Issue:
March 18, 2013

CEOCFO Magazine - The Most Powerful Name In Corporate News and Information

Bringing to market a Patented Groundbreaking 100% Software Solution to replace VPN on the Internet, Dispersive Networks, Inc. and their Virtual Dispersive Networking (VDN) is providing a High-End Smart Router with Unmatched Security in Networking

Technology
Network Security

Dispersive Solutions, Inc.
2555 Westside Parkway, Suite 500
Alpharetta, GA 30004
678-648-6395
www.dispersivesolutions.com

Robert W. Twitchell, Jr.
CEO

BIO:
Bob is the Founder and CEO of Dispersive Solutions, Inc., a company pursuing secure networking with a dispersive computing platform. Starting in 2001, Bob was founder, CTO and consultant of TeraHop Networks, a Delaware company that pursued container tracking and first responder technology.

Prior to that, Bob was Chairman and CTO of Intransit Networks, Inc., a Washington startup that pursued inventory tracking and control technology. Prior to Intransit Networks, Bob was at Nokia, where he served as Value Added Services Manager, CDMA Markets, and was responsible for strategy and implementation of location based services.

As Product Program Manager of Value Added Services with Nokia, Bob negotiated contracts with suppliers and subcontractors, put together the team to develop the GPS accessory (3 partnerships and 4 subcontractors), developed a WAP software platform, and setup the program for the Nokia 3285. He was responsible for Marketing, After sales, Quality, Manufacturing and R&D in all of his assignments as Product Program Manager. He led the development of the Nokia 9000 "Communicator" for the US market whose record setting 11-month development to market has not been repeated.

Bob was responsible for building the Texas Wireless Data team for Nokia where he hired the first sixty people in disciplines including Hardware, Software, Mechanical, Test, Marketing and Quality. Previous time was spent with Motorola Paging Infrastructure where he was responsible for the development of paging software that was deployed in Singapore, Tokyo, China, United Kingdom and Italy, and Harris Corporation (Electronic Warfare) where he worked on classified projects and designed the audio conferencing chip for the International Space Station. Bob has a Masters Degree in Electrical Engineering with a Master's Thesis involving DSP, Neural Networks and Voice Recognition.

About Dispersive Solutions, Inc.:
Dispersive Solutions utilizes a patented groundbreaking core technology, Virtual Dispersive Networking (VDN) that transcends multiple industries, providing unmatched security in networking and communications. VDN is a 100% software solution, with implementation as easy as a software download.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: Mr. Twitchell, Dispersive Networks has a groundbreaking core technology. In laymen's terms, can you explain what you are able to do that others cannot?
Mr. Twitchell: Basically, in order to control security, you need to be able to control routing on the internet. People tell you it is impossible to control routing on the internet because there is a lot of legacy hardware from companies like Juniper and Cisco, therefore, if you cannot change legacy hardware then you cannot change the way routing works. The way routing works on the Internet is essentially, when you send a packet out, the routers figure out the fastest path from point A to point B, and send the entire package that way. The real problem with this, which is causing the majority of the problems on the Internet when they talk about all of the problems in cyber security, is something called the "man-in-the-middle" attacks. This is where a hacker gets in the middle between a router and the recipient device, and is able to copy all of the packets going from point A to point B. The bad guys take this and reroute it, get a copy and send it to

China, or some other destination, and then they have all of the information that you sent, plus a lot of information about how to hack your network. What we do is we dispel that threat by essentially creating a deflect out on the internet, and we do that by putting routing on servers, computers, and mobile phones. There are many routers on the internet, but there are a lot more servers, computers and mobile phones. If you put the routing on the servers, computers and mobile phones, you can create independent paths on the internet, thereby splitting the traffic up; so essentially the "man-in-the-middle" attack only gets a fraction of the traffic. Therefore, that fraction of the traffic is not useful to the hacker, and it creates a secure communication across an open internet.

CEOCFO: Is this software that would go on, let us say, a mobile phone? Is it something in the hardware? Can you give a little more detail about this for the more technically challenged individuals?

Mr. Twitchell: We are 100% software solutions. There is no hardware that has to be changed out on the internet. The issue, again, is with the legacy hardware that is out there is trying to make it change, which you see many companies out there trying to change the routing. What you end up having is what they call the "weakest link" problem. This is where you have one really high-end smart router with all these great new features, and all of the other routers basically cannot do them, so the old routers cannot be forward compatible, and therefore you cannot make it work like you would like to have it work with all of these new routing algorithms. We solve that problem by turning it into software and then breaking up all of the connections for every application you run on your computer.

CEOCFO: Where are you in the development and/or commercialization process?

Mr. Twitchell: We have several customers on the government side that are actually using it, testing it, and have deployed it. Our focus has been on the government and DoD side. The reason we did that is because we started over in banking, we talked to a few banks, and they said, "Wow, this is really great stuff! We have never seen anything like it before, and as soon as the government puts a stamp of approval on it, we will use it!" We got a very clear message that we needed to head over to the government side and go get validation, and we have shocked them. They have looked at our technology and they were not expecting to see anything like this for ten years.

CEOCFO: What is the "Ah ha!" moment when you are trying to explain to someone and convince them that it really can happen? When do they get that moment that it might work?

Mr. Twitchell: We talk to some really, really smart people, very technical, experts in their areas, and our first meetings always go the same way. The first thing they say is, "You cannot do that." Then we explain to them that we are going to show them right after the presentation that it is working. Then the next thing they say is something like, "Oh, you must be doing peer-to-peer networking." Then we explain how we do our stuff, and it is different. Then the next thing they say is, "Oh, well you are just like BitTorrent", or "You are some kind of virtual machine, or virtual niche." Then we explain what we are doing there, and then there is usually something else that they say that we are like, and then we explain that difference, and then there is an "Ah ha!" moment at that point. We have done this with academia, we done it with DoD experts, and we have done it with a whole bunch of people that are very technical on the commercial side too.

"I have been doing startup now for twelve years. If I did not have patience then, I have patience now."- Robert W. Twitchell, Jr.

CEOCFO: There always seems to be a way for the bad guys to find a way around solutions. Can you convince me that that will not happen with Dispersive Solutions, Inc.?

Mr. Twitchell: This is the number one problem out on the Internet, because most people try to rely on algorithms. When you rely on algorithms, maybe they cannot break your algorithm, but they can steal it. If they cannot steal it, they can try to guess things, and eventually they can break it. Once they break one, then they break every one of them out there. What we do is create what we call a "Spread Spectrum Protocol"-- we call our technology Spread Spectrum IP Networking, and it is analogous to what we do on the battlefield. One of the things in my background is electronic warfare. I worked on modems and jammers at Harris Corporation. Essentially the reason military communications has been secure on the battlefield is because there are really two types of radios: one is called a direct spread radio, and the other is called a frequency hop radio. A direct spread radio spreads information over a bandwidth and the bad guys have to figure out how you are spreading that information over the bandwidth, and how wide it is, and so on. With that constantly changing, it makes it difficult for them to do that. What happens with a frequency hop is a transmitter and a receiver have to stay in lockstep so they can communicate, and as you hop from frequency to frequency, the transmitter and receiver have to stay in that dance, and then you can communicate. What we do on the battlefield is we combine those two technologies. We do something very analogous to that with our technology, where we basically spread the information over deflects, which are those computers, servers, and mobile phones, and we can arbitrarily pick how often we are going to split it. Computers can handle thousands of connections at a time, and therefore we can spread the traffic up to two, three, five, ten…we have actually simulated two hundred and fifty splits during a single communication. Of course, devices have multiple IP addresses, for example, your mobile phone has a Wi-Fi IP address and it also has a mobile IP address for the network. That would allow us to communicate over both of those two, and of course, we can hop on ports as well. Without moving it, the bad guys now have to figure out how to put it all back together, and

with it being different every time, they now have to figure it out every time. Our stuff is not an algorithm to break, a lot of it is just arbitrarily picking out how many times you want to split it up, what encryption keys you want to use, what directions, whether you are going through servers, computers, or mobile phones. There are many mobile phones on the Internet, and the hackers have to watch them all in order to figure out what traffic they are trying to put back together. It is very difficult for the bad guys to have to figure out every communication. It is kind of like, if you took Fort Knox and you have all of that gold there, you have trillions of dollars of gold, but you take it out and make it all into flakes and spread it all over North America and you make the guys go pick it up, it is not economical.

CEOCFO: Have people been trying to come up with a concept like this, which you have figured out, or is this concept very new?

Mr. Twitchell: The concept is very new. Our technology uses virtual machines for signaling, that is a key part that is missing off the internet, since our VMware and Citrix use virtualization for processing and storage, we are actually using virtualization for networking so we can create all of these separate communications that work different ways. This is a wide-open area where I have put in a large number of patents. I have seventy granted patents from my previous startup. The first patent for Dispersive Networks, Inc. has been granted, and essentially, we have much more pending. This is a wide-open area, and people just have not thought of it. It is a very simple, basic concept. The security on the Internet is a very, very complex problem, and you do not solve complex problems with more complexity, you solve it with simplicity.

CEOCFO: You mentioned the DoD is working with it; when do you get the results of their first deployment?

Mr. Twitchell: We have already been going through tests, and we have already deployed to certain companies. We have done a press release with a company called BTS. Dispersive Networks actually has the patent, and it is licensed to Dispersive Solutions. I am the CEO of Dispersive Solutions, and it would be the place to find out more information.

CEOCFO: How do you, as the CEO of your company, deal with the frustration of knowing you have something that could clearly make a difference for everyone in the world, yet takes a long time to get it accepted?

Mr. Twitchell: I have been doing startup now for twelve years. If I did not have patience then, I have patience now. It is definitely learned. As the saying goes, you are trying to get people who have done business a certain way to understand a different way to do it, and, again you always get that first "We do not understand it." You know, it just takes patience. You have to explain to people that you always want to jump ahead, but we believe we will be on every PC, every server, and every mobile phone on the planet eventually. With this technology, the patent has been granted, and everyone who has looked at it has just been unbelievably impressed. We can give you a full demo where we are splitting traffic five different ways while you are talking using a Voip program over two android tablets, downloading a video, and connecting with email all at the same time.

CEOCFO: Do you have a plan once DoD is ready? Are there industries you will be rolling out first or will you be going to OEMs? What is the strategy?

Mr. Twitchell: We look for partners in a market. We are negotiating. I cannot say much right now because we are under an NDA, but we are negotiating directly with a company to roll this out to utilities. I helped with many different things in DoD. I helped with stopping GSM phones from being used as IED detonators, and I am very proud of that. National security is very high on my radar, and at the end of the day, the energy grid is the most important part, because if you turn the power off, finance does not work, communications does not work, controlling of the water and the damns does not work, and things like that. At the end of the day, Utilities is one of the most important places for us to go to secure. I am sure you have seen in the papers about Iran, and the damage that was done at the uranium reactors, and the counterattack that they did against our financial institutions in the United States and some financial institutions in Europe. Our technology makes it dramatically harder for those kinds of attacks to occur.

CEOCFO: Is Dispersive Solutions funded through all of what you need to get full commercialization, or will you be seeking additional funding?

Mr. Twitchell: We are seeking additional funding. We are in negotiations with several companies on strategic investment, but we are looking for friends. In different markets, this has got applicability such as in telecom, medical, just about any market that uses corporate security, obviously DoD, and so on. We are definitely looking for partners and we are looking for additional capital. The expensive part is the marketing of the technology in all of the different markets. We are definitely going to need much help in that arena.

CEOCFO: Why should investors and people in the business community pay attention today to Dispersive Solutions?

Mr. Twitchell: The key message here is our technology secures information in motion on the Internet. The technology that is in use today is the VPN. The VPN was hacked, and if you do a web search on CloudCracker using "dollar sign 200", you are going to find a service that will break a business class VPN for two hundred dollars. Our technology is being tested by DISA (Defense Information Systems Agency) as a replacement for the VPN, and as far as I know, they are not testing anyone else for that technology.

Dispersive Solutions, Inc.
2555 Westside Parkway, Suite 500
Alpharetta, GA 30004
678-648-6395
www.dispersivesolutions.com