Green Computing

Carl E. Landwehr
Associate Editor in Chief

Butler Lampson's provocative opening address at the US National Science Foundation's 2005 Cyber Trust meeting this fall proposed a security architecture for ordinary computing based on two colors: red and green. A typical user would have two environments: a red (risky) one, open to the myriad enchantments and attacks of today's Internet, and a green (safe) one, which would be much more protected and have limited communication with the red world.

In the red environment, you could browse the Web, download, view, and compute whatever you like. On the green side, you could do your taxes, maintain your health records, and keep your communications with your stockbroker or, I suppose, your paramour. The green side would be carefully locked down and, in most cases, professionally managed.

The decision of what information could enter the green side would be tied to the sender's accountability. To be accountable, the sender would have to pledge something of value—reputation, money, friendship—so that the recipient of a malicious message or program could penalize the sender. Today's Internet and the applications that use it provide relatively weak support for this kind of accountability, but perhaps it could be strengthened.

The scheme could be implemented using two separate machines, but, Butler argued, most people won't put up with that (just ask former CIA director John Deutsch—only a presidential pardon rescued him from the consequences of using his classified office laptop to access the Internet from home). More likely, it would mean two different environments on one machine—separated by a virtual machine monitor, for example.

Anyone concerned with computer and communication security in the context of military systems will recognize this approach. Encryption devices have long had a red side, where data is unencrypted and vulnerable, and a black side, where the data is encrypted and safe. The US military, which probably depends more on the open Internet than any large company, has tried to segregate its networks and systems into two classes: those that are relatively open to the Internet and those that are accessible only to cleared individuals.

Of course, military information is classified into more than two categories, but efforts to support automated labeling and manipulation of multiple levels and compartments have generally foundered on the complexity of the interface presented to the user.

But are two domains really enough? As individuals, we easily separate what we tell our doctors from what we tell our lawyers, our stockbrokers, and our librarians. But the technology we've been able to create so far doesn't adequately hide the complexity of this kind of segregation or provide the assurance of separation we might want.

Later in the same meeting, Joel Birnbaum, former senior technical advisor to HP, made a strong case for the urgent need to find ways to hide the complexity of managing security. Moreover, David Brailer, the US National Coordinator for Health Information Technology, made it clear that if you live in the US, your health record will be increasingly automated. Hopefully, this automation will reduce errors and costs, but it is also likely to put more sensitive information on your own computer. (Video and viewgraphs of all three talks, and other related information, is available at www.ics.uci.edu/~cybrtrst.)

A rich R&D agenda flows from these points. We need computing and networking environments that support many forms of accountability, but we also need to understand how to construct systems with interfaces simple enough to be usable, yet capable of supporting the kinds of security policies we employ intuitively every day. It's hard to think of a simpler place to start than a separation of one environment into two; if we can't handle that, then what can we do? As Butler pointed out, whether you think a red/green solution will work or not, it's clear that nearly all of the computers people use in their homes today are red, not green. We need to start getting the red out and moving toward green computing. ▢