HOW I BUILT A CYBER SECURITY RESEARCH CENTER FROM GROUND ZERO

Dr. Bhavani Thuraisingham

Louis A. Beecherl, Jr. I Distinguished Professor of Computer Science
Director of the Cyber Security Research Center
Department of Computer Science
Erik Jonsson School of Engineering and Computer Science
Box 830688, EC 31
The University of Texas at Dallas
Richardson, TX 75083-0688
Email: bhavani.thuraisingham@utdallas.edu
Voice: (972) 883-4738 ; Fax: (972) 883-2349
URL: http://www.utdallas.edu/~bxt043000/

November 2, 2010

1. INTRODUCTION

In this article I have given my views and experiences in putting together a cyber security research center from ground zero. To put together a successful research center in academia, you need to focus on four aspects: ***Research, Teaching, Professional Activities and Technology Transfer***. More importantly you need to build a strong team: I strongly believe in the motto "***It's all about teamwork***". Finally, you need to plan step-by-step and "***ensure sustainable growth***". Below I will discuss how we put together such a center and provide an overview of our research, teaching, professional and technology transfer activities. For each area I will give my background and what I did at the university since October 4, 2004 to promote cyber security. I will conclude with our plans for the future.

2. RESEARCH

My Research Background Much of my research over my 30 year career has been in secure data management systems. I started this research in 1985 and have made significant contributions to the field. In particular, I utilized my PhD research in theory of computability with my systems expertise in industry to develop secure data management system designs and prototypes based on fundamental principles. My specific research contributions until 2001 were in secure relational data management, inference problem secure object data management, secure distributed data management, and secure real-time data management. Between 2001 and 2004, while at NSF, I established the data security program and started my own research in secure semantic web and data mining applications. When I joined UTD in October 2004, I was a Fellow of IEEE and AAAS, and had also received IEEE Computer Society's 1997 Technical Achievement Award for outstanding contributions to data security. I had published about 60 journal papers, over 100 conferences papers, 6 books, and had 3 patents. I had given about 30 keynote/featured addresses at various international conferences.

UTD Research: I joined UTD on October 4, 2004 as tenured full professor of computer science and director of the Cyber Security Research Center. While I was given a reasonable startup package as a professor, there was no funding given for the Cyber Security Research Center. Furthermore, UTD had spent over $1m on a lab called SAIAL (Security Analysis and Information Assurance Lab) prior to my joining and requested me to utilize SAIAL for the center. On the positive side, UTD had just been awarded the NSA/DHS Center for Excellence in Cyber Security. Furthermore, AT&T had given UTD a $50K gift for cyber security research for becoming the Center of Excellence and the school gave matching funds of another $50K. Prof. Edwin Sha, a PhD from Princeton, had prepared and taught an excellent

course on information security both at the undergraduate and graduate level. Some of the faculty were already doing some research in cyber security. The Jonsson School of Engineering had received as $300m grant from the state. Nevertheless, due to the fact that I was new to academia, I had the daunting task of not only establishing my own research but also to develop the UTD's cyber security center virtually from ground zero.

After an initial assessment of the cyber security research at UTD, I decided to focus on data security as I was considered an expert in that field. I felt that it would be challenging for us to compete in other areas of security at the national level. Furthermore, assistant professor Latifur Khan, a PhD from USC, had many research interests in common with me and therefore I began a collaboration with him in the areas of assured information sharing, data mining for security applications and secure semantic web. I introduced the second cyber security course at UTD and that was in data and applications security. I used the textbook I had just written as it was the only textbook at that time. We were able to create substantial interest in this topic among the students. With respect to SAIAL, while I felt that it was built to support classified work and yet we were not a classified facility, it would be an excellent vehicle to showcase our systems to the customers and also conduct network penetration testing as well as digital forensics experiments. Furthermore, the lab had excellent computing power which we could use for research in areas like secure grid. Finally, for the gift we received from AT&T, we gave out awards within UTD to 5 faculty members to continue their research in the field.

At the end of my first year, Prof. Khan and I were successful in obtaining a research grant from AFOSR on assured information sharing. We also hired an assistant professor, Murat Kantarcioglu, who had completed his PhD at Purdue in data security and he was an expert in data privacy. By that time, we had a few PhD students in data security. We organized the cyber security conference to make the local community aware of our research. During the second year we expanded our research base and received a second grant from AFOSR with Prof. Kantarcioglu as the PI on data integrity and Prof. Khan and I established collaboration with Raytheon. In the Fall of 2006, we added one more person to our team, Assistant Prof. Kevin Hamlen, who joined us from Cornell after his PhD in secure programming languages. We now expanded the courses to include cryptography, data privacy and secure languages. In addition, Prof. Khan introduced data mining for security applications as part of his data mining course. We made excellent progress on our research grants by publishing papers in top journals and also began to publish papers in top conferences. One of the significant outcomes of our work was a 1 page write-up that we prepared for the MURI BAA that came out in 2007. Our one page was included in the BAA which was quite significant. I graduated around 6 MS students with thesis.

Our activities converged in 2007. Prof. Hamlen received the AFOSR YIP, we received our first NSF research grant and Prof. Khan received grants from NGA and NASA. The collaboration with Raytheon was flourishing and we had submitted a MURI proposal. The research funding for the center surpassed $1m by September 2007. While my research focused on assured information sharing, data mining applications in security and secure semantic web, the team's research now included secure geospatial data management, privacy, secure languages and applying social sciences for cyber security. We started building a brand – the team that conducts interdisciplinary research in cyber security. We introduced additional courses in cyber security.

The year 2007-2008 was very productive. We expanded our sponsor base to include IARPA and received substantial research grants. The most significant was the success of our MURI proposal. Also, my first PhD student graduated and obtained a job as senior security analyst at EBay (she is now on Wall Street with DTCC). Our research funding was about $9m. We also expanded our research to include secure cloud computing and ontology alignment. We started research collaboration with Kings College London and the University of Insubria which helped these two universities to get research funding from EOARD (USAF in Europe). We also received the NSA/DHS Center for Excellence in IA Research.

During 2008 - 2009, we continued to excel in research. Our sponsor base now included NIH and ONR via Prof. Kantarcioglu. Prof. Kantarcioglu received the NSF Career award. My second PhD student graduated in December 2008. I organized the NSF Data and Applications Security workshop, to provide directions in the field to the government sponsors. We were now being recognized as one of the best teams in data security. Our research appeared in press releases outside of UTD (e.g., Boston Globe). We also appeared a few times in CW33 News discussing the challenges in cyber security. Our research funding was about $11m. We also established a long-term collaboration with UTD's Schools of Management and Economics Policy and Political Sciences.

During the year 2009 - 2010, while my team continued to get grants from NSF and AFOSR, my focus was mainly on technology transfer and cyber security education. We developed several tool repositories (e.g., Semantic Web, Data Mining, and Data Privacy). These tools have received a lot of positive feedback from the research community. In addition, we also established a company (Knowledge and Security Analytics) as a UTD spin-off company. We filed a patent on our stream mining research and had several invention disclosures. While I continued to write books in data security which I use as text books for my class, we started converting PhD theses into books (e.g. Design and Implementation of Data Mining Tools, Data Mining Tools for Malware Detection). My third PhD student successfully defended his thesis in October 2010. The team graduated several PhD students in cyber security. I made use of SAIAL as a cloud computing lab and also used it to conduct digital forensics experiments. In addition, a few other professors were using the lab to conduct security testing activities. Our notable achievement is that AFOSR selected our research on secure cloud computing to do a press release on their web site in June 2010. We expanded our collaboration with Rockwell and together we have now submitted DARPA proposals. We established research collaboration with IBM Almaden Research Center. We are also trying to go beyond data security. I have included Prof. Kamil Sarac who works in network security as a core member of the team. I collaborate with Prof. I-Ling Yen on secure infrastructures and Prof. D.Z. Du on applying complexity results to security problems. I was instrumental in UTD getting the NSF cyber security scholarship award (to be explained under my Teaching). Finally, we have started research collaboration with IIIT New Delhi on data mining for counter-terrorism and are hoping to replicate the success we have had with our European partners and help our Asian partners get funding from AOARD (USAF in AsiaPac).

I believe that to succeed in academia one cannot just be a manager. One has to lead and at the same time make significant technical contributions. Therefore, while building the cyber security research team, I have also made my own significant research contributions to policy-based information sharing, inference control with trustworthy semantic web, and data mining for cyber security. In the area of policy-based information sharing, together with my student, a system was designed that would share data but at the same time enforce appropriate policies. We also developed measures as to how much information is lost due to the enforcement of policies. In the area of inference control-based on semantic web, together with my student, we designed a system that reasons about the policies and determines what information should be released to the user to protect against logical and association-based inferences. In the area of data mining for security applications, together with students we designed data mining algorithms that would detect various types of suspicious events as well as malware. Since joining UTD, my research has been published in several prestigious journals including IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions in Dependable Computing, IEEE Transactions on Systems, Man and Cybernetics and ACM Transactions on Information and Systems Security. I have now around 100 journal publications, over 200 conferences, 10 books, 4 patents (one pending), and over 90 keynote addresses. I was rewarded by not only receiving a distinguished professor title at UTD, but also by receiving 3 prestigious external awards in 2010: the 2010 Research Leadership Award for "Outstanding and Sustained Leadership Contributions to the Field of Intelligence and Security Informatics" presented jointly by the IEEE Intelligent and Transportation Systems Society Technical Committee on Intelligence and Security Informatics in Transportation Systems and the IEEE Systems, Man and Cybernetics Society Technical Committee on Homeland Security; the 2010 ACM SIGSAC (Association for Computing Machinery, Special Interest Group on Security, Audit and Control) Outstanding Contributions Award for "seminal

research contributions and leadership in data and applications security for over 25 years"; Distinguished Scientist of ACM for Significant Research Contributions to Computing. In addition, I was also elected fellow of the British Computer Society in 2005.

Where do I want to take UTD's Cyber Security Research 2011 and beyond? My goal is for UTD to continue to excel in data security, but also venture into others areas, especially systems and network security. Together with the team, we are in the process of finding niche areas and hope that UTD will support us in hiring one junior professor in systems security. I am also trying to expand our sponsor base to include DARPA, Army and DHS as well as work with additional corporations. More importantly, I plan to graduate 7 more PhD students by December 2012 and convert several PhD theses into books. Being involved with national strategies and plans for cyber security research will continue to be our goal. Finally, interdisciplinary research will continue to be the key to our success.

3. TEACHING/EDUCATION

My Teaching Background: Soon after my PhD, I took visiting faculty positions at New Mexico Institute of Mining and Technology and later at the University of Minnesota between 1980 and1983 in order to raise my son who was an infant at that time. During this time I taught several graduate courses in my field (theory of computation) as well as undergraduate courses. Later, while in the computer industry in Minneapolis, for six years I worked at the University of Minnesota as an adjunct professor and member of the graduate faculty in computer science. While co-advising students, I also taught several courses in computer science at the junior and senior undergraduate level as well as a seminar graduate course in information security. Later while at MITRE Corporation for 13 years, I was an instructor at the MITRE Institute and through the institute taught several courses to MITRE and its sponsors at several sites. I also gave several tutorials at conferences sponsored by IEEE and ACM. I was an instructor at AFCEA teaching courses at several Air Force bases. Between 1999 and 2001, I taught as adjunct professor at Boston University (Metropolitan College).

UTD Teaching: I joined UTD on October 4, 2004 as tenured full professor of computer science and director of the Cyber Security Research Center. My main responsibility was to develop the cyber security research from ground zero. UTD had recently obtained the designation of NSA/DHS Center for Excellence in Information Assurance Education. After an initial assessment, I found that while Prof Edwin Sha has prepared and taught an excellent course in information security both at the undergraduate and graduate level, we needed more courses. Even though cyber security education was not my responsibility, I felt that education was key to the success of our research. Therefore since joining UTD, I have played a major role in cyber security education.

I first introduced a course in data and applications security, which is my area of expertise, in Spring 2005. Around that time I published my book on this topic and used it as the text book as it was the only book available at that time. Since then I have been teaching this course every year. This course is very popular among the students and the enrollment for this course is usually 50+ each year. I also taught a version of this course at the undergraduate level. During the latter part of Spring 2006, UTD established a minor in information assurance education and this minor consisted of three core courses: one is information security taught by Prof. Sha, the second is data and applications security that I taught. Due to the fact digital forensics is a popular topic, UTD requested for me to teach this course as the third course for the minor. Even though this is not in my area of expertise (as digital forensics combines technology with legal and social aspects), I took on this challenge in Fall 2007 as there was a strong need for this course. For this class I worked with Richardson Police Department, UTD Chief Security Officer and the North Texas FBI and organized guest lectures and lab tours. This class also enabled the students to use SAIAL lab to conduct experiments. I purchased a forensics tool called ENCASE out of the cost share funds I received for research as I felt that working with tools was critical for the success of this course and the department did not have funds for the tools. I will continue to teach Digital Forensics until Prof. Kevin Hamlen is

ready to teach this course in Fall 2012. While I have been teaching the digital forensics course, Prof. Kantarcioglu has taught the data and applications security course for the undergrad students in order for our students to obtain the minor.

During Fall of 2005 I taught a course in biometrics. I have not had the opportunity to teach this course again due to the fact that I introduced another course on trustworthy semantic web which has become an annual course. While the initial focus for this class was for PhD students, there was a huge demand for MS students to take this course. This is also one of the more popular courses at UTD and the enrollment is usually 50+ each year. I use my book as the textbook as there is no book that addresses security for semantic web. In the future, during one of the summer sessions, I plan to teach the biometrics course again.

While developing the Cyber Security Research Center, I have put together a strong research team (Please see Research section). This team has also contributed toward UTD's education in cyber security. For example, in addition to teaching data and applications security at the undergraduate level, Prof. Murat Kantarcioglu teaches a regular course on cryptography and an occasional course on data privacy. Prof. Kevin Hamlen teaches a course on secure languages. Prof. Khan has introduced data mining for security application as part of his course on data mining. I coordinate with Prof. Kamil Sarac for him to teach a course on Network Security. As a result, we now have a fairly strong education program in cyber security.

During Fall 2009, I felt that we were now ready to apply for the NSF Scholarship for Service (SFS) Program in Information assurance. I discussed with the department head and we felt that Prof. Sarac would be ideal to head this effort. I organized a visit with NSF program directors and introduced Prof. Sarac to the directors. In addition, I also visited prior recipients of this award at NYU Poly, Mississippi State University and University of Tulsa and obtained copies of their proposals for Dr. Sarac. I also contributed a great deal to the proposal writing. I addition, we also established an MS Track in Information Assurance starting Fall 2010. We were successful in getting this very important $1.8m award during the first try. This is significant for us as we can now use this grant to hire US citizens and train them in IA so that they can get federal jobs. Furthermore this also gives us opportunities to apply for additional large education grants in IA through NSF and other agencies.

Federal jobs in IA require CISSP certification. Therefore, to get the confidence of the federal sponsors who provide the funding to NSF for the SFS program, I studied and completed the CISSP certification in June 2010. This certification is highly regarded in the IA industry. During the summer of 2010 I taught the Information and Security Analytics course which covers the ten modules of the CISSP examination. I will be teaching this course periodically so that our students can take the CISSP exam if they choose to. I also completed the Terrorism Studies certification at St. Andrews University in Scotland (which is considered to have the top terrorism program in the world). This certification will help me to better prepare courses in data mining for counter-terrorism which I teach to our government sponsors periodically.

Another course I am planning to introduce in the summer of 2011 is on Building and Securing the Cloud. Cloud computing is a major research area for us due to a large grant from AFOSR. We are developing a secure cloud at UTD. I am writing a book on secure cloud computing which I will use for my class next year. I believe that cloud computing is the way of the future and therefore it is important for UTD to be one of the leaders in this field. I am also in discussion with the department head to introduce certificate courses to the industry on information security and cloud computing.

What do I envisage for the future for cyber security education at UTD? My main goal is to make UTD the #1 University for government, industry and students around the world in IA education. I will continue to work with Prof. Sarac and the rest of the UTD team to make this happen. For example, we found that no one was available to teach the Data and Applications Security course at the undergraduate level for spring 2011. I volunteered to teach this course as I felt that it was important to maintain the continuity even though this would mean that I would teach 4 courses for the two semesters while none of the other

professors to my knowledge teach more than 3 courses for the year. While this would be a major undertaking for me while still maintaining a large research program, I believe that teaching this course is important for our students. My second goal is to get the industry and government involved in our education program by giving us problems to solve and giving guest lectures. I believe that our students have to be trained to excel in industry, government and academia. My third goal is to continue to establish new programs in cyber security. One such program is an integrated cyber security MS degree together with the Schools of Management and EPPS. This would put us in a much better position to apply for IGERT and other education awards. My final goal is to continue with my professional education to better prepare students for practical careers in industry and government and the next step is to get my certification in penetration testing and ethical hacking from SANS Institute. I will also be requesting UTD to hire one more faculty in IA to meet the ever increasing demands in this area.

4. PROFESSIONAL ACTIVTIES

My Professional Activities Background: Prior to joining UTD, I had served on conference program committees since 1987 and as program chair since 1992. I had served on at least 60 program committees and was program chair for about 15 conferences. I have also worked as reviewer for several conferences, journals, NSF and agencies such as NSA, DHHS and CIA. I have served on panels at the National Academy of Sciences and given talks at the White House Office of Science and Technology Policy and the United Nations. I have also served on several editorial boards including IEEE Transactions on Knowledge and Data Engineering, ACM Transactions in Information and Systems Security, IEEE Transactions of Dependable and Secure Computing and many more journals. I have also given tutorials at conferences and given lectures for IEEE and ACM and served as a Distinguished Lecturer for IEEE between 2002 and 2005. I have also given talks at conferences organized by WITI and SWE as well as CRA-W, and participated in Women of Color conferences organized by Career Communications Inc.

UTD Professional Activities: I joined UTD on October 4, 2004 as tenured full professor of computer science and director of the Cyber Security Research Center. My main responsibility was to develop the cyber security research from ground zero. Since joining UTD, I have developed the Cyber Security Research Center into an $11m research program and a $2m education program. My professional activities have contributed a great deal toward enhancing our research and education in Cyber Security.

I have continued to serve on program committees and chair conferences. To date I have served on well over 100 program committees and chaired about 20 conferences. I continued to serve on the editorial boards of several journals and between 2005 and 2008 I served as the Editor in Chief of Elsevier/North Holland's Computer Standards and Interface Journal. I have continued to be a reviewer/panelist for NSF. I have also continued to give talks at university and local chapters of IEEE, ACM and SWE. In addition, I have also given talks to high school students at UTD. I also chaired UTD's Cyber Security Symposium in 2005 and am planning the next symposium for 2011. I have brought together the defense contractors at UTD together with the Metroplex Technology Business Council to focus on cyber security activities. I have served on IEEE CS committees since 1997, first as part of the conferences and tutorials board and later as head of the Kanai and Technical Achievement Awards committees.

Recently I have been appointed to two important councils: ACM-W and ACM Policy. As part of ACM-W, I will be motivating women to form ACM Chapters. As part of ACM Policy, I will be advising on privacy and IP issues. Another activity I am involved in is putting together a proposal on NSF ADVANCE to support women faculty in STEM. I have also participated in East West Institute's efforts on protecting children in cyber space.

I have served on several councils and committees at UTD. In particular, I was the chair for CS Department Head search committee in 2008 - 2009, I was a member of the VP for Business search committee 2005 - 2006 and was the member of the School of Engineering dean's search committee 2007-2008. I have also served as head of the promotion and tenure committee for 4 professors (3 for associate

and 2 for full professor) and served as head of the 3rd year committee for one professor. I have served on the committee for tenure and promotion for one other professor.

What are my goals for the future with respect to professional activities? First, I will continue to be a major player in cyber security activities both nationally and internationally. Second, my goal is to motivate the junior faculty at UTD to excel and participate in various activities and chair conferences. Members of my team have begun to chair some important conferences for IEEE. Finally I would like to support and promote women and underrepresented minorities in academia and will continue to work on proposals to support such activities.

5. TECHNOLOGY TRANSFER

My Technology Transfer Background: This is an area I have not had the vast experience like I have had in research, teaching and professional activities. I worked for the commercial industry for 6 years before I joined MITRE for 13 years. While at Control Data Corporation I worked in a product development environment and developed some of the layers of the CDCNET product. This gave me the knowledge of the product development process. While at Honeywell I was in a research organization, but we were involved in some technology transfer activities. For example, the distributed data dictionary system we designed and developed was transferred to Honeywell's Residential Control Division. We also worked on applying expert systems for process control and that work resulted in transferring the technology to Honeywell Industrial Automation Control Division. I also did some work on applying object technology for control systems and this work was transfer to Honeywell's Commercial Control division. While at MITRE I worked on real-time systems experimental research and this was transferred to next generation AWAVS system.

UTD Professional Activities: I joined UTD on October 4, 2004 as tenured full professor of computer science and director of the Cyber Security Research Center. My main responsibility was to develop the cyber security research from ground zero. Since joining UTD, I have developed the Cyber Security Research Center into an $11m research program and a $2m education program. My professional activities have also contributed a great deal toward enhancing our research and education in Cyber Security. During 2009 - 2010 my main focus has been on technology transfer.

Here are some of the activities we have carried out so far. We worked on two SBIR proposals to get the experience in 2009 before we started the company. While these proposals have not been funded, the process was very useful to us. About the same time, we made several invention disclosures including on policy-based information sharing, stream data mining and location aware geospatial computing. We also formed a company called KSA (Knowledge and Security Analytics) which is a university spin-off company and have written a business plan for the corporation. We are developing the technologies further so that we can market them to potential customers. We are actively pursuing SBIR/STTR grants. We are also planning to apply for Texas Emerging technology Funds in early 2011. KSA is jointly owned by Profs. Thuraisingham, Khan and Kantarcioglu.

Where do I want to take KSA into 2011 and beyond? Our current challenge is to maintain our research, teaching and professional activities and at the same time develop KSA. Our professor jobs are #1 for us. Therefore, how can we develop a successful company but at the same time continue to excel as professors? We will talk with other entrepreneurial professors who have succeeded and learn from their experiences. We believe that having a successful company would also mean success to the university as the university is part owner of KSA.

6. FUTURE OF CYBER SECURITY AT UTD

Before I discuss the future, I will mention the lessons I have learned. First of all, would I have done things differently? In general I would say no. However, I feel that there are a few things I might have done differently. During the first year, I rushed and submitted proposals without careful planning. This was

partly due to the intense pressure I was getting from the administration to get grants. In fact, I was asked the question “Can you bring $2.5m in 1.5 years if I give you 10K to fund the cyber security conference?” Also, I should have asked for some funds to support the center. But because I did not come from academia, I did not have much to show in terms of getting competitive funding and this put me at a disadvantage. I should have thought more carefully and submitted no more than 2-3 proposals in the first year. Nevertheless the proposal that AFOSR funded during the end of my first year was a tremendous win for us as that propelled us into success for the future. Also with my startup funds, I did not want to put all the eggs into one basket. While I wanted to develop secure semantic web technologies, I used the funds on several small projects that included privacy-preserving data mining, secure social networks, secure semantic web, data mining for security and secure geospatial data. On the positive side, these areas have resulted in some large projects for us.

One area I did very well is on building a strong team. As I mentioned earlier, “it’s all about teamwork”. Therefore, getting the right people together was a success. We would like to include one more person in systems security and that would make our team complete. Also, we waited a while before applying for the NSF SFS grant. This is because we wanted to have a solid base in research and education before I felt we could succeed in executing the grant. I am very pleased with the research, teaching and professional activities we have carried out so far. With respect to technology transfer, our major challenge isl being successful entrepreneurs while continuing to excel as professors. There has to be tradeoff between rushing to publish and disclosing the IP.

In the future, we want to continue excelling in research, teaching, professional activities and improve on technology transfer. We want to collaborate more with the local corporations. DFW has over 800 hi-tech corporations and I would like to build a consortium with these corporations. We would also like to write more proposals with defense contractors and also collaborate with other companies.

There is expected to be unprecedented growth in “anything cyber” including cyber security and cyber analytics. Therefore, we are very well-positioned to take advantage of all the government and industry have to offer in this area. Finally, motivating the very bright junior professors and educating the students have been very rewarding experiences for me. Our junior professors of today and our students will be UTD's Cyber Security Research Center of tomorrow.