

04 February 2004

## **Fact Sheet**

### Summary of Changes in The College of Engineering's Data Communications and Computing Environment

The College's Communications and Computing environment will be moving from an open Internet access to one that is closed. This means that open unfettered access to the College's network, services and computing environment will cease. For most people, there will be little or no noticeable effect on access to College servers and data. Individuals that access the College's resources by dial-in or off-campus ISP suppliers will still have access to network and services by installing a Virtual Private Network (VPN) client on their remote computer and connecting to the College's VPN server. The VPN server provides a tunnel into the College network and uses data encryption to protect and secure information between College resources and the remote system.

Aside from having to use a VPN connection for remote access to the College's communications and computing resources, there are a number of procedural and policy changes that will go into affect after this semester and into the summer months. Most notably, all the College twenty-four standalone facilities will have operational hardware firewalls systems with built-in local VPN services. The firewalls will close down the networking and computing resources in buildings and prevent unauthorized access to services and data; the net effect will be to prevent hacker access to computing resources. Unfortunately, nothing the College or University does will prevent or mitigate the effects of hacker activities originating within a building or full-scale Denial of Service (DOS) attacks that slow down all Internet traffic.

Firewalls accomplish their network protection function by applying rule-sets and closing ports actively used by hackers to exploit system vulnerabilities. Within the College and among buildings, the initial rule set allows complete and apparent open access to the communications and computing environment. Furthermore, faculty and staff will have outgoing access to the Internet. However, unfettered incoming access from non-College buildings or off-campus sites will be denied; requests for server or services access exceptions to this policy will be evaluated and authorized/declined on case-by-case bases.

Although the methods by which faculty and staff access the College's network from off-campus, one constant remains: faculty and staff will continue to have access to all College resources. Everyone accessing College resources will have the same access rights then as now; the added advantage will be that logins and data communications will be encrypted and secure.

- Secure web mail access will still be available by logging into <https://mail.engr.psu.edu/exchange>

- Internet access through a service provider (such as Adelphia) will still be available; however, faculty and staff using this access approach will need to install a secure VPN client on their home or portable computing device.
- Dial-in access via the University's modem pool will still function; however, users will also be required to use the VPN client and log onto the network using their University Access account.
- For those faculty and staff that prefer to simply transfer files, ECS has established a Secure File Transfer Protocol (sFTP) site. Users choosing to use this approach rather than logging into the VPN may access this server for secure file transfer. This server provides secure encrypted data transfer access to any shares on any College server's shares to which the user is authorized access.

Another major paradigm shift will occur in Wireless networking procedures; changes in network accessibility through wireless access points have become necessary for numerous reasons. Many access points are deployed throughout all College buildings because of the conveniences they offer and their ease of deployment. Unfortunately, the majority of the deployed access points operate in an insecure mode or with minimal and easily compromised security. The insecurity of these wireless access points opens the College's network to both theft of services and intellectual property espionage.

Under the new College security model, all wireless access points are required to be registered with ECS. The network connectivity afforded by these access points will be achievable by user employing the VPN client on their computer. Rogue access points remaining on the network, not registered or brought on-line after the firewalls are fully operational will have their network connectivity disabled.

The availability of wireless computing to faculty, staff and students will increase under this new security model. ECS personnel will be deploying access points within the College buildings and are working with ITS personnel to make seamless wireless computing available across campus. This is a project in progress; deployments will occur as implementation procedures and cost models are better defined.

Within the College, and at any one time, there are approximately one hundred and twenty-five (125) ad hoc email servers operating; this number includes mail services operational on individual desktop systems, laboratory servers and departmental servers. One of the initial rules being activated on the building firewalls will block port 25 access to Simple Mail Transfer Protocol (SMTP) email services. Anyone believing that they must operate an email server will be required to submit a request for inbound relaying of emails through the College's email gateways. One may apply for inbound relaying by emailing [firewalls@engr.psu.edu](mailto:firewalls@engr.psu.edu) or by filling in the required information on the web site located at [http://www.engr.psu.edu/firewall\\_exceptions](http://www.engr.psu.edu/firewall_exceptions).

Establishing inbound email gateways will expand the ability of ECS to provide an additional service for easy identification, marking and user client rerouting of SPAM. Next to viruses, SPAM is the single most annoying category of email messages on the Internet today. The problem with SPAM filtering, as the University found out, is that it's not perfect and valid emails will be incorrectly classified as SPAM. Until better commercial detection and filtering applications become available, ECS' approach will be to have the email gateways will append the following to the subject line "\*\*\*\* SPAM \*\*\*\*".

A user's email client can be set up to detect the appended identifier and automatically redirect all such classified messages to a folder destination of their choosing. On a schedule of their choosing, users will need to review messages in the designated folder and decide which are important and which can be discarded. The purpose of this approach is to ensure that no one loses incorrectly classified important email messages from mailing lists to which they subscribe or receive from colleagues. For example, the following is similar to an email a faculty member identified as lost when run through the ITS SPAM filter: an email to graduate students with a subject line of "Test File", a single line message such as "Here is a test file for you to run and evaluate the results, and an attachment such as "test.exe" never reached its intended recipients.

So, regardless of the final destination of email being directed to an approved server, all incoming email will be processed through a redundant pair of College email gateways. In addition to acting as an email gateway, these servers will provide commercial SPAM recognition algorithms that mail server administrators may choose to use to detect potential SPAM emails. On a scale of 1–10, any incoming email that is identified as a level 3.5 or higher falls into the SPAM category. The server administrator can then choose to place these so designated emails into a special SPAM folder for later screening or perform any other desired actions on the emails.

Under no circumstances will the College's email gateway or email server management team automatically delete emails identified as SPAM; emails so designated must be automatically redirected to an appropriate location by the recipient, a rather simple task when an email has the new designator appended to the subject line. This approach to dealing with SPAM is absolutely necessary at this time because there are no SPAM detection packages available today that have the ability to quantify an email as SPAM with one hundred percent accuracy.

As pervasive as active email servers are in the College, there are also a significant number of individual, research and department web servers operating in the College. As seen in the past, these systems are also a hacker's delight and unless they are properly administered and updated, these systems will be compromised. In a manner similar to email servers, individuals or organizations having a valid need to operate and manage a web server will be accommodated in this new networking paradigm. One may apply for a web server firewall exception by emailing [firewalls@engr.psu.edu](mailto:firewalls@engr.psu.edu) or by filling in the required information on the web site located at [http://www.engr.psu.edu/firewall\\_exceptions](http://www.engr.psu.edu/firewall_exceptions).

All requests for exceptions to the College's new policies will be addressed by a Firewall Exception Review Committee. This committee consists of the following individuals:

Chairperson: Dr. Gary Gray — ESM  
Dr. Francesco Costanzo -- ESM  
Dr. Jeffery Mayer — EE  
Tom Long — ECS  
Joe Lanager — ECS  
Matthew Lindenberg -- MNE  
Scott Heckman — IE

Once alerted that a request for Firewall Policy exception has been received, Committee members will make every effort to review and render a decision within 72 hours, weekends excluded.

In summary, the changing Internet environment coupled with numerous requests from faculty is resulting in a major networking philosophy in the College. The feature richness and functionality of the Internet and data communications and computing will exist in this new environment; however, the mechanism, implementations, policies and procedures relating to the implementation are changing.

**Implementation Scheduling:**

- Installation and initial operational testing.... 1 December 2003 – 16 January 2004
- Firewall rules configurations and VPN services activation.... 19 January – 28 February
- Activation of firewall rules for testing .... 8 March
- Permanent firewall rules activation ... on or about 1 June

Questions regarding this document may be directed to any member of the ECS Networking and Support personnel.