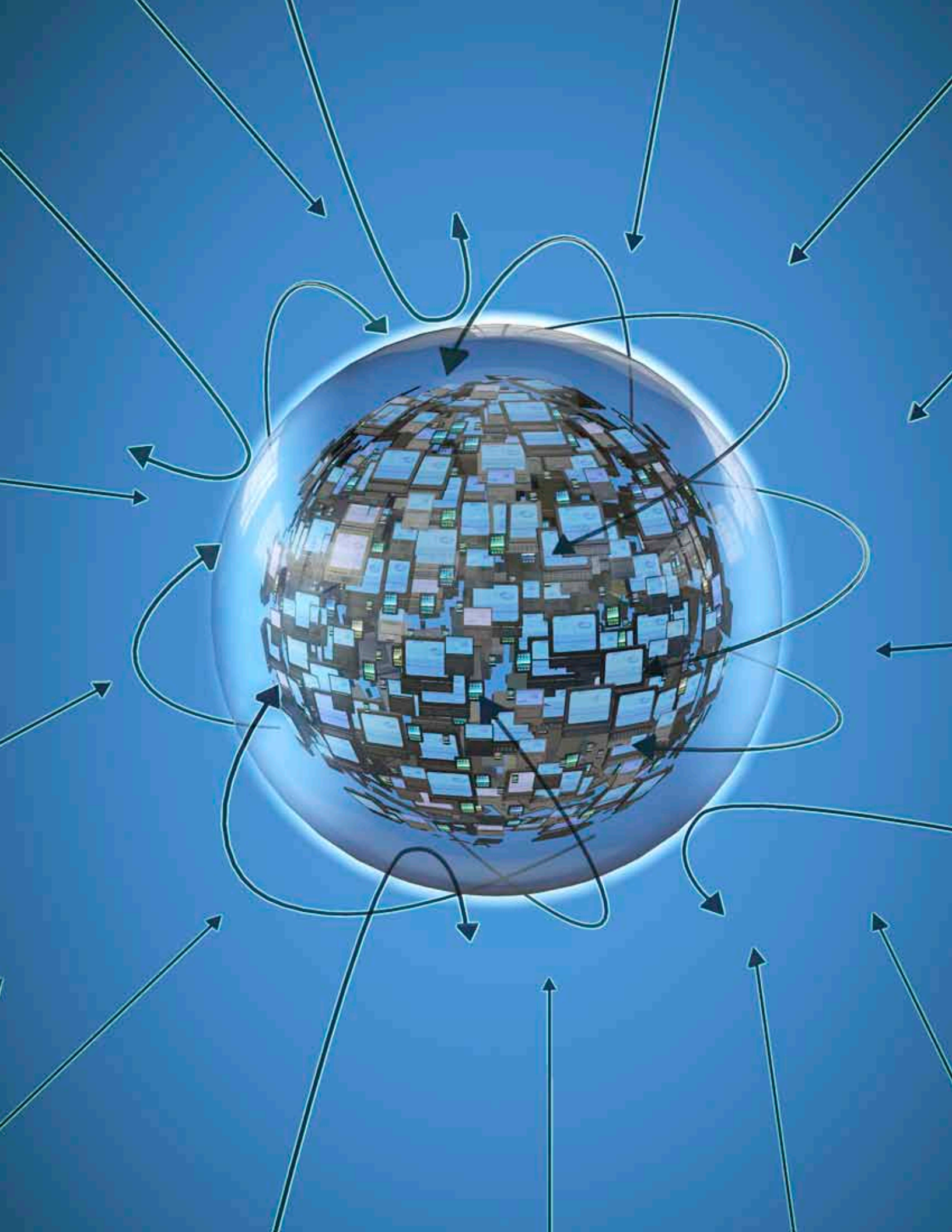

BOLSTERING

CYBER SECURITY

THREATS TO THE SECURITY OF COMPUTING RESOURCES RANGE FROM PC-PARALYZING VIRUSES TO CYBER ATTACKS RAISING THE SPECTER OF INTERNATIONAL FINANCIAL CHAOS – AND WORSE. NJIT IS STEPPING UP TO THE CHALLENGES OF CYBER SECURITY WITH RESEARCH, EDUCATIONAL PROGRAMS AND OTHER INITIATIVES.

You see nothing suspicious at your bank's website as you enter the usual security information. But a day or two later you discover that the balance of your checking or savings account is zero.

Your log-in information and your money have been stolen by cyber thieves who are becoming increasingly adept and aggressive. Strong defenses are needed to keep this scenario from becoming a widespread reality.

Hardly a day goes by without the world's news media reporting cyber attacks that escalate with the growing benefits of computing technology. Hackers are attacking for perverse amusement, to steal personal financial information for a thriving criminal underground, and to hone capabilities for waging the wars of the future. With security experts and hackers engaged in a contest of moves and countermoves, the highest level of vigilance is needed to defend computing resources.

ILLUSTRATION: RANDY LYHUS

PROTECTING THE CLOUDS

At NJIT, the College of Computing Sciences is a focal point of initiatives for bolstering cyber security. Assistant Professor Reza Curtmola, for example, works on cloud computing, an appealing option for streamlining IT operations and reducing costs. Essentially, organizations hire a vendor to provide "cloud" services over the Internet, such as applications and data storage.

"There are many cost-saving advantages to this arrangement, but there are also engineering challenges and significant security risks," Curtmola says. "In addition to the technical challenges of commodifying this innovation, the issue of security is perceived as a major obstacle to success in the computing marketplace. But at this stage in the development of cloud computing, we have a chance to break the typical pattern where security is added only as an afterthought, usually after attacks happen. Since cloud platforms are still in their infancy, security can be part of the initial design."

With the support of a Faculty Early Career Development grant of more than $500,000 from the National Science Foundation, Curtmola is seeking to make the relationship between data owners and what they've entrusted to the clouds more secure. In large measure, when data is outsourced to a cloud storage provider, the owner of the data loses control over its integrity. How does the owner really know that safeguards for data are adequate and that there hasn't been unauthorized access? Or is data being properly managed and preserved over time? The range of applications that can leverage cloud storage is limited because existing cloud platforms do not operate very transparently.

Curtmola intends to build a practical remote-data-checking (RDC) framework to assure long-term integrity and reliability of remotely stored data. Overcoming the limitations of current RDC protocols and existing cloud-storage architectures will mean, Curtmola says, that "You won't have to rely just on the word of your provider that all is well with your data."

PHOTO: JED MEDINA

Clockwise from left: Assistant Professor Reza Curtmola, Associate Professor Cristian Borcea, Associate Professor Guiling Wang

PHOTO: JOHN MICALE

SECURITY ON THE GO

With the proliferation of laptops, tablets, smart phones and other devices, computing power is everywhere and very much on the go. The combination of computing, mobility and wireless connectivity offers a wealth of new capabilities – and new security challenges. Meeting these challenges is basic to the work of Associate Professors Cristian Borcea and Guiling Wang.

Borcea is exploring ways to enhance the intelligence of smart phones with sensors designed to monitor pollution, traffic conditions and other aspects of our environment. He is also researching systems that enable social interaction with superior performance, trust and privacy.

According to Borcea, peer-to-peer networks linking friends via their personal computers or other devices could be an attractive and potentially more secure alternative to sharing social information on services like Facebook. The same strategy could be used to share applications by creating "social clouds" with secure privacy and communications protocols, as opposed to relying on companies such as Amazon and Google. "Both of these concepts avoid a 'Big Brother' scenario where a centralized server or service can learn too much about us based on the information we entrust to them," Borcea says.

PHOTO: JED MEDINA

In addition to exploring the capabilities of peer-to-peer networks, Borcea is teaming with NJIT colleagues, researchers at other universities and industry experts to address security issues unique to wireless interconnection. These include authenticating a mobile user's location and maximizing trust in ad hoc, or decentralized, networks, since familiar safeguards such as firewalls do not work for wireless communication. The need for effective security is fast increasing as we make more purchases and manage our finances with wireless devices – activities that require transmitting credit-card and other financial information.

"AT THIS STAGE IN THE DEVELOPMENT OF CLOUD COMPUTING, WE HAVE A CHANCE TO BREAK THE TYPICAL PATTERN WHERE SECURITY IS ADDED ONLY AS AN AFTERTHOUGHT." — Assistant Professor Reza Curtmola

One innovation that has emerged from Borcea's collaborative efforts is to leverage the capabilities of a secure co-processor to build a "trusted kernel agent" into the operating system of mobile devices. The agent ensures that only trusted software is allowed to run on or communicate with a device by verifying compliance with specific security policies. Otherwise, the agent will bar a suspected attacker from the network and prevent unauthorized access.

Most recently, Wang's research has focused on the potential and security of wireless sensor networks. The sensors that interest Wang are typically designed to collect data about the environment in which they are deployed, store that information, and transmit it to a central database. "They can be put to work in many places not so friendly to humans and be constantly alert to dangerous conditions," Wang says. Capable of forming self-organizing networks, these devices can collect data in remote or inhospitable areas about weather or pollutants, warn drivers of traffic congestion when embedded in roads, or signal that a bridge or other structure has deteriorated to an unacceptable degree.

As with ad hoc and peer-to-peer computing networks, the wireless foundation of remote sensing presents special security issues. Wang and her colleagues are working to develop encryption techniques that are both more effective and economical, methods to detect whether data collected by sensors has been tampered with, transmission technology that makes unauthorized access as difficult as

[continued on page 14]

CYBER ATTACKS

SHAKEN TO THE CORE

Threats to cyber security are growing rapidly in number and potential seriousness.

"Hackers Shake Web to the Core," a recent front-page *USA Today* story, reported attacks on companies that ensure the authenticity of Web pages where millions of people bank and shop. Hackers infiltrated firms that issue digital certificates verifying that pages accessed via popular Web browsers are indeed the pages they purport to be. Although the hackers were detected and thwarted, forged authentication certificates would have made it very difficult to differentiate the genuine Web pages of banks and retailers from pages created by the hackers to steal users' identifying information.

The list of companies, government agencies and other organizations that have come under attack continues to increase. The security company McAfee verified in 2011 that a cyber attack lasting five years – very likely directed by a foreign government – infiltrated and stole data from the United Nations and American corporations. In 2011 alone, the Privacy Rights Clearinghouse estimated that the data of more than 22 million people in the U.S. was comprised, with security breaches impacting Sony, Lockheed Martin, the United States Senate, the CIA, the FBI, Citigroup, Gmail, PBS and numerous other targets.

Hackers have even reached into space. In 2007 and 2008, it appears that hackers interfered with a U.S. satellite jointly managed by NASA and the U.S. Geological Survey. The attack was through the satellite's connection with a ground station in Norway, and the station's link with the Internet.

Leon Panetta cautioned the Senate Armed Services Committee during his confirmation as secretary of defense that the U.S. is likely to face cyber warfare as part of future international conflicts. He said that the next Pearl Harbor could be a cyber attack that cripples the country's electric-power grid, manufacturing facilities and financial infrastructure.

"WHEN YOU TALK TO A CEO OR FINANCIAL OFFICER, YOU HAVE TO PRESENT SECURITY OPTIONS IN TERMS THAT WON'T MAKE THEIR EYES GLAZE OVER." – Senior University Lecturer Dionissios Karvelas

possible, and network architecture that minimizes damage after an attack.

The need to protect sensor data varies greatly with application, Wang says. For example, a high degree of costly security is not warranted for monitoring the availability of spaces in a parking garage. But it is of far greater importance when sensors gather commercially valuable information or intelligence on 21st-century battlefields. For these applications, it is not only necessary to keep data from being intercepted and deciphered. Concern is compounded by the need to ensure that data has not been altered – or even completely replaced by misleading "disinformation."

SHARING ESSENTIAL KNOWLEDGE

Curtmola, Borcea, Wang and faculty colleagues also share leading-edge cyber security knowledge with students enrolled in the College of Computing Sciences. As concern about security grew with the evolution of computing technology, the subject became an important part of the college's curriculum – at first in individual courses and now in dedicated degree and certificate programs.

Senior University Lecturer Dionissios Karvelas has been actively involved in developing security-focused courses and a recently introduced master's program. He cites a number of key points that underline the value of these additions to the curriculum.

"As we put more and more functionality into devices and applications, this functionality can be used for malicious purposes," Karvelas says. "Therefore, it is extremely important for designers to ensure that an application not only offers the functionality that the user expects, but also that this functionality cannot be subverted for malicious activities."

Cyber security has become a serious concern in manufacturing products that did not require such specialized knowledge just a few years ago – automobiles, for instance. Substantial electronic intelligence now controls

NJIT'S COMMITMENT

BEYOND THE LAB AND CLASSROOM

The university's commitment to cyber security extends beyond the lab and classroom to the exploration of threats and solutions with experts from industry, government and other academic institutions.

■ Co-hosted by the Department of Computer Science, the biannual Security and Privacy Day workshop in December brought computer security experts from the New York metropolitan area to the NJIT campus. Among those participating were researchers from Columbia University, New York University, Princeton, Rutgers and Stevens. The December 2011 workshop was the first to be held at NJIT (http://web.njit.edu/~crix/SnP11). Assistant Professor Reza Curtmola, the workshop organizer, hopes that the event will return to campus in coming years.

■ In November, NJIT and the Marine Corps Reserve Association hosted a symposium at NJIT that focused on domestic and international cyber terrorism. Colonel (Ret.) Walter Conner and Brigadier General (Ret.) William Marshall, NJIT associate vice president, welcomed those attending. Topics included the effects of cyber terrorism on U.S. public and private targets, and strategies for minimizing damage and loss of confidence in organizations and institutions. Another focus was the role of state and federal law enforcement in countering cyber terrorism and balancing individual rights with effective cyber security.

■ Organized by Professor of Electrical and Computer Engineering Yun-Qing Shi, the 10th International Workshop on Digital Forensics and Watermarking was held in Atlantic City in October. Opening remarks were given by NJIT Senior Vice President for Research and Development Donald H. Sebastian. More than 30 papers on multimedia security were presented. They covered topics that included steganography, or hiding information in images, detecting hidden content, analytical techniques to determine if electronic image files have been altered, and techniques to protect the integrity of images.

PHOTO: JED MEDINA

Senior University Lecturer Dionissios Karvelas

the engine, brakes and other onboard systems. Services that can unlock doors remotely, detect the deployment of airbags, or immobilize a stolen vehicle require a wireless portal that could allow attackers to seize control of critical systems with the intent of causing harm.

Karvelas emphasizes that the importance of cyber security expertise is growing in many other industries. It is needed to protect the nation's power grid, financial institutions, chemical plants and refineries. Exercises testing the vulnerability of industrial supervisory control and data acquisition systems have shown that hackers can "ramp up" chemical and refinery process units to the point of catastrophic failure.

These trends translate into a growing number of stable employment opportunities in security for those with the right knowledge and skills, Karvelas adds. "Organizations are less likely to outsource security responsibilities, and you have to be a U.S. citizen to work in cyber security for the government. One of my students told me that the security staff was the only IT group unaffected by a recent cut-back at his former employer."

To meet the increasing demand for a workforce skilled in all aspects of cyber security, the College of Computing Sciences recently introduced the new MS degree in Cyber Security and Privacy. "We have designed a very strong program," Karvelas says. "It provides a solid theoretical foundation as well as invaluable hands-on experience for our students through practical exercises and exposure to a wide variety of attack and defensive tools. For instance, we have several exercises where students load a vulnerable 'virtual machine' on their own computer and practice with various attacks and countermeasures without being constrained by the time schedule of a campus computer lab."

It is also important to prepare students to make the case for cyber security in language that managers who are not expert in computing technology can understand. "It comes down to the bottom line," Karvelas says.

"Information assets have a certain value, and it makes sense to protect them with measures that do not cost more than their value. When you talk to a CEO or financial officer, you have to present security options in terms that won't make their eyes glaze over. The challenge is for all to agree on the most cost-effective solution that meets the desired security goals."

Today, the cost of cyber security can be high in many instances – but worth every penny. ■

MS in Cyber Security and Privacy:
http://cs.njit.edu/academics/graduate/mscsp.php

Network security certificate:
http://adultlearner.njit.edu/programs/networksecurity-cert.php

Author: Dean L. Maskevich is editor of NJIT Magazine.

COLLEGE OF COMPUTING SCIENCES

A DECADE OF CYBER-SUCCESS

In 2011, NJIT's College of Computing Sciences passed the milestone of a decade since its founding. Reflecting on how computing has evolved over the past ten years, Dean Narain Gehani says that much has changed, and changed quickly.

"Not too long ago, most students studied to become generalists in computer science," Gehani says. "That's not the case today. There's a strong trend toward domain specialization – to become expert in areas such as system administration, bioinformatics, business and computing, or security. Employers want graduates to enter the workplace with domain knowledge, graduates who essentially have a double major."

Gehani says that the administration and faculty at his college are very mindful of the need to accommodate this trend. "It's what current and prospective students expect."

For example, there will be an emphasis on developing the resources to prepare students for work in the field of mobile computing and networking. As Gehani explains, designing software for the convergence of computing and communications requires taking many new parameters into account – including the screen size of mobile devices, how the architecture of wireless networks affects video and data transmission, and the considerable challenges of security in the wireless world.

Looking ahead to the future of the College of Computing Sciences, Gehani also says, "I don't have a reliable crystal ball. But I think it's safe to say that there will be a growing demand for graduates with the right skills, with the education we are working to provide."

http://ccs.njit.edu