

Network Security

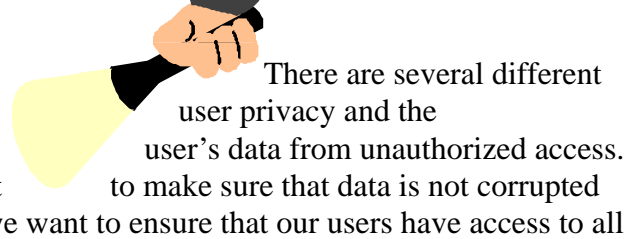
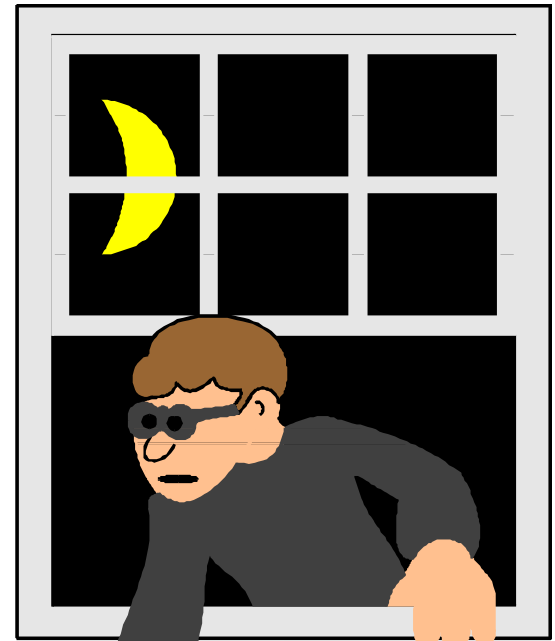
In the “good old days” of computing, when companies had huge IBM mainframes that were kept behind locked doors and accessed only via dumb terminals or by experienced technicians, the issue of security was fairly straightforward. Security was generally achieved by limiting access. In our heavily networked day and age, and with the explosion in size and scope of the Internet, the issue of security has become much more complex.

What exactly is meant by “security?” aspects to consider. One is the issue of confidentiality of data: we want to protect The second issue is data integrity: we want or deleted. A third issue is availability: we want to ensure that our users have access to all of our network services at all times.

What are some common types of security breaches and how do we prevent them from happening? Well, we’ve all heard stories of hackers breaking into bank systems to steal funds electronically or of spies breaking into military systems to obtain military secrets. Much more common, however, are denial of service attacks. Hackers will send an email bomb or flood of ping packets to bring a system down. The recent Melissa virus, while actually a macro virus, had the effect of a denial of service attack. Several large companies on the Internet were forced to shut down their email systems due to the flood of email generated by the virus. Hackers usually take advantage of security holes to gain access to a computer on the network. Breaking into one machine is rarely the goal of a hacker, however. They will usually “set up shop” and then use that machine as a way to break into other machines on the network. Security “incidents” can last weeks or months, comprising break-ins to multiple machines using several different tools and security holes.

One of the first steps towards improving network security is to put together a security policy. Cheswick and Bellovin, the authors of *Firewalls and Internet Security: Repelling the Wily Hacker*, define a security policy as “the set of decisions that, collectively, determines an organization’s posture toward security.” At first glance, you might think that everyone’s security policy should be to make their network and computers as secure as possible. There are other factors that must be considered, however. First are the needs of the community involved. A military site with classified information will require a high degree of security. An academic site like Harvey Mudd College, on the other hand, has very different requirements. The concept of academic freedom requires that users have unrestricted access to resources like the Internet and library catalogs and databases.

(continued on page 4)



not always) provided as part of a package of integrated systems that includes alumni records, development, financial accounting, human resources, etc. The student systems are key to the colleges' operations and success because they support the academic programs, and because many other systems either feed into or out of these core systems. At present each of the colleges has its own student systems, some of which have common roots but all of which are managed and operated separately."

"What is the impetus for the colleges to move to a new system?"

"The Council of Presidents has mandated that The Claremont Colleges seek a common solution for student administrative systems. It is the collective recognition that all of our current administrative systems will likely become obsolete and/or unusable within a few years, and collective action will provide both new functionality (e.g., cross registration) and operational efficiencies. Because our systems were developed independently over a period of almost 20 years, they do not easily permit sharing of software or convenient exchange of data among the colleges. Since several campuses were already exploring options for new computer systems, this is a unique opportunity for the colleges to realize significant functional and financial advantages by pooling resources and proceeding cooperatively.

The application that is the primary catalyst for this effort is registration. The presidents want a system that will permit the students of The Claremont Colleges to cross-register for courses in a more timely and effective manner than they now do. Currently, because of the differences among our student information systems, cross-registration is unacceptably cumbersome. A new system must provide for on-line, real-time cross-registration."

(continued on page 6)

ditor's Notes

This month's issue of *Occasional Downtime* is devoted to two topics of concern to our users at HMC: network and computer security and the ATIP project.

Computing and Information Services is always thinking about computer and network security, but a recent break-in on Turing in the Computer Science Department has made it a more visible topic on campus. In this issue's article we describe the general concepts of computer and network security and discuss ways in which security can be improved.

You may have heard people talking about the Administrative Technology Improvement Project (ATIP). This is a project involving all of the Claremont Colleges so we thought it might be useful to provide a brief description of the project and its purpose. We've also provided pointers to Web sites where you can find out more.

This will be the last issue of *Occasional Downtime* before the end of the semester. We hope you have a productive and fun summer!

—Elizabeth Hodas

Occasional Downtime is published bimonthly by the Computing and Information Services Department at Harvey Mudd College. It is also available in a variety of formats on the HMC Web Server. Comments and questions can be directed to downtime@hmc.edu.

Users must be able to easily collaborate with others located both inside and outside their community. And, since many faculty and staff work at home or while traveling, they must be able to access network resources from remote locations.

Another issue is cost. A high level of security is usually expensive, both in terms of hardware and software and in staff time. There is also the convenience factor. A high level of security can have a negative impact on user morale and productivity by making simple procedures more complex.

All of these factors must be considered and balanced when designing a security policy. The security policy itself is simply a description of the activities and services that the institution has decided to allow or to restrict.

How does an institution go about implementing a security policy? There are two levels that need to be examined: host security and network security. System administrators play a major role in maintaining and improving host security. Software is inherently buggy and hackers are quick to take advantage of any security hole found. The UNIX operating system has historically been particularly vulnerable to hacker attacks. The system administrators of shared hosts on campus such as Orion, Thuban, and HMCADM spend a significant amount of time monitoring their systems for security breaches. They also have to be quick to be up to date on all software patches as they are released.

System administrators can take advantage of several security tools to help them. A program called *COPS* (Computer Oracle and Password System) will scan a UNIX system and warn the administrator of potential problems. *Tripwire* will monitor the permissions and checksums of important system files and detect files that have been replaced, corrupted, or tampered with.

Users can also play an important role in improving host security. The most common way that hackers break into systems is through user passwords. Enough users pick bad passwords that hackers can often “crack” or guess passwords. Since users often use the same password on several machines, hackers can gain access to multiple computers on the network. Choosing a “good” password and keeping it confidential is an essential step that all users can take to help improve computer security. While using the same password on multiple machines is convenient, users should not use the same password for systems or resources outside of HMC as they do for HMC systems.

Another problem is that many protocols, including telnet and FTP, transfer passwords as “clear-text” (i.e. unencrypted) over the network. Hackers can “sniff” packets and steal passwords. In some cases system administrators may therefore choose to disable these protocols and require that more secure protocols be used instead. This is what happened in the wake of the break-in on Turing in the Computer Science Department. Telnet and FTP have both been disabled. Users must use SSH (secure shell) to login to Turing instead of Telnet.

System administrators can also take steps to help users choose good passwords by implementing features that prevent users from choosing particularly bad passwords such as their login name or a word from a dictionary. Using a “shadow” password file is a way system administrators can protect the password file itself from hackers. A shadow password file is hidden in a secure directory that is readable only by the root account.

Users and system administrators can do a lot to make it more difficult for hackers to break into the host machines on their network, but unfortunately it simply isn't possible to make them totally secure. Another, somewhat more radical, level of

security can be provided on the network level by a firewall.

A firewall is a system or group of systems that sits between two networks. The firewall enforces the security policy of the community by restricting or blocking access that the community has decided is unacceptable. There are basically two types of firewalls: network level firewalls and application level firewalls.

Routers can act as a type of network level firewall by using packet filtering. The network administrator can specify rules that tell the router to drop or reroute packets based on their source or destination addresses or ports. So, for example, the network administrator could configure the router to block telnet communications unless they were initiated from inside the HMC network.

Applications level firewalls are usually machines running proxy servers. Proxy servers prevent traffic from passing

directly from one network to another. They are software applications that accept requests from the user and then act on their behalf. Proxies can provide extensive logging and auditing services, as well as another level of authentication. HMC has been testing a Web caching proxy server this semester, not for security purposes, but as a way to reduce network traffic and conserve bandwidth.

Computer and network security is always an matter of concern at CIS. The recent break-in in the Computer Science Department has raised many issues regarding our current security policy. A mailing list, `comp-security-1@hmc.edu`, was created in order to provide a forum for discussing a revised security policy for HMC. If you are interested please join the list by sending an email message to `listkeeper@hmc.edu` with the command "subscribe" in the body of the message. 🐾

SOURCES

- ▼ Baker, Richard H., *Network Security: How to Plan for It and Achieve It*, McGraw-Hill Inc., 1995.
- ▼ Cheswick, William R. and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley Publishing Company, 1994.
- ▼ Cooper, Frederic J. et al., *Implementing Internet Security*, New Riders Publishing, 1995.
- ▼ Greenwald, Michael et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF", *OnTheInternet*, May/June 1996, pp. 24-33.
- ▼ Hendry, Mike, *Practical Computer Network Security*, Artech House, Inc., 1995.
- ▼ Howard, John D., *An Analysis of Security Incidents on the Internet 1989-1995*, Carnegie Mellon University, 1997, <http://www.cert.org/research/JHThesis/Start.html>, Accessed on March 23, 1999.
- ▼ Madron, Thomas W., *Network Security in the '90s: Issues and Solutions for Managers*, John Wiley & Sons, 1992.
- ▼ Nemeth, Evi et al., *Unix System Administration Handbook*, 2nd edition, Prentice Hall, 1995.
- ▼ Pabrai, Uday O. and Vijay K. Gurbani, *Internet & TCP/IP Network Security: Securing Protocols and Applications*, McGraw-Hill Inc., 1996.
- ▼ Ranum, Marcus J. and Matt Curtin, *Internet Firewalls Frequently Asked Questions*, <http://www.interhack.net/pubs/fwfaq/>, Accessed on March 23, 1999.

ATIP continued from page 3

“Would each college and all of the administrative functions have to move to the same new administrative computing system?”

“The immediate goal is for the core student records and registration system to be the same for all participating colleges. Other administrative systems (e.g., admissions, development and alumni relations, human resources) may or may not be purchased from the same vendor as the student

maintenance, and operation of the new software. This is one aspect of ATIP.”

“What is process re-engineering and why is this part of the issue?”

“Process re-engineering is a buzz-word for the analysis of how work is done, particularly with regard to paper and information flow. The purpose is to analyze a work process with an eye toward simplification and improvement, especially for the customer (another campus user, students, parents who receive a bill, etc.) This is a good idea in any case but, because we are talking about multiple independent institutions, it will be essential to document, refine, and redesign some of these processes so that we can all work off the same information systems as much as possible.”

“Does this mean that we’ll have to change some of our work procedures?”

“Yes, absolutely. No office will be able to continue doing everything the way it always has. No canned software package in the world is flexible enough to allow for this, and when we consider seven entities, it is clear we will all have to make compromises in how we do things (e.g., how data fields are defined in admissions, or how the student bill looks, or how grades are posted). Because this will be a big challenge psychologically for all of us, it is essential that supervisors of all administrative functions understand the implications of process re-engineering and support this effort fully. We all know that intercollegiate efforts in Claremont can be very complex, difficult, and frustrating. They inevitably involve compromises that we might not make if we were on our own, but the Council has mandated this effort because of the substantial functional and financial advantages of cooperation. Full support at all levels of each institution is essential to the success of this significant project.”

“...all of our current administrative systems will likely become obsolete and/or unusable within a few years...”

information system, but the Council of Presidents has asked for a common solution across campuses for each of these functional areas.”

“Would this system be centrally located and controlled?”

“‘Centrally located and controlled’ is only one of many options being considered, and it is not anyone’s first choice at this point. In fact this was a recommendation of the COLLEGIS consulting firm, brought in by the presidents last year, but it was rejected for numerous reasons. However, much more information and analysis is needed before making a final decision in this area. It may be that we end up with separately managed installations of the same software or a hybrid system that includes some centralized functions and some separate functions. This would enable our systems to work and talk to each other when we want them to, while allowing us to retain as much autonomy and college control as possible. The ideal solution should also save us money, collectively and over the long term, on the purchase, installation,

Tricks & Tips

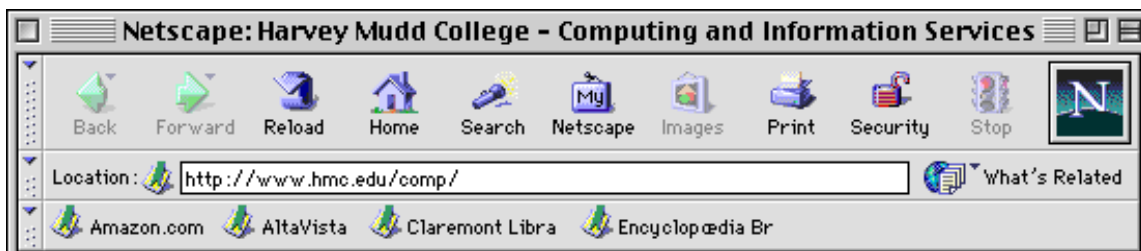
& Tricks

NETSCAPE'S PERSONAL TOOLBAR

Netscape's bookmarks are a quick and easy way to get to sites that you access frequently. However, if you're like most people, your bookmarks list has quickly become pretty long and cluttered. You can use folders and separators to help you organize and manage your bookmarks, but that can just add another layer of submenus that you need to hunt through to find the bookmark you want. Netscape Communicator offers another tool to help you quickly access your frequently used sites—the Personal Toolbar.

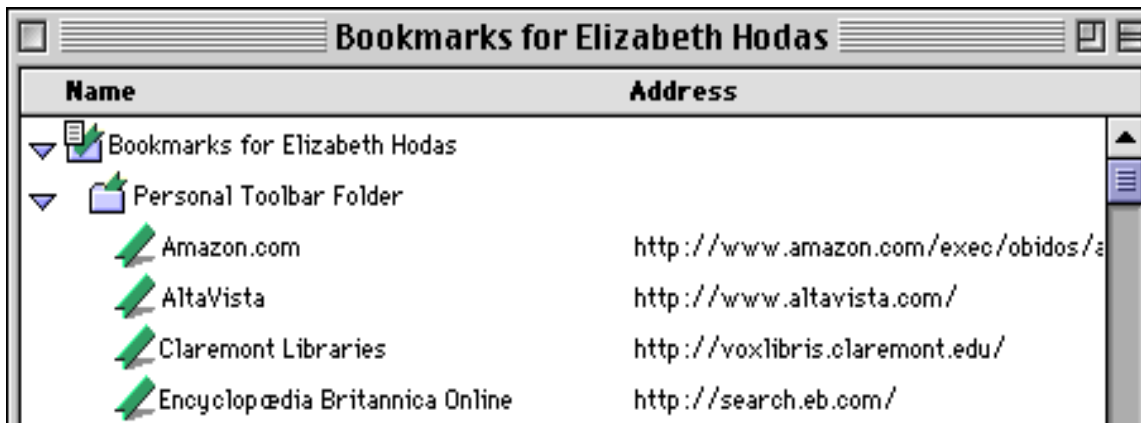
Put your most frequently accessed bookmarks on the Personal Toolbar and you'll quickly see how convenient it can be!

The Personal Toolbar appears as a folder in your bookmarks file so that it's easy to edit or delete items from it. To do so, open your bookmarks file by selecting Edit



The Personal Toolbar appears at the top of the Netscape window, below the Navigation and Location Toolbars. (If you don't see it, it may just be closed. Go to the View menu and select Personal Toolbar from the Show submenu.) You can add bookmarks to the Personal Toolbar by first

Bookmarks from the Bookmarks menu. Open the Personal Toolbar folder by double-clicking on it. To delete a bookmark from the Personal Toolbar select it by single-clicking and selecting Clear from the Edit menu on the Macintosh or Delete on the PC. To edit the bookmark



going to the site you want. Then click on the little bookmark icon next to the location window and drag it to the Personal Toolbar. The name of the bookmark will now appear on the Personal Toolbar. It acts like a button so that with a single click you can go directly to your

select Get Info from the Edit menu on the Macintosh or Properties on the PC. 🐘

QUESTIONS *and* ANSWERS

Q: I want to print to a different printer in my building from my PC. How do I do that?

A: Most of the time when you print from your PC you are printing to the printer that has been configured to be your default printer. There are times when you might want to print to a different printer, either because it has capabilities that your printer doesn't or because there is a problem with your default printer. If your computer has been configured with multiple printers, then changing to a different printer will be simple.

In the application that you are using select Print from the File menu. Click on the arrow next to the box labeled "Name" and select the printer you want from the pop-up list. Then continue as you normally would. If the printer you want does not appear in the pop-up list, you can call the Help Desk at 7-7777 for assistance in adding the printer.

You can also easily change your default printer. Go to the Start menu and select Printers from the Settings menu. Select the printer you want by single-clicking on it. Then select the Set Default command from the File menu.

Q: How can I find out which rooms are available when I need to schedule a meeting?

A: For rooms scheduled through Facilities and Maintenance (Sprague Board Room, the Green Room, Platt Private Dining Rooms (PDRs), Garrett House, and Linde Recreation Center rooms), you can check the on-line calendars. To actually schedule the room, you must submit your request through Stolleworks, but finding

out first which rooms are free will help you plan your request.

To access room calendars first telnet to GEORGE.ADMIN.HMC.EDU and enter CALENDAR as the userid (no password required). This will first display the once popular, but now seldom used, HMC all-campus calendar. To switch to a room calendar, type U (no return needed). You will be prompted for the calendar you want to view. Calendar names are:

GH - Garrett House
GR - Green Room
Platt - PDRs in Platt
Rec - Recreation Center
Sprague - Sprague 4th floor conference rooms

When you enter a calendar, you will see a display with a calendar on the left and a work box on the right. The events are displayed within the work box. Use the arrow keys to move around the calendar and change days. As you do so, the date and the text within the work box change to reflect the day which is highlighted on the calendar.

Days with events have an asterisk (*) or a plus sign (+) next to them on the calendar. The asterisk indicates one window of text. To view it, simply move to that day. The plus sign indicates multiple windows of text. You will see the first window when you move to that day. To see the other windows, use either the + key or the "Next Screen" key to scroll forward and the - key or the "Prev Screen" key to scroll backward through the windows. To exit from CALENDAR, enter a Q. ↵