

# DESCRIPTIONS

## **A. Campus Standards for Authorization (rel)**

With the work started last year on Central Authentication, it is important to move forward with a campus cooperative model that handles both authentication and authorization. This model should be able to support loading of directories (ie: Active Directory and OpenLDAP) with attributes designed for people from central sources. These directories can be used to determine authn for machine/service access. An implementation guideline should also be developed.

## **B. Providing servers to aid in security scanning (ktr)**

Provide at our expense a server on our subnet, controlled by the security officer, to aid in monitoring and detection of security issues.

## **C. Enhance MTUNET (jamyles)**

Provide a fully functional portal that provides better input facilities and works with any standard browser. This should allow modification of pre-orders before they are converted to work orders. Also provide a data warehouse to system administrators with all relevant MTUNet data. This would be a table or collection of tables in an SQL database, and would allow system administrators to use their own tools to query data on their hosts in MTUNet. Finally, provide complete documentation for MTUNet, including theory of operation and user interface documentation.

## **D. Campus Instant Messaging Service (jamyles)**

This would be a messaging service for use by students, faculty, and staff campus-wide. This service should be based on a standards-compliant software such as Jabber, and should use the ISO system for authentication. IM clients for all common platforms should be tested and supported, including native and web-based clients. Other features that should be included are conferencing, privacy features, and support for group-managed role accounts.

## **E. Central management of software licenses/contracts (jamyles)**

Centrally manage software licenses and contracts. This includes handling contract and license negotiation and renewal, legal issues, and coordinating group software purchases.

## **F. IT service monitoring and reporting (jamyles)**

As more and more critical services are provided by IT, system administrators need better monitoring and reporting tools for those services. Right now, the IT hotline and status web page are not always up-to-date, and don't provide real-time status. Maybe making Nagios and other monitoring systems available to system administrators would solve this problem.

### **G. Web replacement for local news groups (jpbialas)**

This has already been done with the phpbb project.

### **H. Support for bulk mass email (klfrazier)**

Currently ACS is writing and supporting a process to send bulk text emails through banner. We would like this system or a new system to be created that can also handle mass HTML emails. We would also like policies for its use. Several departments have been waiting for this functionality/policies since the email committee was formed and would like this problem addressed as soon as possible.

### **I. Interim Wireless Policy (rel)**

A small working group should be established to develop an interim wireless policy that is reviewed by the CAC. This policy would provide some direction in the deployment of wireless networks on campus in a cooperative fashion.

### **J. Network clocks (rel)**

Someone had to support the clocks. Guess it was my time.

### **K. Programatic API to NID (tj)**

I'm interested in an interface to the NID (or whatever incarnation the NID is in) to facilitate automation in accounting and account-related tasks. SQL schema and queries, or Perl modules would be the first choices. This API would allow the creation of a primary userid/uuid pair (the 'login' table right now), the management of active account lists (currently the 'active' table'), and the creation and management of email aliases ('alias' and 'alias\_job' tables). The current NID programs work okay, but do not lend themselves to programmed automation.

### **L. Ability to run queries on card access system (who has access to which doors) (rel)**

Some basic tools to review what people have access to doors that are of concern to administrators who request access for them. This would allow for the self auditing of access to labs.

**M. Capability for Instructors to access instructional materials via network regardless of location. (pmraymon/kraus)**

An issue that is often brought to our attention in ETS is the need for instructors/students to be able to access their H: drives from the lecture halls and classrooms. Currently there are several ways that this problem is addressed:

- a: Citrix client/server
- b: Windows Remote desktop
- c: COE Domain

These solutions work well in certain instances. To provide a more complete solution, we'd like to see a plan to implement 802.1x on classroom and lecture hall network ports to control port access and VLAN assignment for computers that may be brought in by lecturers and presenters.

An intermediate solution should include providing a centralized DHCP server and system administrator ability to easily add/delete/change DHCP information for lecture hall network connections.

**N. Centralized Reclamation and Disposal of IT equipment. (pmraymon)**

Old PCs could be refurbished or parted. Systems and parts could be resold inter-departmentally or to the public through a storefront or via eBay. Obsolete and defective electronics could be collected and sold for precious metal recovery. Ideally, income from the sales would offset the cost of the operation and disposal of hazardous wastes.

**O. Guest access to university network services. (kraus)**

Create the ability to grant university-sponsored guests access to network resources including ISO login/password, Rovernet or other network access, central email, etc. on a time-limited basis.