Polytechnic University of Puerto Rico
School of Engineering and Geomatic Sciences
Electrical and Computer Engineering and Computer Science Department

PI: Alfredo Cruz, PhD
NRC Award # NRC 27-10-511

NRC Performance Progress Report Narrative
Period: Ending March 31, 2013.

The following activities have taken place during this report period:

Through this grant, PUPR continues to contribute to NRC's priority of developing professionals with the skills to defend against cyber-attacks and vulnerabilities, for the protection of critical infrastructure.

One of the Fellows was able to participate in the co-op program at LLNL for a second time (due to his excellent work) in February 2012. He was working in the Information & Communication Services group as a software engineering student in several business projects that will be put into production soon. This Fellow has successfully defended his Master thesis in "Mobile Ad-Hoc Networks (MANET)", with Co-PI Dr. Jeffrey Duffany and is going back to work with Lawrence Livermore National Laboratory (LLNL). His thesis focuses on the study of MANETs to learn how the network reacts to different situations when it is being taken to the breaking point. The fellow is aspiring for a possible full-time job opportunity as a computer scientist at LLNL, a DoE Laboratory which complies with the NRC contract agreement. The fellow wishes to continue this research for his PhD, which he is considering to start in a few years.

During this period, we were proud to graduate the first of the four NRC fellow students who were initially selected. The other three students are very busy on their thesis/project work; and we have a new student in her first year. All have shown a great interest and dedication to complete their degrees successfully and contribute to the shortage of qualified professionals in related areas of nuclear engineering.

Fellow Graduate Student Oscar P. C. Successfully Defending his Thesis

Graduated Fellow Oscar P. C. thanks the NRC Fellowship Committee for the opportunity:

"To the NRC Fellowship Committee:

I would like to thank the Nuclear Regulatory Fellowship Commission (NRC) for their financial support during my Master's degree in Computer Engineering and the opportunity at receiving the fellowship. Without this opportunity, I would not have been able to participate of the internships at Lawrence Livermore National Laboratory. I'm currently in California working at the lab once more on the same group I worked last year with the possibility of a full time job after graduation in the summer. Again, thank you for this opportunity.

From: Oscar P C"

Internships

Fellows have been able to make many connections from all the conferences and workshops , and learned about the many opportunities and resources available to graduate students that are out there. One has applied to many summer internships in the area of cyber security and have had a number of interviews. She has received two summer internship offers: one for the Research Alliance in Math and Science (RAMS) at Oak Ridge National Laboratory in Oak Ridge, Tennessee, and one at Lawrence Livermore. She has also been accepted for a two day externship with Deloitte in August 2013 in their Center for Security & Privacy Solutions in Washington DC.
Another returned to her studies after finalizing the summer internship at LLNL. She then attended the Polytechnic University of Puerto Rico job fair in October where she talked with representatives of several federal government employers. She applied for several job openings in different branches of the federal government and currently has two conditional job offers.

Conferences and Workshops

Since September 2012 students had the opportunity to attend five conferences. Participants of these conferences were fully sponsored by travel scholarships:

- **October 11 – 14, 2012 - SACNAS National Conference. Washington State Convention Center, Seattle, WA.**
- **October 16 – 18, 2012 - 7th International Conference on Malicious and Unwanted Software. Fajardo, Puerto Rico**
- **November 10-15, 2012 – Supercomputing 2012 (SC12), Salt Lake City, Utah**
- **February 7-10, 2013 - 2013 Richard Tapia Celebration of Diversity in Computing, Washington, D.C.**

Description and impression of the five conferences attended:

October 11–14, 2012 - SACNAS National Conference. Washington State Convention Center, Seattle, WA.

This is an interdisciplinary, highly interactive and transformative conference that motivates, inspires and engages participants to achieve their highest goals in pursuing education and careers in STEM fields. Conference programming is specifically tailored to support undergraduate and graduate students, postdoctoral researchers, and career professionals at each transition stage of their career as they move towards positions of science leadership. One of our Fellows presented a poster in this conference. The poster

by Fellow Patricia Becerra titled: "Understanding Mobile Malware through Reverse Engineering" is included in the report with the proper attribution to the NRC.

NRC Fellow Patricia Becerra at the SACNAS National Conference

October 16 – 18, 2012 - 7th International Conference on Malicious and Unwanted Software. Fajardo, Puerto Rico
This conference is held yearly in Puerto Rico and gathers worldwide researchers in the area of malware. Our NRC Fellows where the only students invited to attend this international meeting.

November 10-15, 2012 – Supercomputing 2012 (SC12), Salt Lake City, Utah
SC is a high performance computing (HPC) conference that included technical papers, tutorials, posters and speakers. There were some of the most well-known figures in high performance computing and representatives from the biggest companies in the area of HPC. Some of the invited speakers include Ann Almgren, Lawrence Berkeley National Laboratory, Arthur S. Bland, Oak Ridge National Laboratory, Kirk Cameron, Virginia Tech, Alan Gara, Intel Corporation among many. The keynote speaker was Dr. Michio Kaku is a theoretical physicist, best-selling author, and popularizer of science. As the co-founder of string field theory (a branch of string theory), he continues Einstein's search to unite the four fundamental forces of nature into one unified theory that will summarize all the physical laws of the universe. His talk was based on his book *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100*, which was published in 2011. Based on interviews with over 300 of the world's top scientists, Dr. Kaku presented the revolutionary developments in medicine, computers, quantum physics, and space travel that will forever change our way of life and alter the course of civilization itself.

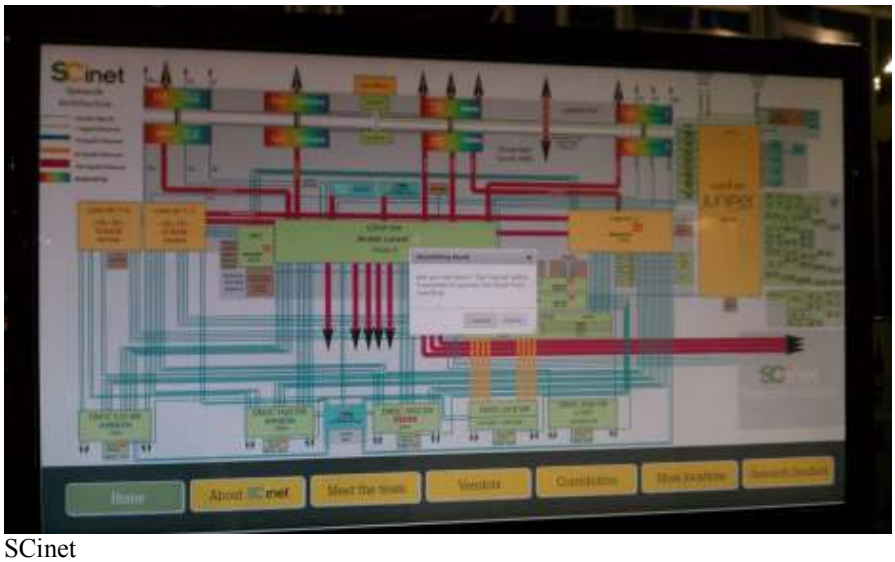
Keynote speaker Dr. Michio Kaku


Fellows at the exhibitor floor.

There were great lectures, workshops and Birds of Feather Sessions and in particular, our students were interested in HPC applied to cyber security. One of the birds of feather sessions was titled *Cyber Security's Big Data, Graphs, and Signatures* and it was great to see HPC applied to the very real problem of network security. Today's problems are no longer limited to malware using hash functions. Interesting problems, such as coordinated cyber events, involve hundreds of millions to billions of nodes and similar or more edges. Nodes and edges go beyond single attribute objects to become multivariate entities depicting complex relationships with varying degree of importance. To unravel cyber security's big data, novel and efficient algorithms are needed to investigate graphs and signatures. This session brought domain experts from various research communities to talk about current techniques and grand challenges being researched to foster discussion.

These conferences offer students many opportunities to network with people from the industry at the exhibitors, where they presented products and explained how they addressed problems in HPC.

There was also an impressive, leading-edge, high-performance network assembled called SCinet assembled as a platform for exhibitors and attendees to demonstrate new HPC innovations. This network was a collaboration effort from different vendors and partners and we were able to see it first hand. Just as computational researchers are examining scalable computing and storage models, network researchers are developing innovations for improving science data transport that connect these computational resources. Below is an image of the network.



SCinet

February 7-10, 2013 - 2013 Richard Tapia Celebration of Diversity in Computing, Washington, D.C.

Three Fellows had the opportunity to attend the Richard Tapia Celebration of Diversity in Computing Conference in Washington, D.C. to. One of the fellows was chosen to present a poster of her research in the conference. The title of the poster by Fellow Yesenia Diaz

is: “Audio Fingerprinting with Robustness to Pitch Scaling and Time Stretching.” Her poster and the attribution to the NRC support are included in this report.

The 2013 Richard Tapia Celebration of Diversity in Computing Conference is organized by the Coalition to Diversify Computing, sponsored by the Association for Computing Machinery, and in cooperation with the IEEE Computer Society and the Computing Research Association. The conference celebrates the technical contributions and career interests of diverse people in diverse computing fields and strives to help all attendees, and especially students, build vital connections that will serve them well both professionally and personally.

As allegedly one of the best conferences students have attended (their opinion), this conference was geared towards a general Computing audience and therefore everyone could understand the lectures even if they were from different areas in computing. There were speakers with impressive credentials and from well-known universities and companies. One of the favorite lectures was “CyberSecurity - The Weak Link in Our Infrastructure” by Anita Jones, University Professor Emerita, University of Virginia. She spoke about how today’s perimeter defense model (on which most cyber security relies) does not work. It reviewed past research, state-of-the-art practices of information security today, and options for improvement.

But most importantly, this conference was a great opportunity for our Fellows to meet some of the brightest students studying and researching in STEM (Science, Technology, Engineering, and Mathematics) fields right now. There is nothing better for our fellows than to meet very intelligent, energetic, ingenious, and hardworking students from all across the nation. It was great hearing them talk about their experiences, research, goals and methods used to solve particular problems.

Fellow Diana D with Dr. Richard T

Fellow D at the Conference

In the near future, our Fellows are scheduled to attend the following conferences:

- **April 4-6, 2013 – CRA-W 2013 Graduate Cohort Workshop, Boston, MA**

  Initiated in 2004, the CRA-W is being generously funded by Microsoft this year, along with significant support from Google as well as contributions from Yahoo!, IBM, and other contributors. Grad Cohort aims to increase the ranks of senior

women in computing by building and mentoring nationwide communities of women through their graduate studies.

- **April 9-12, 2013 – 12th Annual Security Conference, Las Vegas, NV**
  The 12th Annual Security Conference attracts a nice mix of participants from academia, government and industry. Co-organizers for the 2013 event are Virginia Commonwealth University, Plymouth University, University of South Carolina and DePaul University
- **June 13-14, 2013 - DOE-Sponsored National Laboratories Professional Development Workshop for Underrepresented Participants (CMD-IT NLPDev) Oak Ridge National Laboratory –** The workshop includes panels of successful professionals discussing strategies for navigating the professional ladder, effective methods for networking within the lab as well as the broader community, being an effective team member from the perspective of team managers as well as team members, effective communication, and proposal opportunities.
- **WISE 2013: Women's Institute in Summer Enrichment -** June 23 – 28, 2013 at University of California, Berkeley. The summer 2013 program theme is Privacy & Security. Topics to be covered are:
  - Privacy and security of social networks and mobile applications
  - Online tracking and targeted advertising
  - Privacy issues related to mobility, healthcare, and on-line commerce.

Thesis and Research Work

In the past decade wireless networks has been experiencing exponential growth. We have seen great advances in network infrastructures, and the emergence of wireless devices such as tablets and smart phones, all becoming more powerful in their applications. Because wireless network technologies have greatly improved, we see wireless networks being used beyond the coffee shops and homes and into the workplace. Unfortunately, with this mobility and convenience also comes risk.

In December 2011, a security researcher named Stefan V released a paper describing a new attack on the Wi-Fi Protected Setup. The flaw was discovered in the PIN-External Registrar method used to authenticate client devices. V discovered that when the client authenticates with the PIN, the PIN is actually split into two separate four-digit pins, and to make matters worse, the final eighth digit is actually used as a checksum for the PIN. This means that rather than the original number of 100,000,000 possible PINs, there are actually only about 11,000. This drastically reduces the time to brute force the PIN. Attack tools have already been released to exploit this, and on average some take as little as a few hours to successfully brute force the PIN.

One of our NRC Fellows is exploring the WPS vulnerability and attempts to find out the prevalence of the problem as it still exists today, even after more than one year after its discovery. She has been surveying networks in the area to get an idea of how many wireless routers are equipped with this feature and therefore vulnerable, using backtrack 5 and some of its tools including airmon-ng, reaver, and kismet. She also used the wiggle Wi-Fi application on her android phone to identify networks with this feature.

One of the fellows continues to work with Co-PI Dr. Jeff Duffany on the thesis work: "Understanding Mobile Malware". The research is helping to explore how Android Malware works, because this operating system represents the second most popular environment for mobile malware, and to find out how to defend this platform from malicious attacks. In this research, reverse engineering is used as the tool to understand the structure and functionality of the malware. A virtual environment is created for the analysis of the mobile malware to understand how the behavioral analysis, as well as the code analysis, are conducted to determine how you can alert the users to recognize a downloaded malware and what they can do to avoid it. The objectives of the thesis include: Understanding the vulnerability that was exploited with the result that the system is compromise; studying the different viruses that have attacked the android platform; studying the gravity attack and measures to combat; penetrating into the compromised data to study its origin and to obtain information on the compromised machines.