THE
UNIVERSITY
OF RHODE ISLAND

THINK BIG WE DO℠

Proceedings of the

CYBERSECURITY SYMPOSIUM

April 11, 2011

Produced by Ann B. Carlson, Ph.D.

Table of Contents

Proceedings of the URI Cybersecurity Symposium

On April 11, 2011 the University of Rhode Island (URI) held the first in what is planned to be an annual symposium on cybersecurity. Cybersecurity concerns permeate our society and our daily lives and the issues of the safety, security and integrity of cyberspace will only be more critical in the years to come. URI is well positioned to contribute to the local, state and national efforts to address these issues. The symposium, moderated by Peter Alfonso, URI Vice President for Research and Economic Development, brought together a sizeable body of expertise in cybersecurity from the State of Rhode Island and beyond. It opened with addresses by URI President David Dooley, Congressman James Langevin (D-RI), Senator Sheldon Whitehouse (D-RI), and General Keith Alexander, Commander, U.S. Cyber Command and Director of the National Security Agency. In each of the three focused sessions the audience heard first from a Federal department or agency – including the Department of Homeland Security, the FBI Cyber Division, the U.S. Internal Revenue Service and the Defense Advanced Research Projects Agency (DARPA) – on the national perspective, then from an industry representative – including Dell, and Verizon, and finally from URI researchers and graduate students about unique activities and opportunities at URI in addressing the challenges presented. Arthur W. Coviello, Jr., Executive Vice President of EMC Corporation, provided closing remarks. This Proceedings offers a short summary of the main discussion points and challenges introduced by each of the speakers. A post-workshop review by the moderator is also included.

Opening Remarks

David Dooley, URI President

Cybersecurity is a pressing concern for Rhode Island and for our nation. We stand at a moment that is in many ways unprecedented, as we have come to realize the urgent need not only to examine the implications of cybersecurity for defense and homeland security but also for education, business, critical infrastructure and so many other aspects of our daily lives. We have, collectively, a number of challenges to overcome if we as a nation are going to build the kind of security that our people deserve. Times like these call for collaboration, cooperation, and participation broadly across the sectors of government, education, and business. That commitment exists here in Rhode Island, and we have the interest and expertise to step forward as a full partner in both better defining the challenges and producing the remedies needed in order to protect the security of our way of life.

The issue of cybersecurity touches each one of us in a variety of ways. We have questions about the integrity and privacy of our email exchanges with families and friends. We wonder about the security of on-line purchases and financial transactions and the use of ATM machines. Even more so, we have questions about our community and national infrastructure and our national security. We confront identity theft, phishing, on-line fraud, threats to critical infrastructure, and the possibility of cyber warfare. In a society and economy dependent upon the internet, ever increasing computing power, and related advanced technologies, we can only anticipate that issues of safety, security and integrity in cyberspace will be with us for years to come.

The University of Rhode Island is particularly well positioned to contribute to the local, state and national effort to address these issues. URI has nationally recognized education programs at the undergraduate and graduate level in digital forensics, and we offer internships with the Rhode Island Digital Forensic Center, Naval Criminal Investigative Services and the RI State Police Computer Crimes Unit. URI graduates are actively sought out by government agencies and private industry.

URI operates the Digital Forensics Lab (DFL) that performs casework for local agencies and attorneys. The DFL staff designed and built the Rhode Island State Police Computer Forensics Lab, which handles all law enforcement digital forensics work in the state and which is being considered by the National Institute of Justice as a model for the rest of the nation. In research, the URI digital forensics program is the highest funded program in the nation by the U.S. Department of Justice and its researchers are involved in a number of projects related to national and homeland security, many of which will be highlighted in this symposium.

Our state is honored to have a Congressional delegation dedicated to meeting the challenges in cybersecurity. As co-chairman of the Commission on Cybersecurity for the 44th Presidency, Congressman James Langevin led a landmark study on the issues in cybersecurity and laid out a roadmap for beginning to respond to those challenges. He has introduced major cybersecurity legislation in the House of Representatives and he is co-founder and co-chairman of the bipartisan House Cybersecurity Caucus. Senator Sheldon Whitehouse, as chairman of the Senate Judiciary's Subcommittee on Crime and Terrorism, has conducted a series of hearings on cybersecurity and also chaired the U.S. Senate Select Committee on Intelligence's Cyber Task Force. He has been closely involved in efforts to develop comprehensive cyber legislation in the Senate.

This symposium, through its speakers and attendees, brings together a sizeable body of expertise in cybersecurity in the State of Rhode Island. This forms an important base from which we can move forward together, with new energy and commitment, to contribute in this important field.

Congressman James Langevin

In our growing reliance on cyberspace for critical services, national defense, and daily needs, and also in the open and trusting architecture of the internet that our adversaries may exploit, our country faces important cybersecurity challenges. These include the targeting of our critical infrastructure and the systems that protect our sensitive classified information. The already challenging and complex threats are growing in dynamic ways, making it nearly impossible for us to stay ahead of the thousands of new attacks or new vulnerabilities that are discovered literally every day.

One of the most significant changes in our recent culture has been the extent to which the internet has affected the daily lives of the American public. Because of this shift, serious new vulnerabilities have emerged. In 2010 alone, researchers recorded 662 breaches at large companies or federal agencies that left 16.2 million records exposed, and it is estimated that there are 1.8 billion attacks on our government servers every month. Some estimate the cost of cyber threats to our economy as $8 billion annually. The CIA Director and Director of National Intelligence believes our susceptibility to cyber terrorist attacks could potentially result in the

shut down of government agencies, power grids or financial markets. He has noted that, "the next Pearl Harbor could very well be a cyber-attack."

As a member of the House Armed Services and Intelligence Committees, I have seen firsthand how securing our networks against hackers, terrorists, organized crime, and foreign powers has become an ever-greater component of our national economic security strategies. The government's challenge of defending the .mil and .gov networks is the responsibility of the new U.S. Cyber Command, led by the NSA director, General Keith Alexander, and the Department of Homeland Security. The dedicated men and women of these agencies work incredibly hard to develop solutions to protect these networks from attack. However, our nation still stands largely unprepared to deal with the very real threats. The government currently has only a limited role in offering assistance to private owners of our critical infrastructure and .com networks. And we are still struggling with how to defend critical systems while preserving civil liberties and privacy, also critically important.

As a co-chair of the Center for Strategic and International Studies' Commission on Cybersecurity, I have spoken countless times about the current deficiencies, and I have called for reform. I am working with leaders like Senator Whitehouse and others to bring our nation in-line with the technical realities facing us. I introduced legislation that would protect our critical infrastructure and address current weaknesses in our security policy by increasing coordination among federal agencies and between the public and private sectors. There is currently no one single person or office leading our government's efforts to keep our networks safe. My proposal establishes one national office, with proper policy and budgetary authority, to oversee cybersecurity while ensuring the government and military can acquire the best technology and undergo regular reviews to evaluate their performance.

However, all the best ideas won't keep us secure without the right people to execute them. Experts have estimated that the U.S. has fewer than 1,000 people with the advanced security skills needed to effectively compete in cyberspace. The reality is that we need 20,000 to 30,000. Thus, the cornerstone for this effort must begin in the classroom; from our secondary schools to places like URI's Digital Forensics Center. Cyber skills should be a core fundamental of the science, technology, engineering, and math fields, which are all critical to improving our country's innovation.

Last year I hosted the Rhode Island Summit on the Economy, where sector leaders came together to brainstorm the best paths to economic recovery. Two common themes emerged; we need to close the skill gap for the jobs we currently have, and we must encourage collaboration between the business and education sectors to increase sustainable job growth opportunities. Along with partners including the Rhode Island's Department of Education, Science and Technology Advisory Council, and Tech Collective, I helped launch a program to foster computer security skills at the high school level. We recently kicked off a new Rhode Island Cyber Foundation Competition that "aims to make cybergeeks cool!" We want to show the next generation that an interest in computers is not just a hobby; it can become an excellent career.

In Rhode Island, we have the drive and the talent to rise to this national security and workforce challenge. We need institutions like URI, and we need all of you here today. This symposium is a way to bring together business, government agencies, and regional academic partners. We must harness all our talent and incorporate the perspectives of public and private entities to build the competitive research base, cyber workforce, and cybersecurity industry that meet our national

security needs. We are active and invested partners in a common goal. I'm excited to get started.

Senator Sheldon Whitehouse

This symposium is quite timely. The Obama Administration is coming to the end of its yearlong "interagency process" on cybersecurity, and it will soon be prepared to reengage with Congress on this issue. The threat is serious and action to protect our country is overdue. The Senate Commerce and Homeland Security Committees reported out bills in March and June 2010, respectively, and the Intelligence Committee Cybersecurity Task Force completed its classified report in July – authored by me, Senator Mikulski and Senator Snowe. We are ready in the Senate and I hope we will work on a major cybersecurity bill this year. The House likewise should act, and I believe the legislation introduced by Representative Langevin will be an important and foundational document.

The urgency is pressing. Malicious actors in cyberspace have already caused significant damage to U.S. interests. U.S. government computer networks are probed millions of times each day, approximately 9 million Americans have their identities stolen each year, cyber crime costs American businesses with 500 or more employees and average of $3.8 million per year, and intellectual property worth over $1 trillion has already been stolen from American businesses. I contend that we are on the losing end of the biggest transfer of wealth in history as a result of theft and piracy.

Public reports disclose major hacks into Google, DuPont, NASDAQ, and the e-mail marketing company Epsilon. A recent MacAfee report[1] on Night Dragon attacks on the U.S. energy sector is sobering in its conclusion that "well-coordinated, targeted attacks such as Night Dragon, orchestrated by a growing group of malicious attackers committed to their targets, are rapidly on the rise. These targets have now moved beyond the defense industrial base, government, and military computers to include global corporate and commercial targets."[2]

In the course of my work I have been talking about cybersecurity with leading executives. One green-energy CEO reported to me that his email was attacked 60,000 times within the 2 hours after the release of a press report highlighting a new product at his company, and that 40,000 of these attacks originated in China. I asked another CEO of a well-known internet company for an analogy: "Is it like my son's video game with the zombies at every window trying to tear their way in?" "Definitely the zombies," he said, "or worse."

We have a real issue on our hands and it touches our lives in so many ways. Cyber attacks can shut off your electricity, knock out your cell phone and your laptop, shut down the ATM, compromise banks electronic records, compromise credit and debit networks, and even interfere with the law enforcement and first responder communications so vital to our communities.

We can't afford for cyber vulnerabilities to be our nation's "dirty big secret." Government and private sector leaders have got to come clean about our exposure. Too much information about attacks on government is withheld as classified, and too much information about corporate attacks is withheld as proprietary. American institutions and industries and Americans

[1] http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
[2] ibid. Page 13.

themselves need to be empowered in self-defense, so that they can energetically and informedly engage in their own protection.

There have to be basic rules of the road on our information superhighway. We don't allow cars on our geographic highways with headlights out and mufflers dragging, yet we allow computers dripping with malware and slaved to "botnets" unrestricted access on most of the information highways. We need a cyber 9-1-1: Who do you call? Additionally, how can we pre-position defenses for our critical infrastructure; since attacks come at the speed of light, worms and viruses can lurk silently in systems, and some attacks can only be defeated if they're prevented. By the time that cyber 9-1-1 call comes, it's too late. Finally, what can we do to resource and ready our public safety agencies for this new theatre of operations? Does law enforcement have what it needs? Have we translated the laws of war, principles of sovereignty, and conventions of covert operations from geographic into cyberspace in a way that telegraphs to our enemies what we'll tolerate and what we won't? The Cold War was won after a long, sustained campaign of deterrence – what wall of deterrence will protect us in cyberspace?

We've got work to do, real work, upon which the safety and security of our economy and our nation depends. We had better get cracking.

Keynote Address

General Keith Alexander, Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service (NSA/CSS), Fort George G. Meade, MD.

Cybersecurity is one of the most important issues facing our nation today. Just think: in 2000 we had about 500 million mobile phones. Now there are about 5 billion out there. Just about everyone on the planet has one. Going mobile has given us better capabilities. Cell phones and social networking have forever changed the way we communicate and collaborate, even our politics. And we have a plethora of applications that will help us solve the challenges of today and the future. It's the wave. It's coming. We have to be prepared for it.

When I look at the cybersecurity threat, I see three threat levels to consider. First there is exploitation, that's been going on for years but it doesn't mean that it's ok. A McAfee report[3] estimates a $1 trillion loss to the global economy from the pirating of intellectual property alone. Our government is also losing secrets, and even companies who lead in cyber knowhow have been hit. Even more serious, there are disruptive attacks. In 2007 Estonia was hit with a massive distributive denial of service attack, which took down their ability to communicate and their banking sector. When the Russians came into Georgia, the invasion was uniquely accompanied by a cyber attack on the Georgian infrastructure. Latvia, Lithuania, Kyrgyzstan and Azerbaijan have also been hit by disruptive attacks.

The highest level of threat, what I'm most concerned about, is destructive attacks. These are coming. The potential threat can be illustrated by some accidentally destructive incidents. In August 2003, a cascade event shut down the Northeast power section of the national grid in four minutes. It was rooted in a software problem. In Russia, an accident that destroyed ten huge

[3] www.mcafee.com/us/resources/reports/rp-underground-economies.pdf

hydroelectric turbines and killed 75 people happened when a malfunctioning turbine was activated remotely but no one knew that the sensing system that should have given early detection of the problem was offline. These issues happened even though those involved had the best of intentions. What happens when there is actual intent to destroy?

In 2008 the Department of Defense recognized malicious software in our networks. It was transferred by our own people who used thumb drives to copy information from unclassified networks onto classified ones, bringing with it malicious code. This was the key issue that convinced the Secretary of Defense to form the United States Cyber Command. We work in partnership with the National Security Agency and the Department of Homeland Security as the first line cybersecurity defensive team. Then on May 29, 2009 the President gave a key speech on cybersecurity, pointing the vector ahead. He said that cybersecurity is key to our economy and key to our national security, and that we've got to do something about it. Deputy Secretary of Defense, William Lynn, responded to the President's challenge in an article on the Pentagon's cyberstrategy in Foreign Affairs magazine.[4] I want to concentrate the remainder of my comments on two aspects of the challenge that he addressed – active defense and extending that defense to critical infrastructure.

Let's talk about active defense. If you look at how we defend our systems today, it's very much a static capability. We put up a defensive system like McAfee or Norton 360 and we trust it to do the job, until somebody figures out how to break the system and then we patch it. It's reactive instead of proactive; we have to do better. We have to go the full depth of what's possible in cyberspace to secure our systems. We need an active and adaptive capability inside the networks, and highly trained, experienced network operators looking for threats. We need a system that can communicate, inside the system and outside to know when we have a problem between industry, our allies, and our national networks. The idea of an early warning in cyberspace is a new concept, but we've got to have that capability to be able to move seamlessly to ward off threats.

My second focus issue is extending this defense to the critical infrastructure. My mission in the U.S. Cyber Command is to defend the military networks. The responsibility for critical infrastructure falls to the Department of Homeland Security and to the industries themselves, who may, through no fault of their own, be lacking in cybersecurity expertise. Until now, it has not been a great priority for them. But partnership and sharing of expertise is going to be key for the future. How do we extend our capabilities and communicate what we know?

Finally, we have to do all this while addressing concerns about civil liberties and privacy. I am confident that civil liberties and privacy are not at the expense of cybersecurity; they will benefit from cybersecurity. Ensuring protection that does not go too far is an issue of accountability that the American people should demand and that we should provide. We can do both, and we should. The question is how to put them together. I want to assure you that the people at the National Security Agency are very concerned about this and every member of the workforce is required to go through training on handling personal data and protecting it.

When you look at what our nation has been able to do in cyberspace, it's extraordinary. We are the nation that started the network; we ought to be the nation that secures it. This gathering today represents our nation's best innovative talent. With your help, we will do it.

[4] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Session 1: Cyber Threats to Critical Infrastructure

Critical Infrastructure has been defined by the U.S. Department of Homeland Security as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."

Critical infrastructure is generally viewed as including telecommunications and information technology providers, government facilities, the defense industrial base, emergency services, nuclear reactors and associated materials and waste, energy, transportation, dams, postal and shipping capacity, agriculture and food, banking and finance, healthcare, and water. Basically, it is the civilian, non-defense side of cybersecurity and much of the infrastructure is in private, rather than government, hands. Ensuring security, reliability and availability of such systems is critically important and recognized as a very challenging task.

Douglas Maughan, Director, Cyber Security Division, Department of Homeland Security

Cybersecurity in Washington is being driven by the Comprehensive National Cybersecurity Initiative (CNCI). Although the initiative includes 12 major focus areas, I will concentrate today on cybersecurity for critical infrastructure, while also mentioning some aspects of coordination, new R&D topics, and education.

We are familiar with cybersecurity for business systems, but it's only in the last few years that we have been trying to do the same thing for control systems and there is a difference in priorities between the two. Control systems rely on availability first, then integrity and finally confidentiality while business/IT systems have that priority essentially reversed. In control systems, latency is unacceptable. We have to have real-time control. Reliance on higher capability computer systems, for example with Smart Grid, will also be a significant future requirement.

In the Energy sector, we can see several challenges. Open industry standard protocols are replacing vendor-specific proprietary communication protocols. Standard computational platforms are increasingly used to support control system applications. The interconnectivity of enterprise networks with the internet increases vulnerability, as does the increased reliance on external communication. There is also more and more use of smart sensors and controls and field equipment. DHS published a roadmap in 2006 for ensuring secure control systems in the Energy Sector going forward.[5] Implementation will require significant public private partnership. The roadmap identifies four specific targets. First we need to assure that energy asset owners have the ability and commitment to perform fully automated security state monitoring of their control systems networks, with real-time remediation capability. Second, develop and integrate protective measures in next generation control systems and architectures that offer built in, end-to-end security that will replace many older legacy systems. Third, accurately detect intrusions and implement response strategies in control system networks that

[5] http://www.cyber.st.dhs.gov/docs/DOE%20Roadmap%202006.pdf

automatically provide contingency and remedial actions in response to attempted intrusions. Last, sustain security improvements with energy asset owners and operators working collaboratively with the government and sector stakeholders to accelerate security advances.

Within DHS, we have designated securing cyberspace as one the major agency missions. We are focused on knowledge products and innovative technologies and on getting them from lab to operational environment and production, including outreach to venture companies and others to secure backing and integration into the economy. Many of our R&D efforts are in domain name system security and security protocols for routing infrastructure. In the Finance sector we have a project called DECIDE, to help develop tools in security and risk management, and we are working on projects in identity management. For oil and gas we have a joint project with five major companies, creating an organization called LOGIC that will raise the bar for the entire oil and gas sector in advanced supply chain collaboration and controls. And, in the electric sector, we have TCIPG, developing adaptive, resilient, and trustworthy ("smart") cyber infrastructure for transmission and distribution of electric power. I also want to mention our interest in education and engagement. Enrollments in computer science and computer education are down 50% from five years ago while these jobs are some of the fastest growing in the job market. The Administration's National Initiative for Cyber Education (NICE) is especially focused on education in the K-12 and undergraduate arena. Finally, I want to mention that the Administration's research agenda will be published in May, representing the interagency agenda, and that our DHS roadmap for cybersecurity research is available on our website.[6]

Theresa Murray, Regional Catastrophic Planner, Rhode Island Emergency Management Agency

We have been working on a state emergency operation and incident management plan since 2009. We follow the National Incident Management System, a consistent nationwide template that enables federal, state, tribal and local governments, nongovernmental organizations and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents.

The plan's second emergency support function, communication, calls for coordination with telecommunications and information technology industries, and for the protection, restoration, and sustainment of cyber and information technology resources. We are developing a cyber disruption support annex to the plan that outlines actions and responsibilities involved with any cyber disruption in the state. The key to it is to identify critical systems and have a coordinated approach that will allow rapid response to restore service and mitigate any damage caused by any emergency with cyber-related issues. We have conducted several awareness briefings, brought together major stakeholders at a workshop in March, and are having a cyber disruption response team selection meeting later this month. We have been fortunate, under a regional catastrophic grant program, to receive funds to assist us in developing and testing our plans and conducting exercises. I particularly want to make you aware of a DHS program of cyber resilience reviews that offers a survey to help you identify weaknesses and strengthen cyber awareness in your business or agency.[7]

---

[6] at www.cyber.st.dhs.gov.

[7] For more information about the CRR, contact the CSEP program at CSE@dhs.gov.

Yan Sun, Associate Professor, URI Dept. of Electrical, Computer, and Biomedical Engineering

We have heard that the power grid is vulnerable to cascading failures, and we also know that information on how to cause cascading failures and on network vulnerabilities has been published and could be of use to hackers of malicious intent. The behavior of cascading failure is very complicated – we have already heard how a 2003 failure at a single plant in Conesville, Ohio resulted in a cascading failure that spread to large portions of the Midwest and Northeast, with a total of about 50 million people affected. The research community is pushing the concept of the smart grid as a solution. Can it solve the problems? The answer is yes, if we can understand how cascading failures occur and if we can catch and detect the signal of a cascading failure in the early stage. That's two big "ifs." Dynamic control of the smart grid can help us detect the start of a cascading failure and to stop the failure. On the other hand, this requires communication along the grid for control messages, and this opens the door for cyber attacks.

At URI, we study the problem from the attacker's perspective to identify and understand the vulnerabilities of the power system. We have discovered new metrics that help to reveal and characterize the most vulnerable aspects of the system. Some of these metrics are "percentage of failure," the number of failed nodes divided by the total number of nodes; "required redundancy," the minimum required system tolerance value such that cascading failure will not occur when one node is taken down; and "risk if failure," the risk of single-node failure in terms of causing cascading failure. We have compared attack strategies, from simple to complex, to discover the how such attacks would proceed. And we have identified some of the most dangerous to the current grid. Our ultimate goal is to deliver defense solutions and tools to help decision makers understand their vulnerabilities and manage risks.

Session 2: Cybersecurity: Cyber Forensics

Electronic data and evidence can easily be manipulated and modified. Cyber Forensics or Digital Forensics are the tools and methods used to preserve, collect, validate, identify, analyze, interpret and document evidence derived from computers and networks. It is central to law enforcement and to the understanding that enables prevention, recovery and reconstitution of data.

Jeffrey Troy, Deputy Assistant Director, FBI Cyber Division

Although it may seem strange, the FBI is not focused on the victims of cyber threats. Instead, we have a threat focus strategy. We try to look at the data on all the attacks and to identify all the malicious groups that are out there, and then we try to identify the actual infrastructure that they are using to try to attack the U.S. With this information, we try to put strategies together for how to defend ourselves. Our threat focus groups are large, intergovernmental groups that are highly cooperative and have had great success in providing some understanding, preventing some attacks, and developing mitigation strategies. However, there is still a large problem.

It's the very technical sophistication of our applications together with the lightning fast speed of propagation of applications and information, including information about security problems, that opens up new holes and more vulnerabilities in the system. Other tools of data storage and computing capacity are also both providing tremendous service to users and opening up vulnerabilities at the same time. Additionally, the volume of attacks has dramatically increased as the nature of the groups perpetrating them has changed. It's a global problem and we need global norms and diplomatic outreach, as well as technical solutions, to solve it.

The FBI has done much to upgrade our forensic tools and improve our forensic processes including on-site triage, consolidation of analysis, and increased data sharing and coordination. Innovative new tools and processes will continue to be needed to provide us with more visibility into the problem.

Daniel Dickerman, Special Agent, IRS Criminal Investigation

The IRS is actually in the forefront of computer forensics. Long before most individuals ever owned a computer, the IRS had a need to capture, recover and analyze digital evidence from business computer systems. This capability spawned a set of procedures and tools that were used by all of the then Department of Treasury agencies, all putting our brains together and learning about the types of threats we might encounter. At that time, the skills of computer forensics were almost entirely within the law enforcement community. However, both the problems and the tools were much simpler in those days of stand-alone machines and limited data storage. Jumping into the 21st century, we have a totally different situation. We have more experts, better tools and better computers. New technologies such as networks, mobile devices, social networking, and game consoles present new challenges. Especially with the advent of cloud computing, there are the questions of data access, location, jurisdiction, and preservation. Our vulnerabilities and our forensics tasks are much more complicated as well. Dealing with encryption is an ongoing problem. We face pishing, malware, hacking, and more.

Probably our greatest challenge is how to keep up. New tools and skills are required. And the law is often way behind the technology. The evidence is no longer just "static," we need real-time acquisition and analysis. How do we decide what's important to analyze and where to just remediate? We need to know how to make the best judgment call. With encryption, anonymous proxies, and ownership/jurisdictional boundaries, we have increasing difficulty simply finding the perpetrator or the evidence. Forensics must continue to evolve in new directions; memory parsing, wear leveling and ensuring the real wiping of data in solid state memory, quantum computing, and it just goes on and on. Law enforcement can't do it alone any more. We are encouraged to see the growth in academic and research programs, as well as the increase in cybersecurity partnerships. Public awareness is essential. Everyone must have a basic understanding, so that they are not unintentionally used in the threat against the government or the threat against companies. URI can make important contributions in each one of these areas.

Alan White, Director of Network Security and Risk Consulting for North America, Dell/Secure Works Inc.

From an industry perspective, the lack of computer security professionals, as well as their tendency to be entrepreneurial as independent contractors, is making it increasingly difficult for us to keep up with the challenge. We need to employ our own people who have the appropriate technical skill sets, programming ability, and the skill of "how to think like an attacker or hacker." That's a difficult skill to teach, perhaps, in an academic classroom. For Dell, it can take 4-6 months to fill a position. We get a lot of applicants but it's really tough to find someone with the appropriate skill set who can contribute quickly.

My message is two things; we have threats and we have needs. In threats, we are focused on hackers and attackers that specialize in malware creation, cyber espionage, exploitation of research, "hactivism," cyber crime, financial laundering, and botnet herders. The talent behind these groups is high and we are competing with that. As soon as we find a way to defend, they find a new way to exploit. Industry needs timely malware analysis, countermeasure development, reverse engineering, counter intelligence, forensics, threat modeling, trending and statistical analysis, and researchers to analyze what's happening right now and ultimately predict and prevent advanced or entirely new threats. We have to have the tools to understand what the next thing is, to get ahead of it, and to manage that threat. In defending the industry, our goal is to make the cost of doing business for the hackers go up, such that it isn't worth it for them to spend the effort to compromise our systems. Universities offer the next generation of industry experts who will be essential in meeting that goal.

Victor Fay-Wolfe, Professor, URI Dept. of Computer Science and Statistics

URI's Digital Forensics program was one of the first programs at a major university to address digital forensics through a computer science department. We have a multi-pronged approach in teaching, service and research all directed toward digital forensics. The interplay between them is one of our strengths. Our working lab on campus is analogous to a teaching hospital. Our student interns work with our experts to solve real cases, and from the cases we develop real-world research problems.

Our curriculum is delivered completely online, as the result of a National Science Foundation (NSF) grant. We have innovative lecture techniques and ways of getting information and challenges out to students for them to work on. We also have training and certification programs, including training in advanced techniques. We offer a variety of workshops and meetings, partnering with the police, local companies, and other groups and agencies. We also offer internship programs that get our students out into the community in real cases. The students love it and our partners love it. The lab, originally funded by Congress, is now self-funding through our service program. We've done all kinds of cases from murder, political corruption, or corporate espionage, to stalking. The URI designed and built state police computer crimes lab, with URI staff in residence, is an innovative design that is being considered as a national model. The entire state of RI centralizes their purchase of advance computer forensic tools through this lab, giving everyone access and exploiting the economies of scale.

Real world cases at URI yield exciting research problems. Some examples of current research, funded by the Department of Justice and the NSF are child pornography detection using

computer vision and machine learning techniques, data security, cloud forensics, and lastly my research graduate student will be talking about a research project in steganography detection.

At URI, we don't let research "die on the vine." We transfer research into real products, with many partnerships with local companies and law enforcement agencies. We also address workforce issues. Many of our graduates are in prominent positions and we are doing our best to make links that provide our students with real world skills and put them into places where they can contribute. Our newest direction is towards a URI Cyber Security Center that will leverage our strength in digital forensics, bringing in the entire internet component including security and information assurance. We are taking the initial steps towards establishing the center this year. You will hear more about its research component in the next session.

Kevin Bryan, Doctoral Candidate, URI Dept. of Computer Science and Statistics

Steganalisis is the method of detecting hidden evidence in digital media files. Related to it, steganography is the idea of hiding a message in plain sight. In an encryption, it is very clear that I, the sender, have sent a message to you, the receiver. With steganography, I'm trying to obscure that. You don't necessarily know who is receiving the message, or even that it is there. All kinds of messages can be sent like this, usually short messages like stolen credit card information, but also foreign intelligence or trade secrets.

Steganography is possible because of how data is stored and compressed. For example, in image steganography (JPGE/MPEG), changing a color storage value by ± 1 does not significantly alter the look of the image. Distributions of changed values can be embedded globally in the image and can be reconstructed as an embedded message. An indication of data embedding can be determined by examining some very specific statistics.

At URI we have been able to build models of steganography through embedding images with a steganography tool and then collecting statistics from clean and altered images. For an investigation, we can collect statistics from a suspect file and use the models to predict whether the image has data embedded in it, and we can approximate the amount of data embedded. Our accuracy so far is around 95% down to 20% embedding rate. As a result of our work, we have been able to transition a JPG and MP3 detection engine to Wetstone Technology's Stego Suite.

Session 3: Network Security and Trust

Network security and trust relate to software that protects data, routing and other network activities through analysis of such factors as who should have access to a system, who can modify a system, what actions are unreliable, what types of functions should be performed, etc. When transmissions meet the requirements of the software, they are considered trustworthy. When the software identifies an action outside the expected, then questions of trust in the system arise.

It is well known that current distributed networking systems often do not offer sufficient security. This problem is partially due to the lack of trust among network participants. When network participants do not know how to trust each other, they either naïvely believe in others'

good intentions or are paranoid. The naïve users suffer from malicious attacks, whereas the paranoid users introduce low efficiency and availability into the network. It is essential to understand how to establish trust relationship among network devices, between the network and its operators, and among users who are connected or utilize the network.

Peiter "Mudge" Zatko, Program Manager, Information Innovation Office, Defense Advanced Projects Agency

In DARPA we play the foil. We challenge assumptions that we have used to build and base our offensive efforts. But, if we are only ever doing that nobody wants to work with us and we can't transfer our technologies, so we also collaborate. My job has been to challenge and redirect how we look at the problem and how we measure success.

Malicious cyber activity is getting worse and worse, actually growing exponentially, which looks really scary. But, there are still a lot of unknowns about what exactly the attacks have been. In many ways we are actually divergent with the threat. For example, the complexity and cost of our defensive efforts against malware have grown almost exponentially while the costs and complexity of malware for the hackers have stayed almost constant over the last two decades. We may have unintentionally embraced and maybe even fostered some of this divergence. Additional security layers often create vulnerabilities, as our operating systems and applications get more and more complex the number of bugs in the system also multiply and can be exploited.

It's not always technology that is the solution; in fact it may be part of the problem. Business solutions are also important. It's necessary to understand the incentives of all the players and predict the responses. We'll use the context of game theory to reveal the problem. Remember, if it looks like people are behaving irrationally, they're not – you just don't understand the game. For example, the anti-virus industry is a subscription service. The value they present is to identify and patch vulnerabilities and they do a good job at that, but they are not incentivized to actually solve the problem. In the case of repeated exploitation of a particular vulnerability and repeated patches issued by the anti-virus security company, we have solutions that work for the adversary and for the security industry. The only people they don't work for is the user. When we look for true solutions, we need to understand how incentives work and know that cross-incentivization can create these divergent patterns.

Marcus Sachs, P.E., Vice President of Government Affairs for National Security Policy,Verizon

Verizon has been working for several years studying large-scale data breaches – how large companies get broken into. Hackers tend to go after the very simple solutions. For example, I noticed a one-line data attack on Google recently, just a URL that could be typed into the URL bar that could circumnavigate the page's CAPTCHA. It turns out that these kinds of simple attacks are oftentimes the most frequent ways that attackers use to get in to steal data.

Applying security devices can reduce risk, but often at more cost than is justified for the amount of risk they reduce. It's never possible to get a computer or network totally secure. Varieties of different types of risk reduction technologies can be combined to reduce risk to acceptable levels, but how these different types are employed, and in what order, can have significant

impact on cost for relative risk reduction. When we have breaches, we can analyze and determine why the security failed. For example 98% of stolen information comes from servers, not endpoints. Why do they go after the servers? That's where the data is! 85% of the attacks were not considered technically difficult – hackers go after the easy stuff. The number one piece of malware we find is the hidden back door; number two is key loggers. The number one way a hacker gets in is stolen credentials. We know how to protect against these pretty easily, but they still sit on top. All the things we have found are available in our report,[8] which is a study in failure that shows companies are not generally following the best practices. Some of the scariest information we found is that from break in to compromise usually takes just minutes, but from compromise to discovery is usually months, as is discovery to containment. The machines actually know that they've been breached, but nobody is listening.

The bottom line in our report is that mitigation should be focused on: eliminating unnecessary data and keeping tabs on what is left, ensuring essential controls are met, checking those two steps again, testing and reviewing web applications, auditing user accounts and monitoring privileged activity, filtering outbound traffic, and monitoring and mining event logs. Everything is best practices. Those companies that follow best practices generally don't get broken into. Yes, there is always risk, but significant reductions don't always require heroic measures.

Yan Sun, Associate Professor, URI Dept. of Electrical, Computer and Biomedical Engineering

URI's innovative approach to addressing security problems is based on a unique trust infrastructure. Trust is well known as the driving force for collaboration in social communities. At URI, we bring the concept of trust to computer networks. Distributed computing and communication systems rely on collaboration among network participants. When network participants do not know how to trust each other, network operations suffer. Participants that naively trust will be victimized but mistrustful participants will ignore opportunities and their resources will be wasted because of inefficiency.

I classify the role of trust into three categories. The first category is prediction and diagnosis. When a network entity establishes trust in other network entities, it can predict others' future behaviors and diagnose their security properties. Second is simplification and abstraction. The design of network protocols and applications must consider the possibility that some participants will not follow the protocols honestly, so we need a defense of the protocol. But if individual protocols all have their own defense, we face the problem of repetitive monitoring that is highly complex and defenses may be non-compatible. Ideally, a trust infrastructure across the layers can help to integrate piecemeal defense solutions and allow the system to take action against a suspect node by reducing its level of trust while the node is being assessed as a risk. The third role of trust is in integrating social needs into system design. The most vexing security problems today are not just failures of human technology, but result from the interaction between human behavior and technology. The end user can be the weak link and needs both decision support and accountability. Trust infrastructure can provide incentive for honest and responsible end user behavior. Of course, trust based solutions do not replace traditional security services but work with them to increase security and reduce risk.

[8] http://www.verizonbusiness.com/databreach

The theoretical foundations of our URI research address the following questions. What is trust? In social science, there are more than 20 definitions of trust. How do we quantitatively evaluate trustworthiness? What are the mathematical properties of trust values? And, is trust evaluation vulnerable to attacks? Obviously yes, the hackers would try to make their values of trust high and others low. How do we guard against this? We are doing a number of research studies on trust-based networks. You will hear more about some of them from the following speakers. We are also developing analysis and evaluation tools to evaluate which models are better and under what circumstances. We also monitor attacks and seek to understand how real users attack trust evaluation. A number of our graduate students are doing very interesting work on advanced schemes to thwart attacks against trust management; some of these projects are highlighted in the poster session.

Lisa DiPippo, Associate Professor, URI Dept. of Computer Science and Statistics

I will highlight a specific example of how we at URI have taken this concept of trust and applied it to securing wireless routing. We have been pursuing this project with the company mZeal Communications, who have done some of the testing and implementation. Our concept has been applied to wireless sensor networks that collect and send data to a base station. The devices are small and low cost and must have secure routing of data from node to node, typically based just on distance, to get the data ultimately to the base station. The security issues are similar to those in other types of networks. Data confidentially concerns can be handled by encryption, but that doesn't answer getting the data safely to the endpoint. Nodes in networks can be malicious. Some attacker might place a node in your network that imitates a valid node, redirects transmission or does not forward data, or only selectively forwards data. We have developed a framework for various types of trust to make routing decisions. For example, forwarding trust, reporting trust, and predictability trust. An overall trust value can be determined from a combination of all trust metrics and used in routing decisions that can then be based on both trust and distance. The impact of this work is to increase the assurance of delivery of critical and sensitive data in networks as well as increase our ability to detect sophisticated attacks on routing. We've recently begun extending the application of trusted routing to other types of networks, as well as the principles to any system where behaviors can be monitored. The concept of trust and the research we've built around it is a unique feature of the research in the new URI Cybersecurity Center.

Yuhong Liu, Doctoral Candidate, URI Dept. of Electrical, Computer, and Biomedical Engineering

My project involves how to use trust management in biomedical systems, specifically for the safety assurance of neural-controlled artificial legs. The neural signals can be easily contaminated by diverse disturbances that originate in electronics or sensor failures or contact failures between the sensor and the user's skin, which lead to errors in user intention that could result in tumbles, falls, or injury. To secure the safety of these artificial legs, we proposed a trust-sensor interface that can dynamically evaluate the reliability of the entire system. There are three components. To date we have concentrated on the abnormal detector and sensor level trust evaluation, and our future work will address system level trust evaluation.

Closing Remarks

Arthur Coviello, Jr., Executive Vice President, EMC Corporation & Executive Chairman, RSA, The Security Division of EMC

The quality of the symposium today was so rich that my first comment is that this should be the first in a series of ongoing symposia on the subject. It's especially apropos that I'm speaking to such a diverse audience, because the fact is that our only hope for understanding and getting ahead of a rapidly evolving cyber threat landscape is a true public/private partnership. I also have a special word for the students in our audience. You have grown up in an information economy that will only become richer with ongoing innovations. All economies are dependent on confidence, and our job in cybersecurity it to inspire that confidence. An economy based so much on globalization and world trade is inextricably tied up with and built on our critical infrastructure. I can think of few more important and rewarding careers today than cybersecurity and quite frankly, as you have heard so much today, we can use your help.

To get ahead in the cybersecurity landscape it is essential to know who is attacking, why they are attacking, and what an organization's vulnerabilities are. There are many different types of attackers working against many different types of organizations. In my company, RSA recently fell victim to a very sophisticated cyber attack and information relating to our secure ID was extracted. Fortunately, we discovered the attack contemporaneously and were able to shut it down quickly. We began immediate remediation for ourselves and for our customers. But my company is a security company, sophisticated in our ability to defend our organization. And still we suffered a breach. There have been many other recent attacks in the news – five major attacks in just the span of two weeks. None of these attacks were the least bit related; there is no single enemy. We need to redefine the way security is addressed and implemented to address these new realities, and we must act faster. Adequate defense depends on a clear understanding of the likely attacker, the attack target, and the attack methods, as well as the ability to map that information into a security program that is as adaptive and agile as the attackers themselves.

There tend to be three kinds of attackers. First are the criminal elements, including both petty criminals and organized crime. Petty criminals also feed their information into the more organized criminal networks, especially by selling identity information. Criminals often employ information gatherers who operated botnets and other collective resources used in attacks. They extract information or leverage extracted information and use it to attack others. There are the harvesters who actually mount the attacks, and even full-service criminals who design system attacks from end-to-end and sell them to others. They even sell maintenance contracts and subscription services. The second group is non-state actors, including anti-establishment vigilantes, or "hactivists," and terrorists themselves. Hactivists, motivated by their own self-righteous causes, tend to be as sophisticated as organized criminals but the attacks look more like what you would see from a nation state. True terrorists have passion and some ability but, at least so far, tend to lack the money and resources to operate their attacks. However, as terrorists generally have a goal of targeting critical infrastructure or causing major disruption, this group could soon pose very serious threats and we need to be proactive. The third major category is the nation state, actors whose online activities are directed by a particular nation or government.

If, as Clausewitz tells us, war is the continuation of politics by other means, these groups represent a new way to conduct "politics" with all the potential devastation of traditional war but without the cost, bloodshed and vilification. The size and scope of attack that a nation state could engineer vastly exceeds the capability of any corporation, private group or individual. These attacks could be devastating, and we don't even know how to bring the full force of international law to bear. We need to do a better job of defending ourselves.

Our adversaries in cyberspace currently having the upper hand and we are brought to a new phase in our security perspective. We must abandon many failing assumptions and outmoded behaviors. We must come to grips with the harsh reality that we have entered a more dangerous and complex state where change is the only constant. We must confront the continual, adaptive efforts of our opponents with equally dynamic, pervasive, innovative, and agile approaches to security. This requires adherence to three core principles: First, our approach must become logical and information centric. Second, the approach must be risk based and adaptive. And third, our approach must be built in and automated, as dynamic as the virtual assets we protect. Adopting these core principles will emancipate IT security staffs to be proactive, an aspect that will be critical to our success. Our security depends on a strong security ecosystem that, in turn, depends on a public/private partnership with better and more real-time models for information sharing. With the talent and dedication represented in this room I am confident that we will regain the upper hand and that we will secure the future of our information economy for the next generation and beyond.

Congressman James Langevin

Clearly we have our challenge before us, a dynamic challenge that will require a dynamic response. There is obviously a lot of great work going on across the country and, as we have seen today, here in Rhode Island. Our speakers highlighted the need for partnership across all sectors. We won't solve these problems without communicating with each other or without thinking outside of the box. We have started an ongoing dialog and need to continue talking and building on the successes we have achieved. Creating a talented and skilled workforce will also be essential in solving this problem, as well as securing the jobs that will keep these workers and students within our communities. Rhode Island has demonstrated the unique ability to take on small scale, cutting edge initiatives and act as a model for innovative ideas and partnerships. We have the demonstrated ability to adapt to new challenges. I know that we will adapt to the challenges that we have been presented here today, and that we have great things coming. Thank you all very much.

Reviewing the Symposium

Dr. Peter Alfonso, URI Vice President for Research and Economic Development

Our first Cybersecurity Symposium was by design, and perhaps by necessity, a far-ranging but brief examination of an array of issues: (a) the scope of the cybersecurity threats and challenges, (b) the need for a better prepared workforce and more aware citizenry, (c) the demands upon forensics as a means of preventing as well as understanding and reconstructing attacks and penetrations, (d) the imperative of protecting critical infrastructure, and (e) the need for research over a broad range of engineering, computer science, social and behavioral and related issues.

URI is proud of the support which it already offers in many of these areas:

1. We continue to offer a broad range of undergraduate and graduate courses and training, certifications, workshops and other support. In the Fall 2011 semester alone, we enrolled 260 undergraduate and graduate students in the cyber degree program and other cyber-related courses. URI expects to receive NSA Center of Excellence certification for our Academic program by the end of the year. We are supporting training for federal, state, local and private sector entities.
2. We continue to expand our capabilities in digital forensics. Our laboratory services law enforcement, judiciary, emergency preparedness and first responder and related communities. Our services enable us to collaborate with many partners and to make the benefits of those collaborations available to our students.
3. Our research efforts continue. In fiscal year 2011, investigators from URI have been awarded $1.7 million in federal grants to further our understanding and best management of cybersecurity threats in our nation and the world. In the past five years, URI has received nearly $4 million in external funding for Cybersecurity-related research.
4. And, we are particularly proud of the relationships which are emerging across a network of higher education institutions, state and local government and the private sector.

Finally, we continue to applaud the contributions which our distinguished Congressional delegation is making in this timely and important field. We are fortunate to have their leadership.

URI is committed to its work in the cybersecurity field and looks forward to the next level of accomplishment and leadership.