

**NetEvents EMEA Press Summit Barcelona 2011 Palo Alto Networks**

# Thinking Secure? Or Just Feeling Secure? The need to accelerate creative innovation on this side of the law

*Date: Mon, 02/21/2011 - 14:09*

**Nir Zuk, serial entrepreneur & founder, Palo Alto Networks, at NetEvents EMEA Press Summit Barcelona 2011**



Nir Zuk, serial entrepreneur & founder, Palo Alto Networks

Amazing things happen when creative minds move to Silicon Valley. It began in 1954 when cash-strapped Stanford University, not allowed to sell off its land, hit on the idea of leasing it to hi-tech companies. Stanford's so-called "secret weapon" developed into a hive of creativity, welcoming brilliant unknowns destined to become household names – such as Bill Hewlett and Dave Packard, Steve Wozniak, Steve Jobs – and defining the future of information technology with semiconductor giant-to-be Intel, also Xerox PARC and the birth of Ethernet, WYSIWYG and the GUI. Nir Zuk began his career far from Silicon Valley, but showed early signs of being just the sort of moth to be drawn to that flame. His focus was on

network security having, as a 16 year old whizz kid in Israel, written some of the first computer viruses on his Dragon 64. Happily for the industry, he then u-turned his passion to address protection, working at Check Point to create stateful inspection technology – the basis of all today's security systems – and the first commercially viable firewall.

From there he founded OneSecure and built the world's first IPS system, which was bought by NetScreen then sold on to Juniper for over four billion dollars. Too much the creative firecracker to put up with big, bureaucratic organizations, fate has now taken him to build another Silicon Valley company from the ground up. With Palo Alto Networks, Zuk developed a dynamic new approach to fixing the firewall he previously designed.

What can we learn from Nir Zuk's story to better understand and pre-empt the next generation of ever-more IT-savvy cyber criminals? How does he see cyber threats evolving into the mobile environment? Having been drafted as a computer kid into the Israeli army, how does he see the growing role of intelligence agencies and the prospects for cyber war? Prepare to be surprised by Nir Zuk, his radical mind, sharp insights and outspoken viewpoints, as he paints for us a picture of cyber attack and defense now, then five and then ten years to come.

## **Keynote presentation**

Good morning, everyone. Thank you for having me here. I'm the Founder of Palo Alto Networks, as you heard. I'm not going to talk about Palo Alto Networks today.

I want to talk about innovation, specifically innovation in security. I want to show you the state of current innovation in network security, and what it means.

So let's start. Innovate or die – Those are the two options that every high-tech company in the world faces. They either innovate or they die. Let me give you a few examples before we jump into security.

Does anyone here have a cellphone? Does anyone here have a smartphone? Does anyone here have a Nokia smartphone? Did anyone here have a Nokia phone ten years ago? – Exactly. What happened? Nokia did not innovate, and they let other companies innovate and run them over. They're dead. I just don't know how they're going to survive this smartphone war. The Wall Street Journal recently commented on Nokia, saying, "consumers aren't standing in line for hours to pick up a Symbian smartphone... no matter how hard the company tries to spruce it up."

Another question: Does anyone here have a Microsoft phone? No. Okay. Is anyone here using Microsoft for search? One. Is anyone here using Microsoft for web email, Hotmail? Three of you. Okay. What happened to Microsoft? Look at Microsoft versus Apple – They just stopped innovating. They thought that they controlled the world, that the entire world was in their hands and that everyone would continue using Microsoft software

forever, and in the meanwhile others came from behind and passed them. Another example: Does anyone here have a car? Is anyone here driving a 3-ton SUV?

Is anyone here driving a hybrid car? I also have a hybrid. In 1997 Toyota came out with the Prius. In 2003 GM decided to respond by coming out with an even bigger, uglier, more gas-consuming car called the Hummer. And we know where GM – or as we call them, Government Motors – are today and where Toyota is. Toyota innovated and now they're the largest car company in the world, whereas GM is not anymore.

Okay. Innovation is important. And if you don't innovate, you die. These are just three examples. Everybody thought Microsoft was invincible.

Everybody thought Nokia was invincible in the cellphone market, and GM in the car market, but they're not because they haven't innovated. So innovation is very, very important.

Now let's look at security, an area that I'm an expert in, specifically network security.

I want to take you back a little bit to 1995. Was anyone here on the internet in 1995?

What were you doing on the internet? Email and Web browsing, right? This is what a web browser looked like in 1995. This is what Yahoo's website looked like in 1995.

This was the internet. And this was an email client in 1995. That's it! There was nothing else on the internet in 1995.

If you look at security on the internet in 1995, nobody was concerned about hacking because the worst you could get in 1995 was a virus. And the only way to get a virus in 1995 was through a floppy disc. Right? This is what an Apple product looked like in 1995. And this was the movie, Hackers, in 1995, starring Angelina Jolie. In 1995 Hollywood came out with this movie, and in this movie this kid hacked 1,500 computers in one day and caused the Dow Jones to drop 7 points in one day because of this hack. This was what Hollywood was dreaming about in 1995. And then Bill Gates was on the cover of Time magazine in 1995 – Master of the Universe. We know where Microsoft is today, right?

Let's jump forward to 2011. Now it's Mark Zuckerberg on the cover of Time magazine. It's not Bill Gates anymore. And the movie, Hackers, much worse than that became reality with WikiLeaks. Today anyone with a computer can bring down a country. Back then Hollywood thought that bringing down 1,500 computers in one day was a good plot for a movie. Apple's products look like this today. And the internet is not just web browsing and email anymore. The internet is Facebook and it's Salesforce.com and it's Webex and it's Sharepoint. And the internet is Skype and file sharing, and Rapidshare, which is a web-based file sharing site based in Germany, and Dropbox and Gmail, and many, many other applications. Is anyone here using the internet just for web and email

today?

Now why am I telling you all these stories? The reason I'm telling you all these stories is because, and it might be surprising to you, the technology that enterprises use to protect their networks today, the firewall technology, the intrusion detection and prevention technology, the anti-virus technology, the anti-spyware technology – all that technology was developed around 1995 and it hasn't changed since then.

We are using the technologies that were developed when the internet looked like this to protect today's internet. Really, nothing has changed. Nothing has changed since I built the firewall and Check Point, and then I was also the Chief Technology Officer at [Netscreen]. I built a firewall at [Netscreen]. And then I built a firewall at Juniper, and everybody else was copying these firewalls, all the other vendors. Nothing has changed since then in the core technology of the firewall. And the same applies to anti-virus, IDS and many other technologies deployed on networks. There has been no innovation.

However, we are now at the age of application and user enlightenment. Today, users do whatever they want on the internet. Users demand to use more than web and email.

Are you going to be okay using just web and email? Probably not. It just doesn't make sense anymore to use just web and email. But the security technologies are only for web and email, right? So let's see what this means.

First, there are a bunch of applications out there that should not be on a network, applications like file sharing. In this case, you can see the growth in the use of webbased file sharing, things like Rapidshare and other applications that are similar that are used for file sharing. This is data from corporate networks. So in 2008, 28% of corporate networks in the world had this kind of traffic on them. Now we're talking about 96% of networks. Almost all the corporate networks in the world – and that includes Europe, of course – have browser-based file sharing on them. But there's no reason for these applications to exist. You should get rid of them.

But there are other applications, like Salesforce, Webex, Sharepoint. We see them all the time. I'm sure many of you are using at least some of these applications. These applications are on many enterprise networks because enterprises want these applications, because these applications are important for the business to conduct its business. But these applications have dangers associated with them.

Sharepoint – If someone stores a file with a virus in Sharepoint, and then everybody else in the enterprise accesses that file, now they have that virus. Webex – This is a great tool for conferencing, for web-based presentations, but it also allows desktop sharing. It allows anyone from the outside to control a desktop on the inside of the enterprise without any supervision, once the user enables that. Webex also allows file sharing. It

allows someone from the enterprise to send a file to someone on a Webex conference without going through any traditional file checking mechanism, like virus scanning and data leakage scanning, and so on and so forth. And Salesforce.com does the same thing. You cannot control the content that goes through Salesforce.com. That can be dangerous. Confidential information can be shared through Salesforce.com.

So these applications are desired by enterprises; enterprises use these applications.

But they carry risk. They carry a lot of risk, and enterprises today need to take that risk in order to use these applications.

Facebook – Do enterprises want to have Facebook? Ninety-six percent of enterprises in the world – and the same number is true for Europe – have Facebook on their network. Ninety-six percent of enterprise networks in the world have Facebook on them. Some of them do not want Facebook.

Some of them say, we don't want to allow Facebook. They actually try to block Facebook, but it's impossible. Two weeks ago Facebook announced that they were switching to HTTPS. All Facebook traffic is going to be encrypted very soon. There is no way to block Facebook. You can see the numbers here.

Some enterprises say, look, we want to use Facebook for marketing. We want to use it for as a collaboration tool, but we can't because it's not secure. We cannot control what kind of content is being published via Facebook and we cannot control what kind of bad things are coming into the enterprise via Facebook. So they block it, even though they want to use it. And there are others who want to use it, and they allow it despite all the risks associated with Facebook, because they don't have a choice.

They want their business to be able to do its business, so they allow Facebook.

And there are other applications, like Twitter and LinkedIn. What are you going to do about LinkedIn? Are you going to block LinkedIn? The business needs to use LinkedIn, right? I use it all the time to find people to find and connect with people, to recruit people from our competitors and from other companies. What are you going to do, block LinkedIn? Well, if you allow LinkedIn, there's a lot of risk associated with it. Content is being published into LinkedIn that you don't have control over, and things come in from LinkedIn that you don't have control over. What are you going to do with it? You can't allow it because of the risk, and you can't block it because the business needs it.

And Twitter and Facebook are the same thing. You cannot allow it because there is a lot of risk associated with it, and you cannot block it because the enterprise needs it.

And Skype. Anyone here using Skype? Skype is a very dangerous application. Once you allow Skype to go through, there is no control on Skype, because Skype can do file transfer, it can do desktop sharing, it can

tunnel other applications through it.

There is an application called EEE-something, that allows you to tunnel any kind of application over Skype. There is no control over Skype. So, are you going to allow it or block it? Well, good luck trying to block it, even if you want to block it. All of you are using it, you see. People want to use Skype.. And if you try to block it, there's tons of tools out there for bypassing security.

Just go to Google – you can do it right now. This is a screenshot from just a few days ago entitled Proxy Bypass. You will find hundreds of ways to bypass network

security today. We actually see those tools on enterprise networks. About 15% of enterprises in the world – and again, the same number is true also for Europe, because about one-half of the data I'm presenting here comes from Europe – have these kinds of applications on them that are used to bypass the traditional security mechanisms.

[Tort], Ultraserver, applications like LogMeIn and GoToMyPC and other applications, completely bypass network security.

So what is the conventional approach to protecting the network, the one that hasn't innovated for the last 15 years? It looks something like this. You put it like this, and then you say, I'm going to secure web and email.

Enterprises are spending a lot of money on securing web and email. The network security market, according to Gartner, is about \$9b today, growing very soon to \$10b.

Ten billion dollars a year is spent on securing two applications: web and email.

Facebook? You either let it go or you block it, but you let it go. LinkedIn, no problem, let it go. Skype, it can go. You just protect web and email. Ten billion dollars are spent on protecting web and email, and \$0 is spent on protecting all the other applications.

It reminds me of this. I hope nobody takes offence at the next couple of slides. I just want to demonstrate something. You know what this is? This is the Maginot Line on the French and German border. This is what we're doing today. This is a map of it.

So, after WWI France built a line to block the Germans – today we're building lines to block web and HTTP, and we're hoping that no one will come from here. Right?

Facebook is here and Twitter is here. We hope nothing happens there. We just protect web and email. And we all know what's going to happen, right? That's the way network security looks today because of lack of innovation.

This is what Albert Einstein defined as insanity, when you do the same thing again and again and again and again, expecting different results.

Every three years enterprises refresh their network security. Every three years they buy a new firewall, they buy a new IPS, they buy new proxies, they buy new whatever, and they go out for a bid and they look at all the

different vendors. Usually they stay with the same vendor, but maybe they switch, but all the vendors are doing the same thing. They are just protecting web and email. They don't touch any other applications, yet enterprises expect to be more and more secure, or at least be as secure with all the changes that are happening in the world. That's not going to happen, and if you think it's going to happen, you are – according to Albert Einstein at least – insane.

So what are the big vendors saying when faced with the question of, what do we do with Facebook? What do we do with Twitter? What do we do with all these applications? What do we do with Salesforce.com? What do we do with Webex?

What do we do with Sharepoint? Their answer is this: Block it. Go to any big vendor in the security industry, the large five, and they will all tell you, well you can either block Facebook or not block it. We suggest that you block it, otherwise you'll get a lot of bad things through it. You should block all of these applications. We'll continue to secure your web and email – everything else should be blocked. That's their answer.

That's not innovation. That's actually going backwards, right? Basically, what they do is they make the IT department say no to everything. Okay, if you think about it, the role of the IT department in the enterprise is to enable the enterprise, right? The IT department doesn't sell anything. They don't market anything. They don't develop anything. Their role is to enable the enterprise. Enterprises spend whatever, 5%-10% of their revenues on IT because they want the IT to enable the business.

However, over the last ten years, there has been a shift where the security group inside the IT department has learned how to say no to everything. Facebook – no. Webex – no. You can't; it's not secure. We cannot secure it. I want to use this – no. The security department, by default, says no because they know that the only thing they can securely enable is web and email. They have become Dr No. They just say no to everything.

What is the innovative approach? So what do we do about it? It's very simple. It's very simple what needs to be done about it. I'm sure you already know the answer.

What you need to do is to take security and extend it to all applications. It's that simple. Instead of just focusing on web and email, and saying all the rest should be blocked, or all the rest should be allowed, or whatever, you should securely enable the use of all these applications. Whatever you do for web and email, you should do for Facebook, Webex, Gmail, Salesforce.com, Sharepoint and for any other application that you decide to allow through your network. Exactly the same.

If you scan web traffic for viruses, you should do the same thing for Webex traffic, and you should do the same for Salesforce.com traffic. By that, first you regain visibility and control. You can actually start seeing your network, not in terms of web and email, but in terms of all applications. And more

importantly, you can safely enable the workforce to use these kinds of applications.

Today, if you allow your workforce to use Webex, they can do whatever they want with it. They can share their desktop with the world, they can send and receive files, completely bypassing the corporate infrastructure that checks for viruses and data leakage, that checks for anything. They can do whatever they want with Webex.

Blocking Webex, of course, is not an option. What you need to do is safely enable Webex. What does this mean? It means exactly what it means for you when you enable email or web, whatever that is for your enterprise. So, if you scan email traffic for viruses, you should scan Webex traffic for viruses. If you scan web traffic and email traffic for data leakage, you should scan Webex for data leakage. It's that simple. If you scan web and email for exploits of vulnerabilities, you should do the same thing with Webex. And the same true for all other applications that you decide to use on your network. Salesforce.com, Sharepoint – everything you do for web and email should be done for these applications. This is what it means to safely enable an application.

In essence, when you do that, your IT department, instead of saying no to everything, will never say never again to an application. If you're going to ask to use an application, they're going to say okay, we can securely enable it. The same way we enable web and email, we can now enable any other application on the network.

Now, how do you do it? You do it with something called a next generation firewall, and I'm sure we'll talk a little bit more about next generation firewalls today. A next generation firewall is a device that takes whatever you do today for web and email and extends it to all applications. It's not a device that blocks or allows Facebook.

It's not a device that blocks or allows whatever, Webex or Sharepoint. It's a device that allows you to take whatever you do for web and email – virus scanning, data leakage, intrusion prevention, scanning for other bad things – and allow you to do it for all applications, of course including web and email, or at least including web.

Thank you very much.

<http://www.telecomkh.com/en/internet/mobile-telephony/news/news/security/netevents-emea-press-summit-barcelona-2011/palo-alto-networks/2769>