

Fall, 2007
Vol.11, No.3

acuta

Journal

of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education



This Issue: Legislative and Regulatory Issues

Roles and Regulations—Taking Back Control of the Network

Sean Convery
Identity Engines

As recently as 10 years ago, we had it easy: Users stayed put at desktop machines, IP addresses never changed, and IT wasn't on any lawmaker's agenda. Solutions focused on the threats of the time, which, compared with today, weren't many. But now technologies and threats are changing so fast that it's hard to keep up. We can no longer count on a fixed IP address or even on a single device for a given user. We all want network access from the increasingly large pool of devices and access methods, and this has dramatically complicated the security task.

If mobility and increasing device sophistication weren't enough, lawmakers have jumped headfirst into the fray with a variety of regulations that put even more pressure on IT from a compliance perspective. When TCP/IP, IPsec, SSL, NAC, RADIUS, and 802.1X go head-to-head with FERPA, DMCA, CALEA, PCI, and HIPAA, who wins? At this point, no one, because the regulations don't answer the fundamental question of what technologies to use to satisfy them. As a result, organizations must digest and interpret the daunting regulations themselves, reconcile the requirements with the current IT infrastructure, then try to plug the holes without excessive costs—not a formula for success.

While the task of protecting networks and satisfying regulatory requirements may seem overwhelming to even the most senior administrators

today, there is a technology that can be brought to bear in a common-sense way to both protect the network and improve regulatory compliance. The technology isn't really new either. Back in the 1990s it started life as authentication, authorization, and accounting, or AAA, and today's moniker is role-based access control, or RBAC.

Originally used to authenticate dial-up modem users and remote-access VPN clients, AAA's main purpose was to check a user's credentials to validate that the user should be granted the same access as those users "in the building." Users in the building were given full access by virtue of their physical location. All AAA did was give network managers a way to verify that remote users should be treated the same way. But mobility hasn't stopped with remote access.

Now there are wireless networks and new mobile devices, and validating identity is more important than ever. Combine that with the rise of multiple types of users on the network—faculty, staff, students, visiting sports teams, parents, guest researchers, and temporary contractors—and we've got a much more complicated problem. It is now less about proving someone should be treated like those in the building, and more about figuring out which group of people in the building the user should be treated like.

That's where RBAC comes in. RBAC is a superset of network access control

(NAC). While NAC is focused on device health, RBAC is focused on the device itself, the device health, and most importantly the user. It supports multiple network types and multiple groups of users. And the more types of network access and groups of users an organization authenticates, the more beneficial RBAC becomes.

RBAC in its current incarnation is made possible by 802.1X, a new authentication technique focused on the LAN. 802.1X has given network managers a way to authenticate wired and wireless LAN connections in addition to the remote VPN connections they've always authenticated. This is useful in a regulated network because network managers can provide a centralized audit log of all network access. Want to know every administrator that logged in with student record access over the last 90 days? With RBAC, it's all in a day's work. Organizations can now have a single solution that can ensure that devices on the network are healthy.

RBAC can also report on who is on the network and what they've been given access to, regardless of access method or device type. This broad capability also has relevance as a compliance mechanism for many recent government regulations, for example, the Communications Assistance for Law Enforcement Act (CALEA) or the payment card industry compliance standards. An RBAC solution based on 802.1X is the single most effective way to authenticate users and ensure compliance with this regulation.

RBAC in Action

The Southern University Law Center (SULC), located in Baton Rouge,

Louisiana, provides exceptional legal training to a diverse student body and gives educational opportunities to underrepresented racial, ethnic, and economic groups. The institution's IT group faced a complex set of requirements for managing network access for the 100 faculty and staff, 500 students, plus campus administration. The requirements included unrestricted access to the Internet, remote access to the SULC network, multimedia classrooms with full distance-learning capabilities, and simple connectivity for the students. The IT staff of just three full-time employees was also responsible for training and IT support.

As a 100 percent wireless campus, SULC recognized the need for a fully authenticated and encrypted wireless network. The solution needed to support full mobility for laptops (between classrooms and the library, for example) and provide students and faculty—and only students and faculty—with secure access to student information services and to the subscription-based WestLaw and Lexis-Nexis legal search databases.

SULC opted for an RBAC solution that allows the university to maintain a secure, authenticated network and ensure compliance with SULC's network access policies. The solution:

- Enables end-to-end wireless encryption;
- Authenticates each user against SULC constituent groups;
- Provides control over classroom, guest, and library network access;
- Limits wireless access to online course and subscription-based research materials;

- Keeps any work done by students private;
- Prevents students from accessing administrative applications (including transcripts); and
- Keeps student and faculty identity information, as well as tuition payment data, private.

With its RBAC solution, SULC is confident it can ensure data privacy and comply with relevant government regulations, including CALEA.

Until recently, RBAC solutions like SULC's were slow to appear because of the complexity of implementing the 802.1X standard, but today's approaches to 802.1X address the entire rollout, not just the central policy server. When considering RBAC within your own organization, start in a manageable way. Many organizations with mixed wired and wireless networks use their wireless network as the first testing ground for RBAC. They set up just a few roles to begin with: student, faculty, administrator and guest. Just these four roles represent a huge improvement in the capabilities of most networks today and should be considered by any school that seeks to balance the demands of regulations with the evolving security requirements of today's IT infrastructures.

Sean Convery is CTO of Identity Engines. He can be reached at sconvery@idengines.com.

Note: For more information about RBAC in general, check out the NIST RBAC website at <http://csrc.nist.gov/rbac/>. For more information about RBAC and its relation to the network and AAA, check out "Network Authentication, Authorization, and Accounting" In the Internet Protocol Journal Vol. 10 No. 1 and 2 (<http://www.cisco.com/ipj/>).

