What's inside ...

- New Computer Viruses Appear without Notice - the *MyDoom* Lesson
- Email Firewall Figures
- Be-aware of SCAM
- Sending *Signed Email*
- Network Outlets in Student Hall reach 4000+
- More Gases for our Campus Backbone Switching Engines
- New 54 Mbps 802.11g Wireless Technology Gaining Popularity
- Enhancements in Lecture Theater PC
The "MyDoom" Lesson

New Computer Viruses Appear without Notice

New computer viruses may appear at any time and it can propagate across computers in a very rapid speed. Just like the recent computer virus "Mydoom", it spreaded on the Internet quickly on 27 Jan 2004 and in just a few hours of its outbreak, thousands and thousands of computers worldwide has got infected. This virus was found to be the fastest spreading virus so far (even faster than the notorious "SoBig.F" virus appeared last year). According to some statistical survey, one in every 5 emails on the Internet was contaminated by "Mydoom" at its peak.

"Vaccine" Not Ready at first

Just like the recent "Bird Flu" (Avian Flu) we most concern nowadays, there is no vaccine available for new breed of viruses during its first outbreak. The anti-virus vendors did take a few hours to develop the "vaccine" for "Mydoom.A". That is, during the first few hours of the outbreak, the new virus may have the chance to appear in your mailbox without notice. The "Mydoom" virus hides itself in an email attachment like ZIP file, etc. Users didn't aware, open the attachment that they are not expecting and got infected immediately.

Measures Taken to Stop the Outbreak

- Apply "vaccine" to ITSC Email Firewall

Once the "vaccine" (updated virus signature) is available from the anti-virus software vendor, ITSC email firewall will get updated automatically. Further propagation of "Mydoom" can then be stopped by our email firewall in that morning. For your reference, you may refer to the number of viral emails being rejected by our email firewall in the other Channel article "Some Figures on our Email Firewall".

However, please be aware that even "vaccine" for Mydoom.A is available doesn't mean we are 100% bulletproof. New kind of variants like Mydoom.B,
Mydoom.C, etc and other new viruses will always come to existence before they can be detected by anti-virus software in our email firewall.

- **Isolate the Infected Machines**

To minimize any possible damage / loss when a computer is being infected by a computer virus like "Mydoom", the best and effective way is to disconnect it from the Internet till the machine has been properly disinfected. Disconnecting the infected machines from the Internet serves two purposes:

- Stop any further mass mailing, distributed denial-of-service (DDos) attack to other computers or possibility of releasing confidential files.
- Prevent further damages caused by hackers through those backdoors created by the virus.

During the "Mydoom" outbreak, we have disabled several network ports in the student hall to prevent any further disruption to others and our network service as well.

- **Test & Recommend Disinfection Tools and Procedures**

There are different disinfection tools available from different anti-virus vendors a few hours after "Mydoom.A" has been identified. ITSC tested a few of them and recommended the best disinfection tool and procedures to departmental support staff, CFO or end users for their infected machines.

Of course, disinfection on new viruses is much relied on the availability of disinfection tools made by the anti-virus vendors and the cooperation of the owners of those infected machines.

- **Block Network Ports**

Proactive efforts are spent to identify possible malicious network activities through network monitoring. The "Mydoom" virus open network ports on your infected computers and listens for incoming connections. This created a backdoor for hackers to access those infected computers at any time easily. Hence, ITSC have blocked these unnecessary network ports in our campus border router in order to prevent any further damages caused by hackers from outside.

- **Close Monitoring of our Email Servers**

ITSC have also kept close monitoring on our email servers to ensure our servers can still work properly under such abnormal increase of traffic loading during the burst. We
noted that it is almost a 5 times increase in the number of email messages during the outbreak of "Mydoom".

Is my Machine got Infected?

As some users keep receiving "rejected emails" or warning messages on possible Mydoom's infection from other Internet Service Providers or postmasters, they may think their machines are infected by "Mydoom" or there are something wrong with their HKUST email accounts.

In fact, these "rejected emails" or warning messages are not related to users' machines or their HKUST email accounts as they are caused by a "Mydoom" infected machine (anywhere in the world) using a "fake" or spoofed sender email address. It just happened that your email address appeared in the address book or a document file of an infected machine. You will stop receiving these warning messages once the infected machine has been disinfected or those viral messages have been stopped by corresponding ISP's email firewall.

If you still have doubt, you can scan your machine with your anti-virus application with updates on its latest anti-virus signature.

Non-HKUST Email Accounts not Protected by our Email Firewall

Users should also note that your personal email accounts at Hotmail, Sina.com, etc are not under the control of our email firewall and you should pay extra precautions when using these accounts. These non-HKUST email accounts are maintained by the corresponding Internet Service Provider (ISP) and they may not have anti-virus or anti-spam setup on their email servers. Under such circumstances, protection from known virus attack when using these accounts can only be relied on your own desktop anti-virus application.

Your participation

New viruses are coming out everyday and maybe in any new form. It'd be better to prevent a problem from happening at all than to remedy the damages after it occurs. Hence, to prevent your computer from any virus attack, please follow closely to these good practices such as

- Handling email attachments with great caution. Don't open it if you have any doubt.
- Install and update your desktop anti-virus application to get the latest virus signature.
- Running Windows Update to get the latest critical update from Microsoft.
Enable your Personal Firewall to protect your computer from others to access.

In any case if you have received our virus warning email, do scan your machine for possible virus infection and disinfect the infected machine immediately. With the cooperation from everyone of us, we look forward for a stable and secure I.T. environment here.
Some Figures on our Email Firewall

To protect known computer virus coming from the Internet and to make it easier for users to get rid of annoying spam messages, ITSC has set up both virus and spam detection on our email firewall since 2002. Below please find some recent figures for your interest.

**Virus Detection**

During the recent "Mydoom" virus incident, our email system has handled over 736,000 emails delivered from all around the world on a single day. Over 44% of these emails are detected as "Mydoom" virus infection and are being rejected. Among the other "good" emails, a large amount of them are bounced emails from other Internet email servers caused by "Mydoom".

The chart below shows that the number of emails processed on one of our email firewall in January 2004. You can note that it is almost 5 times increase in the number of messages during the outbreak of "Mydoom".

![Virus Detection Chart](image)

**Spam Detection**

The problem of spam is really a headache nowadays. According to the figures on our email firewall, around 50% of emails arrived in our email servers are SPAM messages.

The following chart shows a "Spam Ranges" report detected on one of our email firewall in January 2004. You can note that there are around 20,000 messages in average daily are being considered as SPAM in one of our email firewall, i.e. those in the 90%-100% Spam Range. If you are using our [Spam Detection Service](#), these spam
message will be delivered to the "AutoTrash" folder instead of your Inbox which can help you to sort them out more efficiently.

Am I free from virus/spam with all these figures?

Your HKUST iMail Inbox should have already been protected from all the known email viruses. However, new viruses come out almost everyday and there is always a time lag for software vendors to release the latest virus database, you are advised to handle email messages with great caution, e.g.

- Never open email attachment that you are not expecting.
- Keep your desktop anti-virus software and virus definition up-to-date.
- Request the sender to have their digital signature ("Signed Email") on their messages, etc.

For the problem of SPAM, our Spam Detection Service do help you to get rid of a great number of unwanted emails arriving at your Inbox but of course it cannot be 100% guarantee. If you would like to enjoy our Spam Detection Service, you can enable it via your HKUST iMail Personal Settings. For details please refer to the web page at:

http://www.ust.hk/itsc/email/spam/detect/service.html
Be-aware of SCAM

Recently, our users may have received emails which claim to be from Visa, banks or other financial institutions to lure people into providing their account details. This kind of message is commonly known as "Scam". The issue of online scamming is getting more serious on the Internet nowadays and the ways being used is getting more tricky.

Scammers will use various techniques to make their emails look legitimate and attract victims to provide their bank account number / password by entering information into a fake web page, etc. Users should be very cautious when receiving this kind of emails. Most financial institutions never request account details via emails so you should become immediately suspicious of any such email you receive. If there is any doubt, you should contact the bank directly. Examples of some notorious Scams or Con-tricks are like:

- Nigerian Letters - Letters from Nigeria, etc which ask for your bank account number in order to get a share of some inherited money.
- Online Shopping Scams - which ask for your credit card number to make a purchase online, but of course you will never receive the goods.

To avoid falling into these tricks, the only way for everyone of us is to raise our cautiousness. Scammers may use new technologies to find new ways to trick their victims. So, all of us should be very careful about this.

Hong Kong Police does provide some information and advice about this kind of international fraud on their web site too at:

Sending "Signed Email"

"Signed Email" Support in HKUST WebMail

Starting from November 2003, you can send "Signed Email" with your Personal (Smartcard) e-Cert through our HKUST WebMail service.

In the past, you will need to configure your email clients like Microsoft Outlook, Netscape Messenger before you can send "Signed Email". With the "Signed Email" Support in HKUST WebMail, you can now do it easily using the Internet Explorer web browser.

For details on how to send "Signed Email" through HKUST WebMail, please refer to the following page:

http://www.ust.hk/itsc/email/webmail/sign.html

"Signed Email" from Departmental Account

In order to have assurance on both the message content and sender's identity in sending important message to users, HKUST Certification Authority has started to issue a new type of digital certificate, namely the "Role e-Cert", to departmental accounts. You may have already received a number of "Signed Email" sent from different departments such as those from Office of the President, Finance Office, Personal Office, Library, ITSC etc.

One of the benefits to send "Signed Email" is that users can easily be assured that the message is really sent from the departments as sender's identity has already been verified by our HKUST CA. It can help to discard viral emails with a spoofed sender address coming from machines infected by a mass mailing worm such as "Mydoom", etc.
ResNet Now Provides 4,000+ Network Outlets for Students

Our student hall residential network, aka ResNet, has recently been extended to cover our new student hall - currently being called New Hall. Network service for this new hostel commenced on 23 Jan 2004 which was around the time of first move-in. This new hostel provides an additional 602 in-room ResNet ports, or around 18% increase in ports count. As the premier HK tertiary institution to provide student hall network service since 1991, HKUST has now installed over 4,020 network points for our student hall residents.

The table below indicates the growth of registered ResNet users for the past several years:

<table>
<thead>
<tr>
<th>Academic Year</th>
<th>No. of Registered ResNet Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 / 01</td>
<td>2,793</td>
</tr>
<tr>
<td>01 / 02</td>
<td>2,671</td>
</tr>
<tr>
<td>02 / 03</td>
<td>3,051</td>
</tr>
<tr>
<td>03 / 04</td>
<td>3,594</td>
</tr>
</tbody>
</table>

(as at 25 Feb 2004)

Facts & Figures

Listed below are some interesting facts and figures of ResNet:

- ~200 network switches are deployed, providing 4,000+ dedicated 10 Mbps connection per user

- high proportion of ResNet users have computers connected to ResNet
  - 89.3% for 2002/03
  - 89.4% for 2003/04 (up to mid Feb 2004 - further growth to be expected)
• growing number of students using notebook computers:
  ◦ among all hall machines, ~47% are desktop PCs and ~53% are notebook computers

• typical daily Internet traffic pattern:
  ◦ high usage from 10 pm to 2 am
  ◦ low usage from 5am to 9am

There is an apparent trend that a growing number of our students are equipped with their own computers in the dormitories. It is estimated for 2003/04, roughly 9 out of every 10 ResNet students will hook up one or more computers to our student hall network.

For more information on ResNet, please refer to the ResNet home page:

  http://www.ust.hk/itsc/ResNet/
More Gases for our Campus Backbone Switching Engines

The current switched Gigabit Ethernet network backbone of HKUST was first instituted back in 1999, when at that time we were migrating from an older 100 Mbps FDDI to the newer 1,000 Mbps Gigabit Ethernet backbone switching technology. At present Gigabit Ethernet (GbE) is still the mainstream backbone switching technology for enterprise networks, though 10 Gigabit Ethernet (10GbE) technology is emerging.

Right now our campus backbone is powered by a set of Cisco Catalyst 6509 backbone switches in a high-availability design setup. A year ago these core devices are handling around 3 terabytes (TB), or 3,000 gigabytes (GB) in a typical day. Now we observe over 6 terabytes (TB) of network traffic flows through these devices on a daily basis, implying that the traffic is roughly doubled for the past year.

To cater for the anticipated traffic growth, ITSC will be upgrading the backbone switching engines to a newer hardware version in Mar/Apr time frame. This upgrade is capable to support up to a 20-fold improvement in aggregate traffic throughput at the backbone level. The table below summarizes the performance comparison of each type of switching engine:

<table>
<thead>
<tr>
<th>Switching Engine Specification</th>
<th>Current</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput of backplane / fabric (Gbps - gigabits per second)</td>
<td>32 Gbps</td>
<td>720 Gbps</td>
</tr>
<tr>
<td>Aggregate packet forwarding rate (Mpps - million packets per second)</td>
<td>15 Mpps</td>
<td>400 Mpps</td>
</tr>
</tbody>
</table>

The new switching engines will also provide the following major additional benefits:

- stronger and more flexible support in security access control as well as traffic management
- better resiliency in accommodating abnormal traffic surge due to unexpected network attacks caused by network worms or hackers
- support *hardware based IPv6 switching* (instead less efficiently using software) - the current mainstream Internet protocol we are using is IPv4; it is anticipated that this will gradually be migrated to adopting IPv6 as the next generation Internet protocol down the road

- cater for backbone switching for the emerging 10 Gigabit Ethernet (10GbE) technology

In order to leverage on the best performance of the new switching engines, there is a gradual need to replace some of the older port modules of our backbone switches by newer models with faster port speeds. ITSC is actively looking into this area in the coming 12-24 months, with initial upgrade focusing on those high-traffic areas starting in mid-2004.
New 54 Mbps 802.11g Wireless Technology Gaining Popularity

Are you one of those that is making frequent use of our MobileNet service which provides wireless Internet access in designated campus areas? Since September 2000, our wireless MobileNet infrastructure is based on the 11 Mbps IEEE 802.11b standard, which provides a user an effective throughput of up to 5-6 Mbps. Over the years, a growing number of wireless users are now found in campus, and this phenomenon is further catalysed by the growing notebook market with built-in wireless support. You may recall in our notebook ownership program back in Aug/Sep 2003, some IBM notebook models are using Intel Centrino technology with built-in 11 Mbps wireless support.

A faster wireless standard, 54 Mbps IEEE 802.11g, was ratified back in June 2003. This offers an effective network throughput of around twenty-something Mbps. Notebook models with dual 802.11b/g support is coming into market. In fact in January this year Intel had also announced that their Centrino program will offer 802.11b/g wireless chipset. So you should expect to see this new wireless feature getting more commonly found in notebooks, and do watch out for some models with this 54 Mbps wireless support in our upcoming computer ownership program this summer.

Meanwhile, ITSC is working with some network vendors to test out this new wireless technology. Our lab testing will help us outline future MobileNet upgrade plan, and sort out whether there is backward compatibility issue between 802.11b and 802.11g standards. Hopefully we can have at least part of our MobileNet infrastructure upgraded this summer.

Things keep on evolving in the information technology world. This is no exception on the wireless front. Thus, it is not surprising to see that the industry is already looking into still faster wireless technologies, say, up to100 Mbps Fast Ethernet speed or above. For instance, IEEE 802.11n and Ultra-wideband (UWB) are two new wireless standards being developed. This is the norm typically found in the IT world, isn't it?
Enhancements in Lecture Theater PC

In around mid of March, the presentation PCs in all Lecture Theater (i.e. LT-A to LT-G) will be upgraded to include a DVD-ROM drive. This enhancement allows the Lecture Theater’s presentation PCs to be able to read 4.7 gigabytes DVD-ROMs for presentation files, in contrast to the existing 650 megabytes CDROM capability.

At the same time, the remote mouse available in our loan counter will be enhanced to be USB compatible in order to stay with the industrial development trend. To do this, newly purchased remote mouse are all USB compatible. In addition, old or existing remote mouse are added with a USB conversation kit which convert existing PS2 remote mouse to become USB compatible. USB mouse provide the flexibility of “Plug and Play” – that is the remote mouse can be plugged in and ready for use without the need of manually install mouse driver and/or reboot the computer.

Last of all, the Microsoft Office in Lecture Theaters and Classrooms has been upgraded to Office 2003 in align with the most up-to-date requirement of instructional presentation requirements.