

THE INTERNET

Protecting Security and Privacy

Tadayoshi Kohno considers the risks of ubiquitous computational devices.

We are at the cusp of a technological revolution that will make computational devices ubiquitous in our environment—from digital sensors for home-based assisted living to next-generation wireless implantable medical devices for heart pacing and defibrillation. But the wonderful new opportunities these devices present come with potentially serious threats to our data, privacy, property, and even personal safety. For example, while the MySpace generation might flock to future phone-based social-networking systems—systems that could instantly reveal whether the person next to you at the bar is a “friend of a friend” who shares your passion for classic movies and country line dancing—those same systems might be exploitable by sexual predators and other miscreants.

Helping society realize the benefits of these new technologies without simultaneously exposing users to serious risks is the charter of the computer security research community.

Computer security researchers study existing and proposed electronic systems in order to determine and learn from their weaknesses. In my own work with colleagues at Johns Hopkins and Rice University, we discovered that it’s possible to compromise the security of electronic voting machines and change election results. In another example, scientists at Microsoft Research have evaluated the extent to which malicious software on cell phones could disrupt regional cellular communications.

Once we’ve identified significant security deficiencies, we develop improved security mechanisms. Classically, such research has centered on systems that *can* be used securely. But there is a wide gap between systems that *can* be used securely and systems that *will* be used securely. For example, recent results from Harvard University and the University of California, Berkeley, suggest that many users ignore anti-phishing defenses in Web browsers. To fully understand and improve the usability of security mechanisms, we must study users in realistic settings. At the University of Washington, we developed a building-wide network of sensors—the RFID Ecosystem—that

we are using to explore more intuitive and natural methods for controlling digital privacy in future computing environments.

Another emerging theme in security research is the attempt to hold computer users accountable—to find digital

analogues for surveillance cameras and forensic identifiers like fingerprints and DNA. Together with researchers at the University of California, San Diego, my colleagues at the University of Washington and I are developing one such accountability mechanism. Our design preserves a user’s privacy in the common case: while they’re always present, our forensic trails can be “opened” only under very special circumstances—for example, when a court order has been issued.

The next time you’re enjoying the benefits of your latest digital gadget, whether it’s a wireless gaming helmet with built-in brain-activity sensors or a new RFID credit card, you might think about the mischief that could be accomplished by someone who circumvents the device’s security. The helmet could let you

directly control your computer game with your mind, but could it also reveal your private thoughts to malicious software on the gaming system, or to anyone within wireless range? These are the kinds of issues that drive the security research community toward creating a more secure and private digital world. **TR**

Tadayoshi Kohno, an assistant professor in the Department of Computer Science and Engineering at the University of Washington, is a member of the 2007 TR35 (p. 58).



NANOTECHNOLOGY

The Future of Manufacturing

Production of complex systems will soon take advantage of self-assembly, says Babak A. Parviz.

A typical microprocessor integrates a large number (greater than a hundred million) of small (less than 100 nanometers) electronic parts, but the miniaturized systems of the future will also need to incorporate photonic, mechanical, chemical, and even biological devices. The semiconductor industry has had impressive success in producing integrated electronics, but it has been decidedly less successful at mass-manufacturing multifunctional microsystems, partly because the processes used to make different components are incompatible. A major question for engineers is what manufacturing process can mass-produce useful multifunctional, miniature systems. The conventional approach to making engineered products is unlikely to yield a satisfying answer.

The most complex functional systems are found in the biological world. Nature is full of machines with trillions of nanoscale components all working in harmony. The complexity and sophistication of biological machines—in terms of the number of parts, the variety of materials used, and the diversity of functions


performed—is far beyond what any microfabrication or nanofabrication can achieve.

These advanced biological machines are mass-produced in a way that is fundamentally different from the way we produce products such as microprocessors, automobiles, or airplanes today. In nature, components “self-assemble” to yield complex functional systems. Inspired in part by this observation, a number of research groups are working to enlist self-assembly as a method for producing functional products across size scales. The hope is to create a new paradigm in mass manufacturing in which self-assembly replaces assembly of parts one by one. We believe that, in principle, it is possible to “grow” an integrated circuit, a biomedical sensor, or a display.

To get a system to self-assemble from the bottom up, you have to address a few key issues: how the parts are made, how they are induced to recognize and bind to each other in the correct fashion, and how the assembly process can be controlled and streamlined. Chemical synthesis can readily produce a large number of nanoscale “parts” such as quantum dots or molecules that are designed to perform specific functions. And researchers can take advantage of specific covalent bonds or supramolecular bonds such as DNA hybridization or protein-inorganic surface interactions to program the self-assembly process.

Our group has investigated these methods as a way to produce hybrid organic-inorganic transistors and photonic waveguides. Solid-state microfabrication is another technique for producing parts for self-assembly. The parts are fabricated

separately, released, and then induced to self-assemble. Our group has used this approach to construct high-performance silicon circuits on plastic.

This revolutionary manufacturing method offers many opportunities. Growing machines may not be as far-fetched as it once seemed. 

Babak A. Parviz is an assistant professor of electrical engineering at the University of Washington. He is also a member of this year's TR35 (p. 70).

BIOTECHNOLOGY

Cells by Design

J. Christopher Anderson explains the importance and the challenges of synthetic biology.


Living cells are amazing things. They created the oxygen we breathe and the fossil fuels that power our world. They provided the organic compounds that form the basis of many drugs and materials. They feed us, live in our bodies, and protect us from other cells and viruses. They can self-organize. They can learn.

It's clear, then, that the potential range of what biological systems *could* do is enormous. Among the areas that could most obviously benefit from them are health care, chemical and materials production, environmental remediation, and energy. However, most of the systems that would be useful in these areas are unlikely to occur naturally. We probably won't stumble upon a cell capable of serving as an artificial blood substitute, for example, or one that harnesses sunlight as transportation fuel. These systems must be engineered.

Synthetic biology seeks to build non-natural systems by adding DNA sequences—effectively, little genetic “programs”—to well-studied cells such as *E. coli* and yeast. This is, at heart, an engineering problem, one that

requires both new “software” (new sequences of DNA) and new hardware (the DNA itself—and the methods for putting it into cells). Synthetic biology has thus far dealt principally with the software. But making the DNA that can be put into cells is difficult and expensive; it has been the fundamental impediment to progress.

Today, long sequences of DNA can be synthesized chemically by commercial vendors at a cost of \$1 per base (the DNA “letters” A, T, C, and G). Considering that the sequences we design today are on the order of 10,000 bases, and we want to redesign entire four-megabase genomes, the costs quickly become astronomical. We hope the price will drop, but an alternative lies in the automated assembly of standard biological parts. Here, we don't synthesize each DNA program with base-level precision. We instead begin with a library of “basic part” DNA sequences. A robot joins these sequences into complete genetic programs using a standard assembly reaction. It is analogous to building electronic devices from a box of transistors, capacitors, and resistors rather than building the whole system at once by lithographic methods. The key is making the technique robust, low cost, and highly automated.

Synthetic biology will really take off once it has transformed itself into an information-driven discipline. The key to that transformation is automated synthesis. The potential is clear—we have no shortage of naturally evolved examples that tell us where the technology *can* go. We just have to figure out how to take it there. 

J. Christopher Anderson, a member of the 2007 TR35 (p. 60), is a postdoctoral fellow in the Department of Bioengineering at the University of California, Berkeley.

