

Information Security Issues in the College of Arts and Sciences

Overview

Protection of personal information on USC networks and computers is a major concern and must be addressed at all institutional levels. During the next several months, we will take steps in the College of Arts and Sciences to increase protection of confidential information. Major emphasis will cover procedures and policies that establish technical standards and increase personal awareness about information security.

Technical Documentation and Standards

Information security breaches can be minimized by focusing on three technical areas.

Our first line of defense is the university firewall that restricts access from the Internet to computers located on campus. I have initiated a project with UTS Network Services to document and evaluate all firewall settings for all CAS systems. This documentation identifies all computers that are open to direct scans and attacks from the Internet. By working with technical staff in each department, outdated firewall rules will be deleted. This updated documentation also will provide UTS with information that will decrease processing load on UTS firewall equipment.

Firewall documentation will lead toward implementation of a next technical step-- identifying and establishing standards for all critical servers and network devices that contain sensitive information or are open to the Internet. Well-known exploits for file, web, email, and database servers are published and used to gain unauthorized access to vulnerable systems. I will work with college and department technical staff to insure that all CAS servers and network devices are properly configured and updated on a regular schedule. Although a properly patched system will greatly decrease a possibility of a successful attack from the Internet, it will not completely eliminate the possibility of an intruder gaining access. The goal is to minimize the chances of a security breach by installing security patches as soon as they are available.

As a final step, UTS firewall information and network information collected from local scans will assist in migrating desktop computers and devices from public to private network numbers that are less vulnerable to attacks from the Internet.

Personal Information Security Awareness

Implementing technical policies and procedures can protect critical servers, but technical solutions cannot prevent compromises caused by careless handling of sensitive information. Personal information security awareness must be emphasized as part of an overall solution. For instance, sensitive information should not be stored on removable media. Personal passwords must meet minimum standards and be protected. Precautions must be taken when sending or reading email and opening attachments. Departments or individuals must keep their desktop computers updated with latest security patches and install other utilities that block spyware and other malicious programs.

I'm working with the UTS Information Security department and our CAS technical staff to increase individual information security awareness and set up information channels to provide specific information about security procedures, policies, and announcements. Information channels are a CAS information security web site (<http://security.cas.sc.edu>) and a college security email alias (security@cas.sc.edu).

During a recent Web Managers meeting held in the CAS Research Computing Center, UTS Director of Information Security covered several information security and privacy topics. I will schedule similar sessions with CAS staff and faculty and work with the UTS Information Security staff to establish technical solutions and increase personal security awareness.

A Work in Progress

Although an immediate goal is to set an information security baseline during the next several months, refinements are part of an ongoing process and require participation by all faculty and staff. Given the diversity of the College of Arts and Sciences, the type and degree of participation by department will vary. Communication is important and suggestions from each department are welcome. Send comments or feedback to security@cas.sc.edu.

Philip Moore, Ph.D., phil@sc.edu
Research Computing Center, <http://rcc.cas.sc.edu>
(803) 777-2708