Schneier-Ranum Face-Off: Is Perfect Access Control Possible?

http://searchsecurity.techtarget.com/magazineContent/Schneier-Ranum-Face-Off-Is-Perfect-Access-Control-Possible June 9, 2012

Point: Bruce Schneier

Access control is difficult in an organizational setting. On one hand, every employee needs enough access to do his job. On the other hand, every time you give an employee more access, there's more risk: he could abuse that access, or lose information he has access to, or be socially engineered into giving that access to a malfeasant. So a smart, risk-conscious organization will give each employee the exact level of access he needs to do his job, and no more.

Over the years, there's been a lot of work put into

role-based access control. But despite the large number of academic papers and high-profile security products, most organizations don't implement it--at all--with the predictable security problems as a result.

Regularly we read stories of employees abusing their database access-control privileges for personal reasons: medical records, tax records, passport records, police records. NSA eavesdroppers spy on their wives and girlfriends. Departing employees take corporate secrets.

A spectacular access control failure occurred in the UK in 2007. An employee of Her Majesty's Revenue & Customs had to send a couple of thousand sample records from a database on all children in the country to National Audit Office. But it was easier for him to copy the entire database of 25 million people onto a couple of disks and put it in the mail than it was to select out just the records needed. Unfortunately, the discs got lost in the mail, and the story was a huge embarrassment for the government.

Eric Johnson at Dartmouth's Tuck School of Business has been studying the problem, and his results won't startle anyone who has thought about it at all. RBAC is very hard to implement correctly. Organizations generally don't even know who has what role. The employee doesn't know, the boss doesn't know--and these days the employee might have more than one boss -- and senior management certainly doesn't know. There's a reason RBAC came out of the military; in that world, command structures are simple and well-defined.

Even worse, employees' roles change all the time--Johnson chronicled one business group of 3,000 people that made 1,000 role changes in just three months--and it's often not obvious what information an employee needs until he actually needs it. And information simply isn't that granular. Just as it's much easier to give someone access to an entire file cabinet than to only the particular files he needs, it's much easier to give someone access to an entire database than only the particular records he needs.

This means that organizations either over-entitle or under-entitle employees. But since getting the job done is more important than anything else, organizations tend to over-entitle. Johnson estimates that 50 percent to 90 percent of employees are over-entitled in large organizations. In the uncommon instance where an employee needs access to something he normally doesn't have, there's generally some process for him to get it. And access is almost never revoked once it's been granted. In large formal organizations, Johnson was able to predict how long an employee had

worked there based on how much access he had.

Clearly, organizations can do better. Johnson's current work involves building access-control systems with easy self-escalation, audit to make sure that power isn't abused, violation penalties (Intel, for example, issues "speeding tickets" to violators), and compliance rewards. His goal is to implement incentives and controls that manage access without making people too risk-averse.

In the end, a perfect access control system just isn't possible; organizations are simply too chaotic for it to work. And any good system will allow a certain number of access control violations, if they're made in good faith by people just trying to do their jobs. The "speeding ticket" analogy is better than it looks: we post limits of 55 miles per hour, but generally don't start ticketing people unless they're going over 70.

Bruce Schneier is chief security technology officer of BT Global Services and the author of Schneier on Security*. For more information, visit his website at www.schneier.com.*

Counterpoint: Marcus Ranum

I don't like reasoning by analogy, Bruce, because it often obscures as much as it illuminates. While the "speeding ticket" analogy *sounds* sensible, that's only because it leaves out a whole lot of detail, such as what happens when someone is violating the speed limit and causes another person injury. If you're going 55 in a 30 miles-per-hour zone and cause an accident with injury, "screwed" doesn't begin to describe the situation. I could extend your analogy to access control, but we'd be increasingly moving away from the real topic at hand while arguing about cars; it's pointless.

Here's the problem: if you are supposed to be guarding some data, and don't, and it causes someone injury, "screwed" should be the starting point for describing your situation. I know that talking about morality and computer security is pretty retro, but someone has to point out that data leaks can represent huge headaches or worse for the victims--and by "victim," I don't necessarily mean the holder of the data.

Many organizations are stuck in between letting everyone who wants it download a copy of customer databases to their laptop (which they then lose) or re-designing all their databases to add controls which may or may not help. It's very difficult to get management to invest in re-implementing systems against the threat of something that hasn't happened before. But, it's unacceptable, both technically and morally, to give an expansive shrug and say "It's impossible to get access control right" (with the implication that leaks are just going to happen) when two things are obvious:

- We're dealing with the tip of an iceberg
- Current approaches are what got us to where we are now

As you say, over-entitlement is the norm, and usually makes sense, but that's simply because we are only, just now, beginning to pay the costs for mistakes made years ago. Perhaps 10 years ago it seemed like a big cost-saving to move critical databases to departmental servers, and to make it easy and allegedly more cost effective to grant full database access to those who asserted (sufficiently loudly) they needed it. Now, we are finding that those cost savings may not have been estimated correctly--too bad and too late.

The current trend in data management seems to be to outsource it to places where it can be managed more cheaply--meaning, by definition, that it's being positioned where it's relatively more valuable. Then, they're actually surprised to discover that someone in the call center sold the customer database. I'd be perfectly comfortable testifying that whoever made that decision, which was tantamount to exposing the data, was both incompetent and negligent.

The great, big, lurking disaster that nobody wants to talk about is national security data. You and I both know how much pressure there has been to shift from "need to know" to "need to share"--i.e., increase access rather than limit it. And, again, people hear about Joint Strike Fighter technical

plans leaking, and react with shock and awe. To incompetent and negligent, we can add dangerous and threatening to national security.

I don't think any of the models we're working with are particularly good, and simply wishing we had better ones doesn't mean that better ones exist. Consider digital rights management (DRM)--ultimately, that was about controlling access to data, as well. Companies wanted to control who ("only people who paid") could access media, but still have it be exposed and available.

Whenever I think of access control as a technology problem, instead of a personnel issue, I think about DRM and how badly it has worked; other than straightforward approaches such as controlling who gets to databases, access control systems would have to succeed where DRM has failed. The question we are really asking is "Can we have our data widely exposed, but still safe?" That sounds, to me, a lot like "Can I have my cake, and eat it too?" The only answer that works in the real world is "Pick one."

Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at www.ranum.com.