Encryption and Access Authorization Issues at The University of Alabama

Report to Faculty Senate by Bill Keel, A&S Senator
11-15-00

This summarizes a briefing conducted by Maurice Mitchell of the Seebeck Computer Center on 15 November, 2000, dealing with the coming involvement of encryption and access authorization in a wide range of university business.

Present were representative from student services, University counsel, Financial Aid, and the registrar's office. Bill Keel represented the Faculty Senate and prepared these notes.

We will be doing more and more business digitally as time goes on, not only for our own speed and efficiency but because there are federal mandates to do business electronically. The specific legal drivers here are Government Paperwork Elimination Act (requires contractors of the federal government to implement digital signatures and paperless transactions, now being phased in over 3 years with some agencies well along). This includes administration of student loans. The main time savings is that "wet" signatures are eliminated in favor of secure digital signatures. This is supported by the Federal Digital Signatures Act.

Health Insurance Portability and Accountability Act. This suggests the use of digital signatures for data access.

Family Educational Rights and Privacy Act. This requires the existence of digital credentials for access and privacy protection in, for example, student records.

The NSF's "Fastlane" submission system and the NASA Space Telescope Science Institute's electronic grant management system are existing steps in this
direction.

There are two major issues in dealing with secure digital transactions such as records access and authenticating a sender's identity, which together are supported institutionally by a Public-Key Infrastructure (buzzword PKI):

Encryption: the de facto standard uses pairs of keys, one public and one private to the individual and requiring password access on each use. Encryption and decryption can go in either direction with the same keys, which can be of arbitrary length (up to 1024 bits are currently in use, which, it is claimed, would require some months for the three-letter agencies that we aren't supposed to know about to crack). Some versions of this scheme (such as PGP) are already in scattered use here. In many cases, an employer can keep a copy of the private key "in escrow" with a third party for use in specified circumstances (use your imagination) - but note as well that anyone could use an additional set of keys from some other account, say with a commercial ISP, for any items that under no circumstances should be read by the higher-ups. At any rate, the public key is in a publicly accessible directory (the PK in PKI).

Certification: this is accomplished by a file ("certificate") attesting that you are who you log on as, with authenticity established by connection to a neutral and trusted third party and matching encrypted information. We currently have a contract with one such broker, Digital Signatures Trust, to provide certification as we need it (there is a small cost per certificate). Since individual certificates generally expire within 2 months, there is not a major issue if the identity of the certificate

authority changes due to mergers or other business changes.

Certificates can provide very flexible interaction with a server. One likely example is student records, with everyone able to access directory information, faculty able to access a bit more, but only a few people (for example in the registrar's office) having complete access to the information (with parallels in health services, probably getting even more complicated).

Both encryption and certification can act seamlessly within browser programs, such as mailers and retrieval forms. Certification can work either with or without encryption (and an individual certificate can specify whether it is valid for either or both cases).

One example in the works is the library's "shibboleth" service. The Amelia system will deliver information to any machine in the .ua.edu domain. Shibboleth (see the Book of Judges, chapter 12, verse 6 for the origin of the name) will use digital certificates to allow any authorized UA student, faculty, or staff to access the library information, even if from a machine or proxy outside the UA domain.

Seebeck is soliciting thoughts from the various campus groups which will be affected, with the goal of having the technical support driven by the needs rather than vice versa (doesn't this violate some historical university policy?). A group there has been running a "toy" certification system to get experience with them.

Of all this, what will matter for faculty?

- We will eventually need digital certificates (probably multiple ones) for various purposes, such as access to student schedule or records information. They may also be needed for management of federal contracts and grants (though the real use there may be more in administration than for the faculty).
- More of us will be encrypting email, as more and more transactions occur in this way. Indeed, we should probably be moving faster here, since spoofing an email address is not particularly difficult and there have already been a few horror stories when students fake a professor's address and distribute messages that can cause all manner of trouble.
- Digital certificates will probably replace student ID and PIN for accessing university services, since this provides what is becoming a universally supported access-control and authentication protocol. This should allow us to do some things that would otherwise violate privacy restrictions - for example, making assignment or current average grades available electronically with significant assurance against unauthorized access.
- Compatibility of new software with certificates may be a purchasing issue. The current standard is X.509 U3, for the really curious.