that works, yes.

ROB BOYD: By hobby, right?

JIMMY RAY PURSER: Right.

ROB BOYD: You do this stuff for fun. What are you seeing in terms of your honey pot network, some of the other professionals you work with on the backend? What are the threats that you're seeing that you think we need to spend more time focusing on now?

JIMMY RAY PURSER: Well you know that's a great question because one of the biggest threats that I'm seeing out there today is really folks are getting incredibly complex with some of the bots out there today. Some of the attacks out there are so much larger than just some of the basic arms spoofing, DNS spoofing, and still those still apply. Those still work but some of the other

threats out there are heavy duty, I mean it's like they're being done by state-sponsored-type of hackers out there. And man they are very in-depth, they're incredibly up to date and they're really, really tough to stop.

ROB BOYD: Well let me ask you about this because a lot of people throw out a term like, hey, you often need to worry about Web 2.0. And, one, it feels so generic and it feels so unspecific. What does that mean? If I say, hey, you need to worry about Web 2.0, how would you begin to define what it is I need to worry about in that regard.

JIMMY RAY PURSER: I'd say stop reading stuff from analysts and then after that I would say that Web 2.0 if you will is really -- what we're really talking about is data leakage and correlation. You know one of the things that really is a huge threat on the network, even if you're doing everything right on your network, folks can take snippets of what you're doing correctly and correlate all this stuff together from different news reports, stuff out of the anchor database, your DNS entries, everything around there that correlates this together. and get a pretty good idea of what's going on with your network. I use a great tool called Maltego which actually allows me to gather and correlate a lot of that information and I can make a pretty darn good guess on what's going on behind the firewall.

ROB BOYD: Well it's interesting, I think one of the things you always have to battle is -- the thing I worry about is someone that's just got more time and patience than I do. Because we're always busy and we're looking for the quick fix and so that's a lot to battle but things do keep changing. I want to bring in another security expert with us. Please welcome Pat Peterson, he's a IronPort security researcher. Thanks for joining us today Pat.

JIMMY RAY PURSER: Pat, what's up man?

PATRICK PETERSON: Doing good, doing good.

ROB BOYD: And also Patrick Peterson. Hey we've had you on the show before in 2008. Last year we were on a stage of similar ilk and well we're still here, we're still talking about security. Things must've changed. What would you characterize as being different from then versus now?

PATRICK PETERSON: Before I get to what's changed, I got to share what hasn't changed.

ROB BOYD: Fair enough.

PATRICK PETERSON: Bots.

ROB BOYD: Okay.

PATRICK PETERSON: In 2008 bots were the epicenter, ground zero for online crime and guess what? Here in 2009 bots are where it's happening again and I make a prediction. Next year we're going to be talking about bots, bad guys putting malware on computers, turning them into bots, figuring out how to herd them together and then make some money. That's what hasn't changed.

ROB BOYD: Well and so here's the thing. So I think we both made some -- I already see you're getting your...

JIMMY RAY PURSER: Yes, yes, no, I'm clicking.

ROB BOYD: Your glance, be prepared.

PATRICK PETERSON: Be careful where you click though.

ROB BOYD: So here's the thing. We say bots in a real generic sense and I got to think looking at anybody out here, you probably heard something that generic in a couple of other booths maybe perhaps as you're wandering around the RSA floor. So here's

where we want to go a little deeper. You're a security researcher, Jimmy Ray is a security researcher and I'm enjoying being in the middle of you two.

JIMMY RAY PURSER: You pick up the tab for beer.

ROB BOYD: Exactly, I'm more than happy to. The idea though is, what is specifically -- first of all I think the fundamentals of a bot, what are the key elements that we need to understand so that we can then take that a step further? Because I don't want to deny anybody the ability to fully get your geek on here.

PATRICK PETERSON: You bet, starts with infection. They've got some software, they want to run it on your computer, they need to infect it. Lots of ways to do it, that's where it starts. Once it gets infected and once they multiply and propagate, and then they've got to control it and make some money. Infect, propagate, control, make money, lather, rinse, repeat. You can make a fortune and cause all of us a lot of pain and even maybe lose a little hair.

ROB BOYD: Do you agree that is kind of the fundamentals? I mean are those the areas where if we'd looked at what's being done differently, if we were, and we will in just a moment -- you know Conficker obviously has been making the news. And we talked about what's different about Conficker that's driving results that as a security person you go, wait a minute, that's new, that's different. Let me go back. You've been analyzing this one quite a bit. It's been in the news quite a bit. Where do you give it some props, some respect in that same fundamental aspect?

PATRICK PETERSON: So you asked me what was different and I think Conficker is a great example of what's different which is a tremendous amount of criminal sophistication and specialization. I spend 24 hours a day sometimes before a security show researching these guys. Every time I'm blown away at how sophisticated they are.

ROB BOYD: What examples would you cite? And I'm going to get your opinion on this too by the way.

JIMMY RAY PURSER: Sure.

PATRICK PETERSON: So one of the best ones is you guys talked about vulnerability. Five thousand six hundred and thirty-three of them kind of makes me want to yawn. But one of those was what Conficker went after, a vulnerability in Microsoft products that allowed them to use a network-based worm to infect ten million computers. Now that's pretty good.

JIMMY RAY PURSER: And that's only in 87.

PATRICK PETERSON: Exactly and that's pretty good but it's not that sophisticated. But then what do they do a month later? They upgraded the code because they got control of these and now they were running a triple threat, network-based worm, USB and they were attacking internal corporate file sharers to replicate that way. That's pretty good work in 30 days and they weren't done yet.

ROB BOYD: So a commitment to continue is improvement you think.

PATRICK PETERSON: Absolutely, absolutely.

ROB BOYD: That's one of the elements you would cite.

PATRICK PETERSON: Later on they upgraded to Version C, 85% of the code was new. SRI did this analysis, 85% of the code base is new. How many people out there writing software, security or otherwise, have a new release with 85% new code? Well the criminals do.

ROB BOYD: Yes, we don't want to start expecting that out of too many vendors.

PATRICK PETERSON: NO.

ROB BOYD: Okay, fair enough, go ahead.

JIMMY RAY PURSER: You knew the thing about when I did some disassembly of Conficker B and C -- I didn't disassemble A because to be honest with you when I first saw A, I'm like who cares?

PATRICK PETERSON: You always wait for the execution to come in. You want to see good code. A might just be experimental?

JIMMY RAY PURSER: Yes, it was kind of -- I'm like, that's interesting but it's not really that interesting, you know?

PATRICK PETERSON: Yes.

JIMMY RAY PURSER: What really kind of stuck me about B and C was the incredible amount of knowledge that went in there. We're talking about folks that actually used algorithms from RSA like MD6. MD6 was released in October and the virus came out in October. They found out there was a buffer overflow at MD6 that allowed them to exploit it. We noticed that when they updated the C version, that buffer overflow was fixed, so you've got people behind this that are incredibly brilliant, that they understand Windows systems. Because Conficker does not run as an executable, it runs as a DLL and it's actually executed from rundll32 which is a file you have to have.

PATRICK PETERSON: Yes.

ROB BOYD: So turning off some of the auto runs, that's not necessarily going to help you...

PATRICK PETERSON: Right.

JIMMY RAY PURSER: Well it's not doing anything you know, and it installs itself as a service, so it keeps starting up. And so I've got people that are designing this -- people, a team -- that's designing this bot that understands the Windows architecture very well. They understand how to hide it really well. They understand how to secure it and they're following the perims to patch it. And of course Conficker finally did execute and it was this lame antivirus program which I laughed because I'm like, you know what? That was not what it was intended to do. That was obviously just something to kind of kill the bot. My concern is with that level of intelligence and sophistication, what's the next thing that's coming out? Because I thought Storm was the coolest bot I'd ever seen back in '04. I'm like, man alive, that was really something else. And I thought it would really take a big effort to actually get something to beat that and I couldn't imagine in a million years that Conflicker did and does what it actually does. It is unbelievable, it's an incredible engineered bot. I've never seen anything like it, it's really amazing.

ROB BOYD: Do you agree with those points as far as kind of...

PATRICK PETERSON: I agree completely, impressive as hell. MD6, when I heard about it, I thought it was a joke. I didn't actually know there was an MD6. And these guys are not just putting it in their bot -- ten million computers that are me, you, my mom, my grandmoms -- but then they're patching it as soon as the vulnerability's announced.

JIMMY RAY PURSER: Yes, the same week.

PATRICK PETERSON: The other thing that's really important to note is that one of the biggest battles going on right now against the criminals is in command and control. They inspect the bot...

ROB BOYD: That's the exact thing you look for, right, to be able to identify it.

PATRICK PETERSON: Exactly.

ROB BOYD: You've got to check in somewhere.

PATRICK PETERSON: Exactly, they infect the bot. That's not how they make money. They've got to tell it, send some spam, steal some keystrokes, infect your neighbor. They've got to be updating that software all the time. Writing the patch doesn't get it patched, they've got to control it. So what are the good guys doing? The Conficker Working Group, a lot of security researchers are figuring out how are they talking to that bot? Let's interrupt it. What do the bad guys do? They say, we'll talk to 500 domains every day and you've got to shut down all 500. We did. They upgraded it. Now we're going to talk to 50,000 domains every day. You've got to go register 50,000 domains a day to keep up with them and, oh, that's not enough. They've put another peer-to-peer protocol on top of that to try to keep control of the bot net and keep us from cutting off the communication between the bot and the criminal who wants to make some money. It's impressive as hell.

ROB BOYD: Well there must be some smart people that are making more money doing that in that market versus a legitimate market and therein lie some of the problems which is trying to figure out, how do you motivate people to begin? Hey you're so smart, why are you pouring your energy in that direction? Well have you seen my cash?

PATRICK PETERSON: Yes, absolutely.

ROB BOYD: But are we starting to see some of the monetization now on the Conficker side?

PATRICK PETERSON: We are and Jimmy Ray mentioned that one of the biggest mysteries of Conficker is it created one of the biggest, most successful bots around. For six months they didn't make any money off it but just recently Conficker started downloading another bot called Walladeck. And it started downloading this fake spyware, Spy-protec, that basically flashes ups lots of warnings and says, you're infected, you need to buy my software to clean yourself up. It seems rinky-dink but the studies that we've seen show that the people doing that are making millions every year because consumers don't have the backgrounds to know the difference between a legitimate warning and somebody who's tricking them. So it's the first thing that they're doing to make money. I wish I could say it was the last but I don't think so.

JIMMY RAY PURSER: Well wait a minute know because you and I disagree here then. So do you think that that was the intended target of Conficker, was to download Walladeck? I mean we saw that back out in January and then it be the (inaudible). Because when I saw that, I'm like, that's a fake payload.

PATRICK PETERSON: No, I think they are an equal opportunity money maker. They've got the platform of ten million PCs. They'll do anything with it to make the money.

JIMMY RAY PURSER: Well that's true.

PATRICK PETERSON: I think this is going to make them some good money but it definitely wasn't what they had in mind. But hey, $100,000 or a million dollars or five million dollars, even it it's not their ultimate end, is a good stepping stone from them.

JIMMY RAY PURSER: Yes, that's true.

PATRICK PETERSON: But there's more to come.

ROB BOYD: I know you want to remain technical but I want to ask him a kind of business-oriented type of question. Do you mind that?

JIMMY RAY PURSER: All right, I'll sit here and daydream. I'll twitter here while you're doing that.

ROB BOYD: All right, strategery -- well, yes, exactly. Don't jump to the answer just yet. The idea is -- I always find it fascinating. You were just quoted in some of the announcements that have been coming out this week about what's happening in Russia and Ukraine. And some people are under the misconception that the same people who are designing these things from a

technology perspective are the same people making money from the spam or the other things. But it's actually distinctly different. They're providing services to each other. We've still got two minutes left. Could you give us a little glimpse into that world?

PATRICK PETERSON: Very quickly, Cisco makes networking gear. They don't necessarily make the chassis or the chips for every one. We work together with partners. The criminals are doing the same thing. Someone figured out how to infect PCs but they don't actually have the business model for this fake spyware removal or the business model for sending spam, for fulfilling pharmaceutical products. So what we've seen is the growth of organizations like a GlavMed or like a Spamit where they say, we're in the business of making money off bots. Sign your bots up for our affiliate program, send the spam for us, we'll take the credit cards, we'll ship the drugs, and we'll give you a nice fat commission. They do it for pharma, they do it for the scareware/spyware. And their ability to work together as specialists in targeted areas makes them much more successful and dangerous than if each criminal organization had to do everything soup to nuts.

ROB BOYD: It's amazing how much it literally mirrors real life, real business principles. These guys have marketing programs, they've got people following up. I think some of them are running help desks and things of this nature to make sure that the machine keeps turning and such like this. I think the key takeaway here -- and thank you for your time by the way -- is the fact crime still pays. I mean it's cheesy, I realize. It's the title of the show but that's what we do. We write this stuff so it stick together. So good information, good stuff.

VALERIE ST JOHN: And gentlemen, we'll take a pause on that very optimistic note. Switching gears here a little bit, the Cisco security framework gives you total visibility and it gives you total control. We'll take a look at keeping you safe coming up.

VALERIE ST JOHN: And we're at the RSA Security Conference in San Francisco talking about, yes, crazy as it sounds, security. A security conference seems like a pretty safe place so why don't we talk about...

ROB BOYD: It's a good place to begin talking about that.

VALERIE ST JOHN: SAFE. Lets go with a safe horizon.

ROB BOYD: All right, absolutely, and obviously you're referring to safe being the SAFE version 2 which has just come out which is the new architecture for security. Cisco's been doing this for quite a while. I think a lot people -- I'm amazed at how many customers have actually built a lot of their architecture against these best practice documents because they're tested, because they're worked on. But there's some fundamental differences in how they're being approached and I want to cover those. One of the things that jumped out at me just from an ease of understanding the complexity that surrounds trying to do security from an end-to-end perspective, from this taking every device into account and all the things that you want your network to do, but it's this notion of they divide it nice and clean in between control and visibility. And actually not in that order, visibility and control, and specifically -- and I took some notes here -- but it's this idea that you would, under visibility which to me has always been about, how can you stop something if you can't accurately identify it? So you've got a level of accuracy that's required there.

JIMMY RAY PURSER: That's the problem, right? I mean that's...

ROB BOYD: So both you've got to have visibility, identify how do you classify your users, your devices and all those things that are occurring, and then stepping into the control framework to say, now what do we do about these things?

VALERIE ST JOHN: So you've got a lot of modules here, potentially seven but I understand you're going to narrow it down for us to talk about campus edge, and I'll let you take it away.

PATRICK PETERSON: Thank you very much Valerie.

ROB BOYD: Yes, here's the thing, right? So there's seven core modules associated with the SAFE blueprint.

JIMMY RAY PURSER: Right, right.

PATRICK PETERSON: I don't think we call it the blueprint any more actually, that's a dash back.

JIMMY RAY PURSER: Yes, I don't think we do either. I think you're absolutely right.

PATRICK PETERSON: I mean we still call it SAFE.

JIMMY RAY PURSER: I think it's just called documentation, design guides or whatever.

ROB BOYD: But the module's always like -- because I think for one if you ever look at these things, there's an overwhelming layout of all the different points of presence in the network you potentially could or should address. But they broke it in so that you can say, you know what? For my particular risk situation, I am concerned with the Internet. I'm concerned with how I structure my DMZ. I'm concerned more with reliability and availability and things of this nature. So you can pick and apply it in the situation that makes sense to you, right?

JIMMY RAY PURSER: Right, right, right.

ROB BOYD: What kind of things -- specifically we're going to dive into the Internet module because we can't cover everything here. There's not enough room on this show and we've got one segment to play with. So with the time that we've got though, as you look at the Internet Edge module, what are you seeing in terms of best practices that you always agreed with and some things maybe that even surprised you?

JIMMY RAY PURSER: Well you know here's the thing. The terminology that's used in the SAFE documentation is Internet Edge. And it kind of really caught me off guard a little bit because that's a different way to look at it. I mean typically I'm looking at the Internet as a demarcation point and what the SAFE documentation does is it's actually saying, you know what? Look here, this is the edge part of the network. This is an ingress/egress point where we can apply some pretty good controls that have really been battle tested and time tested, that type of stuff. But it really depends on how you're connecting to the network or how you're connecting to the Internet, where your peering arrangement is with your provider, that kind of stuff.

ROB BOYD: I want to say I was kind of surprised you wanted to dive into this particular one because to me when I think of Internet Edge, that's a pretty time-tested thing there, right? You've got inside/outside, it's usually pretty well defined when you talk about that module.

PATRIC PETERSON: Yes, not really.

ROB BOYD: But you think it's something that was worth diving into. You think there's some best practices that we need to be looking at there?

JIMMY RAY PURSER: You know there really is because there's some things from the folks. You know the people who do the work know the work. I mean that's always been my argument for awhile. And the folks that are working with the Internet are our providers out there, our service providers that are looking at the threats and they're saying, you know what? Here's what we're doing to keep redundant and mitigate a lot of the problems that we're having at this higher layer. You know we have BGP4 peering arrangements out there. Well BGP4 does have some issues there that make it open for different denial of service attacks. So we've partnered with these folks and said, okay, look, if we did a time to live, then we could actually set up our TTLs and really prevent some of that injection from happening. And yes, that would be great if once we could make the protocols stronger and all that stuff but for right now this is what works. Providers also decided that, you know what, an access control list is really not enough. We need this new access control list, this I Access Control List, this Infrastructure ACL. And I mean you could imagine what other ACLs must look like. Well we can still take that same principle and now move it down to our network because it's been bulletproofed and (inaudible) tested and really implemented.

ROB BOYD: So as we're talking about this edge model and before we get into the IACLs, because I know I want to get to that and you're going to show us a few things here, but there were a couple of things that were listed as threat vectors in this particular area that you wanted to make sure that we got some lessons around. Data leakage and modification...

JIMMY RAY PURSER: Massive.

ROB BOYD: Unauthorized access and ID theft...

JIMMY RAY PURSER: Yes, huge.

ROB BOYD: The network side, what is left, so we'll talk about that -- it seems like that might be kind of old -- and this idea of abuse and service disruption. What areas in there do you think we're not focusing well enough on?

JIMMY RAY PURSER: You know a lot of the stuff actually has to do with, even denial of service attacks we're causing on ourselves, you know, just some misconfiguration and things of that nature. I mean we mentioned that in Segment 1 about all the vulnerabilities and stuff and if you think about it, here you are. You're a security administrator and you're doing everything right. You're trying to fix your network, you're configuring everything. And there could be a simple vulnerability, a zero data that somebody discovers and they're able to skirt their way through above your overflow, an iframe, whatever the case may be, and they're able to exploit your network in a way you maybe never known. I mean you see all the (inaudible) released. Who's got time to read all that crap, man?

ROB BOYD: No one's reading it. I think that's one of the challenges.

JIMMY RAY PURSER: No, of course not, and I mean that's what -- some dude over at Microsoft put out a paper on what he called the Defender's Dilemma where it's the attacker's advantage and the defender's dilemma to what part of the network am I going to defend. And this massive attack surfaced. Where am I defending? And my attackers can pick any point around that circle to kind of come in.

ROB BOYD: Well they've only got to find one way in, right?

JIMMY RAY PURSER: Well you can find one way in.

ROB BOYD: Yes, we have to protect everything.

JIMMY RAY PURSER: Yes.

ROB BOYD: Okay, so we understand that principle there. You mentioned ACLs, this one threw me off as well and I noticed this as I was going through the updated documentation. All this stuff just came out this week, so something to take a look at if you've not updated yourself, this stuff continues to get better. ACLs to me are old school. I mean everything -- we've been down that road, it seems kind of dry, kind of static. What is it about -- obviously you were talking about IACLs which is Infrastructure ACLs. Can you explain what the benefit to that is? And maybe we can use that as a takeaway point for something people here could chew on to go apply in their own situation.

JIMMY RAY PURSER: Well you know ACLs are really the meat and taters of security. It's what we're kind of really starting out and to kind of carve and move some traffic. And you've got to look at it kind of as a binary function, like we're doing a And function. We're saying that this And this equals a one, a pass or a fail condition. And that's really what we're looking at in a ACL, so that gives us a lot of power because hackers still have to follow the same rules that you and I do to communicate. That's what makes systems open, is that we've got a defined set of rules. And the best hackers I've ever seen in my life that I've worked with and chased down and went to court to prosecute, that kind of stuff, are the people that really don't understand a thousand gajillion different tools. They understand how stuff works, they understand how to deliver payloads in ICMP. They

understand how to take an MP4 stream and then know that, in a typical MP4 stream, I've got a lot of buffering in there that I could insert packets in. I could do covert channeling and I can use these standard protocols to slip my crapware between there and slip through your network. I know you told me not to say crap, I'm sorry, anyway. But you know it's people who really understand how things work and that's where these zero days come in. And the new infrastructure ACLs are trying to account for that behavior.

ROB BOYD: I was waiting for you to come back around on that because I thinks that's interesting what you're saying but does ACLs apply to that in terms of mitigating actions, that's going to help in that? Because you obviously are setting yourself up to say how we can do those differently?

JIMMY RAY PURSER: Well, yes I am.

ROB BOYD: Well take it away Captain.

JIMMY RAY PURSER: Thanks buddy. You know what? ACLs are kind of one of those things where they're kind of like head lice. You get a little bit of them and then they start to grow like crazy. And there's VACLs, there's...

ROB BOYD: It would help if you'd cut your hair a little more often.

JIMMY RAY PURSER: Well you've got to have a place to keep it you know.

ROB BOYD: Yes, all right.

JIMMY RAY PURSER: And well I'm in Wisconsin, so I got to keep all the heat in I can. You know you've got VACLs, you've got ACLs, you've got RACLs. I mean there's all kinds of ACLs out there today and IACLs are really no different Rob in that they're not really a feature as much as they are a way to do access control lists. There really is no feature that I can go in there and say, set config iacl. It's really a way of doing an access control list that allows us to really shape the traffic. Let me show you what I'm talking about.

ROB BOYD: I was also curious, do we know if anyone ran it past Apple? Are we allowed to call it an IACL, or do they have any kind of thing wrapped up on that?

JIMMY RAY PURSER: Well, you know, I don't know, maybe.

ROB BOYD: Something for me to check that out.

JIMMY RAY PURSER: That might be a future lawsuit. If there are any lawyers out there, that'd be a good thing to...

ROB BOYD: Yes, if you're watching at home and you want to make a few bucks...

JIMMY RAY PURSER: Yes, make a couple of buck, what the heck, you know?

ROB BOYD: That'd probably be something to check out, all right.

JIMMY RAY PURSER: We all need gas in the Ferrari. So I've got actually a notepad of an ACL that I actually configged here just before we came onstage. Now an IACL is very restricted, very defined for my network. It really does pinpoint exactly the behavior of the traffic I want because you have to understand these come from service providers. They've been bulletproofed, they've been tested and they are really watching. They know exactly what their traffic is, what they're permitting and what they're not based upon offsets, based upon fragmentation, really getting into the meat and taters on how this stuff works. Now the best way to figure that out is to write what we call a Discovery ACL and so...

ROB BOYD: Okay, this is a precursor to the...

JIMMY RAY PURSER: Yes.

ROB BOYD: Obviously the information gathering, okay.

JIMMY RAY PURSER: Because we've really got to kind of figure out what the traffic is on our network. It's hard to really know even using things like NetFlow and NBAR. I mean those are pretty good ways as well but I wanted to run this through an ACL and I want to see -- you know ACLs are just standard logical processor. It's an And process, this And that equals one or zero for pass or fail, so I want to run this through that same process to see what I'm matching. So typically the first thing I do when I go to set up an IACL is I'll set up a Discovery ACL. And you can see right here I'm doing access lists...

ROB BOYD: Do you want to point on here or do you want to circle with your cursor there to make sure we don't miss something? Oh, there you go, okay.

JIMMY RAY PURSER: Yes, there we go. So on this one what you see me doing here is I created an extended access control list and the key to this is that I actually got log statements at the end of each one of these. So I can actually track, see which one of these are hitting. I'm just doing a Permit, I'm not denying any traffic at all, I'm just permitting. And of course like any ACL, this is just a standard extended access control list. My last statement is my Permit IP Any Any and I'm logging this stuff, so I can see the behavior of my network.

ROB BOYD: This is part of the discovery process we're talking about.

JIMMY RAY PURSER: Yes, this is what I think is going on with my network.

ROB BOYD: Okay because I don't see any unique statements here yet.

JIMMY RAY PURSER: No big tools, nothing that big.

ROB BOYD: Pass the mic over.

JIMMY RAY PURSER: Now my next thing...

ROB BOYD: We've got to work on our dancing.

JIMMY RAY PURSER: That's true man. So the next thing I'm going to do is I'm going to check my hits. I'll do a Show IP Extended Access Control List command and what I'm doing is I'm looking at my hit rate and seeing what I'm matched in this area. So I'm...

ROB BOYD: Read this out loud because I'm just guessing that the people can't read this as well as we'd like.

JIMMY RAY PURSER: So I'm looking at my Permit EIGRP Any Any Log, I've got 76 hits on there. I'm looking at my ICMP, I didn't get any hits, nd so on and so forth, TAC AS, NDP, whatever the case may be. But the real important one to take a look at on this type of design is right here, Permit IP Any Any Log, how many matches I have here. Any matches in Permit Any Any means I've got 24 hits that I didn't classify up here and typically means I need to go back and redo that. I need to have it so that I have no hits down here or as little as possible because there's always an implicit Deny All at the end of an access control list, right?

ROB BOYD: Right.

JIMMY RAY PURSER: So what I'm doing here is I'm trying to limit what my wildcard hits are down here so I can build, an IACL is very, very, very, very granular.

ROB BOYD: It's specific, so the idea here is you're saying, I've got too many hits here. So you're just simply trying to narrow it down and start spreading what really is in this big pile?

JIMMY RAY PURSER: Yes, exactly right.

ROB BOYD: Okay, take us through it.

JIMMY RAY PURSER: Trying to (inaudible) it out, so as I do that, I'm going to actually set up a basic -- this is still part of the discovery. And I'm going to set this up with my source destination information. I'm going to start getting very particular how I'm setting this up but as you could see I'm actually putting my network addresses in here, where my traffic is permitted to. And I'm getting very granular so I can test to make sure this stuff is working like I want it to work. And then of course my Permit Any Any Log to -- that's the only thing I'm logging down here is that I'm going to catch anything that did not hit here and find out what else I need to do to change my network. Now this is not a command you leave on, any of these commands, for a long time. It's just to profile your traffic out and that's really what I'm doing here to validate. Now I've got some pretty good data and I'm feeling pretty good about myself and I'm ready to actually go down and start working on my IACL. A good IACL has four separate modules and four separate methods that we're setting this up as.

ROB BOYD: What are those four Jimmy Ray?

JIMMY RAY PURSER: Well I'm glad you asked Rob. So one of the things we're going to do is on Module 1, and we'll typically set this up. We'll set up four modules. Let me go ahead and see if I can lasso all this. Now on Module 1 what I'm doing is I'm really denying any use of any special IP addresses like RFC 3330 in any anti-spoofing countermeasures I want to set up. Now RFC 3330 is actually the stuff that is kind of reserved, we're not using. You know any of the 1918 RFC addresses are kind of embedded in there. I think I even got a sample over here real quick, so yes, right there. And so you could download this and actually look. There's a really cool table in here that actually shows...

ROB BOYD: Now is this stuff you'd find in the SAFE documentation, or this is a little bonus from you today?

JIMMY RAY PURSER: Oh no, this is all bonus stuff here. So you can actually download this and this will show you special case uses for different IP addresses that should be blocked in an address that's really used for only special things. So if you're not running cable TV on your network or any of that stuff, these are addresses you could almost block right off the top.

ROB BOYD: Want to block that, yes.

JIMMY RAY PURSER: (Inaudible).

ROB BOYD: No, no, they are but yes, you'd probably know I hope.

JIMMY RAY PURSER: If you've got to hack your own table router, that's a good one to look for.

ROB BOYD: So before we run out of time...

JIMMY RAY PURSER: Are we getting close?

ROB BOYD: We are getting close.

JIMMY RAY PURSER: Are you serious?

ROB BOYD: I know time always flies when you're having fun. How would you kind of bring us forward on this?

JIMMY RAY PURSER: Okay, so our Module 1 is really where we're denying special uses, anti-spoof stuff. So you can see that I've

got all those plugged in there individually. And in Module 2 is actually what I'm going to permit. This is my explicit stuff, this is the traffic that I'm letting through here. And as you see right here I've got some BGP statements in mainly because I was testing some of that stuff this morning from a hotel room. Worked pretty good too. And that's what I'm going to let through. My Module 3 is where I'm going to do a implicit deny to protect my infrastructure, so this is stuff that absolutely cannot go and access any part of my network. And then Module 4 is where I'm going to allow any traffic to transmit through. This the stuff I'm just allowing through, this is my escape clause right here, IP Permit Any Any.

ROB BOYD: You got to have that at the end.

JIMMY RAY PURSER: And there you go, and that's how an IACL is made up, four separate part. It's not a feature, it's just a methodology that's been time-tested by our service providers.

ROB BOYD: And that methodology is within the SAFE documentation and such, so...

JIMMY RAY PURSER: Yes, it's actually documented really well.

ROB BOYD: Okay, so this just being one small example of the things that you can get out of the SAFE documentation. If you're not reading that, final thought for an engineer that has never actually looked at this stuff, maybe you didn't realize the value.

JIMMY RAY PURSER: Oh man, you know what? The SAFE 2 documentation is definitely pretty happening. I mean that is some great stuff. There are really very specialized documentation to really match the area that you're focused on, data center, voice, wireless, whatever the case may be. And it's not a lot of marketing fluff in there, there's no, hey, buy Cisco and nuh, nuh, nuh. It really shows you the configs and how to set this stuff up and really take advantage of it. It's really cool stuff.

VALERIE ST JOHN: Great stuff guys. On that note, it's time for a little bit of a pause. Switching gears, the Worldwide Web, the Information Superhighway, the Interscape, whatever your term of preference. Of course I'm talking about the Internet and what is our interface into this massive matrix we all depend on so much? The browser, but is it friend or foe? That's next.

VALERIE ST JOHN: And online, on-demand, and on the go. And today onsite here at the 2009 RSA Security Conference, this is TechWiseTV, technology you can use from geeks you can trust. And let's flush this out a little bit. We were talking earlier; I've got the ever persistent Bot to worry about, right?

ROBB BOYD: Yes, yes, we're not letting that go.

VALIERIE ST JOHN: We've got the infrastructure design guides to kind of help us along here, but there's more to consider, isn't there?

ROBB BOYD: Yes, there is a lot more. And I think the thing that was fascinating to me was this notion of how much actually happens behind the scenes with your browser. If we go back and we look at it, we of course want to -- back to the interscape, not interscape, now I'm using Valerie's terminology, but this notion of mosaic, that was the word I was looking for.

JIMMY RAY PURSER: Oh, mosaic, yes. You're taking an old school, baby.

ROBB BOYD: Well, the idea is here, the browser opened up this world for us, right? It's made it easy, it's made everybody, including my mother, to get online. I can always tell when she's online because I get a lot of email.

JIMMY RAY PURSER: Oh, yes, yes, yes.

ROBB BOYD: But the thing I don't think many people understand however, is that it's evolved a lot. So although the view into it, you always think I'm viewing a webpage or I'm visiting a webpage. And it's all about me going to this one site, and it's a trusted site. It's a name like TechWiseTV or cisco.com or CNN or something like this, right?

JIMMY RAY PURSER: You know, I heard you could trust those geeks there.

ROBB BOYD: Yes, we are geeks you can trust. But the idea there is, is that all that's really happening behind the scenes? And this is where I wanted to get -- Kevin, if you could come up and join us. Please welcome our guest Kevin Kennedy, security geek probably day and night actually.

JIMMY RAY PURSER: Kennedy, are you kin to Ken Kennedy from WW Wrestling?

KEVIN KENNEDY: I'm not. I've heard that before, but, no, sorry.

ROBB BOYD: I thought about the WWF references on the show.

JIMMY RAY PURSER: Yes, you have, but I thought it was live, I could slip one in.

ROBB BOYD: Yes, there you go, sneak it on in. But, Kevin, how accurate is that? Take a seat, please. Let's understand what we're talking about here. A little coffee chat. Okay, so what is happening behind the scenes with the browser? I mean, I've kind of highlighted over it, but walk us through some more detail here. What do we need to know and how does that change what we are doing?

KEVIN KENNEDY: Yes, you're absolutely right. So most people think you type something into the browser, the URL into the browser, you're going to that site. The reality is, what you're getting, something completely different. You're getting the recipe for that site. So it's telling you all the elements that make up how to create what we're looking at. Here are the ingredients, so get a dozen eggs, some flour, some nuts, you whip it all together and you've got what you want.

ROBB BOYD: You've obviously never eaten at my house.

JIMMY RAY PURSER: I'm getting hungry. Somebody go get me a sandwich.

KEVIN KENNEDY: Go get a scone, yes, that sounds good. So on the website it's saying, hey, go grab this script from a server in the Ukraine, go up north, grab an image from a server in Canada. I've got this flash object sitting off on a server in China just for you. And the user sees none of this. They see the URL that they typed, but the fact is, the browser can go anywhere and get anything from any server in order to create that page. That's one of the things that's really powerful about the web, but it also creates an incredible challenge from a security standpoint to protect users.

ROBB BOYD: How many objects are we talking about here? I mean, are there just a couple, is it just advertising? Is it for legitimate non-advertising related stuff?

KEVIN KENNEDY: Common sites have 150 or more objects, dozens of different domains that all come together to make that page. And that's really the challenge that the criminals take advantage of it. What they're doing is they embed, you know, you've got your 150 ingredients to make a good webpage. They add the 150 first, which is a malicious script in the Ukraine. Your browser goes and fetches it. And all of a sudden just by going to the same site that you've gone to every day for the last year, you're infected. And it's happened to businessweek.com, it's happened to msnbc.com, thousands of other lesser-known sites, so it's a real problem.

ROBB BOYD: Well, so the vulnerability of this user being taken advantage of in a general sense, as I've heard you discuss it, it's this iFrame, especially the iFrame vulnerability. And I don't think a lot of people, including myself, could accurately explain exactly what that is. So I'm wondering, can you walk us through, what is the iFrame, why is it critical to the experience, and how is it being taken advantage of?

JIMMY RAY PURSER: You know, iFrame is really a very cool feature inside of a web browser in that it allows me to launch a

browser or another frame inside that web browser. Kind of a nested sub-working, if you will. And here's -- let me show you, I'll show you --.

KEVIN KENNEDY: I can tell you're a coder when you think, saying nested sub-routine is a way to explain it and in plain English.

JIMMY RAY PURSER: Here's a piece of XML code or some web code that I actually copied from our webpage techwisetv.com. And so you can see this is all pretty basic stuff. And by looking through here, this is what your browser's actually doing. You can see it's actually calling all these different commands, all these style sheet commands, which is also really cool vulnerability too. The cascading style sheets, oh, man, that's happening, but we'll save that for another show. But one of the things that I'm looking for, if I'm going to write an iFrame attack myself is, I'm going to look for, and I've kind of highlighted it. I'm going to look for a way to kind of exploit PHP mainly because it's easier to spell to actually the one I attach. And so the command I'm looking for, the PHP segment I'm looking for, is actually calling an iFrame legitimately and it's passing information to an array. Now every time I pass information to an array, that means I've got a lot of unsigned variables I can actually take advantage of and insert information into. So what I did was, is that I inserted a small piece of code in here that's an iFrame source attack and it's redirected everybody to jimmyraypurser.com via PHP, and I've got the frame hidden, my visibility is hidden, you can't see the display, and there we go. Now all of a sudden you're downloading my code or I can have this in here a 100 times and launch now a service attack on a web browser. So now maybe the people that are going to techwisetv.com, and I'm pretty mad about, let's say, I don't know, cisco.com. And I say, okay, I'm going to attack cisco.com and I'll just put everybody start connecting to here. If I put a 100 entries in here, I've got a 100 iFrames opening per browser, per everybody using, see how this scales across. It'll start overwhelming web servers pretty darn quick. So it's a simple attack that is really, really, really difficult to spot. It slipped past firewalls. It goes through the universal hacker access port, Port 80, and it's really tough to get through. So doing everything right. Still get you hit by something like this.

ROBB BOYD: Okay, good explanation. So this highlights I think, Kevin, what I'm curious about. I'm assuming, I don't know if you have more visuals -- can I sit down again?

JIMMY RAY PURSER: Yes, yes.

ROBB BOYD: I didn't know you had that actually.

JIMMY RAY PURSER: Oh, really?

ROBB BOYD: (Inaudible).

JIMMY RAY PURSER: (Inaudible).

ROBB BOYD: No, I'm glad you did. I'm glad I asked. But here's the thing, right? I think we often think of URL filtering as the way you address threats like we're seeing on the web, right? If I have web issues, I do URL filtering to protect me from bad sites. It seems very logical. I think what we're talking about here obviously, with the way he's saying that the code works, what you're taking advantage of is a very legitimate site can continue to do very legitimate business, but be compromised unbeknownst to even the site operator, correct?

KEVIN KENNEDY: Absolutely.

ROBB BOYD: So how do you begin dissecting that? Because I mean it's not seen even by the people that own the site, so who do you blame, how do you protect yourself, where do we start?

KEVIN KENNEDY: Yes, I mean, that's exactly the challenge. And you're right, URL filtering, it's great for acceptable use, it's not a security technology. And so when you look at how you defend this, you have to look at each of those objects independently. And you have to understand not just what it is that's interesting, but where is it? What is the reputation? Is that something that I can trust or is it something that I should prevent from coming in. And you have to do that, at a granular level, every single one

of those objects you want to inspect.

ROBB BOYD: Well, give us a peek behind the curtain because you mentioned reputation filtering.

KEVIN KENNEDY: Yes.

ROBB BOYD: We know that's something that we benefit from and we're starting to move this into more products from a Cisco side. IronPort brought a lot of this intelligence to us. Are you about to bring something else up we need to be aware of?

JIMMY RAY PURSER: Oh, yes, keep on talking.

ROBB BOYD: So move out of his way. But as part of the setup, I'm curious, on the reputation filtering; give me a peek behind the scenes. How are you guys determining this kind of thing because it still doesn't seem simple?

KEVIN KENNEDY: It's not simple at all. It takes a lot of data. And the thing that we're doing with Cisco is, we're looking across our entire install-base at Security Appliances. We're bringing data back in, we're augmenting that with -- and that's IPS, that's email, that's web. We're seeing all of that traffic. We're seeing all kinds of independent feeds. Five hundred analysts working around the clock to analyze this to find threats. And then we're also looking at things that are innate to the server. So we're looking at when was it registered? Who registered? Is it dynamic fast flux DNS or is it a static DNS that's been there for a long time? We look at all those factors and we're able to turn that into risks for it's very predictive, it's not reacting. It can block threats sometimes before they're even officially launched because you see a pattern of bad behavior, because you see repeatable trends, that sort of thing. So that is how Cisco helps to protect people, and we're using it across all of the security products or many of the security products, email, web. And now it's coming into the ASA and the IPS.

ROBB BOYD: I love that with the announcements this week, as we're taking that intelligence and spreading it. And it's not about how smart we are actually; it's leveraging a lot of the intelligence of customers, which I think is...

KEVIN KENNEDY: Exactly.

JIMMY RAY PURSER: Well, it's a dynamic backend is really what's tying this together to make this realistic, right? I mean, when we're really talking about setting the device up, it's not a static configuration that we kind of set it up and hope that a packet comes in here, magic happens, and all of a sudden I'm safe.

ROBB BOYD: Trust me.

JIMMY RAY PURSER: We're really talking about another team behind here that's actually researching, assigning a credit score, if you will, to these databases, to these resources and applying whatever control we have, which is pretty darn sweet. But I've got a question to ask you because I played around with the WSA a little bit and I ran some attacks through it and it caught them all. And I was incredibly impressed, number one, how fast it was.

ROBB BOYD: You're such a suck-up.

JIMMY RAY PURSER: Because, well, you know what, here's the thing though. It's because you have to -- and correct me if I'm wrong, right? So if we've got a network design here and I've got the Internet setting right here and I'm coming in, I've got to have the WSA in path for this to work. So it goes through my network, whatever, down here. And then I have my clients all connected up, so that all this traffic from my clients is passing through this device to actually get it to work okay. You know, I'm real skeptical of proxies unless I'm actually trying to hide stuff like (inaudible) or something. So for deployment, if you're sitting in a conference room and you're telling me that, okay, well, this is setting in line, you've got to setup proxies here. My first thought is, you know what, the last thing I want to do is sneaker-net all these machines or have my clients be able to just unclick and get out or use different browsers to circumvent what I'm doing here. How are you guys enforcing this traffic to go through this device?

KEVIN KENNEDY: Yes, so first of all, it's important to be a proxy when you think about how dynamic the threats are and how much knowledge it takes of what's going on in order to actually stop them. It's important that we be a part of that conversation, and that's why it's a proxy platform. In terms of how do you deploy it? Lots of well-known techniques you can use. WCCP redirection to do it transparently. You can use PAC files in the clients, very automated. And in terms of failure, yes, you're in the path, but you can load-balance on PAC files, you can use load-balancers. There's lots of ways to make this work seamlessly and still get all of those security benefits of being a proxy and being a direct participant in the conversation.

JIMMY RAY PURSER: Okay, well, that's pretty cool because that's one of the things that anytime I put --. If I'm designing a network and I'm putting something in path, the one thing I do, this is obviously a massive single point of failure in my network, so I probably want to run at least a couple of those in here. And the way I'm actually controlling redundancy or load-balancing through here, if you will, is with the PAC file. Because actually I have both of these listed here and the PAC files downloaded during the DHCP process, is basically what we're looking at?

KEVIN KENNEDY: Yes, that's one way. There's multiple ways. You can absolutely do the PAC file. You can put in ACE load-balancer in front of it. There's a lot of different ways to do this --.

JIMMY RAY PURSER: Oh, sure, a load-balancer, I didn't think about that. That's true, that is true.

KEVIN KENNEDY: Yes, so lots of ways to address. And you're absolutely right; you don't want this to be a single point of failure. Web is business-critical, that's why it's so important to hackers as well as businesses. That's why Port 80 is always open. You have to keep it open. You have to make sure it's there. Lots of ways, from a deployment standpoint, to make that happen without reinventing the wheel.

JIMMY RAY PURSER: So now just getting your recommendation then, so if I'm looking at a way to deploy this or whatever, what are some advantages of doing PAC files, WCCP. Because WCCP sounds pretty darn complex, depending upon your environment of course. Well, I don't think you'd ever want to static configure this stuff. But what deployment tips or guidelines do you recommend in say a 1500 seat type of company?

KEVIN KENNEDY: So a lot of this is environment-specific, so it depends on your priorities and that's why we support multiple modes. PAC files are great because they are using the built-in mechanisms for I'm a proxy, all of the proxy auth and all of that. It's fundamentally built into the technology, so it works very well. There's advantages to that. But there's people who want to do it transparently with zero-touch on the client, zero of anything like that, so WCCP is supported. There you're starting to go around and use different loopholes and how proxy auth works, and so it has a set of tradeoffs. We don't strongly prefer either. We like to work with customers to figure out what's right for their environment.

JIMMY RAY PURSER: That's pretty cool.

ROBB BOYD: How satisfied are you feeling, Jimmy Ray?

JIMMY RAY PURSER: You know what, I mean, I truly don't want to suck-up here, but coming from the IronPort team, I'm a big fan of the email appliance anyway. And you know what, that really takes a lot because I was a big Barracuda fan. I installed a bunch of those things. And when I first started doing your stuff, I'm like, no, I don't want to mess with it because I like this one. And then I heard from, actually from Samantha here, and she's like, well, you slapped me around a little bit. And sure enough, that is a lot better product. So I've been a huge fan of yours. I played around this for a little bit trying to hack through it, trying to slip some attacks in, and it caught every single one. And so I'm actually nothing but impressed, really great stuff.

ROBB BOYD: Well, Kevin Kennedy, thank you so much. This is good information. You satisfied him and -- oh, we got a round of applause. We don't always get that every time, Valerie, that's quite nice.

VALERIE ST JOHN: Great artistry, by the way, Jimmy Ray, very, very talented.

ROBB BOYD: We'll be selling those online later.

VALERIE ST JOHN: Great stuff, guys. Okay, remember when the firewall was king, the big man on campus, was a super cool thing to have? What happened? It was only briefly mentioned here today? Is it still relevant? Or put it another way, can we safely ignore it? Coming up next.

VALERIE ST JOHN: And from the floor of the 2009 RSA Security Conference in San Francisco, we are TechWiseTV and we're talking about what else, security. We commandeered the Cisco booth. Clearly Cisco could use a little bit tighter security, but nailing things down a little bit here.

ROBB BOYD: We're working on that, we're working on that.

VALERIE ST JOHN: We're facing new threats, right?

ROBB BOYD: Yes, yes.

VALERIE STJOHN: And we're going to have to come up with some new responses. But what's happened to the old standards? Have we completely put the firewall out to pasture? I'll let you take that one away.

ROBB BOYD: Thank you for that. So, Jimmy Ray, she brings up a good point. I think this comes up a lot because I think --.

JIMMY RAY PURSER: I probably should have been paying attention, huh?

ROBB BOYD: Well, I'll refresh you. That's all right. The idea from a security perspective is, is new threats come out. What's our answer from kind of a vendor perspective, and I put this, the industry as a whole. Well, I've got another box for you, right? I've got a really smart, fast box that's going to solve this next problem and I think we get this complexity overload, right? We have too much stuff coming in. So I do think it's healthy to look back and go, we started with SAFEs, we talked about architecture. We've talked about ways that things can be done differently. But if I think about how is the firewall change because it's still present in the network, so what are doing differently? We've obviously made some announcements this week about adding in the sensor-based network and that information into the firewall. And then we've also got the IPS, which I don't hear a whole lot about. IPS kind of being the -- to me, for the longest time, I think everybody just perceived that as the buzzword update from IDS, moving from detection to prevention because we thought that might sell better?

JIMMY RAY PURSER: I did. You know what, I'll be honest with you, first time I heard the term IPS, I'm telling you, I started laughing. Because I'm like I can write my own scripts to do HTTP resets, I don't have to buy another box. That's the dumbest thing I ever heard of in my entire life.

ROBB BOYD: But there's still some value there, right? Are we looking at it from the wrong angle? Because these devices, are we saying do need to throw them out, they don't have as much relevance because it's on to the new shiny thing? Are you saying that from a -- because again I'm trying to give you an excuse to set you up architecturally here. How should we be approaching it now based on the threats we've been discussing here today?

JIMMY RAY PURSER: Well, you know, Robb, it really depends on the type of network that you have, right? There's a really good reason for the term IPS. There's a really good reason for the term IDS. And IPS is really what we're installing in-line in the network. It is right in the middle of the traffic flow. It is at an intercept point to actually, via a very proactive measure in my network, to actually do countermeasures, to do some reconfigurations. And to actually interact with the traffic that's on that network and really take some action on it. And IDS is a passive device. It's actually listening on bridging that traffic all via SpanPort, via PassiveTap -- whatever the case may be. It's just sitting there gathering data. And I'll be honest with you, in today's network, I don't see, unless you're a security researcher, there's really not much of a need for an IDS out there today. If you need IDS, you don't want -- honestly, I want your money, of course it'll help our stock, but I would just download

(inaudible), configure that up and I'd watch my traffic that way.

ROBB BOYD: But that's just about visibility, right?

JIMMY RAY PURSER: That's just about visibility, that's it.

ROBB BOYD: And what's the point of visibility if you're not doing anything about it, which is why the marketing language caught up. But you're saying there's technology there too.

JIMMY RAY PURSER: You know what, because there's a lot of false/positives. There's a lot of ways to really trick an IDS and kind of flood it with a bunch of false/positives, and kind of slip your attack right between it, very common. I mean, that's kind of how we do it and stuff, right? An IPS, a little bit differently, it's installed in-line. But the mistake that I'm seeing right now, when it comes to folks setting up IPSs, are that there's a huge need for them, obviously. I would not setup a network without an IPS. There's no way in this world I would ever do it.

ROBB BOYD: Do you look at it still though as it's a visibility component primarily for you? Or why are you saying --.

JIMMY RAY PURSER: No, no, I look at it as a reactive piece on my network that's going to take action when things kind of start to fall apart. But the problem with it is, is that a lot of folks are setting up networks very redundant and very survivable. So my traffic is forwarded asymmetrically everywhere in this network. IPS will fail if you treat it like a piece of networking equipment. I cannot have asymmetric traffic flows going through an IPS and expect it to work correctly. Let me show you something.

ROBB BOYD: Yes, I was going to say, I feel a lesson coming on here. A little whiteboard maybe?

JIMMY RAY PURSER: Yes, let me show you what I'm talking about. One of the things that, you know, we were talking about Configure and one of the things, able to detect Configure but we may not be able to take the command and control. We may not be able to catch some of the updates but we can detect something else and the flows don't make sense. And so they're discarded as false/positives or --.

ROBB BOYD: We don't even know how to assign it to the actual part we're trying to --.

JIMMY RAY PURSER: We honestly don't know what it is. So we've got to be able to look at ingress/egress traffic on that same flow. So what I want to look at here -- let me open this up, I have now a handy-dandy slide here.

ROBB BOYD: Oh, look at that, you did prepare something again, did you?

JIMMY RAY PURSER: Look at that. Heck, yes, man, what are you talking about? Like Club Med. Let me flip this around a little bit.

ROBB BOYD: All right, I'm going to flip over here so I can see it better.

JIMMY RAY PURSER: All right.

ROBB BOYD: Oh, oh, we're still sideways.

JIMMY RAY PURSER: Yes, take me just a second here. But one of the things that needs to be kind of considered when it comes to setting up an IPS, is that really it's not another piece of networking equipment. It is really, it's a specialty product that needs to be configured as a specialty product. So for example if I'm setting up trunk links, okay, look here. So I've got my IPS units right here and they're setting in-line. Now typically, and this actually comes from the SAFE documentation too, so we're staying right on track, you can download this stuff and read it.

ROBB BOYD: Way to stay with the theme, I like that, all right.

JIMMY RAY PURSER: But, yes, I'm pulling for our team, baby. So what we're looking at here is basically, this is my traffic flows. And what I'm doing first off is considering the fact I don't want any asymmetrical traffic going through here. If I have traffic coming from a client, it needs to go out, go back to the Internet. And then as it comes back in -- let me change colors here, let's go with blue -- as it comes back in, it's quite possibly going to be assigned to this switch. And it needs to come back through, it needs to come back through this very same IPS and be detected because I need both these flows on that same IPS, right?

ROBB BOYD: So you're saying to do it right, really restricts your ability to even route your network in the way that it's efficient for the network.

JIMMY RAY PURSER: Yes, yes, exactly. Because a lot of people are saying, well, now I can't -- if I want this to work, I can't be redundant in my network. And that's really not (ianudible) at all.

ROBB BOYD: So then you're forced to choose security or availability?

JIMMY RAY PURSER: Exactly -- and where are you going to -- I mean, come on --.

ROBB BOYD: It's not a question we want to have to answer.

JIMMY RAY PURSER: No, man.

ROBB BOYD: So, Jimmy Ray, what would we do?

JIMMY RAY PURSER: Well, I'm glad you asked, Robb.

ROBB BOYD: All right.

JIMMY RAY PURSER: You know what; I typically always want to setup an EtherChannel between by devices. Because I really like --.

ROBB BOYD: Just for sync or data?

JIMMY RAY PURSER: Both. I mean, I really want to make sure that I've set these EtherChannels up. But setting up an EtherChannel, the problem with it, what happens is, is that each switch is going to calculate my EtherChannel and it's going to assign a hash based upon a predetermined value that it has, so it's going to hash out all this traffic. And so each switch, as I get traffic, will assign a different hash value, and my traffic can flow asymmetrically and that's what I don't want. So typically what I'm going to do is, a couple really quick things to make sure that this works in a redundant fashion.

ROBB BOYD: Okay.

JIMMY RAY PURSER: Check it out. All right, so first thing I'm going to do is, I'm going to put an IDS switch, or an IPS switch, right here in the middle.

ROBB BOYD: This is between the information exchange on those?

JIMMY RAY PURSER: Yes, yes. And then I'm going to use VRF right here, and I'm going to VRF a couple of these VLANs together. In this instance I'm VLAN-ing VLAN 14 and 15. In this instance I'm going to use VRF and I'm going to VRF VLANs 12 and 13, so I can actually group these in an instance. So I can actually handle that traffic accordingly and I can actually balance that a little bit better. Now, as my client starts to communicate...

ROBB BOYD: It still feels like you've got an issue with the asynchronous on this so far.

JIMMY RAY PURSER: You're absolutely right. And so what happens is, is now, and as you see, that's just based on colors to make it a little bit easier. I've got this VRF instance assigned over here, this VRF instance assigned here, and then this one there, and that one there. So I've actually got my groups broke down and assigned, for instance on each one of these IPSs. And so the trick is, is I want this hash when it runs through this center switch, this is where I want my hash value computed. So that wherever this traffic goes out and where it goes back in and it re-computes the hash, it's going to be the same, and that traffic's going to be assigned to that same link that it actually came out.

ROBB BOYD: And you're hashing it to make sure you're looking at the same traffic and it's not been spoofed somewhere else, right? Is that the primary reason?

JIMMY RAY PURSER: It's so you can know which links to flow the traffic out of because --.

ROBB BOYD: Oh, okay, you've got to match that back up. So you're depending on this to re-identify the routes?

JIMMY RAY PURSER: Yes, because then the EtherChannel, what EtherChannel is going to basically do, very rudimentary how it's going to look. It's going to look at these links, it's going to assign a binary bit value to those. It's going to look at the source and destination information and it's going to run an exclusive OR process on those. And that exclusive OR is going to assign that traffic down one of these links, and that link is going to get a hash value. And so no matter what that traffic is, my hash value is always going to be the same. So coming back out, I want that hash value to be assigned here because I always want to leave and come back on the same exact interface, the same exact port trunk. And that's the key to making sure that this IPS can see both sides of that conversation. That's how we actually want to make sure this works correctly. So in this instance I've actually got this size where I want to set my traffic up. So let me show you how this works.

ROBB BOYD: Everything you're talking about here, by the way, while you're finding that pin, are we still in the realm of things that are just based purely on design? So not that I don't want us to always sell more Cisco stuff, this is designed, for the most part, right?

JIMMY RAY PURSER: Yes, no, I don't really care whose products you buy. Obviously I own stock in Cisco, so if you buy some that's great. But if I don't, I really want your network to be secure. I don't want the bad guys to win. I don't care if you buy if from Juniper or whoever the case may be.

ROBB BOYD: It's hard to shop online if the network's down anyway, right?

JIMMY RAY PURSER: Exactly. So you've got to design your network accordingly. And I'm using VRF over here to group my VLAN instances together to give me a way to assign common hash values. And to configure this stuff up, I put a switch in the middle as really my hash computator is really what it amounts to.

ROBB BOYD: So that's really the only device we've added in this situation, assuming you're already running IPS?

JIMMY RAY PURSER: Yes, yes, yes. And so as I'm setting this up, and this is real important, when you're setting up an IPS, a lot of people actually will set this up; they'll treat this as another switch or router. And they'll say, well, I just setup a port channel here and I'll channelized these links together, I'll plug them all in, and life is good. And that's not how it is. Because I'm going to have my traffic, my hash value, if I don't put this switch here, my hash value is going to be computed differently here and it's going to be computed differently here. So my traffic is going to be asymmetrical. I'll come out this interface, I'll come back on this interface. And this IPS could drop valid traffic or it could mss traffic that's really pretty dangerous. And the same on the other side. So I've really got to be symmetric in how this traffic flows to make sure I get both sides. I've got to be redundant; I've got to be symmetric. It looks complicated, it really honestly isn't. I mean, really, it takes time to set it up, but it's really not that tough.

Crime Still Pays: Winning the Network Security Arms Race

ROBB BOYD: Well, you know what I love, as we're running out of time here -- I know, I know, you always complain. But it's just the notion that we're talking about security architecture. And we've kind of come full circle on something here. We talked about some new threats. But in actuality, as much as all of us have new shiny hammers that we want you to buy and to solve the latest new issues to address, there's some good old school knowledge that gets applied correctly in certain situations that's going to bail you out probably better than you're maybe giving it consideration for. So in this situation you're saying, don't blame the box, it hasn't failed. The firewall, the IPS, these things can be very relevant as long as you understand what they're capable of doing and where exactly they're going to do their best job.

JIMMY RAY PURSER: Yes, and real quick, before -- I know we've got to wrap up --.

ROBB BOYD: That was a beautiful summary and you did it to me again.

JIMMY RAY PURSER: It was great, but I've got to finish up something, man. Look, if you're going to plan for an IPS out there, one of the most important things to do is when you're setting up your redundant links in here, is to make sure you know your traffic, know thyself, right? So when you set these up, make sure you run the command test, EtherChannel. Whatever your IP address source and destination is, that switch is going to spit out what link that traffic's going to go back and forth, and then you know how the hash is going to work and if your traffic is going to work fine. And that's all I have to say.

ROBB BOYD: I just wish you were more passionate.

VALERIE ST JOHN: Guys, I hate to stop Jimmy Ray. Once he gets going it's like putting a wall in front of a really cool windup toy, but we got to go. So we left our audience with a lot of information, their eyes are glazing over. Boil it down for us. What are the key takeaways?

ROBB BOYD: They're glazing over with excitement, I should hope.

VALERIE ST JOHN: Of course they are.

ROBB BOYD: I think here's the thing I want to walk away with, and there's about three things, including an update from our friends at Cisco Learning Network. The idea here is that we've been talking about web threats. We're talking about understanding new ways, new things that we need to be aware of and how we're going to address those. And make sure we're not ignoring those threat vectors and some of the things that were identified. One of the beauties of the IronPort products and stuff, permit me a little more selling here for a moment, is that you can try before you buy. You've got different ways of making sure these are right for your particular situation. At the same time, don't ignore the architectural pitch. So the SAFE documentation, it's free, it's not Cisco-specific per se, although you will find a lot of very good information of course, as far as how you can be effective with it in a Cisco environment, but don't ignore that resource. A lot of smart people put a lot of very good test and methodologies, good stuff to take advantage of. Final point just real quick, for all you security lovers out there, Cisco Learning Network just announced that they came out with an update to the CCIE security lab. So for those of you who are waiting for that economy to turn back around, and yet another way for you to continue to push it yourself, position yourself for the upturn from a career perspective as well. So I would say, that's something to be checking out too is the new CCIE security lab.

VALERIE ST JOHN: Very good. And wrapping up here for my colleagues, Jimmy Ray Purser and Robb Boyd, I'm Valerie St John, and thanks for watching TechWiseTV. And thanks to everybody here in our audience for joining us. And to checkout future episodes, find out what's going on or to see a complete archive of previous episodes, go to the Cisco Interaction Network at cisco.com/go/interactive.