In My Opinion: Kris Gopalakrishnan, Infosys • VC Talk: Gaurav Shah, DeGroup

PUBLISHED SINCE 1997

siliconindia

BUSINESS & TECHNOLOGY IN THE U.S. & INDIA SEPTEMBER - 2011 SILICONINDIA.COM

Securing You Against the Unknown

Dr. Parag Pruthi

$ 2 US/INR 150

06

0 74470 91626 0

SILICONINDIA INC.
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

NIKSUN: Securing You Against the Unknown

By Vimali Swamy

2008 was a year of grave challenges for Dr. Parag Pruthi. The moving in of a new tenant in their building complex and associated electrical work led to a massive fire breakout within NIKSUN's headquarters, destroying over 250 large servers along with its data, and almost everything else. Water from twelve fire trucks and the soot from the smoke was all over the lab, data center, desktops, inventory, everything. Quite ironic for a company that plays in the data security space! Added to this was the fact that the majority of investors were also being "cashed out." To make matters worse, it was a time when the industry was deeply entangled in the clutches of the recession. For anyone else, this would have spelled doomsday but for Dr. Pruthi this was a chance for a new beginning. A chance to undo legacy systems and build a new infrastructure and business that is great! Up from the ashes grow the roses of success!

Business means different things to different people. For some it is trying to make a quick buck and exiting and for some it is taking the business to a successful IPO. But Dr. Pruthi has a different ideology. He believes that it is the creation of a lasting and successful business able to withstand the test of time that matters, and not the temporary wins and losses. "People often assume that having great technology and a business is the same. But it is not. A great business is one which creates wealth, sustains growth, rewards the people who are a part of the enterprise and continues to create a difference in the lives of those who utilize your offerings. It is about creating a legacy. At the end of the day, I want to build a great business and for me the journey has just started," says Dr. Pruthi. It is with this vision that he has steered NIKSUN from a humble startup in

1997 to a beckoning force within the network security space.

Headquartered in Princeton, New Jersey, NIKSUN today is the only network security and performance monitoring solution that is like the DVR and Google for the network. Just like a DVR, NIKSUN can simultaneously capture and store network traffic in real-time at up to 20 Gbps rates. Just like Google, NIKSUN inspects, mines, correlates and indexes everything traversing the network at multi-gigabit rates, gaining the deepest insight of security threats, performance issues, and compliance risks. Using a single console, just like going to google.com, NIKSUN also provides 100 percent search, analysis, and visibility across networks, providing incredible power with a simple click and real-time contextual visibility. With its forensic insight, NIKSUN is turning a whole new chapter in the industry's approach towards network security.

The Great Security Challenge

The Internet is one of the greatest revolutions of our time but has also brought with it many challenges to governments, law enforcement agencies, and public as well as private organizations. From the constant barrage of attacks by nations and organizations to penetrate critical information assets and planting malware to siphon information; to rouge cyber thieves trying to hack into financial accounts of those who are influential, cyber threats are here to stay. Based upon the intensity with which the world has become reliant on the Internet, it is safe to say that cyber space is the new battleground.

In addition, the explosion of mobile devices and remote access technologies, make protecting data much more difficult, and managing the current technologies more time consuming and less effective. The number of IP devices — from 1 billion in 2010 — is expected to reach 50 billion in 2020. For cyber criminals this is just the expansion of their playground. The good news is that organizations are awakening to the need for more robust security measures and are adopting them rapidly, but are they sure that these steps are enough?

An investigative report released by Verizon Wireless and U.S. Secret Service stated that from 144 million breaches in 2009, 2010 saw the numbers drop to a mere 4 million

A recent investigative report released by Verizon Wireless and U.S. Secret Service stated that from 144 million breaches in 2009, 2010 saw the numbers drop to a mere 4 million, bringing a ring of joy amongst many companies and a false sense of relief that the measures taken were sufficient.

But earlier this year the industry witnessed major outages in Amazon and Sony's cloud infrastructure, including a massive security breach at security companies like RSA. Another incident included Google's user's profile information being easily accessed.

Dr. Pruthi states that the report is just an indication that the cyber criminals have become smarter and are covering their tracks well. "Unlike the hacker of old days who only breached networks to gain fame and be in the limelight, criminals today do not want publicity. Security attacks, intrusions, and hacking attempts today are sophisticated and harder to detect," he explains.

According to Dr. Pruthi, the recent disclosures of massive cyber attacks is a warning to organizations – private & public alike, that their traditional security measures just became ineffective because they need to worry not about the known, but about the unknown.

Why are Traditional Methods Passé?

Today, most businesses are moving massive amounts of data across network boundaries to associates, customers, vendors, and employees. Making sure that information is offered unfettered, yet in a secure fashion, while still following corporate guidelines, is becoming more important as the need to share and make information available instantly is vital to a corporation's success.

That situation leaves those charged with network security uneasy and, worse yet, unsure if their network is strong enough to prevent an attack or compromise. In-house testing and taking the word of security vendors can only build a limited amount of confidence in installed security systems. In simple words, businesses need a new approach, that of a DVR and Google, not only to analyze traffic and prevent breaches, but also to make sure attacks have not occurred in the past without being noticed, and to provide undeniable proof of any malware intrusions.

Business leaders need to constantly question themselves on how they are protecting shared data, detect if information is compromised, validate their security practices, and determine the counter measures they should have in case of a suspected breach.

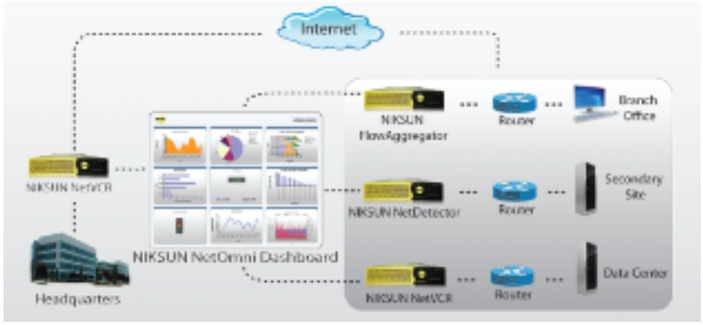
Traditional intrusion detection systems can only raise an alarm in the event of a breach; they can never answer the crucial questions that might help prevent such occurrences in the future. It is similar to having a house secured by an alarm system. In case of a breach, one will be alerted but until one does an entire search it is difficult to know what is amiss or who caused the breach. And in no way can one prevent a break-in the next time. It is the same with data being stolen on the Internet. Only that data on the Internet, when stolen, does not appear absent physically. So, despite alarms, one might never know what data was stolen, let alone who stole it. What one needs is a preventive measure that is proactive, and this is where NIKSUN comes in.

Security: The NIKSUN Way

With its forensic approach to security, NIKSUN captures and reveals all traffic that moves over the network. Its patented technology platform and latest release Alpine allows consolidated IDS, forensics, packet capture, flow & SNMP analysis, VoIP monitoring, and other capabilities. And it packs all of these functions into a single, unified platform offering a single management console to provide IT management with instant situational awareness of security threats, network operations, capacity planning, application profiling, and more.

Compliance, e-discovery, and security auditing are becoming key issues for both public and private companies. Enterprises today are actively exploring how they can analyze traffic in real-time to prevent data leakage and enforce security policies. NIKSUN, with its real time network monitoring solutions, fits the bill.

So how does NIKSUN achieve this? Say your organization's network has been hacked. Do your security



measures allow you to quickly trace the incident to find the root cause and make sure it doesn't happen again? The traditional paradigm relies on static disk dumps or portable probes deployed after the fact. If the hacker carefully covered his tracks, how do you ensure this does not happen again and do you even know that it happened at all?

Major outages in Amazon and Sony's cloud infrastructure, including a massive security breach at security companies like RSA, indicate insufficient security measures within organizations

NIKSUN's NetOmni Alpine in conjunction with its flagship appliances NetDetector and NetVCR, offer unparalleled data-in-motion surveillance to track attacks and performance problems as they happen and isolate the data in question so that a diagnostic procedure may be initiated. Real-time alerts are facilitated based on performance thresholds, policy rules, and signature and anomaly definitions. Users may then respond to these incidents and apply extensive forensic analysis options that significantly reduce mean time to resolution of problems. With the NIKSUN solution all guesswork in the incident management equation is replaced by insight, intelligence and constructive action.

NetVCR can monitor quality of service in networks and Web servers by capturing network traffic to understand application and protocol utilization, source, destination, and a myriad of other metrics. NetDetector is used for security forensics to analyze recorded traffic data, and it can issue an alarm to a system administrator about possible network hacking and preserve the evidence for 100% confirmation of the attack, the method of attack and the data that was breached.

For example, some time ago The Royal Institute of Technology, Sweden was connected with Stanford University in California via a dedicated T-1 line provided by Swedish provider Telia. Using NIKSUN NetVCR, a telecommunications professor at the Royal Institute of Technology says he detected and traced intruders that broke into the shared campus network, which extends into three other Swedish universities and Estonia. "The most prominent intrusion in our network was made by a cracker who broke into one of the

NIKSUN Team

Web server hosts in the network and used it to set up a smurf attack targeting a site in Germany," says Bjorn Pehrson, a telecom professor who was conducting research between the two universities. "Thanks to the data we were gathering with the NIKSUN NetVCR tool, we could reconstruct the break-in in detail," he adds.

But NIKSUN's NetOmni is the cherry on top of the company's offerings. Driven by the growing activities of business and social networking, it offers important capabilities to businesses that are exploring and growing their collaboration efforts. Businesses have started to realize how easy it is for knowledge workers to share information across company boundaries. It is a situation that is raising concerns with those tasked with network security and compliance initiatives.

NetOmni Alpine operates at multi-gigabit rates across heterogeneous networks, allowing organizations to simultaneously capture, correlate, and analyze all data-in-motion across their global enterprise, which provides true, 100 percent situational awareness. This ensures that organizations can identify data leakage problems, perform e-discovery tasks, and audit communications, allowing them to determine if communications and collaboration events fit within company policy.

The uniqueness in the Alpine range of products is their ability to thwart zero-day attacks. The common feature of Zero day attacks is that there are no signatures or approach to stop them until their impact is noticed and signatures are developed. These attacks can be launched through emails, spear-phishing links or through targeted exploitation of vulnerabilities in servers and other devices. Also there is usually a large gap (days to weeks) between the launch of an attack and development and deployment of updated signatures. Once the revised signatures are deployed, they can only stop instances of a zero day attack going forward. NIKSUN's holistic solution provides an efficient and accurate approach to detect the vulnerabilities before the signatures are formed.

Each of the company's products is ably supported by the NIKSUN Knowledge Warehouse (NKW). Based upon years of research and experience, the NKW utilizes sophisticated algorithms for analysis and retrieval of data and is a store house of very rich meta data. The NKW also consists of linked data. These linkages help users to exploit the data rich warehouse to quickly find the information of interest. Analysis is further aided by user customizable analysis views and reports in terms of both information displayed and layout; this is sort of similar to my google or my yahoo. Customization is per user and templates can be stored and shared for use by other users. The ability to drill down with a single mouse click from one view to another makes analysis extremely quick and user friendly. As analysts look for faster ways to drill through information, this feature along with the ability to tab through screens of interest on the newly introduced clipboard speeds up the process without losing context.

Some time back the US Secret Service used NIKSUN's analytical technology to capture and mine data warehoused in NIKSUN's Network Knowledge Warehouse to reconstruct incidents of identity theft. "Using our solutions and other investigative techniques, the government was able to isolate the incidents of identity theft and trace the incidents back to criminals on a global scale. The department nabbed over twenty eight criminals in over six countries engaged in credit card and identity theft within a single day," says Dr. Pruthi.

The Man behind NIKSUN

It was his vision of helping businesses and governments realize the potential of the Internet that led Dr. Parag Pruthi found NIKSUN. A visionary with focus on innovation, Dr. Pruthi has guided NIKSUN from small start-up to being a global leader in advanced network analysis and visibility (NAV) solutions. Built on the building blocks of his doctoral research to model high variability phenomenon in networking, Despite a great technology as its backbone, Dr. Pruthi believes that it is the value that holds a company together. "It is ethical business sense, value to customers and dedication and wellbeing of one's people that makes a great organization," he says.

He brings with him over twenty-five years of expertise in network security, surveillance, data warehousing / mining, and systems performance management. A Bachelor's in Electrical Engineering and a Master's in Computer Science from Stevens Institute of Technology, he also has a Doctorate in Telecommunications from The Royal Institute of Technology in Stockholm.

Prior to founding NIKSUN, Dr. Pruthi was at Bellcore, Telcordia and other research institutions, where he focused on his passion of solving important problems in security, telephony, broadband, and wireless network management. During this period, Dr. Pruthi was instrumental in developing leading edge tools for large-scale collection and analysis of data from production carrier and enterprise networks. He holds 30 patents issued and pending. He is also recognized as one of the foremost experts in advanced cyber security technologies, and advises on cyber defense strategies with some of the highest levels of governments and enterprises around the world.

At the end of the day, with NIKSUN he believes in leaving a legacy of a business which should inspire his teenage sons and other young minds out there.


Dr. Parag Pruthi

NIKSUN, essentially, achieves its tasks — of warehousing, mining and gathering intelligence from distributed network data — using a hybrid approach. Since there are new applications being deployed on any network and the nature of the applications changes frequently, "the problem requires hardware-software expertise and a systems-based approach to solving many of the network monitoring, security, surveillance and forensics needs of tomorrow," says Dr. Pruthi.

What Next?

With cloud computing and mobility driving the industry, for NIKSUN, the market for their solution has just opened up. And this is evident from the transition that the company has undergone in the past few years. After years of building a strong, and unusually broad, foundation, and having a very limited clientele, NIKSUN in the last three years has undergone a massive expansion in its presence in the industry. The company today is flying high with over 1000 customers across 30 countries and the count is ever increasing. It is working towards becoming become a household name in the next 3-4 years—by having large scale deployments of its security products in enterprise networks around the world—and doubling its sales figures. The company has also won several awards and accolades and has been recognized as the top security vendor by InfoWorld, Secure Enterprise, SC Magazine, CRN and more.

Though this is a matter of great pride for Dr. Pruthi, he says he is just 'a regular guy doing his regular job who just happens to have the most intelligent and dedicated people working for him'. But what he ultimately aims for is to be able to make the industry proactive to the unknown threats that loom ahead in the coming years. To create this industry wide awareness, NIKSUN held the first World Wide Cyber Security & Mobility Conference in July this year in Princeton, New Jersey. The event not only brought significant industry leaders together to collaborate on the ever changing cyber security landscape, but also provided a dynamic platform for security and mobility professionals to connect and share the latest innovations in cyber security and mobility vision, practice, and technology. In addition to this, it also offered a post-conference workshop for its global network of partners, customers, and prospects on topics such as advanced threat mitigation, protecting critical assets, and improving network performance and operations. Dr. Pruthi and team now plan to continue this conference across many locations, creating the legacy that he dreams of.

For Dr. Pruthi, the journey has just begun and he believes he still has a long way to go in this marathon. With cutting edge technology as the backbone and value rich business practices, aided by the brightest and smartest people by his side, NIKSUN is sure to be a forerunner in this marathon for years to come. SI