# There Ain't No Inside, There Ain't No Outside . . .

There ain't no good guys, there ain't no bad guys,
There's only you and me and we just disagree

—*"We Just Disagree," words and music by Jim Krueger*

Although Jim Krueger might be right that there are no good guys or bad guys in a romantic disagreement, in computer security, there are definitely good guys and bad guys. What there isn't, however, is an inside or an outside.

MARC DONNER
*Associate Editor in Chief*

In the 1990s, before Web browsers emerged, corporations owned or licensed all of the information on a corporate computer display—it was inside. Being inside was a proxy for trusted, whereas being outside meant being untrusted . . . for everything. Security experts warned that these simple solutions were too coarse, and that the principles of least privilege and separation of concerns should be adopted, but everyone ignored this advice.

After the Web became pervasive, however, users could reach outside from the corporate network and its computer systems. It became easier and cheaper to share information with clients and suppliers. Corporations embraced these opportunities to speed up their businesses, increase their reach, and cut their costs. Economics drove businesses to implement these drives to efficiency with outsourcing, supply-chain management, and other business innovations, and governments supported them with deregulation. In the process, all this activity eliminated the distinction between inside and outside on corporate networks: "Oh, that application is hosted at a partner colo." "Yeah, we outsourced our statement and confirmed printing." "That server is owned by a data provider—we let them station it in our machine room."

Businesses increased their reliance on external partners, and the number of exceptions to the "only employees inside the firewall" rule grew rapidly. Nonetheless, we blithely carried on as if the "Tootsie Roll Pop" security model—hard crunchy outside, soft chewy inside—was still meaningful. That's partly because we didn't have mature alternatives (a few consultants and vendors notwithstanding) and because the threats were still manageable despite the progressive failure of our core approach. Moreover, we still don't really have any idea how to secure our systems' components so that they're secure but still robust, flexible, and easy to use.

A few years ago, Stu Feldman of IBM Research observed that when working with one or two people, the problems are computer science, but when working with 1,000 people, the issues are sociology. (Stu claims he actually said "crowd control.") Translated, this means that getting our system architectures adapted to an inside-less world involves more than just figuring out how to secure a database server or control access to an application host. It means educating the larger community of people who use and rely on our systems about the implications of architectural choices and the costs and timescales of system migrations. The recent press coverage of major corporations losing large volumes of data contributes to that educational process. One of the larger losses, that by CardSystems, was of data held in the course of its work that supported the clearance of credit-card transactions. CardSystems didn't own the data it held, and the hacking incident exposed the importance of a flaw in its data-retention policies. If it hadn't held on to information that it didn't need and wasn't authorized to retain, the loss of information suffered when its system was cracked would have had much less impact.

## Erratum

In the July/August 2005 Conference Reports department, EICAR should have been correctly identified as the European Institute for Computer Anti-Virus Research. We regret the error.

—*Eds.*

Although we might scorn the subsequent press coverage as superficial and sensational, it tells the public that data loss is happening and that we all better be concerned. Suddenly, nonspecialists are realizing that such arcane and abstract things as data-management policies and security architectures can and should matter to them.

So, how are we doing? Unfortunately, we're still too focused on computer science topics and not enough on sociology ones. Ralph Gomory, back when he directed IBM Research, said that real problems, the ones you encounter when you rub shoulders with people out in the world, stimulate the most interesting research advances. What can you do to help? Get out of your office. Collaborate with someone who's not a computer scientist or engineer. Think about the overall outcomes and interactions of technology, policy, and the behavior of people, and then act accordingly. ▢

## Responding to Hurricane Katrina

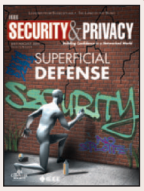
The United States is currently facing one of the greatest natural disasters in our history. We empathize with the pain and suffering of tens of thousands of Americans in the Gulf region including Louisiana, Mississippi, Alabama, and Florida.

On behalf of the 90,000 IEEE Computer Society members worldwide, the Computer Society offers its condolences and support to the people of the Gulf coast area affected by the tragedy of Hurricane Katrina.

For information on how you can help those affected, please visit

www.ieeeusa.org/about/Katrina

## How to Contact *IEEE Security & Privacy*




### Writers

Visit www.computer.org/security/author.htm or log onto Manuscript Central at http://csieee.manuscriptcentral.com/. Authors must use Manuscript Central to upload their submissions. First-time users must create new accounts.

### Letters to the Editors

Send letters to Kathy Clark-Fisher, Lead Editor, kclark-fisher@computer.org. Please provide an email address or daytime phone number.

### Subscription Change of Address (IEEE/CS)

Send change-of-address requests for magazine subscriptions to address.change@ieee.org. Be sure to specify *IEEE Security & Privacy*.

### On the Web

Access www.computer.org/security/.

### Missing or Damaged Copies

If you are missing an issue or received a damaged copy, contact membership@computer.org.