Princeton researchers envision a more secure Internet

February 18 2008

Like human society itself, the world's computerized infrastructure is wondrously complex, both spectacularly fertile and deeply flawed.

The Internet is, without question, a worldwide success. More than a billion people use it. On many places on Earth, the World Wide Web and e-mail have become so integrally woven into the fabric of life that it is hard to remember that just 20 years or so ago the Internet was an idea in its infancy. Banking, air travel, the electrical grid -- all have been transformed by computers and the Internet.

But the near-magical powers that the digitized world provides can be harnessed both for good and for ill. A recent report produced by the National Research Council and the National Academy of Engineering -- while delineating the great promise of our networked culture -- also warns of "ominous threats."

"Cyberspace in general, and the Internet in particular, are notoriously vulnerable to a frightening and expanding range of accidents and attacks by a spectrum of hackers, criminals, terrorists and state actors who have been empowered by unprecedented access to more people and organizations than has ever been the case with any infrastructure in history," write the authors of "Toward a Safer and More Secure Cyberspace," which urgently calls for a substantial increase in funding for cybersecurity research. The report argues that most of the players who are dependent upon cyberspace are unaware of how vulnerable and defenseless they are, and that the nation is "paying enormous costs for relying on such an insecure infrastructure."

Just how can a system that is as complicated as human society be made more secure? Some of the most influential thinkers on this question sit just a few dozen steps away from each other in the engineering complex on the Princeton campus: Edward Felten, director of the Center for Information Technology Policy, focuses on software and policy; Ruby Lee heads the Princeton Architecture Lab for Multimedia and Security; and Larry Peterson and Jennifer Rexford are key players in the Global Environment for Network Innovation.

While these researchers may be physically proximate, their unique visions on how to best ensure cybersecurity can seem worlds apart. What follows are portraits of these pathfinders at the frontiers of security research.

A 'clean-slate' redesign

Peterson is chair of the computer science department and a force behind the Global Environment for Network Innovation (GENI), a National Science Foundation-backed effort to build a test-bed Internet -- one that parallels the actual Internet but which researchers can use to run all sorts of experiments.

"The research community has lots of potential solutions to our vast array of security problems, but currently we have no way to investigate and validate those solutions," Peterson said. "GENI will enable us to figure out what works and what doesn't."

GENI is often referred to as a "clean-slate" attempt to redesign the Internet from the ground up. Peterson said that while GENI may indeed lead to a wholesale reshaping of the Internet, it might also lead to more incremental changes.

"It is an extreme position to believe that we are going to replace the entire Internet," he said. On the other hand, Peterson noted, the Internet itself is a model for its own reinvention. "Thirty years ago the Internet was the crazy clean-slate idea on the block and telecommunications was the entrenched system," he said.

Peterson likes to say that this is computer science's opportunity to do fundamental research in a way that has never before been possible. The GENI testing ground is to computer scientists what a particle accelerator is to physicists or a space telescope is to astrophysicists.

Peterson has described GENI as "our moon shot" and as the computer field's equivalent of the International Space Station, calling it "our chance to do big science."

Most important, as Peterson sees it, GENI would give the research community a chance to profoundly influence the future of the Internet. He points out that if the Internet continues on its current trajectory, industry will dominate all important decisions about its future. "If industry continues to chart the course of the Internet we won't ever be able to have a national debate on privacy and security," said Peterson.

Peterson argues that a blue-sky project like GENI is essential because deeply innovative research cannot be done on the Internet; experimentation would jeopardize the stability on which existing commerce and other business depend. Researchers need a separate test bed where they can safely try wild new ideas, he said.

So far the Internet has proved to be exceedingly innovative "at the edges" -- for example, giving the raw material for an inventive 19-year-old to bring the billion-dollar music industry to its knees with the invention of Napster. Peterson sees GENI as the means to train innovative thinking on the technological core of the Internet, instead of peripheral applications.

GENI will allow researchers to experiment with new approaches to specific aspects of the Internet. It also will allow them to play with new technologies that ultimately may supplant the network of networks that currently serves as the Internet's nervous system with something we can scarcely yet imagine -- say, an entirely wireless infrastructure or one that operates chiefly on optics.

Above all, Peterson -- like his GENI compatriot Jennifer Rexford -- firmly believes that the best way to address security is through the network. "We can't wait for all personal computers to become more secure," he said. "The network needs to be able to quarantine compromised machines so that we can limit their collateral damage."

Security from the start

While Peterson contemplates a clean-slate version of the Internet, Lee, the Forrest G. Hamrick Professor of Engineering, talks about "clean-slate" design with personal computers, PDAs and cell phones in mind. That is not to say that the potential impact of her work is any less far-reaching than Peterson's. "I'm working on individual computing devices rather than entire networks," she said. "But there are trillions of those devices."

Lee -- who was a member of the Committee on Improving Cybersecurity Research in the United States, the group that produced the report mentioned earlier -- observes that researchers in academia are in a position to make contributions to Internet security that simply cannot be made in the realm of commerce.

"In industry, successful entrenched products cannot be completely changed overnight -- rather they have to be improved gradually," said

Lee. "When we do research in academia we have the freedom to consider all possibilities -- including designing security from the beginning rather than as an afterthought." The good ideas, she said, will inevitably migrate to industry.

Lee's ultimate goal is to prevent inadvertent exposure of sensitive information and also to inoculate computers against threats like viruses, worms and bots so that they cannot infect, or be used to attack, other machines. She aims to do this by building fundamental security features directly into the hardware of a device. Members of her lab are working to build "trust anchors" into computer hardware to which different software can be tethered to provide important security coverage.

"Computers were not originally designed with security as a goal," said Lee, who -- as chief computer architect at Hewlett-Packard in the 1980s -- helped lead an industry revolution in computer architecture. "I'm trying to rethink the design of computers so they can be trustworthy while retaining all their original design goals, such as high performance, low cost and energy efficiency. Also, usability is important. If people find security a hindrance, they will find a way to bypass it."

According to Lee, many researchers do not think it is possible to build security features into computer hardware without slowing the computer or causing it to consume lots of power. However, research done by her lab demonstrates that this is not the case.

"These hardware 'roots of trust' are actually quite deployable on consumer devices like desktop computers or PDAs, and also in sensor networks and larger servers," said Lee. Her work is part of the SecureCore multi-university research project -- funded by the National Science Foundation Cyber Trust program and the Defense Advanced Research Projects Agency -- whose goal is to integrate essential security into the hardware, software and networking at the core of mass-market computing and communications devices.

In addition to her cutting-edge research, Lee teaches a popular undergraduate lecture class on cybersecurity in which the students split roughly 50-50 between engineering and non-engineering majors.

"I'm trying to train the future policymakers, lawyers, entrepreneurs and company executives to understand what the technology can and cannot do," she said. "There are political, economic and social dimensions to this problem. Technology alone will not solve the problem of security in cyberspace."

Short-term, high-impact research

When it comes to research, fellow Princeton computer scientist Felten takes a different approach from Peterson and Lee, not just in his vision but in the execution of his vision.

Clean-slate efforts may require buy-in from many different players, cost hundreds of millions of dollars and take years to implement. Felten, a professor of computer science, and his nimble band of graduate students specialize in projects with short time horizons -- say, nine months. Much of their high-impact work can be performed on an ordinary personal computer.

Peterson, Lee and Felten all can be thought of as contemplative, big-picture generals in the campaign to make the Internet a safer place. But while Lee and Peterson work to harden the core technological armamentarium, Felten is dispatching graduate students to the front lines, where they prod for specific vulnerabilities -- and then forge new software to fortify chinks in the ramparts.

Felten's graduate student Bill Zeller, for example, recently demonstrated the vulnerability of several high-profile Internet sites, including one of the nation's biggest newspapers and one of the world's largest online banks. Zeller hacked into the online bank account of a fellow student (the student had given Zeller permission to try) and stole $100 out of the student's account. Zeller and Felten are preparing a paper on their research but have privately told the companies about the vulnerability and supplied them with a software fix to the problem. In 2006, Felten and his students famously hacked an electronic voting machine, drawing worldwide coverage by most major news outlets while they advocated new ways to make the system safer.

"People like to write about the problem-finding that we do because it is dramatic, but that is only part of my work," said Felten, who was recently appointed as a member of the Washington, D.C.-based Center for Strategic and International Studies' Commission on Cyber Security for the 44th Presidency. "We work equally hard at finding solutions."

Recently, Felten appeared several times on Capitol Hill, testifying about voting security before the House Administration Subcommittee on Elections and briefing the Senate Science and Technology Caucus on botnets, invisible robots that can stealthily turn a seemingly innocent PC into a malicious zombie. Felten's blog, www.freedom-to-tinker.com , is considered must-reading by many journalists and thought leaders.

Named recently by a consortium of technology magazines as one of the most 100 influential people in the field of information technology, Felten believes that many important problems with the Internet have less to do with the technology itself than with the way in which people use it. He points out that hardware solutions can only partially protect against denial-of-service-attacks like the one last spring when hackers caused thousands of computers around the world to send messages that overwhelmed websites in Estonia and temporarily crippled the government.

Felten shares Lee's view that Internet security is not merely a technological question. But he does not share Lee and Peterson's optimism that trust features built into hardware or networks can protect against the myriad dangers lurking in cyberspace. "A lot of the problems and issues have to do with interactions between users and computers -- it's the human interface that is problematic," said Felten. "I'm skeptical about what you can do at the core of the technology."

Spectrum of solutions

If Felten is at one end of the spectrum in his vision of how to best make the Internet secure in the future, and Peterson and Lee are at the other end, then Rexford stands in the middle. Or, perhaps more accurately, Rexford stands simultaneously at both ends of the spectrum -- a shrewd strategist who sees the advantages of simultaneously pursuing seemingly opposite research agendas.

On the one hand, Rexford, a professor of computer science, is a key player in GENI.

"GENI would really open up the intellectual space in thinking about the Internet," Rexford said. "Often people kill off interesting lines of inquiry because they aren't compatible with the Internet as it exists today. So we end up shutting off the part of our brains that is thinking outside the box."

On the other hand, Rexford has been working for several years on improving routing protocols -- the rules by which information is shunted from one path to another across the Internet. In this, Rexford is aiming to increase security incrementally over time -- taking in many ways the opposite of the "clean-slate" approach that GENI promises.

The Internet is essentially an aggregation of 25,000 or so separately operated networks of computers. They are stitched together by the "border gateway protocol," which is notoriously insecure.

The system works fine when all the players are honest. But some players are not, and thus arise the unfortunate phenomena of identity theft, spam and denial-of-service attacks. "If you lie about who you are you can easily reroute Internet traffic," said Rexford. "Which is why it is so crucial that we address this vulnerability in the system."

Felten, Lee, Peterson, and Rexford are by no means the only researchers at Princeton wrestling with security and information technology. In electrical engineering, Paul Prucnal and members of his lab are building stealth communications networks with optics; Niraj Jha recently received a major National Science Foundation grant for building architectures for secure embedded systems; and Hisashi Kobayashi and Mung Chiang have concentrated their powerful analytical skills on various aspects of communications security. In computer science, Robert Tarjan is conceptualizing trustworthy systems with well-understood security and privacy properties; Andrew Appel is casting a vigilant eye on electronic voting security; David Walker is pursuing secure software applications; and Boaz Barak is working in fundamental cryptography. And H. Vincent Poor, dean of engineering and an electrical engineer, is exploring new ways to provide security in wireless communications, the use of which continues to increase dramatically.

It is precisely the unfettered proliferation of inspired yet divergent research agendas --epitomized by the work currently under way at Princeton -- that offers the promise of security to the ever-increasingly networked world. In certain respects, all of these researchers are intellectual heirs of Robert Kahn, one of the cofounders of the Internet who earned his Ph.D. in electrical engineering from Princeton in 1964. Like Kahn, they are boldly challenging the status quo, imagining new possibilities.

At a recent event at Princeton, Kahn posed the following provocative question: Just how will the research community -- where many of the really innovative ideas have originated -- influence the future of the Internet, now that it is so deeply insinuated into our society? "That," he observed, "is one of the more interesting problems of our time."

Source: Princeton University, by Teresa Riordan

Citation: Princeton researchers envision a more secure Internet (2008, February 18) retrieved 25 April 2024 from https://phys.org/news/2008-02-princeton-envision-internet.html