

JOIN THE COLLECTIVE WISDOM:



NEWS



PREDICTIONS



COMMUNITY

Find out more >> **the stance**



[Back to article](#)  [Print this](#)

Access control, monoculture, and accountability

In medium to large enterprises, access control lists don't scale, so we need new ways to monitor data

By Jon Udell

September 17, 2004

Two years ago I bumped into a powerful idea that I knew I'd be hearing about again. In a blog entry [about ACLs](#) (access control lists), I cited a speech given by Dan Geer to the Security Industries Middleware Council. Geer was then CTO of @Stake, a security consultancy that fired him last year for co-writing a much-publicized [Computer and Communications Industry Association report](#) asserting that a software "monoculture" -- such as Microsoft's dominance has created -- is an inherent security risk.

The monoculture idea is self-explanatory, but the concept of accountability needs some unpacking. Along with Geer's [SIMC keynote](#), you might want to listen to Doug Kaye's [interview with Geer](#) on the ITConversations Web site. Geer argues that access control lists -- although they'll remain a vital ingredient of information security -- can't take us where we now must go. The reason is that linear growth in the number of people you authenticate, or the number of resources you control their access to, or both, results in geometric growth of the matrix of checkboxes you must fill out. Every checkbox requires an explicit choice, and it gets impossibly hard to keep up.

The way forward, Geer suggests, is not to abandon ACLs but rather to augment them with aggressive monitoring that holds people accountable for behaviors that can't economically be permitted or denied. ACLs don't scale because checkbox maintenance requires a scarce resource: the human decision-maker. Accountability does scale because event logging and data analysis ride the favorable current of Moore's law.

This notion is compelling because, as Geer points out, our free society works in a similar way. We don't have to ask permission for most things, but, "If I sufficiently badly screw up," Geer says, "there's some expectation that will be discovered, and I'll be found, and I'll be made to pay."

The means of discovery is surveillance. In the physical world we rely on eyewitnesses and increasingly, especially in Britain, on cameras. In the virtual world, according to Geer, we're now approaching a critical fork in the road: "To the left, we surveil people. To the right, we surveil data. I'm arguing for data-level file-tracking because if I have to surveil either people or data, I think it's highly important that we choose to surveil the data, not the people."

Not coincidentally, Geer's new company, Verdasys, supplies file-tracking technology. The concept is straightforward: Deploy an agent to the desktop that intercepts and logs all transactions with the file system, and with other services such as e-mail, IM, and the clipboard. Verdasys expects corporations will use this data both to enforce policies and to enable forensics.

The accountability argument is convincing, and I'll be fascinated to see how all this plays out. Ironically, though, it casts the monoculture argument in a new light -- at least for me. I've long lamented Microsoft's failure to establish a strong tradition of event logging on the Windows desktop. Because the relevant Win32 APIs were omitted from Win95, we inherited a generation

of Windows applications that don't gather much useful evidence. Had it ensured broad deployment of such evidence-gathering capability, the Microsoft monoculture might today be a source of mitigation as well as of risk.

 [Print this](#)