NETEVENTS

CLOUD INNOVATION SUMMIT

First Draft

No More Mr. Nice Guy!
Tightening the Screws on Cloud Security

Iben Rodriguez

Director of Cloud and Virtualization Testing

Panellists:	
Steve Pate	Chief Architect, HyTrust
Paul To	Director SDN & Cloud, Spirent Communications
Dennis Moreau	Senior Engineering Architect: Software Defined Security, VMWare
Hongwen Zhang	Co-Founder & CEO, Wedge Networks

All right, good. So Paul's the last one, we'll introduce him first. Paul from Spirent. We have Steve Pate over there, raise your hand Steve, HyTrust, formerly HighCloud Security, some of you might know him from there. Dennis was with RSA recently and he's moved over to VMWare. Hongwen, you're with Wedge Networks.

I'm Iben Rodrigues. I work at NSS Labs and I wanted to take just a few minutes to talk about NSS Labs. Then we'll get onto some questions here for the panel on cloud security.

So NSS Labs has been around for 22 years and I'm pretty new there. I'm helping them adapt their testing methods for cloud and virtualisation. As you can see from the products, they have a huge history of testing products, some of you might know them. They're recently transformed themselves into more of an analytics and research firm. So we're now providing data on the products we're testing and how they work into a cloud security environment and a virtualised environment.

We're the only research firm that actually test the products that we write about. We look at the attack surface of the customers' environments to show which products would work best based on those attack surfaces. Just some examples of how we collect that data.

We have a list of applications, we've got about 100 apps right now that we test, multiple versions of each different app. Those are exposed in the virtual connections to different parts of the world and then we let those exposed machines get attacked, we capture the attack data of how an attacker actually is able to compromise the box. We record that attack data in a big data warehouse and then we can analyse this data warehouse to show which exploits were able to bypass which security controls.

This allows you to make smarter decisions about how you're going to purchase your hardware. We've heard a lot about [defence in-depth] and for the traditional enterprise with the solid perimeter, we had that [M&M] security model where you protect all your sensitive assets inside your network.

That might have worked well when you were just going to buy a firewall and some detection solutions for it, but now with cloud and virtualisation, you have data spread all over the world, you've got people using mobile devices, BYOD. How are they going to have a firewall put around them? You can't do it any more. So we've heard the phrase, the identity is the new perimeter.

Which products to purchase is just becoming more and more confusing, if you have a distributed hybrid cloud environment.

This is just a summary of the output that we have from our tests. We do product analysis reports which are just for individual products, like a specific firewall or a specific device that we've tested. The security value map, I have a slide I'll show you on that. Then a comparative analysis report, is where we have multiple products that were tested.

Some examples of tests we have coming up this year that my team's working on are public cloud assessment, we're testing various [hypervisors], different virtual firewalls and other virtual appliances. So a CAR, say we did a virtual appliance test on [ADCs], we would have a CAR for all of the ADCs that we tested to compare them to each other.

This is an example of the security value map, it's customised for each customer's environment. You can tune the values that are important to you, if you're more worried about performance or malware detection, you can adjust those and have it - the graphs will automatically update for you.

This is an overview of the ThreatCAST system I was explaining, where we have those thousands of virtual machines exposed throughout the world, collecting that threat data. We provide that threat intelligence to our customers.

This is a brief bio for each of our panellists that wanted to - I don't know if you guys want to give a quick work of introduction, just to give us some of your background, what sort of things you guys are working on? Let's start with Steve.

Steve Pate

Hi, I'm Steve Pate. I'm Chief Architect at HyTrust. I've got about a 30 year background in building operating systems, file systems, volume managers, encryption, key [managing] solutions across a whole host of different platforms.

Iben Rodriguez

You've written a couple of books.

Steve Pate

I've written two books, one on the UNIX kernel, one on UNIX file systems and contributed to several others.

Iben Rodriguez

Right on, Paul?

Paul To

So I'm Paul To, I'm Director of SDN and Cloud at Spirent Communications. I'm responsible for solution strategy as well as go to market. So Spirent is a test company, our mission is to help the industry speed up adoptions of all this new, cool stuff that everybody's talking about. SDN, [NF3] and cloud. This is a very important topic about security because we're in [unclear] times that it is one of the leading reasons for people to adopt SDN and NF3 and also it's one of the big adoption barriers.

We are inherently very interested in helping the industry, how do you measure and quantify all these security measures and performance of all these firewalls and security functions that are now weaved into the fabric.

Iben Rodriguez

Yeah, it was the same challenge we're having now with cloud as we had with virtualisation. I worked at VMWare back in 2005 and was surprised that so many people didn't use it. It was such an exciting, new technology. But there was a lot of fear, uncertainty and concern with performance. You always hear about VMWare being slow or something, well all those concerns have gone away and most everyone's using VMWare nowadays in their architecture somewhere. Testing has helped quite a bit to...

Paul To

Testing is all about quantitatively removing the fear, uncertainty and doubts.

Iben Rodriguez

Exactly. Dennis?

Dennis Moreau

I focus mostly on utility computing security, especially as it applies to events threat response, privacy, compliance sort of issues. In that, we're very interested in how we get off of defence, how do we move from relatively static constraint testing, determining whether or not we've provisioned correctly to knowing that something is secure and compliant in every [state] intuition might be driven. So very, very focused

on the dynamics, how to use them to cultivate evidence-based trust, rather than faith-based reliance. To use that to be able to get off of defence.

Hongwen Zhang

Yeah, I'm Hongwen Zhang, Wedge Networks. Wedge Networks really believe that today's security issues can be effectively managed if you actually have this horizontal layer that Martin talked about. This horizontal layer is emerging in many, many different places. So [our] specialty and our product technology platform, it's tried to really [weave] the security - advanced security functions into this horizontal layer by being a hypervisor or common natural transport to make sure that all the trillions of devices can be protected.

Iben Rodriguez

Thank you, let's see if I got. Okay, so I'll just leave this one up here. Which one do you like better? It's both the slides there.

So let's see, we have some questions that we wanted to go over today. I like the Goldilocks zone, it's a pretty interesting goal. I think it's interesting, the reference that Martin used on his slide was [SETL] - everyone know what that is, right? Search for extra-terrestrial life. I don't' think we've found any yet, that I know of, or they haven't told us, at least, if we have.

But the Goldilocks zone is sort of a fable or a myth, so how is it that we think we could actually do this? Is it attainable? We're here to talk about what companies are actually doing with cloud security today and how there are actually some success stories. There's also, of course, a lot of problems you hear about in the news with different attacks and takeovers and compromises. But a lot of those are normally a perfect storm type situation where a number of factors have colluded together to allow these attacks to happen.

So maybe Goldilocks zone is attainable in cloud security with certain technologies. That's what we're going to talk about.

If we treat the datacentre as a large distributed data plane, were would be the best place to put the security controls in that data plane in the large datacentre? How do we - what technology is available today and where are we going?

So we already talked about where we're going, I think Martin has a great vision for how that can be embedded into the hypervisor. Some of that's there today for detection, but what do we see for the distributed datacentre? I'll just go down the list, let's start on this side today.

Yes?

Hongwen Zhang

So I think that really, with the merging of the datacentre, cloud centres and we see a very good places where security can be centralised, which is very, very important for us. We are talking about more connectives go to the cloud and that's go to by the

basic believing of Wedge Networks, basically that if we can secure this part, we would actually secure the whole digital life of the whole planet.

So back to the comments there, I think that really there are many different practices and myself, also, I am the co-chair of the CloudEthernet Forum security group. We have identified several [use] cases, including data privacy, network security and security from the cloud, all those things. I think that is a very good area emerging and there are some very good, promising technologies emerging there.

Iben Rodriguez

So what about existing technologies? Can we talk about some of the things that you guys have seen? Dennis?

Dennis Moreau

Yeah, we've seen very rapid advances in security-centric technologies. Whether that's web application firewalls, next generation firewalls, IPS systems, sandbox detection of advanced threat stuff. All of this stuff has shown significant advance and is deployed in datacentres. Yet what we're doing isn't working [unclear] be crystal clear whether it's the Darkleach exploits of hosted Apache servers or the gumbler exploits of hosted WordPress sorts of instances.

In those circumstances, nowhere is the cloud value proposition working better than as presenting either targets for malware or distribution vectors for malware to endpoints. What's missing in this circumstance is an effective way of dealing with the complexity that occurs from doing this. The complexity comes from several places.

When we bring the cloud into the datacentre discussion, we are bringing in multiple provisioners into the stack. You no longer are provisioning everything you would have in an on-premise enterprise datacentre. So there's a coordination of multiple actors.

There is also the dynamics associated with it. You don't see all the additional movement, load balances, mechanics with scale-up, scale-down, all of the stuff that goes on behind the scenes. A reduction in visibility and an increase in movement.

Then finally, you wind up having to coordinate a number of technologies, all of which have different ways of expressing policy. An IPS system's Snort rules versus the signatures I deployed in my endpoint antivirus versus those things that describe payloads as they detonate inside of sandboxes. All different yet they all need to be aligned in order to provide an effective, layered defence.

We've got to drive the complexity out. What I'm seeing as the principle problem, then, is the architecture for being able to deploy protections, keep them aligned through movement and be able to give me enough context to have an actionable result from all of those logs that are going to be telling me about what's going wrong and where. If I don't have that context, I won't be able to move.

So we see that as the fundamental problem but also the fundamental opportunity for moving from a place where we're bound by complexity to a place where you can actually use the dynamics to our advantage.

Iben Rodriguez

So then it sounds like the tools are there, the components might be present but it's really challenging today to integrate everything and make it...

Dennis Moreau

The Legos are there but the decision support environment and the actionable context are wanting. That is the source of our problem.

Iben Rodriguez

Steve or Paul, do you want to add to that?

Paul To

Yeah, I want to add to what Dennis said. Security is always - security guys always talk about the layered defence. It's always the layer approach. I actually, if I map that to what's going on in this software-defined [ext] world, where everything is virtualised and then everything is programmable, and we see at each of the horizontal layers; at the compute layer, at the storage layer, the overlay and the underlay, each of those horizontal layers have programmability. That's one of the main goals of all the new architecture is separating abstract and control planes and so on.

So I think there are actually huge opportunities where at each of those layers, if you look at - from a control point of view, each of those layers can become very much a coordinated policy enforcement engine. Every single layer, to parallel the layered defence that might be needed for a given situation.

Then also, not this enforcement but also from an analytics and intelligence point of view, I think there would be huge value if each of those layers can provide the intelligence necessary to do threat assessment, intrusion detection, all those kind of things.

Iben Rodriguez

Today they're all managed separately though and even each vendor has their own separate...

Paul To

Adding to Dennis, I think there's a huge opportunity out there to really look at how we orchestrate all these layers.

Iben Rodriguez

Yeah, so back to the previous panel about openness, there's probably a value there just from security. We had a question about the security in openness.

Paul To

Absolutely and I think there's a huge opportunity for the industry and from the different players of the different layers to really work together to provide a cohesive solution.

Iben Rodriguez

Right, we see some of that happening now.

Paul To

Yeah.

Steve Pate

So from my point of view, I think we've consolidated risk over the last several years. We've gone from tens of thousands of physical servers managed by many administrators in different buildings, in rooms with locks on the doors to single box storage and compute with thousands of virtual machines, managed by a single or a few separate administrators.

So we've now gone to the point where we've got administrators with uncontrolled amounts of power. If you think about the Snowden effect, he was siphoning files off at the top level in the stack. If he was running at a virtual administrator layer, he can just steal the virtual machines without any other administrators...

Iben Rodriguez

That wasn't a one-time thing, it happened over a period of time.

Steve Pate

Yeah, over a long period of time. It comes back to what Martin was talking about earlier in terms of [leased privilege]. We've got to have a lot more control over administrators, we've got to understand what they're doing. Things like a two-man rule and multi-factor authentication which needs to come into play. Shionogi was a great example, a disgruntled employee was thrown out of the company, sat inside a coffee shop, got back into the network and deleted all of their production virtual machines.

For one administrator to be able to perform that level of - something catastrophic like that in the infrastructure, that's pretty bad. We've got the same in the cloud and we've got a whole set of issues around virtualisation, especially with data security, that people really don't understand.

Iben Rodriguez

Right. We talk about big data a lot, more and more companies are using big data to collect information about everything that's happening. I've heard eBay, IRS, Facebook of course, they're all using big data to see what's going on with their

consumers or their targets. IRS can collect information about your Facebook activities and if you are reporting one thing on your taxes yet you look on Facebook, you're driving around a new car and all your personal life, they go, hey, this guy might need to be audited or something.

So that's pretty scary. You have administrators with access to all this data, we talked about the NSA problem. How do you protect big data? There are some tools we've talked about, encryption, is that something that's feasible, today, to do in the cloud? Or in a local - both public cloud or private cloud, and how does that work?

Steve Pate

Yeah, absolutely. Think about encryption. So typically people will only deploy it in the datacentre if there's a need, there's a regulation; [Hepper], PCI, FISMA. Their thinking changes when the data leaves the building. So think about notebooks, that's the place where encryption's deployed on physical disks and...

Iben Rodriguez

Yep, they use whole disk encryption.

Steve Pate

Whole disk encryption, so if somebody finds a notebook, boots it up, they're not able to get access to the data. I also find, I think, it changes when you go to the public cloud as well. As soon as my data leaves the building and goes to the public cloud, I want to be in control. I've now got a different set of administrators who manage my data, replicating it, backing up, I don't know where that data is. Some of them may offer encryption but if they hold the encryption key then it's as good as putting your jewels in a safe deposit box and giving both keys to the bank.

Iben Rodriguez

So we're talking about what technology's available today to deploy. We've got big plans for the future but is the technology available today to encrypt your data at rest and own your own keys and recycle those when you need to?

Steve Pate

Yeah. I'll let the others add to it. But you can encrypt in multiple layers in the stack from application level, database level, down at the operating system level, inside the file system or the volume manager. So that's inside the virtual machine alone.

Iben Rodriguez

That means I could use that in a public cloud as well as in - whole disk encryption used to be you'd encrypt your data store. So say you had a SAN or a NAS, you'd need to encrypt the whole thing or part of it to put the VMs on there. But now, in the public cloud, I don't have the ability - like if I'm using Amazon, to encrypt Amazon's disks, right? They don't offer that. But how - so I can actually do that in my...

Steve Pate

Well Amazon provide encryption of S3 storage, they don't provide encryption of EBS which is where all your instances are running. But you can encrypt inside the guest and you can control the keys.

Iben Rodriguez

So the technology's getting there?

Steve Pate

Sorry?

Iben Rodriguez

The technology is getting there to where it can...

Steve Pate

Oh, the technology's there today.

Dennis Moreau

[They're] available now.

Iben Rodriguez

That's what I'm trying to find out. So...

Dennis Moreau

So you can do [A4] in terms of getting just in time decryption for your compute instances in the cloud where the customer holds the keys.

Iben Rodriguez

The customers hold the keys?

Dennis Moreau

Yeah, and in your big data instance in particular, you can look at [Gazine] who's very, very good at being able to enable cryptic shredding so that you don't have to worry about that footprint of your data that went out on that Hadoop store that has all this direct-attached cash. It's encrypted there as well, throw away the key and guess what? All of those cash instances, don't - no longer worry about them.

So at least the orchestrated versions of implementing this stuff were there. It takes management overhead, it's not nearly as [unclear].

Iben Rodriguez

Yeah, yeah. We didn't say it was easy to use but we'll get there.

Paul To

Yes, definitely. I think that data encryption is actually the - a balancing act. Let's face it, a lot of cloud services, at the service, they have to share data. That's really the contradictory part of this whole thing. There are certain industry academic research areas that we are very, very interested in, for example, that allow you to indexing data but not necessarily have complete visibility to data. That can have a very large impact to how things can be organised.

Dennis Moreau

These are in direct tension. If I encrypt everything fully then I limit how much de-duplication I can take advantage of.

Iben Rodriguez

Sure.

Dennis Moreau

Those are in tension and so there is going to need to be that specifically policy directed decision on how to balance those competing interests.

Iben Rodriguez

Right, some things that you just can't do both of, technology competes with it.

Paul To

If I may inject some controversy, there are a lot of international folks here and I want to say, in the new era of Snowden and NSA, what is the trust level in terms of encryption? Again, I think that's - if I flip it around though, I think there's an opportunity for the industry to add another layer of security and defence on top of encryption. Because encryption, I think, is not going to be the only answer. But things like being able to have a policy engine where I can specifically specify where I don't want to locate my storage and VMs. Maybe I want to avoid a certain geo-political region.

Iben Rodriguez

So that's the other question I had. So we've talked about some of the technologies that are available today. I also want to do a time check. Do I have a hard stop? Okay, good.

So is - we've talked about geolocation and network path selection quite a bit but that seems to be more of a future thing, from my perspective. Is that technology available today where I can - I know at Amazon I can say, I'm going to be on the east coast or the west coast but I don't really know for sure where my data is, what machine it's on, who I'm sharing that machine with, what disk drives it's on, et cetera.

So how do I handle geolocation? Paul, you were - I would start with you.

Paul To

I think the technology is there, whether they adopt it for these specific use cases is another question. But I think we are seeing - when I travel - when you and I were at the [LA 123] event, we got a lot of feedback form European providers where they are seeing that there's going to be this rise of geo-politic co-region based cloud providers and I think...

Iben Rodriguez

Right, we see that happening a lot.

Paul To

There's going to be a need for this kind of policy based enforcement of where I want to locate my VM and data and also where I want my data communication path to [unclear].

Iben Rodriguez

There's been a lot of reports of US cloud providers stepping up their game. The topic here is No More Mr. Nice Guy, right? Well they've gotten the message because it's hurting the bottom line of the cloud providers with - there's an exodus of international customers not wanting to use US-based cloud services.

Paul To

We're seeing things like OpenFlow have no issue in terms of - on a per-customer per-application basis, specifying the path. Also, VM place and storage placement's not an issue at all in terms of things like software defined storage and so on.

Steve Pate

So talking about geolocation - sorry, I'm the one who didn't get the company pitch in going first. So we provide controls around your virtual infrastructure as well as encryption key management for public clouds as well. So we already have, built in our product today, route of trust support using Intel's TXT. So from the BIOS through to the hypervisor, all the way up, we can judge what is known as a good [known] host. So if there are any [unclear] involved, we'll prevent your virtual machines from spinning up.

We're also launching products in June of this year built around Intel's geofencing. So we can prevent your VMs from spinning up if they're not running in the right location. Now if you think about your data sovereignty, where my data's moving, regardless of what Amazon or other providers tell you where the data's stored, when we get to the point where we can spin up a VM, get access to the data that might be encrypted and refuse to deliver an encryption key because that data's not residing in the location you want it to. That's where we need to get to.

Iben Rodriguez

So that's almost there, not there yet?

Steve Pate

It's very close.

Iben Rodriguez

Right, interesting. So I'm curious, why - if all these technologies are available, why aren't more companies using them? What's the hold back? I was a security architect for many years and I had challenges getting customers to use technology - simply technology that was available. What are you guys seeing out there?

Dennis Moreau

Well one of the reasons it's not pervasive is it's not cheap. Someone's got to take ownership of those TPMs, assign the [escrow] keys, do the management and the implications on utilisation are significant. If I'm confining things to geolocation, I'm no longer optimising purely for server utilisation of under-utilised capacity.

So the places where this really sings are in the specialised and the hybrid providers who've differentiated on providing exactly this kind of capability and visibility. [Unclear].

Iben Rodriguez

Okay.

Hongwen Zhang

I think that's really the issue with security. It's funny, there are very good security algorithms, the trouble is trying to apply them into the places where you can apply. If we [unclear] sounds very scary, like security is a major thing. But if you look at it, [unclear] truly secure, a country-wide network with these hundreds of millions of devices, that's even a major nightmare to do that.

So I think, really, if you look at it, distribution mechanism is a very, very important to contribute a security solution in at least horizontal layer is really the key.

Dennis Moreau

Yeah, scaling that route of trust for a distributed system is the core [objective].

Paul To

I would also offer that the - it's a cultural issue. So on one hand, when we talk to customers, so service providers, datacentre operators, when you go in to meet with them, the people that are operating the inter-datacentre connectivity, the WAN guys, it's a different group than the intra-datacentre networking guys. Then the server

people is a different group and then security is probably a different group, and then NF3 is kind of a grey area.

We see the parallel happening on the vendor's side.

Iben Rodriguez

Each team has their own management systems and procedures and whatnot.

Paul To

Right, and we obviously, VMWare are doing the compute stuff and then you have storage and then all the overlay guys are doing their own stuff and then you have the underlay. That's why we're part of this forum called the CloudEthernet Forum. The mandate is really looking at bringing all these layers, people together and constructing this - what I call vertically integrated use cases. I think security should be a leading one to drive this talk between all these different operating domains and vendor domains.

Iben Rodriguez

I wanted to open up for some questions, too, we have a few minutes left. Anybody have any questions? No, I have one more.

Maneet Divash

I have a question. [Maneet Divash], NetEvents. Both - two people briefly mentioned key management and I think this is something that when you blithely talk about encryption and obviously the issue of utilisation's another one - blithely talk about encryption, there are a lot of dependencies and there are a lot of issues involved in just encrypting stuff. Perhaps you could explore some of those?

Iben Rodriguez

Yeah, so to - just some background, use Dropbox for your stuff, they say that your data's encrypted but you don't actually own the key. You can't go in there and change that key, you don't know if they had employees come or go or disk drives were lost. You have no visibility into that. So how does and enterprise manage their own keys? It seems like a very complex issue.

Steve Pate

So encryption's actually pretty easy. There's a lot of open source tools out there, a lot of the operating system vendors provide encryption tools. Pretty much none of them provide key management. Even Microsoft with SQL Server, Oracle with...

Iben Rodriguez

Just write the key on a post-it note, put it on the administrator's...

Steve Pate

Potentially, Oracle, you stick it in a file, they call it a Wallet, on the same system. So not very secure.

Iben Rodriguez

Never store your keys inside the vault, right?

Steve Pate

Yeah, exactly. So you need separation of keys and data. So if you look at the PCI specification or anything else that governs data security, you need to keep the keys somewhere else. Everyone's heard of Bruce Schneier, the famous cryptographer, he said, key management is typically the Achilles heel of an otherwise great solution. If you think about a lot of encryption solutions, laptop, you've got to be there to type in a password to unlock the key. You're typing a password, you're weakening the key.

So you really need those keys to be separate. Then if we're thinking of our datacentre or we're thinking about public cloud, where do those keys reside? There are several options. You can store the keys in your own datacentre, there's a lot of key management solutions out there. You can run your key servers in the cloud. Many of the encryption vendors provide keys as a service. So your keys could be stored in a different cloud from where your data is.

Then if you look at some of the capabilities like Amazon are providing, they have a thing called CloudHSM where they've got physical appliances that live inside Amazon's premises, so you can store your encryption keys in there and they're provided by FIPS certified hardware, so Amazon can't get in and even if they try and get into the box, the keys are going to be shredded.

Dennis Moreau

A key observation there is that when you do encrypt, the encryption mechanism, both the key protection, key distribution, key generation, all of the stuff associated with that has to work at scale, just as reliably as the rest of the system, because lose the keys and...

Iben Rodriguez

Yeah, you lose all your data.

Dennis Moreau

...the ultimate denial of service. You can deny all data.

Iben Rodriguez

It's almost, yeah, if you don't have that ready to go then there's probably more risk than encrypting.

Dennis Moreau

Incredibly so. So in all of the circumstances; scale-up, scale-down, fail over, business continuity, you've got to be able to have that continuity of capability. That complicates the heck out of what would normally be relatively simple, I've got my keys, I manage them in a local, single vault.

Iben Rodriguez

Right. One last - we've got a question here?

Anthony Caruana, CSO Magazine Australia

Anthony Caruana, CSO Magazine Australia. If anything's happened since Snowden's revelations last year it's that the world has become far more complicated and the line between good guys and bad guys is very blurry now, with governments obviously being openly involved in much more surveillance. The Australian Government is talking about releasing legislation to compel organisations and individuals to hand over encryption keys.

So if that happens, are encryption keys becoming useless? If the government is going to force us to hand them over for their own surveillance purposes?

Dennis Moreau

This has pushed us to precisely what we see in the market dynamics, that there is a strong movement toward the encryption keys being handled by the folks who are responsible for and interested in protecting the data and are not available to the service providers and the plumbing. So while the federal agencies and legal agencies may indeed subpoena access to the data, they're going to get encrypted data. They will have to go to the folks who are liable, who are impacted, who have legal standing in order to get the keys to look at the data.

I think that's a direct response to the concern that you're directing. In that case, encryption becomes your only way to not spread your legal and accountability exposure for the data when you're using outsourced capabilities. Does that make sense? Is that responsive at all?

Anthony Caruana

Yeah.

Iben Rodriguez

I can tell you from a technology perspective, there's a few new encryption solutions - I don't know if any of you use Kali Linux for example? But they recently - they've always had whole disk encryption as part of their Linux distribution but now they've introduced the idea, during install, that you can configure a nuke key. So when they ask for your encryption keys, you can actually give them the wrong one and it will actually delete all of the keys, thus making your data unavailable.

So if you have a backup of your data somewhere else, on your local datacentre, tape, whatever...

Anthony Caruana

[If the] law gets passed, that would be breaking the law [unclear].

Iben Rodriguez

Well, there's the law and then - I'm just saying, from a technology perspective, there's other technology solutions out there. I don't know how many people have been subpoenaed for some data and said, oh, well we can't find those records. They're gone, they're missing, the server isn't in use any more.

Steve Pate

Move the data out of Australia.

Iben Rodriguez

It's not in the country any more.

Steve Pate

But at the end of the day, if the service provider has the keys, the government comes in, they'll give them the keys. If you hold the keys, the government comes to you, you get your legal team in place. That's as good as you can do.

Iben Rodriguez

It gives you a chance to do something about it. So the one question I was going to ask if there's no more questions is about supply chain management. Can you guys just briefly talk about the need for supply chain management when it comes to cloud security? Because this is one of the topics that's come up quite a bit and I don't think people understand how important this is.

So let me give you an example. So when you use a cloud provider now, you go to Amazon or any of these guys, you have to use one of their images. If they don't have an image, you have to make one and it's a lot more work to make a new image for a virtual machine and put it up there. We've had this problem in different customers where they are using images, they don't know where they came from. So supply chain management would be, where do you get your firmware from, where do you get the operating system images, how are the systems build?

You have a lot of regulations like PCI that says, you need to have a documented build process. It's not enough to just go and say, I got this image from the internet. They're stored in DropBox or different places. So let's discuss real quick about how to deal with that.

Hongwen Zhang

I think that one critical piece of this is the trust level. How do you actually define trust levels between all the components? How do you enforce the trust levels? I think that from networking management point of view where you have the networking data flowing back and forth and how you enforce that [at the] choking point is very important.

Dennis Moreau

In this domain, passing and accumulating either the hashes or the identities of the parts isn't enough. You also need to be able to accumulate both the testing and the over time behavioural awareness and the reputation to make that work.

Paul To

So I think the emergence of this app store idea, you can go to Amazon and you can buy a whole variety of third party images that you can load in your virtual private cloud. We're also seeing the same thing, the idea of OpenFlow and SDN controller, the really interesting thing is you have this ecosystem of application developers that can develop on top of the SDN controller.

So there's also going to be an emerging app store ecosystems. So I think there's a lot we can learn in terms of looking at the parallel of the Apple App Store which is the [unclear] app store.

Iben Rodriguez

This comes down to trust again, so even back to the open discussion. Open solutions can have trust associated with them. They have a reputation.

Steve Pate

So just to end a positive note, it's worth looking up Dell SecureWorks did a study of all the Amazon - well, most of the Amazon AMIs about three or four years ago. The majority had vulnerabilities in, SSH key pairs that shouldn't be in there et cetera. So they worked pretty closely with Amazon and now there's a much stricter set of requirements you have to pass to get an AMI in the marketplace.

Iben Rodriguez

So just to be clear, what that means is that if I downloaded one of those images before, they found that there was SSH keys which would enable someone on the internet who knows that I'm using this image to SSH to my box without my knowledge.

Steve Pate

Exactly.

Iben Rodriguez

Now they've cleaned up their act and there's standards now?

Steve Pate

Yeah, so prior to putting an application in the marketplace, Amazon will scan it for malware and viruses and vulnerabilities. Not perfect but it's much better than where we were before.

Iben Rodriguez

All right. Well we're going to end this. No More Mr. Nice Guy. There's a lot of technology out there to enable you to use the cloud nowadays and it's just challenging to figure out how to use it. Great, thank you.

[End]