CyberPro

November 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: DR. ARUN SOOD

NSCI's Lindsay Trimble recently had the opportunity to interview Dr. Arun Sood, professor in the Department of Computer Science and co-director of the International Cyber Center at George Mason University, Fairfax, Va. Sood's research has resulted in more than 160 publications. His team has developed a new approach to server security, Self Cleansing Intrusion Tolerance. This technology was the winner of the Global Security Challenge-sponsored Securities Technologies for Tomorrow Challenge.

NSCI: What is the main mission of George Mason University's International Cyber Center?

SOOD: The International Cyber Center's objective is to take an interdisciplinary view to cyber issues. In our center, we have an advisory board which has people from industry, people who formerly worked for the government, but it also has faculty from the School of Public Policy, the Center for Infrastructure Protection (which is part of the law school), faculty from the electrical engineering department, computer science and others. The board includes people from all of these groups to emphasize that we take a very interdisciplinary approach.

The second aspect of our mission is that international is an important part of our agenda. What we are really saying is that some of these problems which we are confronted with are so complex that it is better to take a more holistic view than a pure technology view. That's what the center does. Our Web site, http://internationalcybercenter.org, has more details about our mission and projects.

The key points of our mission are to highlight the interdisciplinary aspects and to highlight the international aspects of our agenda. To further note this interdisciplinary aspect, our center is one of the few centers which reports directly to the provost – the chief academic officer at the university. That's an indication of how this is perceived at George Mason.

At George Mason University, cybersecurity, cyber terrorism and other IT disciplines have many people in many schools working on them from their own perspective. The International Cyber Center is trying to do something across all of these disciplines.

NSCI: As co-director, what are your goals for the program?

SOOD: We have two areas that we are working on. The faculty has their own research projects, but we are also trying to build a community of interest in the international cyber agenda. We do this by organizing conferences and professional workshop sessions throughout the year. In the last six months, we had a workshop in Zurich on cybersecurity and global affairs. We also had an event on campus which

focused on international cybersecurity. And earlier this month, we had a workshop in Nigeria, focused on CERT-capacity building in Africa. This is just an example of the things we do to build this community of interest.

NSCI: Based on your team's research, what do you believe is the biggest cyber threat?

SOOD: I think it's a combination of an inability to detect all malware and the second part – which is almost as bad – is that once people are in your system, it's very difficult to find them. The malware lets people get in and then you can't find them, so people are in the system for long periods, in some cases several months. Not only are people getting in, but once they get in their persistence creates a problem.

In current approaches, malware detection is still a key part. Network attackers are using customized malware and making their attacks very targeted. That's a potential problem too. If only one or two places are being targeted, you don't build this knowledge about what is going on. Your situational awareness is weakened because only the one who is attacked knows what's going on. Targeted attacks, especially in the international security arena, become even more of a problem. The attackers know exactly what information they want and they launch targeted attacks to get it.

NSCI: There have been numerous studies saying the U.S. has a gap between the number of cyber – and STEM, in general – graduates and what government and industry need. Not only are there not enough in terms of quantity, there are also quality issues in that studies say the country is losing its edge. What do you think about this issue? What is GMU doing to help?

SOOD: This is a really big problem and it's not a new problem. This problem has been recognized for some time. I was the chair of the computer science department for a few years and we were very aware that our enrollments in computer science were going down – and we were doing better than the national average. It's a real national problem.

I know that different people have different approaches. One lady I know goes to middle schools to talk about cybersecurity to students and explain the importance of detecting issues. This is just one example. We need to create a mix of policies which will actually create a footprint and increase the number of students interested in cybersecurity, computer science and STEM topics.

Project Seed is an example of how in-classroom teaching can reach out to all the kids. They have been around for 50 years and teach higher level math concepts to elementary, middle and high school kids. For example, I have observed a 10-year-old girl prove two to the power zero is one. This requires multiple steps and she conceptualized and assembled all of the steps. More information is available at www.projectseed.org.

During the Dot-Com Boom, enrollments in these subjects were increasing. It's in this Post Dot-Com Boom that we're seeing the decline. Students are reacting to the environment. It's entirely possible that more students will come back into this arena as the economy changes and people realize there are more jobs available in this area.

I still believe we need to take action. We need more evangelists for these disciplines and show that it's not boring. There's some exciting stuff to be done and exciting results to be obtained. There are going to be lots of jobs in this area.

I'll give you one other example. For STEM work, giving students the opportunity to actually do experiments on their own – in the absence of adults – gives them a feel for these things. I think that interaction would be really useful. I think we can build such systems. For example, in Northern Virginia, we should have an interactive environment where kids can experiment and get a good feel for this.

Some years ago, I went to a museum in California – the Exploratorium – where kids can try different experiments. I was fascinated by the experiments. My kids were in college at the time and they were fascinated by the experiments. We need some way to show elementary, middle and high school kids it's not a dry subject. Especially in computer science, we need to attract many more women and other underrepresented minorities to our program.

The goal is do-able, but it will require an investment of time and money. I don't remember the exact numbers now, but we have two kinds of students in our masters program. Our part-time students are U.S. citizens. Most of our full-time students are foreign-born.

It's a very difficult problem.

NSCI: Would you explain the concept of "intrusion tolerance"? Would you please give us an overview of the Self Cleansing Intrusion Tolerance technology you created?

SOOD: Attracting students to STEM is much more challenging than what I've done with this technology.

The whole concept behind what we are doing is based on the following principles. The first principle is that intrusions are inevitable. No matter how hard you try to stop them, intrusions are going to happen. The second thing is that once an intrusion takes place, people are in the system for long periods of time – days, weeks, months.

The problem is that people get in the system and keep quiet – they're sleeping. Then on command they can do bad things to the system. Our whole idea is that, in addition to the conventional detection and prevention paradigms, we have to do something about dealing with and living with intrusions that take place. That is my formulation of the intrusion tolerance problem.

So, once an intrusion takes place, what do you do about it? What our system does is attack this problem by noting yet another principle – that our servers are really sitting ducks. We bring the server up and we never take it down, unless it gets hit by attackers or something else bad happens. Think in terms of an attacker. The attacker is sitting there and they have all this time to study the server, figure out the vulnerabilities, experiment, etc. We are keeping our servers on all the time.

Our approach is to conceptualize and build systems. Our focus is on service with short-transaction time. We have looked at these kinds of systems and have built servers in which the server is up for only one minute. So, the attacker only has one minute to do bad things. After one minute, we shut it down and we start up another server. We have continuous service, but each individual server is only exposed to the Internet for one minute.

Effectively, we shut the server down after one minute, then revert to a pristine copy of the system and bring it up on another system. What we have done is taken a static server and converted it to a dynamic environment. By converting a static system to a dynamic system, I can change the face of the server every minute by using diversification, which makes it even more difficult for the attacker. I know that diversification adds cost, so I'm not recommending this for all systems, but for high-value systems with critical data, this is something which can be incorporated.

NSCI: What are other implications of this technology?

SOOD: This technology has the potential to solve other lingering computer system problems. There are some positive side effects of this technology which lead to what I would call "operational resilience." For example, many systems suffer from memory leaks. Memory leaks do not appear in the short-term; systems degrade over the longer term. It could take days to find the impact of a memory leak and it could lead to a system crash. Our solution actually avoids memory leaks from impacting system performance. We prevent the leak from having an impact. The leak doesn't have an impact in one or two minutes. In that time, we've restarted the server.

My point is we solve intrusion tolerance, but we've also found a number of other positive side effects, which actually impact the bottom line of operations. In addition to memory leaks, we facilitate the application of hot patches, which basically means I do not have to shut down the server to apply the patch. By reducing the impact of memory leaks and hot patches, the number of stand-by servers you need can be reduced. We're actually reducing memory leaks and the costs of operations and increasing security at the same time.

Our solution also has the impact of reducing security operation costs. More details about the benefits of our approach are available online at www.scitlabs.com.

Benefits of SCIT Technology

Cybersecurity Benefits:

- SCIT removes malware every minute without detection
- SCIT reduces data ex-filtration
- SCIT does not rely on signatures and is threat independent
- SCIT automatically recovers from defacement or software deletion attacks: mission resilient
- SCIT reduces the time from compromise detection to recovery
- SCIT enables the use of different types of diversity, leading to admin cost – security trade-off
- Explicit use of time in secure system design

Operational Resilience Benefits:

- SCIT facilitates the application of hot patches: apply patches without rebooting the server
- SCIT servers have the potential for fast recovery from bad patches
- SCIT avoids failure from progressive faults

NSCI: How can the SCIT be used by the military, industry and/or government? Has this technology been commercialized?

SOOD: We have built systems for Web servers, e-commerce servers, DNS servers and Single-Sign On. If you have these kinds of servers, our technology will work for you. Our approach will also apply to other short transaction servers like e-mail, LDAP, etc. The problem is the scalability of these things, but we have spent extra time building software to ensure the scalability. Our systems have been tested at Northrop Grumman and Lockheed. They have confirmed that this does what we claim. We have had independent validation. We've started a technology spin-off, called SCIT Labs. SCIT Labs is commercializing this technology. We already have three patents issued and we have three more patents pending. We've taken all of the steps necessary to commercialize this technology. SCIT Labs is now talking to potential customers about creating pilots. That's how we will eventually be able to sell this to military, government and industry.

NSCI: What industry, government or international groups has the ICC partnered with on research projects? Have any of these projects resulted in the development of new technology?

SOOD: Our major focus is on intrusion tolerance. This research was initially funded by the U.S. Army. NIST supported a critical infrastructure project. SUN gave us some money to support this. Lockheed and Northrop Grumman were very involved with different aspects of this project. These are some of the people we have partnered with.

The workshop we ran in Zurich was sponsored by the Office of Naval Research and had the eight contributing industry co-sponsors: eBay, SallieMae, Deloitte, Cigital, SailPoint, Netwitness, CSC and Zynga.

We are also working very closely with Lockheed, Accenture and SallieMae on the research we are doing.

NSCI: What do you see happening today that promotes a more global, strategic approach to combating cyber crimes?

SOOD: There are several groups which are involved with the non-profit, commercial and government sectors. The Computer Emergency Response Team (C.E.R.T.) groups are a good example – C.E.R.T. in Africa, C.E.R.T. in Organization of American States (OAS) and C.E.R.T. in Rest of the World.

C.E.R.T. capacity building is by itself not the complete solution, but it's an indication of the international recognition of this activity. Earlier this year, we conducted a survey of C.E.R.T. activity in Africa. People in the OAS saw our survey and have asked us to do a similar survey for OAS countries. We're doing these surveys and pinpointing what needs to be done – formulating the next steps.

Many other people are doing this type of work. But, we're conducting surveys and interacting with people in different countries. I talked about Zurich workshop, but last year, we organized something

with the Office of Naval Research in Oxford, United Kingdom, focusing on cybersecurity and global affairs. This is part of our effort to look at this from an international perspective.

NSCI: Many senior leaders have called for public-private partnerships in cybersecurity research and development. How can your team contribute to these partnerships?

SOOD: We're contributing by building a community of interest. In all things that we do, we try to get an even mix of academics, private sector and government folks. This is our way of trying to build a group that can actually build a broad partnership.

The question is "How do you make these partnerships more effective?" That is a question that requires continuous work and energy. The more public-private partnerships you have, the more energy and funding it takes to sustain them. We need to focus on a few effective partnerships with broad participation and develop them for long-standing relationships.

NSCI: Thank you very much for your time.