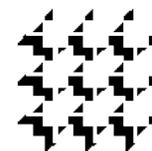


DIMACS

Center for Discrete Mathematics
& Theoretical Computer Science



Rebecca N. Wright
Director

Rutgers, The State University of New Jersey
CoRE Building, 4th floor
96 Frelinghuysen Road
Piscataway, NJ 08854 USA
Telephone: +1 848 445-5931
Fax: +1 732 445-5932
E-mail: rebecca.wright@rutgers.edu
Web: www.cs.rutgers.edu/~rebecca.wright

New Jersey State Legislature Assembly Homeland Security and State Preparedness Committee October 9, 2014

Committee Meeting Description: *The committee will hear testimony from invited guests regarding cyber security threats, standards, and new technologies and ways the public can protect itself against these threats.*

Testimony of Dr. Rebecca Wright, Rutgers University

Chairwoman Annette Quijano, Committee members Pinkin, Russo, and Shepisi, Invited Guests and Dignitaries, Ladies and Gentlemen:

Good afternoon. I am a Professor of Computer Science at Rutgers University. I am also Director of the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), led by Rutgers with a variety of university and industry partners. Among many activities, DIMACS is home to the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA), a Department of Homeland Security Center of Excellence, and a participant in the Rutgers Institute for Emergency Preparedness and Homeland Security, a statewide enterprise that brings together subject matter experts in the diverse relevant fields. Rutgers is also designated as a DHS/NSA National Center of Academic Excellence in Information Assurance Research and Education.

Advances in information technology have led to dramatic changes in the last two decades in nearly every facet of how we carry out our daily lives, from how we communicate with each other to how businesses and government organizations operate. Financial transactions are easily and conveniently carried out via mobile phones and computers; embedded computer systems help improve car safety and maintenance; SCADA control systems allow remote monitoring and control of critical infrastructure systems; implantable medical devices can be controlled and updated without requiring invasive surgery; and wearable sensors help us monitor our health and well-being.

Unfortunately, though not surprisingly, these advances in cyber technology and its adoption have been matched with corresponding advances in cyber threats, which have evolved to reflect the increased importance and extensiveness of cyber activities. Once the realm of hobbyists carrying out attacks for fun or notoriety, cyber attacks are now carried out by a larger and more diverse set of entities including profit-seeking criminals, politically motivated cyber terrorists, and nation-states seeking to carry out cyber espionage or cyber warfare. Attacks and vulnerabilities, which are reported on with alarming frequency and severity in recent months, include data breaches at retailers like Home Depot (with a reported 56 million credit card numbers breached) and banks like J.P. Morgan (with a reported 76 million customers' personal data breached), alleged state-sponsored cyber-espionage from multiple countries, and software vulnerabilities such as Heartbleed and Shellshock in long-deployed software.

Attacks use and combine techniques as varied as malware, computer viruses, social engineering, botnets, spam, phishing, denial-of-service, and use of insider access, in order to carry out end goals such as credit card fraud, identity theft, cyber espionage, and theft of service. Cyber terrorism and cyber warfare could include both attacks on critical cyber infrastructure and cyber-based attacks on physical infrastructure such as transportation systems, drinking water systems, the power grid and power plants, financial systems, health and medical facilities, and more.

How can individuals, businesses, and governments protect themselves in the face of these threats? What can businesses do to protect their customers? And what can state, federal, and local government agencies do to protect their businesses and citizens?

No system can be made totally secure, and there is no single action or guideline that can provide cyber security. But we know many ways and best practices that contribute to improved security. Cyber security is complicated, and attention must be paid to it throughout the cyber ecosystem. Vulnerabilities in one part of the system can create pathways for attack in other parts of the system, such as insecure home computers becoming a platform for hackers to carry out attacks and evade detection. Furthermore, security must be an ongoing process, not a one-time activity. Ongoing monitoring is needed to prevent attacks, detect those attacks that were not prevented, recover from and respond to attacks, and so on. Social and business contexts must be understood. People are not going to give up the technologies that provide them value and convenience, nor would we want them to. Businesses are not going to implement strong security unless it reduces their cost of operation, or their customers or their regulators are demanding it. Yet the threats are real, and the resulting potential costs are increasing. Lack of adoption of more secure systems, methods, and processes is often attributed to associated costs or inconvenience. However, as the cyber threat grows, the cost and inconvenience of not adopting such solutions continue to increase.

There are steps that individuals and businesses can and should take, an important role for governments (federal, state, and local) at both the policy and implementation level, and a critical need for continued research and development and for education at all levels.

For individuals, there is an abundance (even overabundance) of good advice commonly given: maintain good password hygiene, check your credit cards and bank statements regularly and report any issues right away, install anti-virus software on your computers, check your settings on social media sites (like Facebook) to be sure that you know what they are, and adjust them if needed. Individuals can also help drive the security marketplace by adopting the use of stronger security solutions as they become available – such as chip-based credit cards, which some banks are already rolling out, and should be in more widespread use by October 2015. In light of recent bank breaches, you should be particularly wary of so-called “spear-phishing” e-mails that may use hacked personal information in order to appear to be legitimate messages from your bank. For families with teens or younger children, have conversations with your children about family rules, appropriate behavior online, and cyber bullying. Resources such as the Department of Homeland Security’s STOP THINK CONNECT campaign can be helpful.

What businesses can do depends on the nature and size of the business. Generally, it is safer to use existing products and services than to build your own. Software should be kept up-to-date and patched. All companies, large or small, should make use of experts trained in cyber security. For small and mid-sized companies, this is likely best done by hiring consultants on an as-needed basis, while companies large enough to have IT staff should include cyber security experts on their IT staff. Importantly, security should be a priority throughout the company and the company culture, not just relegated to an isolated security office. Given the growing awareness and cost of cyber security attacks, businesses may now find that they can gain a competitive advantage from having strong security practices and by providing strong security to their customers.

At the same time, the burden on individuals and small businesses is higher than it should be. A July 2014 report funded by the National Science Foundation entitled *Interdisciplinary Pathways towards a More*

Secure Internet notes that “current cybersecurity guidance is primarily targeted towards large corporations and the technically savvy user” and “the existing forest of YouTube videos and how-to blogs is difficult to discover and navigate, and lacks authority.” The report recommends that “A set of clear, interactive guides aimed at individual citizens and small and medium businesses should be produced to demonstrate best cybersecurity practices.” While these guides should likely ultimately be developed at the federal level, there may be some state-specific needs as well as the potential for states to drive the process.

New Jersey has a leading role in homeland security through NJ OHSP and due to its role as a major player in the nation’s supply system through its ports and airports, its large amount of critical infrastructure, the number of major companies present in the state, its proximity to New York, and its central dependence on mass transit, for example. We are poised to take a leading role in cyber security as well. As suggested for the federal government in the President's Council of Advisors on Science and Technology (PCAST) report *Immediate Opportunities for Strengthening the Nation’s Cybersecurity* of November 2013, NJ state government could also “lead by example and accelerate its efforts to make routine cyber attacks more difficult by implementing best practices for its own systems.”

Cyber security is not achieved by a single step or isolated action, but is an ongoing process. Continued research and development is needed to ensure that improved solutions continue to be developed and deployed across the entire cyber security ecosystem as the sophistication and frequency of attacks continue to increase. Cyber security is a multidisciplinary endeavor requiring advances in computer science and engineering, public policy, psychology, criminology, and more. Both industry and academia must contribute to these research and development efforts. Our cyber security research at Rutgers, for example, addresses practical privacy for big data applications, hardening the security of SCADA communications systems for energy delivery systems, protecting mobile devices against “rootkit” attacks, secure and flexible cloud computing, understanding and disrupting the economics of cyber crime, secure information sharing, cryptographic foundations, and finding attacks on communication networks and other systems as a way to mitigate those attacks and better understand how to design future systems to avoid vulnerability to such attacks.

Finally, to meet the current and future cyber security workforce needs, as well as to develop an informed citizenry that can safely operate in an increasingly connected and technological world, continued attention to and expansion of cyber security education is needed at all levels ranging from K-12 education to colleges to ongoing professional training for those already in the work force.

Thank you for giving me the opportunity to provide this testimony.