Security on Campus

An Interview with Jeffrey I. Schiller
MIT

Those charged with security on campus face many challenges – providing appropriate levels of security, chosing security technology that can be widely deployed in a timely manner, and getting acceptance from ordinary users. Syllabus talked with Jeff Schiller, MIT's network manager and a security architect for the school's Information Technology Architecture Group (ITAG) to gain some insights about the "negative deliverable" – security.

S: What has been the most important security development in higher education over the past five years?

JS: The most important thing is not so much security per se, but the context. Five years ago, personal computers were used, for the most part, for word processing. Now, the Internet and personal computers have become ubiquitous. We don't talk about whether someone has a computer; we ask how many they have. They are common tools, like pens and pencils. We've become a community that is very much computer-focused. And then we have the Internet to tie all of this together. But the same Internet that might tie my computer to my colleagues' computers and to your computer, also might allow my computer to be touched by people who have less than pure motives. So in some sense I think the biggest thing for security in the last five years is the increased vulnerability that we've had because we are so much more connected. Providing security becomes that much more important because we're that much more connected.

S: Discussions about security seem to center around authentication or authorization. Is there a difference between authentication and authorization?

JS: Very much so. Authentication is proving that you are who you claim to be. Authorization is demonstrating that you have a right to do something that you wish to do. In the case of say, looking at a student record, I might have authorization. Where authentication and authorization get tied

together, is that we often grant authorization only to an identified individual. So, for example, if we have a student—John Doe, and I'm their advisor, there will be an authorization list that says Jeff Schiller is authorized to look at the academic records of John Doe. Then, I have to authenticate myself to prove to the system that this is indeed Jeff Schiller. There are also cases when we have authorization separated from authentication. For example, in order to ride the subway, at least here in Massachusetts, I have a token. And you know, the subway system could care less whether I'm John Doe, Jeff Schiller, or Bill Clinton. If I have that token, I get to go on the train. So, authorization can actually happen in the absence of authentication.

S: What kind of authentication is appropriate for campus networks, or for portal security?

JS: Well, it really depends on what information somebody might get access to, or be able to modify. For example, if I indicate to my portal what class year I'm in so that it could show me what courses were relevant to me, or what parties I might want to attend, then a rudimentary level of authentication would probably be quite acceptable. On the other hand, if the portal allowed me to look at my grades, modify my term address, or update my biographical information, we would have a situation where if our authentication weren't strong, we'd risk one student claiming to be another student, for whatever reason, and creating an embarrassing situation.

S: Are there guidelines or universally accepted conventions for the types of security systems one might deploy on campus?

JS: When it comes to student records, we do have laws like the Family Educational Rights and Privacy Act (FERPA) that basically states that schools really do have to make an effort to protect student records. An interesting question is, when you do deal with sensitive records, what is really good enough for authentication? There is no rule that says "thou shalt use digital certificates." There is no rule that says "thou shalt use a user name and password." There's not even a rule that says that when you send a user name and password over the network you should encrypt it. But I can certainly tell you at many universities people are running what we call sniffers—eavesdropping devices—on the network, and if you send a password over the network without encrypting it, it will be stolen. So we have to make a tradeoff between perfect security versus the cost of providing it and the convenience, or lack thereof, of using it. But

the very first thing you've got to look at is the level of sensitivity that's associated with granting access.

S: So, on a campus, who makes the decisions about levels of security?

JS: I think one of the things you run in to when you get in to higher education is decentralization. For example, the CIO of the university, or the head of the IS department, or the associate provost can set policies on how central administration handles data. But there's always the challenge of what happens in individual departments, particularly when you're dealing with student records. After all, grades are ultimately collated by faculty at the end of the term. Before they turn that information over to the registrar, they more or less get to control its level of security. I think one of the challenges we face in the university is faculty members using very insecure technology to deal with student records. A classic example is faculty members e-mailing grades around without the e-mail being protected in any really strong way. So I think that at the campus level, we try to have a CIO who would like to establish security policies, but actually getting the policies enforced in a decentralized environment is very, very difficult.

S: Then is security hard to sell on campus?

JS: I think it's hard to sell because many people just don't get it. I talk to people and say, "Aren't you worried about somebody reading that e-mail?" And they say, "Who would read my e-mail?" Or, people run computers without a password on them, and say, "Who would want to use my computer?" So you have to start from the beginning, saying that the reason that someone might want to use your computer is so they can then use it to launch attacks on somebody else and it would look like you did it. So one of the things we have to do for security is not only what I would call technical security—putting in the technology and all that—but there's also a huge educational component that has to go with it.

S: On most campuses, do you expect that you can actually integrate all the technology to work together to be secure? Take for example, e-mail…are the various systems going to be standardized enough to work together?

JS: They say standards are wonderful. Everybody should have one. E-mail turns out to be one of the hardest and most problematic cases. There are several standards out there for how to do, for example, encrypted e-mail. The implementations are green. They don't always talk to each other. But even worse than that is that the ease of use of the clients is not yet good

enough to encourage most people to use the security features. Right now the technology requires the user to be a lot more educated on the nuances—you have to understand public key cryptography and have a certificate, or a key pair—and all these are terms that people just aren't familiar with. What people want is a check box that says, "Make this secure," and we have not yet gotten the technology down to that level.

S: Are there any good, common, simple security measures?

JS: One of the things that has helped us improve security is Web-based applications. When they first came out with their browser, Netscape really jumped on the problem of how to provide a secure way to get from a browser to a server. And of course you know that today as SSL, the ubiquitous https and that little lock icon. And so in essence, Web browsers with built-in support for SSL gave us the generic security-capable desktop client. So I can build a secure application and not have to worry about getting a program out to everybody's desktop. If they use their browser, we're okay.

S: What's a good example of that?

JS: One of the things I would like to see is faculty filling out a Web form put up by the registrar's office and entering the data directly into a Web server through a secure channel—then, that data is really never exposed, and it is not left laying around on hard drives. Web-based technology gives us a real opportunity to integrate systems.

S: So you feel that the Web security is fine?

JS: Certainly. But you know, the devil is in the details. With SSL, which is a standard and widely deployed, it is certainly the case that when you enter, for example, your credit card information into a secure page and it is sent over the network, no one is going to be in a position to steal it; however, once it gets onto the server at the bookstore, or wherever it may go, the question becomes how well protected that server is. I become nervous when I see a small shop that isn't very security-savvy set up what they think is a secure Web site—well yes, in transit it's secure, but do they really understand security at their database level? If you're a very large organization and your business depends on the Web, then you're motivated to make it secure. and it probably will be. But there's probably some gray area in between those two extremes that a lot of schools would fall into, and their security could probably be improved.

S: Then there could be problems on either end of a transaction, even when a secure, standard technology is being used between the two sides?

JS: Yes, and another thing to remember is that security is a negative deliverable. You don't know when you have it. You only know when you've lost it. If I have to integrate two systems together, and I don't get my standards right for the actual data formats, then the systems don't work and that's obvious to me and I have to fix it. But if I have two systems talking to each other, but in a totally insecure way, the technology still works. The application still runs. Everything works like it should until somebody steals the data.

S: What's going to motivate campuses to provide really good security?

JS: When I sit down in conversation with other people in higher education, the concern over student records eventually is traced to the FERPA Act, also known as the Buckley amendment, and so there's a feeling that in order to meet the legislation, we have to be providing the required level of service. But some universities also have a very strong sense of privacy and don't want the privacy of their students compromised; therefore they don't want student records compromised. I can't say that it's universally true that there's belief in the privacy of students, but certainly it's there in many cases. There's also the fear of loss of reputation. Nobody in the IT business wants to be the CIO of the university that gets written up in the *New York Times* because they had some breach of privacy.

S: So if reputation is a factor, should good security be one of a potential student's criteria when selecting a college?

JS: Well, let me quote Tom Peters. He said that no one chooses a university based on the quality of its administration. And I don't think anybody has ever said to me, "Jeff, I'm thinking about going to MIT, but I'm really concerned about the security of your administrative systems and whether they're good enough." It just doesn't come up.

S: Are biometrics going to be used soon for normal security in higher education environments?

JS: Biometrics, I think, are farther out than most people think they are. For example, one of the primary benefits to the user of a biometric authentication is that you don't have present anything but your body. But the way we see a lot of biometric systems deployed, you actually have to have an ID card *and* you have to look at the iris scanner or use the

fingerprint reader. Keep in mind that today, we have a lot of people just entering a user name and a password over a secure Web login, and that's working just fine in higher education. If you say that now, you also have to have a card, never mind the biometric, that's just going to be a step up in inconvenience. I think eventually the push for biometrics in higher education will be one to improve user convenience, which is to say not to require you to memorize a password or carry a card.

By the way, here's a little story. I was talking to a vendor of a fingerprint reader that was being designed for use on cash machines, and I said to the him, "You know, I don't really want it to be the case that the only thing you need to get in to my bank account is to have my finger." He got just what I meant and said, "Oh don't worry. The reader can tell whether the finger is alive or dead." I responded, "That's not the point! My finger is much more valuable to me than anything in my bank account." But then he said, "Well, you don't have to worry because I've explained it to you, so now you know that it won't do any good—so you're safe." I protested, "No, that's not true. You don't have to convince me that a dead finger doesn't work. You've got to convince the crackhead whose going try to cut my finger off!"

S: What's going to be important for security in the future, say, in the next five years?

JS: The most important question is about how we can get security technology more broadly defined, deployed, and accepted. Part of the answer is that we've got to make the security technology that we develop be user friendly and incrementally deployable. And what I mean by incrementally deployable is that we have to be able to roll it out on a per student or per department basis, or maybe on a per school basis, but we can't create a security technology that nobody has one day, and the next day, everybody has to have all at once. We call that a "flag day," and you just can't do that. So we've got to come up with strategies to get security technology incrementally deployed. And it's got to be cost effective. It's hard enough to get students, administrators, and faculty to understand the value of security. If you assign a very high cost to it, they're just going to walk away. So we've got to come up with easy to use, cost effective, and incrementally deployable technologies. That's our challenge.