

Division of Information and Communication Sciences

Macquarie University

Network Usage Policy

Introduction

The Division of Information and Communication Sciences (ICS) provides computer networks so staff and students can get their work done. We want the networks to “just work” - with a minimum of fuss and interruption.

Computer networks are shared. The actions (or neglect) of one person can have a detrimental impact on the whole network. To keep our networks running smoothly, we have a policy with some simple rules.

This policy was written for the Division of ICS. It compliments the one set out by Macquarie University IT Services at <http://www.ois.mq.edu.au/policy/ITSecurity>

Having said what this policy is, a word on what it is not: Firstly, this is not a strict legal document. We have tried to make that purpose of each section reasonably clear, and it is the purpose that really matters. Secondly, this policy is not intended to unduly interfere with legitimate academic or administrative endeavor.

Risk

Connection to any computer network involves risk. The larger the network, greater the risk. The ICS networks are fairly large, and like most Universities, they are connected to the largest network of all: the Internet. The risks are real.

We have taken (in our judgment) reasonable measures to mitigate the risk posed by viruses, worms, crackers, hackers, unsolicited email, offensive content, etc. However, these measures are limited - not only by finite resources, but also by the need strike a balance between security, and the accessibility and flexibility expected in an academic environment.

If you do connect a host to an ICS network, you do so entirely at your own risk.

Purpose

In conjunction with 'Macquarie University Information Technology Security Policy and Rules' <http://www.ois.mq.edu.au/policy/ITSecurity> this document defines a framework for mitigating risks and provides guidelines to ensure that networks and network devices can be utilized throughout ICS in a measured and responsible way.

This policy is designed to minimize the potential exposure to ICS from unauthorized use of resources. Furthermore, it manages the risk associated with network connectivity between ICS and third parties by providing policies for the request, approval and use of such connections.

Scope

ICS computers are allocated to people for undertaking ICS/University related tasks. They cannot be regarded as personal property. That is the computers cannot be treated in the same way as a computer purchased with the personal funds.

This policy applies to all ICS staff, students, contractors, consultants and visitors with either an University-owned or personally-owned device used to connect to the ICS network.

It covers all workstations and wireless data communication devices (e.g., personal computers, PDAs, etc.) connected to any of ICS's networks. This includes any form of wired or wireless communication device capable of transmitting packet data.

Devices and/or networks without any connectivity to, or capacity to interfere with, ICS's networks do not fall under the purview of this policy.

Policy

1. Preferred Connection Method

- 1.1. There are two networks available: The **wired network** and the **wireless network**.
- 1.2. Hosts that are owned or managed by ICS SHOULD be connected to the **wired network**. The wired network offers the best speed and convenience for the end user. It also allows remote management, which assists Computer Technical Services (CTS) staff in keeping the system up to date.
- 1.3. Hosts that are owned or managed by an external entity (such as a laptop owned by a student or a visitor) SHOULD connect to the **wireless network** where

available. The wireless network has measures in place that reduce the risk to the university associated with the connection of foreign devices. It is designed to painlessly accommodate ad-hoc connections without requiring time consuming changes to be made to network databases.

- 1.4. Hosts that are owned and managed by ICS may connect either the wired network, the wireless network, or both.

2. Wireless Network

- 2.1. The wireless network is available within building E6A and part of E7A and E7B. See <http://www.mq.edu.au/wireless>.
- 2.2. The SSID for the wireless network is “Macquarie University”.
- 2.3. Users MUST have an ICSID to log into the wireless network. This can be obtained by submitting the form at <http://www.ics.mq.edu.au/cts/>.
- 2.4. Wireless users should avoid downloading large files which can flood the wireless network causing disruption to all other users. Data flooding on wireless network is considered as a DoS (Denial of Service) attack.
- 2.5. Common services which are likely to transmit passwords in plain text are blocked over the wireless network. Blocked services include Telnet, FTP, IMAP, POP and SMB (Windows file sharing). The alternatives are SSH, SFTP, IMAPS and SMTPS instead. Details on <http://www.mq.edu.au/wireless/>.
- 2.6. The user SHOULD ensure that the host is kept up-to-date with the operating systems updates and security patches. An easy way to keep Microsoft systems current is to properly configure Windows Update. Linux or other UNIX based users will need to periodically check the operating system's web site for updates and stay on top of the latest patches manually.
- 2.7. If the host runs a Windows operating system, anti-virus software SHOULD BE installed.
- 2.8. If the host runs a Windows operating system, a personal firewall SHOULD BE installed. Windows XP comes with a firewall which MUST be appropriately configured.
- 2.9. For ICS staff and students, a limited number of laptop wireless access cards are available for temporary loaning at the CTS helpdesk (help@ics.mq.edu).

3. Wired Network

- 3.1. All workstations connected to the wired network MUST be registered with CTS. The registration form is at <http://www.ics.mq.edu.au/cts/>. This process will take up to two working days.(But often much quicker)
- 3.2. If the host is running a Windows operating system, an anti virus client MUST be installed unless prior approval has been obtained from CTS. Symantec Antivirus

Corporate Edition software is available at <http://www.ics.mq.edu.au/cts/software>. User should frequently check the definition status to make sure that the anti-virus definitions are updated within one day of the definitions being released

- 3.3. The Symantec Antivirus Enterprise Client is also available to ICS staff for home use.
- 3.4. All connection requests by postgraduate students and visitors MUST be approved by their supervisor/sponsor.
- 3.5. Custodians of a host MUST be able to satisfy CTS staff that it is being kept up-to-date, is virus-free, and does not represent a threat to other users or the network. This requirement is particularly important for hosts running a Windows operating system. CTS have a Microsoft Software Update Server (SUS) which downloads the approved updates and automatically installs them on clients. However clients need to be registered with the server and be on network to participate in this automated process. Consult the CTS Helpdesk.
- 3.6. Hosts that are owned or managed by an undergraduate student MUST NOT be connected to the wired network without prior approval by a Head of Department. Approval will only be granted in special circumstances.
- 3.7. Actions including disconnecting from ICS network will be taken against any host or user found not complying with items 2.6 to 2.8.

4. Wireless Access Points

- 4.1. Wireless Access Points within ICS MUST be installed, and configured by CTS.
- 4.2. Use of RF sources is prohibited in and around the ICS wireless coverage area. This can cause RF noise which leads to interruptions to wireless communications. Departments or individuals who wish to implement any RF transmitting devices in the 2.4GHz or 5.5GHz spectrum(eg wideband cordless phones) MUST obtain prior approval from CTS.

5. Remote Access

- 5.1. Protocols that pass sensitive information (e.g. username and password) in plain text will be phased out when a secure alternative becomes available. For instance, support for Telnet is being discontinued because SSH, a “drop in” replacement for Telnet which encrypts all data, is now widely available.
- 5.2. Further policy is to be developed. Likely topics include RDP, modems, VPN, VNC, ssh tunneling, remote SMB/CIFS, broadband, and home machine updates.

6. ICSID

- 6.1. The ICSID is the username/password you use to connect to ICS computing resources.

- 6.2. You must not share or otherwise communicate your ICSID password with another person.
- 6.3. The ICSID password **MUST NOT** be written on the host or any other readily accessible location such as under the keyboard or displayed on a noticeboard. You are strongly discouraged from writing down the password anywhere.
- 6.4. If you become suspicious that your password has been compromised, you **MUST** change the password using <https://support.ics.mq.edu.au/ics/> or consult the helpdesk for guidance.
- 6.5. You must use a “strong” password. See <http://www.ics.mq.edu.au/cts/notes/> for details on how to construct a password that is easy to remember but hard to guess.
- 6.6. Staff may create a temporary ICSID for their visitors at <https://support.ics.mq.edu.au/> . This allows a staff member to easily let a visitor log in to the wireless network.

7. Prohibited Activities

- 7.1. Peer-to-Peer (P2P) file sharing software is strictly prohibited on hosts connected to any ICS network, unless prior written approval has been obtained from the Dean. P2P services include KaZaA, Morpheus, Limewire, Grokster, Bearshare, GnutellaNet, and many others. In the past, P2P file-sharing has resulted in considerable amounts of network traffic. For many people, the whole point of P2P file-sharing is to breach copyright. This is obviously not an appropriate use of University resources.
- 7.2. Port scanning, packet sniffing, or “cracking” of any sort **MUST NOT** be conducted on any ICS network without prior approval from CTS.
- 7.3. Do not use illegal or “pirated” software on your machine. Not only is this against the law, but pirated software is often infected with viruses.

8. File Storage

- 8.1. Ensure that all important data is backed up regularly. Refer to <http://www.ics.mq.edu.au/CTS/Services/Backup> and liaise with CTS if you require assistance.
- 8.2. Enterprise data should not be stored on desktop computers. Instead, it should be stored on a file server where it is regularly backed up. Most ICS file servers are backed up on a weekly basis. Read the backup policy <http://www.ics.mq.edu.au/cts/CTSONly/backup/backupandrecoverypolicy.pdf> *(This is a CTS only link at the moment)*
- 8.3. Due to resource constraints, there is presently no facility to back up desktop computers.

8.4. Student accounts are deleted at the end of each year, with a subsequent data loss of the home directory and email. Students who wish to retain their data at the end of the year will need to make their own backup. A USB storage device is the recommended backup medium.

8.5. When a staff member leaves the University, their account will be deleted. This will result in the deletion of all their data, including their personal files and their email. It is the responsibility of a staff member to backup their own data before they leave. A USB storage device, or an optical disk (CD-R) is the recommended method.

8.6. Restoring data

8.6.1. The primary purpose of the data backup system is to protect against catastrophic data loss arising from fire, hard disk failure, etc.

8.6.2. Restoration of files is a time consuming activity that requires specialist staff. Users may be requested to provide funds to cover the time taken to perform a restoration if files have been lost because of the carelessness of an individual user.

9. Security

9.1. Firewalls

9.1.1. A number of network firewalls are placed between the ICS networks and external networks.

9.1.2. Purpose of network firewalls

9.1.2.1. To optimize the use of the ICS networks, in particular the undergraduate student labs, by limiting inappropriate network activity.

9.1.2.2. To block network protocols that have a known history of security problems. This currently includes the NFS and SMB/CIFS protocols.

9.1.2.3. To make it more difficult for an external entity to gain unauthorized access (“crack”) to hosts on the ICS network. This purpose is theoretically redundant: If all hosts on the ICS network were correctly configured and maintained they ought to be immune to unauthorized access. However, experience has shown that this is an unrealistic expectation, particularly if the hosts run a Windows operating system.

9.1.3. As a general rule, the network firewalls allow incoming connections only to hosts that have been designated as “servers”. Roughly speaking, the designated “servers” will be the only hosts visible to external networks.

9.1.4. A notable exception to the rule above is the SSH port. This port has deliberately been left open so that knowledgeable staff have a way to pass through the firewall in a reasonably secure manner.

9.1.5. Designated servers are normally managed and maintained by CTS staff.

- 9.1.6. From time to time, a staff member requests that a “special hole” be created in the firewall to a particular port on their desktop machine. Unfortunately, “special holes” dramatically increase the complexity of the firewall rule set. This in turn increases the likelihood of misconfiguration. For this reason, requests for “special holes” will be considered most reluctantly and only after all other options for remote access have been fully explored. CTS will normally involve the Head of Department in any discussion.
- 9.1.7. Due to the complexity of “special holes”, it is normally preferable to list a computer as a designated server rather than to open up a special hole. However, this again involves a number of security issues. This will only be configured after all other options have been explored. CTS will normally ask that the Head of Department be involved in any discussion.
- 9.2. Logged-in computers must not be left unattended. In cases of leaving the desk for a short period, log-out or lock the workstation.
- 9.3. If your computer gets infected by virus DO NOT attempt to remove the virus unless your virus software does it automatically for you. The best thing to do is to stop using your computer and make sure that the infected computer and any media used on it are isolated and un-plugged from network until the problem is fixed.
- 9.4. The installation of a Windows operating systems on University owned computers must only be done by, or done under the direct supervision of, a CTS staff member. Our experience is that Windows is not a “secure by default” system, and bringing it up to a reasonable level of security is a specialist task. In particular the user is NOT ALLOWED to replace an existing OS installation with another, even if that new system is a legally obtained system.
- 9.5. Where applicable, default passwords MUST be changed to “strong” passwords. See appendix 2 for details on how to construct a strong password.
- 9.6. Users SHOULD NOT set up devices to function as file servers of any sort. Doing so opens up a wide range of security issues. If you wish to share files, CTS provides servers for this purpose which can accommodate the shared data but only with the permission of CTS and the Head of Department.

10. Email

- 10.1. ICS monitors and logs all electronic mail activity. All electronic mail coming into or leaving the ICS is scanned for viruses. The ICS mail service implements limits. See <http://www.ics.mq.edu.au/Services/Email> .
- 10.2. It can be tempting to use your inbox folder as a substitute file system. Please don't! Email is not meant for this, and large inboxes slow down the mail server. Limit your individual mail folders to no more that 100Mb and archive or delete messages from your inbox.

Glossary

CTS – Computer Technical Services at the Division of Information and Communication Sciences, Macquarie University.

Data Flooding – the process of sending and receiving so much data to or through a device that its capacity is exceeded and the network slows. Sometime devices simply drop much of the data sent to it for this reason.

DHCP (*Dynamic Host Configuration Protocol*) - a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DoS attack (*Denial-of-Service attack*) - a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

FTP (*File Transfer Protocol*) - common protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer. FTP is not encrypted and therefore not secure.

Host - a network device of any sort that is capable of transmitting packet data. Usually referred to the devices connected to the data network.

IMAP (*Internet Message Access Protocol*) - a protocol for retrieving e-mail messages. The latest version, *IMAP4*, is similar to *POP3* but supports some additional features. For example, with *IMAP4*, you can search through your e-mail messages for keywords while the messages are still on mail server. You can then choose which messages to download to your machine.

IMAPS – IMAP Secure. The IMAP protocol encrypted by SSL/TLS

PDA (*Personal Digital Assistant*) - a handheld device that often combines computing, telephone/fax, Internet and networking features.

Peer to Peer(P2P) - a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer to Peer programs are often used for sharing media files for sound and video.

Port Scanning - systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies “open doors” to a computer. Port scanning has a legitimate use in managing networks, but port scanning also can be malicious in nature if someone is looking for an access point to break into a computer.

Packet Sniffing - A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called *packet sniffers*.

POP (*Post Office Protocol*) - a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol, although most can also use the newer IMAP (Internet Message Access Protocol).

RF Signal (*Radio Frequency*) - any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

Rogue Device – an unauthorized device attached to the network. Rogues placed by employees are typically on the network to facilitate convenient network connectivity. Rogue devices placed by intruders can bypass security measures and gain unauthorised access to network resources.

SAMBA - An open source implementation of the SMB file sharing protocol that provides file and print services to SMB/CIFS (read Windows) clients. Samba allows a non-Windows server to communicate with the same networking protocol as the Windows products.

SMTP – (*Simple Mail Transport Protocol*) - A standard protocol for sending email messages.

SMTPTS – (*SMTP Secure*) - the SMTP protocol encrypted by SSL/TLS.

SSH - (*Secure Shell*) - A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SCP (*Secure Copy*) - A file transfer protocol like RCP but it uses SSH to secure the both authentication and the data transfer from eavesdropping.

SFTP – a file transfer protocol like FTP but it uses SSH to secure the both authentication and the data transfer from eavesdropping. FTP on the other hand just passes the login details in plain text password format which is very unsecured.

SSID - (*Service Set Identifier*) - a 32-character unique identifier attached to the header of packets sent over a WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID.

Telnet - A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network.