Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 11

Visible Traffic, Secure Network: Pipeline's Q&A with Narus CEO

by Tim Young, with Greg Oslan

In approaching the issue of network security, we decided to take a moment to speak to Greg Oslan, the CEO of Narus Systems, a vendor of network intelligence solutions, about the scope of network security and lawful intercept.

Pipeline: How has the approach carriers have taken to network security changed over the last few years?

Greg Oslan: Network security has certainly evolved. The term “security” had a specific meaning a few years ago. People said “well, security is about protecting my networks against worms or viruses and denial-of-service (DoS) attacks.” What has happened over the last few years is that security has taken on the nomenclature of Kleenex. They just bought a box yesterday, and they're not sure why they'd need a new box today unless they have the worst cold on the planet. That's occurred because security in the IP world has evolved into a discussion about how to manage what's on or not on my network. You want to be able to deal with unwanted, unwarranted, or malicious traffic that is trying to get on or has gotten on the network. It could be a worm or a virus. It could be a DoS attack. It could be an intrusion. It could also be spam. It could also be malformed packets coming from a bad network. We always though that security and traditional network management would converge and, in fact, that's the case today. The difference in the IP world is that in the traditional TDM world it was about managing the elements. In the IP world it's about the health of the traffic.

The other element is that security was brought about because there were a bunch of hackers, who tended to be teenagers and college kids who were very smart and somewhat bored and were looking for cool, creative, and somewhat mischievous things to do. While some of those had negative effects, they weren't meant to truly create massive harm. That has changed, particularly in the last 12-18 months. There has been a lot publicly written about attacks on Estonia by Russia, for example, which was really the first publicly announced, frankly, act of war between those two states. We also saw the U.S. accuse China of intruding into its networks. The new battlefield, as we move from a physical world to a virtual world, is the world wide web. It's not the physical battlefield.

Pipeline: So hacking isn't "cute" anymore. It's moved from a small problem to a legitimate battleground.

Oslan: That's absolutely correct. It's become split like anything of that scale. It's political, between governments and potentially a prelude to war. It's organized crime and ways to extort or create economic wealth through ill-gotten means. You still have some of the mischief, but much less so, because that was probably the easiest thing for the government to crack down on. The kids didn't want to go to jail. That's a simple thing. Governments don't care about going to jail, and organized crime doesn't seem to worry about it either. It's gotten so organized that in many places you can buy the capability to attack others. You can buy bots and botnets and bot armies for so many dollars per site or so many dollars per location. It's pretty interesting when people can make money helping people attack other people, but I guess that's what Smith and Wesson did with the gun business.

Pipeline: We talked a bit about some of the types of attacks out there. Obviously, in order to attack major carriers or government agencies, attacks need to display a bit more ingenuity than most. Are there specific trends you're seeing?

Oslan: I think the biggest trend we've noticed is that these are typically well thought-through and well planned. These are not people who woke up one morning and decided to spend a few weeks hacking. These involve months and months, in many cases, of planning. They've been spending years, potentially, probing and finding vulnerabilities, and then going out and building, in the case of broad DoS attacks, bot armies. In the case of intrusions it's very similar. They're looking for vulnerabilities and looking for holes. Once they find it, they often don't attack right away. They think about how to exploit the vulnerability. Is it information they want to take down or do they just want to watch that site for the future? It's a new cold war. How fast can you get in and be undetected and how fast do they detect you and shut you down? It's not unlike when Russia used to see how far their fighters and bombers could get into the Alaska airspace before we responded and chased them away. It's a very similar environment.

Pipeline: So we're still seeing distributed denial of service (DDoS) attacks and worms?

Oslan: New kinds of worms. Polymorphic worms that can take on new shapes and new capabilities that we may not have seen before. You have some that are not just self-replicating, but self-morphing. Viruses themselves have diminished in their ability to do harm. It's been driven to the desktop. A lot of that has been handled by desktop antivirus software. It may be malicious and dangerous, but you don't see many people complaining that a virus crashed their hard drive. We've seen a lot of movement from the desktop to the network. That's why the carriers are now so focused on preventing this kind of attack.

Pipeline: One thing I hear from companies like yours is that they reduce the levels of false positives. How big a problem are false positives?

Oslan: Large, because it's expensive. There was a time when it was okay to overreact to intrusions or worms, but now that we're five or six years into it, and SPs have huge staffs dedicated to preventing this, they're noticing that it's awfully expensive for 15 or 20% of the instances to be wrong. Also, CSPs are moving into an environment in which either they're providing security services to their customers, or their customers are demanding service level agreements that guarantee a certain level of performance related to delivering clean traffic to them. If you're getting lots and lots of false positives, and twice a day telling your customers that there's a worm coming when there isn't one, it makes you look pretty bad. It's a big issue and one that needs to be solved differently than problems in the past. You need traffic visibility. You can't do this a link at a time. Spikes in traffic, particularly large and sudden spikes in traffic, trigger alarms because something is different. Now you've got to determine if that difference is caused by something normal or by something abnormal. The more you can do that through algorithmic intelligence, the fewer people you need on the other end, so the lower cost for your consumers.

Pipeline: Lawful intercept is something that we're hearing about lately. Is the increase of visibility of the issue impacting manufacturers of LI solutions?

Oslan: I think we have to look at the issue globally. Very often people focus on the U.S., which is a microcosm of the global telecom space, representing about a third of it. Well, a ton of IP traffic flows through the U.S., but in terms of the number of service providers, globally, it's a very small piece of the overall picture. When you look at intercept, it's just a component of traffic intelligence. Telecommunications has always been considered a critical infrastructure for the operation, protection, and livelihood of a country. The Internet has never really been looked at that way until more recently. People are understanding that the Internet is becoming a new form, and maybe the only form in the long run, of communications. It has to be protected the same way. Globally, people are looking at it in the same way they've always looked at voice intercept. On a global scale, there is growing visibility and growing need for solutions that give governments the capabilities to track down bad guys, put simply. Nobody wants to do intercept. It's expensive. There's no revenue involved. If that can be a part of a system that creates revenue, however, and also protects their network, that's valuable.

Pipeline: How has Lawful Intercept changed over the years as telecom has moved past PSTN?

Oslan: The biggest change, obviously, is that you had to move from being able to intercept voice traffic on a well-defined channel, to intercepting traffic on an IP network, which is much more distributed, sophisticated, and complicated. The systems required to intercept in an IP world are far more complicated. IP traffic doesn't necessarily go down one link. Packets don't necessarily come in order. They're time-stamped. You essentially have to intercept pieces of the call, or email or whatever, and then reconstruct that session and do that all in real time.

Pipeline: I was recently talking to someone else about the topic of network security, and they were talking about the ingenuity of clandestine communications. One example was one member of a terror cell opening a webmail account, writing an email, and saving the email as a draft, but never sending it. Then the other party was able to sign on under that same account, read the message and delete it, all without anyone ever actually sending an email. Is this the sort of thing carriers and government agencies need to be able to confront?

Oslan: That's dead on. Terrorists communicate in draft folders. Address books. If a name changes within an address, that can be a coded message. Webmail is a very easy method because you can go into Hotmail or some other system, start an account, use it once, and then go open another. The sophistication and complexity is much greater. It's a combination of variety and flexibility of the medium.

Pipeline: We've talked a lot about security and LI over the last few years. Where do you see security headed?

Oslan: We feel strongly that it will all be about traffic intelligence. First and foremost you must understand your network and the traffic that is traversing it. Once you understand that, you can decide what you want to do with it. Is it good traffic or bad traffic? In Japan, a security event is spam. They're not very focused on worms or viruses. They're focused on spam. In China, a security event is Skype. This is encrypted traffic they can't understand. That's considered a threat to national security. Pakistan will tell you it's VoIP and email. Remember the caricature of Muhammad and the hullabaloo it caused in the entire Muslim world, particularly in Pakistan? After that, they wanted to monitor all communication. The definition of what security is will absolutely change, and that's defined by the owner of the network. They'll decide what constitutes good traffic or bad traffic, and in the case of bad traffic, they'll decide if they want to block it, reroute it, or intercept it, or what they want to do with it. I think it will be a system-level approach to protecting a network, as opposed to a narrow view.

Pipeline: Is there anything else you'd like to add?

Oslan: Just that the Internet is very global and that the bulk of the activity exists outside the U.S. Two-thirds of our sales are outside of the U.S., with China and India growing and representing a large portion of the world's population.

Pipeline: Thanks for taking the time to speak to us.

Oslan: Likewise. I enjoyed it.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.