

# VIRTUAL PRIVATE



How valuable is the privacy and integrity of your computer data? Do you think about whether others can access the data you store on your desktop computer and on central servers? The CIS department does! Computer and network security are high priorities at CIS and we've devoted several articles to this topic in *Occasional Downtime* over the years. (If you're interested, you can go to the *Occasional Downtime* Web site to reread old articles: "Network Security," Volume 7, Issue 2, April 1999; "On Guard! New Network Security Measures at HMC," Volume 7, Issue 5, December 1999; "CIS Summer Plans and Projects," Volume 10, Issue 2, April/May 2002.) The security protocols that we have implemented, especially those that prevent HMC computers from being accessed by unauthorized people from outside the HMC network, should help assure you that your data is safe.

However, over the past year CIS has been examining another issue in security: the security of data when accessed from off-campus. For many of our users, it has been increasingly important to be able to access e-mail and other data from remote locations, including residences. Working from home or on the road is now a valuable, if not necessary, day to day occurrence.

Significant resources have been spent in providing dialup services to allow remote users direct access to HMC's interior network. This works well for users who live in the local area since when they dial in through the HMC modem pool they are assigned an HMC IP address and have full access to the HMC network. Problems arise when users who do not live in the local area or who travel are faced with long distance charges. The service is also inherently slow compared with on-campus connections.

Faculty, staff, and students have increasingly turned to other means of accessing the HMC network from off-campus, including ISPs (Independent Service Providers) such as Earthlink; DSL and cable modems; and even wireless. While these services solve some of the issues related to dialup access, they have their own drawbacks. Security is one of them; by using another service's network to connect to the HMC network, users can no longer depend on the security of their data from point to point. Wireless networking is inherently less secure as wireless data is much easier to intercept. Another issue is that when using a third party to access the HMC network, the user no longer has an HMC IP address and thus has no access to internal resources such as HMC-only Web pages, the administrative databases, or electronic databases at the Libraries.

To solve these security issues, HMC is beginning to deploy a Virtual Private Network, or VPN. Using special tunneling protocols along with complex encryption procedures, the security and integrity of data is assured. VPNs form what appear to be a dedicated, point to point, connection between the user and the HMC resource they connect to.

*(continued on page 3)*



# Off and Running With CARS—Part 1

## IN THIS ISSUE

Virtual Private  
Network ----- cover

Off and Running  
With CARS ----- 2

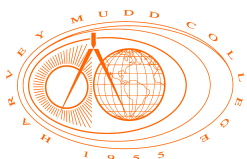
Editor's Notes ----- 3

Slay Spam! ----- 4

Tricks&Tips ----- 7

Q&A----- 8

*Occasional Downtime* is composed on a Macintosh G3 computer using Adobe PageMaker 6.5 and Microsoft Excel 98. The primary typefaces used are Times and Optima. We wish to thank Sally Rich Arroyo of the HMC Office of College Relations for all her help.



The Registrar's Office is the first office at HMC to go-live on CARS, the new student information system. While we've described the implementation process in general terms in previous *Occasional Downtime* articles, we now have the opportunity to describe what the process has been like in real life.

The first major task that the Registrar's Office did using the new CARS system was Fall 2002 Preregistration in April 2002. While Preregistration is usually done over the course of one week, it was extended to two weeks in order to give everyone extra time. Preregistration was of course an important test of the custom-written cross-registration module. The ability to perform true cross-registration between the 5 undergraduate Claremont Colleges was one of the main impetuses for moving to a new common student information system at the Colleges. Fortunately, the process went quite well and the Registrars and faculty alike were pleased at the ability to fine-tune registration limits to the point where faculty could specify how many students from each college they wanted to be able to register for their courses.

While the Registrar's Office began using the CARS system in the spring, the Spring 2002 semester was actually completed using the old administrative database and the Senior class was graduated from the old database. The first academic semester processed from the new CARS system was the Summer 2002 semester. The summer Math program and the summer CS clinic were among the courses processed in CARS, including the assignment of grades. Before grades could be assigned, historical transcript data had to be converted and

imported into CARS. This process was begun towards the end of May and is still not complete.

The transcript data must be imported into CARS in order to perform degree audits and to print official transcripts. At the moment official transcripts are being produced from the old database, but since grades for the Fall 2002 semester will be entered into CARS, the historical data will be entered by the end of this semester in order for official transcripts to be printed from CARS.

The Registrar has also begun entering the requirements for the degree audit process. The general audit, which checks whether core requirements have been met, has been completed. The Registrar is now working on writing the major requirements audit. Another current project is the creation of the Spring 2003 Course Schedule.

While the CARS implementation has not yet penetrated very far into the daily work life of most students, faculty, and staff, some of you may have noticed some changes already. Instead of multiple course lists, faculty should have each received just one unified course list for each of their courses this semester. They will also receive unified grading sheets. At CIS we were able to use the new CARS system to generate the Course and Dorm MuddShots Web pages and the course e-mail mailing lists. We were not able to include non-HMC students in the e-mail lists for each course, but that should be available for next semester.

Look for part 2 of our article about the CARS implementation in our next issue.



In order to create this encrypted connection, users must authenticate to a local server. Once this is done, all further traffic is encrypted end to end. Since the Claremont end of the connection is now within a trusted network, it can safely be used for passing the most sensitive data without threat of compromise. If you want more information on VPNs take a look at: <http://www.vpnc.org>.

Is VPN technology appropriate for you? Ask yourself these questions:

- ▼ Do you use an ISP, DSL line, or cable modem to connect to the HMC network from off-campus and do you want access to HMC or Claremont internal resources such as the HMC student roster, MuddShots, or electronic databases at the Libraries?
- ▼ Do you need to connect to the administrative database from off-campus or from a wireless network?

If you answered yes to either of these questions, then VPN might work for you. Using VPN involves installing and configuring the VPN client on your laptop or desktop computer. We are using the CISCO VPN client which is available for Windows 9X, Windows XP, Windows 2000 and Mac OS X. If you would like to use VPN, please contact the CIS Help Desk at extension 7-7777 or by sending e-mail to [help-desk@hmc.edu](mailto:help-desk@hmc.edu). 🐶

by Roger Wiechman, CIS

## ditor's Notes

If you were to ask me what was one of the most common questions that faculty, staff and students ask the CIS staff, I would have to say: "What can CIS do to stop all of the e-mail spam I get in my inbox every day?" I'm sure we have all noticed an increase in the number of spam messages we receive each day. Unfortunately, there's no silver bullet to fix this problem. But in this issue of *Occasional Downtime* we've included an article on e-mail spam and some tips on how to at least prevent your amount of spam from *increasing*. We also have a *Tips&Tricks* piece on how to create e-mail filters in Eudora. E-mail filters allow you to automatically filter spam into your Trash mailbox.

Other articles include an article on progress in the implementation of CARS, the new student information system, and on a new CIS resource for increasing the security of off-campus access to the HMC network.

We hope you enjoy this issue!

—Elizabeth Hodas

---

*Occasional Downtime* is published five times a year by the Computing and Information Services Department at Harvey Mudd College. It is also available in PDF format on the HMC Web Server. Comments and questions can be directed to [downtime@hmc.edu](mailto:downtime@hmc.edu).



# Slay SPAM!

Receiving volumes of junk mail in both our mail and e-mail boxes has become an inevitable fact of life. This does not have to be, yet, piece after piece of suffocating landfill removal has added an extra 5–15 minutes to my morning uptime ritual. I found this solution to be both appalling and unnecessary when there are alternatives available.

## STOP IT AT THE SOURCE

There are several methods that spammers employ. Here are some of the most common and the preferred solution for dealing with each.

Trade show attendance records, trade magazine subscriptions, and even your favorite grocery store where you have obtained a “membership” card prove that the old adage ‘There is no such thing as free’ still rings true. Trade shows, magazines, and stores will often collect personal contact information in a database and sell contact information based on title, location, and industry. This information is then used to distribute spam through both snail mail and e-mail.

*Tip:* Use a disposable account from one of the free e-mail providers like Yahoo or contact your ISP to see if they have multiple accounts available under your current service agreement. By using a secondary account, you’ll get less spam directed to your regular inbox.

The Internet provides many opportunities for spammers. Leaving your e-mail on a newsgroup, bulletin board, or web page guest book are all invitations for spammers.

*Tip:* Because most spammers use an automated e-mail collector, you could add the term *deleteME* (with separating underscores) to your e-mail address and make a mention of it in your signature for newsgroups and bulletin boards. You’re not usually required to give an e-mail when signing the guest book of a web page and it is advisable to never do so.

Guessing is another method that is less common. Have you ever received e-mails with your name in several different formats and different extensions (i.e.

`your_name@xyz.com`; `your.name@abc.net`; etc...)? There is a listener at the other end that records what messages ‘bounce back’ and will remove them from their further contact list. (They don’t like being spammed either.) Conversely, when you reply to these messages, your address will be escalated to the ‘hot’ list.

*Tip:* Never reply to an unsolicited e-mail. You not only confirm your address to them, but also open yourself to a potential con.

## FILTER, SORT, AND TRASH

When the mail at home is checked and sorted, I have to do it by hand. While this is a chore (and can be passed to those seeking an allowance ☺), computers are quite capable of doing repetitive, small, and very irritating tasks without complaining or going on strike (most of the time). These tasks can be taught to your e-mail program through what is called a kill file or filter.

A kill file is a scripted set of rules that the e-mail program refers to as it gets new

mail. From this file, the program will then discard those messages that have been deemed as junk, send messages to other folders, or forward to a more appropriate address. Common programs where this method of filtering is used here on campus are Pine and PMDF mail. For more information on these types of filters, you can view our documentation library at <http://www.hmc.edu/comp/doc/> and click on the "E-mail" link or more specific questions may be asked through an e-mail to [help-desk@hmc.edu](mailto:help-desk@hmc.edu).

Filters also work by scanning your incoming mail. The difference is that you tell the program directly what to filter and how. The common programs that employ this method are Eudora, Outlook, Outlook Express, and Opera. For instructions on how to create filters in Eudora, please check the *Tips&Tricks* section of this issue.

If you prefer to help strike fear into the hearts of spammers, there is help on the Internet through an organization called Spam Cop (<http://www.spamcop.net>). They are dedicated to keeping a list of reported spam and the message source. They provide members with a unique e-mail address to forward the offending e-mail and will track how many reports in order to best state their case to the owner of the offending address. The Internet service provider (ISP) is the actual owner of such addresses and would be contacted to take appropriate action against the spammer. To get the best results from this service, you'll need to be diligent in your forwarding and make sure to include full message headers. (If you aren't sure how to do this or aren't sure what headers are, feel free to contact your friendly neighborhood CIS department to find out how. Be sure to let us know what operating system and e-mail program you are using. You may call extension 7-7777, or e-mail to [help-desk@hmc.edu](mailto:help-desk@hmc.edu))

#### **SPAM COMES IN SEVERAL FLAVORS**

There are four basic varieties of non-edible

spam. They are commercial, scam, opinion, and hoax.

The commercial variety is by far the most common and solicits readers to purchase from a particular vendor. Such solicitations are usually from a store where you are a registered customer (membership) or from a company who obtained the address through a mailing list that they purchased.

Scams are usually more insidious in that they solicit money or sensitive information (i.e. home address, credit info, social security number, etc...) from the reader. Some such scams are masked as your ISP needing to update their credit information. (Note that most ISP's have a policy of reminding you by e-mailing and asking you to call their customer service to update the information. Neither CIS nor your ISP will ask you to e-mail such information and should be questioned carefully if they do.) Other recent scams include the e-mail from a purported African president who was going to leave his country and needed help to smuggle money out. Another involved a pyramid scheme that wanted readers to send \$1 to each address at the bottom of the e-mail.

Opinion spam is a little harder to define. The best definition that has held true so far is this: sending an opinion via a bulk address where the subject is not in accord with the charter of the mailing list or newsgroup to which it is sent. I would further include that sending opinions directly to those who have expressly stated that they do not wish to receive such messages is also spam.

Hoax e-mail is as damaging or more so than scams. Both can cause real damage in that they mislead the reader toward a given action whether it be to send money or perform a destructive act. The hoax commonly promotes the later action. Have you received an e-mail that prompts you to remove the entire contents of your hard

*(continued on page 6)*

*Spam continued from page 5*

drive if a particular file exists? The file that is given is usually a part of the operating system. (An example is the e-mail warning about the file 'jdbgmgr.exe' which is actually part of the java support in Windows.) These types of hoaxes persist because most readers are good and decent individuals who genuinely wish to help their friends and family, so they forward the message on. A good practice if a

message such as this is received would be to verify its validity through your ISP, CIS department at work, or a visit to <http://hoaxbusters.ciac.org/>.

#### **DO YOUR PART**

Spam is everywhere and hard to avoid, but can be dropped to a manageable level. It takes a little time in the beginning, but becomes a time saver in the long run. Don't take it anymore! 🐾

*by Raymond Allen, CIS*

## What's the Big **ID**ea? New ID Cards on Campus

This summer the Claremont Colleges instituted a new ID system with new ID cards for all students, staff, and faculty. The new card system is provided by Blackboard Inc., the same company that produces the Blackboard course management system. Blackboard's *Optim9000* system comprises an HP 9000 computer, interface hardware, card readers, and software. It is based on a hybrid of two databases: Informix and Raima. A video imaging system for producing the photo IDs is also included. The system is housed at and managed by the Claremont University Consortium.

At the Claremont Colleges, the new cards and *Optim* software are primarily used for identification purposes and by Dining Services. With respect to Dining Services the cards track the students' meal plan usage and their Flex dollars. Students can also set up a debit account that can be used for meals.

HMC is using the cards only for identification and Dining Services. Pomona College, Claremont McKenna College, Pitzer College, and Scripps

College are using the cards for door access. However, only Pomona College is using the *Optim* software. The other colleges are using the new ID cards with their existing door access software. At the Libraries, the new cards are being used for turnstile access at Honnold/Mudd Library and for book check-out.

The Blackboard system supports a variety of other uses for the cards as well. For example, the Colleges are interested in using the cards for on-campus purchases other than food. Coinless laundry machines and purchases at Huntley Bookstore are the two main areas that the Colleges are exploring. 🐾

## FILTERING SPAM IN EUDORA

How many spam messages do you receive every day? 2? 5? 10? 20? If you're up to 10 or more spam messages a day, you're probably wondering if there's anything you can do to stem the flow.

Using e-mail filters is one way to reduce the amount of spam you need to wade through every day. E-mail filters can be used to automate many tasks associated with managing your e-mail, but one of the most common uses of filters is to automatically transfer spam to your Trash mailbox. Filters for spam work by scanning all of your incoming mail. If a mail message matches the criteria that you have provided in the filter, then the message is transferred immediately to your Trash mailbox so that you never see it. Filters generally use subject header keywords or the sender's e-mail address to scan for spam.



Setting up an e-mail filter in Eudora is pretty simple, especially if you have a spam e-mail message to use as a sample. If you receive multiple copies of the same spam e-mail, that's a particularly good candidate for a filter. To create a simple filter, select the spam message by single-clicking on it. Then select the "Make Filter..." command from the Special menu.

The first step is to select the criteria to be used by the filter. There are three possible options: the "From" field, the "Any Recipients" field, and the "Subject" field. The Make Filter command will

# Tricks & Tips

# & Tricks

automatically fill in the fields of the dialog box based on information from the e-mail message that you selected. You can choose which field to use and can also modify the information in each field.

The "From" field (selected by default) is used to match the message against the sender of the message you selected. The "Any Recipient" field is used to match the message against any of the recipients in the message you selected (recipients are contained in the To: and Cc: fields and, in an outgoing message, the Bcc: field). Choose one recipient from the drop-down menu or edit the text in the field. You can select the "Subject" field to match the message against the Subject: field of the messages you selected. In all three cases the header field of the message must contain the data you've entered, but does not have to exactly equal it.

The second step is to choose what action the filter will take when a message matches the criteria you've specified. There are quite a few actions a filter can do, but in the case of spam it will usually be the last option: "Delete Message (transfer to Trash)." When you're done, just click the "Create Filter" button to create your new filter.

You can modify or delete your filter at any time by selecting "Filters" from the Window menu on the Macintosh or from the Tools menu in Windows. A word of warning: Be careful of creating filters that are too general or you may find yourself deleting messages that you actually want to read! Filters can also be used to automate other tasks such as transferring e-mail sent to a mailing list to a specific mailbox or changing the priority of an e-mail sent by a specific person. Use your imagination! The uses of filters are practically endless. 🐾

# QUESTIONS *and* ANSWERS

---

- Q:** I'm using the Microsoft client for Netware and I've set up my dorm computer on the network according to the instructions on the Web, but I still can't login to Kato.
- A:** You must make some changes to your network settings. In particular, you need to change the frame type from Automatic to 802.3. In Windows NT4 and Win9X, go to "Control Panel," launch the "Network" applet, choose the "Network" tab, click on the "Protocols" tab, click on "Properties," and choose frame type 802.3. You'll also need to choose the properties for each instance of IPX/SPX. There are, typically, two per adapter when the client is installed (NWLink and 32 bit). For Windows 2000 and XP, open the properties of "My Network Places," open the properties of "Local Area Connection," choose "NWlink IPX/SPX Compatible Transport," click on the "Property" button, and choose frame type 802.3.
- Q:** How do I register my wireless card?
- A:** Until you register your wireless card you will have limited access to the Internet (access is limited to the Claremont Colleges network). To register your card, send a blank e-mail message to wireless-request@hmc.edu. This is an autoreply e-mail address. It will send you back a form that you fill out and submit. Requests typically take 24-48 hours to process. Once your card is registered you will have full access to the Internet.
- Q:** I want an IP address outside the firewall. How do I request one?
- A:** IP addresses outside the firewall are usually requested when the user wants to host some type of network resource on their machine. If you are hosting a network resource such as a file server or Web server you first need to register the resource before you can get an IP address in unprotected space. To register a dorm resource, send a blank e-mail message to dorm-resource@hmc.edu. This is an autoreply e-mail address. It will send you back a form that you print and fill out. Bring the completed and signed form to our office in Parsons B148. We will send you an IP address by e-mail.
- Q:** How do I reserve one of the CIS computer labs for a class or event? Can I use the Virtual EMS Web site?
- A:** CIS has three computer labs that can be reserved for classes and events: the Parsons PC lab (Parsons B148), the Parsons Macintosh lab (Parsons B144), and the Linde Activities Center PC lab (2nd floor Linde Activities Center). We have not yet completely transitioned to the VEMS system. You can use the Web site at <http://www-fm.hmc.edu/vems/> to check for the availability of the labs, but you cannot yet reserve them through the Web site. To reserve one of the labs please send e-mail to help-desk@hmc.edu with the details of your request: your name, name of event, day and time of event, and which lab you would like to request. We reserve the right to refuse requests for non-course-related events.

