George Mason University provides students access to academic records (grades, transcripts, financial aid, admissions, degree analysis, personal data) and course schedules through WWW-accessible servers containing an extract (copy) of the data from the official records. The extracts are updated nightly or weekly, depending on the application. Access is granted with authentication (PIN number).

We plan to expand intranet operations to support other common administrative uses, such as grade reporting by faculty, in the near future.

Jerry H. Jenkins, Executive Director
University Computing and Information Systems
jjenkins@wpgate.gmu.edu

The University of Michigan uses Kerberos as its network-based authentication system. Approximately 70,000 active users access many Kerberos-enabled applications. Some uses include: students accessing grade and schedule information, e-mail, file systems, directory services, printing, workstation login, Web services, and dial-in access. Kerberos allows us to administer a single security domain and allow single sign-on to our distributed computing services.

Our plans include establishing a public key infrastructure, migrating our Kerberos environment to the OSF/DCE version of Kerberos, having wider use of smart cards to enhance Kerberos authentication, and establishing a more comprehensive single sign-on environment to integrate different security domains.

Ted Hanss, Director
Human and Technical Resource Management
ted.hanss@umich.edu

The University of Virginia is currently in the process of investigating, for probable implementation, Kerberos security; DCE has been installed and is currently in production, but used by few applications. KERBEROS is scheduled for production this calendar year. A few of our users (estimate less than 2 percent) are using PGP on their own. One large mainframe application, Accounts Payable, uses the CICS four-character terminal ID for those mainframe clients requiring update access (dial-in access is limited to browse/read only). We have also implemented SecureID cards on some of our critical mainframe applications.

Richard A. Patterson, Assistant Managing Director
for Security and Capacity Planning
rap@virginia.edu

At the University of Oregon, we offer about ten courses for our undergraduates in physics and astronomy via networked curriculum. The use of PGP and/or Kerberos is really overkill for the purposes of user authentication. A simple fix makes use of the .htaccess file in which the domain name for access is specified. Thus, for some classes that we don’t want the outside world to see, we restrict access to only machines with domain name uoregon.edu. This seems to work fine for student access.

Very recently, we have implemented a PIN system for use with internal departmental voting procedures. The PIN is entered into a forms-based Web page which is processed by a perl script. To date, this electronic voting/authentication procedure is robust and a real time saver.

Gregory D. Bothun, Professor, Department of Physics
nats@moo2.uoregon.edu

At the University of Colorado-Boulder, we currently use some primitive tools such as domain name restrictions and unencrypted table look-up of student PIN numbers. Library databases are restricted by library card identification. Administrative systems use cleartext passwords and simple authorization schemes. There is no encryption of e-mail widely used. Some Web applications use SSL, and Kerberos is used on all central systems to protect system passwords.

We are planning to move to a uniform security environment built on DCE, with privacy of communications addressed by X.509 certificates. We will use DCE for both authentication and authorization, intending to link the authorization into both applications and databases. DCE will be used to manage the X.509 processing. Time frame: within a year.

Kenneth J. Klingenstein, Director of Computing and Network Services
ken.klingenstein@colorado.edu

The University of Memphis currently relies on host-based user authentication systems in addition to a directory-based system for dial-in authorization and access control. In the coming academic year we will implement Kerberos-based authentication and begin converting hosts and dial-in systems to Kerberos under a program called “Universal UserIDs.” This will be among the first steps toward implementing a comprehensive distributed computing infrastructure.

Also in the coming academic year we intend to move to a common e-mail system. One of its specifications is (eventual) support of standards-based authentication, non-repudiation, and confidentiality mechanisms. Although it is one tech-
nology with these attributes, PGP per se will not be required.

I am currently following developments regarding LDAP (Lightweight Directory Access Protocol) with great interest. It appears to be the first approach to solving the unified directory problem that has the technical potential, the weight of standards bodies, and the industry momentum needed to be successful. My “holy grail” is to integrate our various host and application authentication and access control systems with a common directory. Perhaps that will be LDAP.

Tom Barton
Director, Network Services
t-barton@memphis.edu

At Indiana University Bloomington, PGP-encrypted messages play a role in our “distributed account generation system,” which annually manages the creation of tens of thousands of user accounts on a multitude of time-shared systems across the campus. The central generation system encrypts user account requests (including sensitive information such as passwords) for immediate automated processing on the target system.

Aside from using Kerberos in a few traditional ways, we also use it as a back-end authentication service for some WWW-based applications (such as the aforementioned account generation system). Users enter their Kerberos principal name and password into a form (preferably over an SSL-secured connection), and the CGI application verifies this against the Kerberos database. Although this is not at all what Kerberos was designed for, it easily and pragmatically solves a major problem for us: it allows multiple Web servers on campus to authenticate a population of some 60,000 users.

Larry J. Hughes, Jr.
Principal Software Engineer
hughes@indiana.edu

Cornell is using Kerberos for authentication. Although not all of our client applications are Kerberized, we are moving towards that goal. One of our biggest concerns is network security. All of our residence halls are wired, and network sniffing has now become a serious problem. We had several reports of passwords stolen in this manner. We try to encourage the use of Kerberized passwords where this is an option (e.g., Eudora) in order to prevent this. Our Kerberos database also provides us with one single repository for passwords, and all of our distributed servers can authenticate users without maintaining passwords locally. We are able to provide a wide range of services that users can access with their single netID and password.

For the future, we are looking at PGP (or something similar) to provide secure e-mail and signature verification. We hope that digital signatures will reduce the amount of prank e-mail. Encryption of messages will provide protection in cases where confidential e-mail is misdirected or where the network is not secure.

Barbara Skoblick
Security Officer
Office of Information Technologies
bs10@cornell.edu

All students, faculty, and staff at Clemson University use NetWare Directory Service (NDS) version 4.1 for authentication. Authentication clients were written for the mainframe (MVS/RACF), the primary e-mail server (UNIX/POP), and NT World Wide Web servers. The authentication server application NLM runs on multiple NDS servers for fail-over and load balancing. Passwords may be changed from mainframe applications as well as with standard Novell commands. Novell “intruder detection” and password rules are implemented. Future enhancements will include “single-point” network login and password changes from other clients.

Dave Bullard
Director of Computer Systems
dave@clemson.edu

At Université Laval, Quebec City, Quebec, Canada, we are not yet using Kerberos or any other similar tool. PGP is used on an individual basis by those few persons who know what it is, when they think it is absolutely necessary. We don’t foresee a big use of it until it is friendly and fully integrated within popular e-mail tools like Eudora running on Wintel and Macintosh.

About network and information access, the staff (faculty and administrative) is authenticated by local managers when they request access codes and passwords.

For the students, we are still using a paper contract that they have to sign to activate their access code and its password, after they have registered on a server. For authentication, we ask them to attach a filled-out registration form that we are sure they are the only ones to receive. We hope to be able to change that when there can be a secret and secure PIN for each student record.

J. M. Poulin
Directeur adjoint (Associate Director)
Computers and Telecommunications Services
jmpoulin@sit.ulaval.ca
With an overall design goal of “reusing existing resources whenever possible,” security schemes used for touch-tone registration were enlisted at the University of Delaware to provide similar protection to the Intranet applications. ID and PIN (Personal Identification Number) authentication was already known and in use by students and staff for many touch-tone applications. Additionally, PIN-based authorization tables were also in place for existing administrative systems.

In order to protect the authentication information as well as the private records of students, faculty, and staff, Netscape’s Secure Socket Layer (SSL) encryption protocol was adopted. This protocol was selected because of the popularity and success of the Netscape’s Web browser and because its socket-level encryption is ideal for supporting the re-use of existing authentication and authorization schemes.

SSL uses encryption to enhance user privacy by providing a communications channel that is secure against eavesdropping. When an SSL-aware browser connects to an SSL-secured server, all information passing between browser and server is fully encrypted. This secure data circuit allows existing authentication and authorization information to be safely exchanged on the network.

Re-using existing authentication schemes enabled Delaware to quickly and inexpensively provide secured access to all administrative systems.

Carl Jacobson
Director, MIS
carlj@udel.edu

UC Davis has two Kerberos servers for authentication. A directory service based upon a relational database model of all University affiliates has been created to use SQL queries to quickly populate the Kerberos server as the service is requested. This service is available to all departmental machines that wish to use Kerberos for security. A Kerberos password is required for access to student information through the World Wide Web.

Access controls for the Student Information System have been enhanced with the Enigma Logic one-time password system. We have contracted with Cybersafe, a leading supplier of Kerberos software, to integrate the use of the Enigma Logic password system with Kerberos authentication. This configuration will be available in the Summer of 1996 for all UNIX systems at UC Davis.

We are also using RSA certificates in limited applications and have done some work with PGP and electronic mail. However we do not have any plans for widespread use of these systems in the next six months.

Joan Gargano
Distributed Computing Analysis and Support
jcgargano@ucdavis.edu

Computer system security is recognized as a high priority at UC Davis. Information Technology has two staff members acting as Security Coordinators, developing and implementing policy in coordination with campus departments, assisting in the resolution of security problems, and developing security systems for the distributed computing environment.