

Sharing the Network Commons

at

The University of Auckland

Nevil Brownlee

ITSS, The University of Auckland, New Zealand

and CAIDA, SDSC, UC San Diego

E-mail: n.brownlee@auckland.ac.nz

Abstract—The University provides computing and network facilities to its members as part of their common working environment. For this commons to be shared fairly and safely, it is important that all members understand how the network should be used, what risks may be associated with it, and how these risks are to be minimised.

This paper provides an overview of the University's network, our various network-related policies, and our approach to implementing those policies. In addition, some of the tools and techniques used by our IT staff are presented and discussed.

Keywords—Internet Safety, Network Commons, Network Policy

I. INTRODUCTION

commons *sb pl*:

Provisions for a community ... in common; ...

also the share due to each member (Middle English)

Shorter Oxford Dictionary

A. History

Computer networking at our University began in the early 1970s, when we provided remote access to our central batch-processing computer system for the University of Waikato. In the late 70s we began providing remote terminal access to central systems, with terminal rooms for staff at various points around the university, and in the mid 80s we started using Ethernet to link various buildings around the campus. At that time e-mail service was available, with users of the central computers passing e-mail amongst themselves.

Our involvement in wide-area networking began in the mid 80s, with an international X.25 connection to universities around the world. We set up a dedicated link to Victoria University, and experimented with a link to BITNET, the Canadian Universities network. Microcomputers had started appearing on campus in the early 80s, but networking among microcomputers did not become viable until after about 1990.

The Internet emerged late in the 80s, when three large American research networks – DARPAnet, CSnet and BITnet – were linked together forming a single internetwork. The New Zealand Universities established Kawaihiko, a TCP/IP network providing connectivity amongst the Universities. Kawaihiko was connected, via its central node at Waikato, to the Internet in March 1989.

Since then we have continued to expand the campus network, and to improve our Internet connectivity. Microcomputers are now on every desk, all of them are connected to the campus network, and no-one can imagine working without one.

B. Today's University Environment

The University of Auckland is a community of scholars, including around 30,000 students and some 3500 staff engaged in teaching and research. This community is supported by the campus network, which is a common resource, used by all.

The network has about 7,000 connected hosts, located throughout some 114 buildings on three large sites, with links to many smaller sites in Auckland and its surroundings. We use a structured wiring system in all the buildings, providing Ethernet connections to the nearest network switch. There are more than 500 network switches connected into a campus-wide tree based on a 155 Mb/s ATM backbone.

Our network is logically divided into Faculty-based subnetworks, with TCP/IP, Novell IPX and AppleTalk routing between them. Internet connectivity is provided by a central gateway at our 'De-Militarised Zone (DMZ)'. We provide Internet access for all members of the University.

The University network is now a common resource for all members of the University. It is used by students and staff to distribute and to provide access to teaching and research materials, by staff for the day-to-day administration of the University, and by everyone for communicating using e-mail or browsing the web. Since the University community is now heavily dependent upon the network, our IT staff, both in IT Systems & Services (ITSS) and among the Faculties and Departments, are focussed on providing reliable network service at all times.

C. Our Approach to Network Safety

When computers first appeared on our campus they were only used by researchers in the Science Faculty, and one had to become a programmer to use it. At that stage computer users shared a common sense of curiosity about the machines, and – apart from having to ration usage by having a booking system for computer time - we did not have problems with user behaviour.

As computers became common around our campuses we began to have occasional problems with user behaviour, for example we began our experiences with student hackers. It soon became apparent that we needed to make clear exactly what kinds of behaviour were considered inappropriate; at that time we introduced the University's *Computer System Regulations*. These regulations were published in the University Calendar. In addition, a copy was printed on the back of our 'usercode application' forms; every person wanting to use a University computer

was required to sign a declaration that they had read and understood them.

Since then, computers have become ubiquitous around the University, and the network has linked them together, greatly increasing the potential for inappropriate behaviour. Our approach to ensuring that these common resources are not abused or mis-used, however, remains much the same. In summary:

- We have a clear set of policies and guidelines stating what kinds of behaviour are expected of University computer and network users.
- We strive to provide education about network and computer security to all our users so as to make them aware of the risks in using the network, and to help them recognise security-related problems and report them promptly.
- We provide support to all University system administrators, in particular we distribute information about known and emerging security risks.
- We monitor our Internet connection for security attacks of any kind, and we co-ordinate campus-wide responses to any Security Incidents we detect.

II. POLICIES AND GUIDELINES

For any community of people to work effectively in the long term, its members need to agree on conventions for acceptable behaviour within the community. On a large scale, we have laws which we live by, like our traffic laws. Although these might be viewed as a mechanism for assigning blame after accidents, they are intended as a set of rules which make the roads – and therefore our lives – safer for us all. This section describes our University's various network and computer policies.

A. Network-related Policies

Our network-related policies are published on the ITSS web pages [1].

The *Computer System Statute 2000* is a formal policy made by the University Council under the Education Act 1989. It defines what is meant by a computer system, and says (in considerable detail) that members of the University may only use systems to which they have authorised access, and may not use any systems for which they are not authorised. In particular they may not

- use any system so as to cause costs to the University, or to any other person without that person's consent,
- use the system to wilfully impede the activity of any other person, or
- use the system to transmit information which contravenes any copyright, or is abusive or threatening.

Finally the statute also spells out the penalties which the University may impose for any breach of the statute's provisions.

The statute's formal language makes it seem almost old-fashioned, but its clarity of definition has proved very important, both now and through the years since it was first introduced as the Computer System Regulations in the 70s.

Our *Network Security Policy* is a comparatively new document, which addresses the problems raised by having a large number of computers, all of which communicate with each other and with the Internet via our campus network. The Security Policy defines the roles and responsibilities of University members,

setting out a tree structure for keeping University network and computer systems operating properly.

The University's *Network Security Officer* is tasked with defining security policy, promoting its widespread understanding and use throughout the University, and assisting Faculty and Departmental IT staff in recognising and correcting security risks in their systems. The University Security Officer is also responsible for co-ordinating responses to computer security incidents, wherever they occur on campus.

Departmental system administrators are responsible for the systems they administer. This means that they are required to apply software updates to correct known security problems in their systems, as soon as such updates become available.

Individual computer users are expected to be watchful for any unexpected change in the systems they use, and to report any such changes to their departmental IT support staff. In this way the responsibility for detecting and managing computer security incidents is shared by all our users.

The third 'network' policy document is our *Computer Guidelines*, an additional document interpreting the more formal policies, and providing additional suggestions for sensible behaviour, particularly for University members working in our student computing laboratories. The guidelines are not a formal policy document, instead they provide an informal guide to what the University sees as *Acceptable Usage* of its computer and network resources. For example, the guidelines state that University systems are provided for University-related work, and spells out activities which are explicitly not allowed, e.g. using a web page on a University system to sell private goods.

We all use computer networks to communicate with our colleagues, mostly because they provide a rapid, effective way to do this. Unfortunately, because a network may appear to provide a high level of anonymity, it can easily be used to harass others. The University has a strong *Anti-Harassment Policy*, published on our web pages as [2], supported by a strong support network. Naturally the anti-harassment policy covers harassment using the network as a medium. Cases of such harassment do occur from time to time; we continue our efforts to reduce this.

At this stage we have clear policies in place, and we strive to ensure that all members of the University understand both the policies themselves and their part in implementing them. One further important aspect is auditing, i.e. verifying that the policies are being correctly implemented and enforced. We are currently planning improvements in our auditing procedures.

III. SUPPORT FOR NETWORK USERS

Computing support at our University is distributed across the campus. ITSS is responsible for the whole of the network fabric, i.e. for our campus backbone, including all its optic fibre links between buildings, wiring within buildings, and all its switches. ITSS runs our Internet gateway, and many of our large central systems.

Outside ITSS, however, computing is supported by IT staff within Faculties and Departments. These 'on the spot' staff have direct contact with their users, and understand the local needs of their Faculty. ITSS works with Faculty IT Managers and Departmental System Administrators to maintain an effective group of staff who understand, and can respond quickly to, network-

borne threats; this is the University's Security Incident Response Team (SIRT) [3].

The University Security Officer (currently based within ITSS) supports all IT staff, especially the Departmental Systems Administrators. He provides information for users about network security, and about University policies relating to network and computer usage. He maintains strong and ongoing contacts with other security-related organisations world-wide; he disseminates security-related information to the system administrators, and from time to time organises training courses for them. In addition, he co-ordinates Incident Response throughout the University.

A. Internet Cost Recovery

Kawaihiko, the New Zealand Universities network, was connected to the Internet in 1989, under the auspices of a NASA program called PACNET. From the beginning it was obvious that Kawaihiko members would have to bear the full costs of the trans-Pacific link, so we began a development project which produced an easily-understood, fair charging scheme to recover the connection costs.

The scheme [4] was simple – count every byte sent and received by each university, and divide the total monthly Internet costs in proportion to each university's counted bytes. Any excess income was used to fund increases in international capacity.

Kawaihiko provided metering technology to its member Universities, allowing each of them to recover costs from their users in the same way. Since at that time the universities provided New Zealand's only connections to the Internet, other sites connected via the universities, and were charged for their usage by the Megabyte.

At Auckland we set up a charging system whereby staff Internet usage was metered, with ITSS sending bills to departments at the end of each month. Over the years the way in which we buy Internet connectivity, especially international connectivity, has changed considerably, but we continue to charge our users as a means of managing our overall Internet usage.

Arguments about charging strategy have continued over the years. The actual costs of international connectivity are real and high, hence if we stopped recovering them from users we would need to introduce some alternative mechanism to regulate demand. At this stage, I believe that charging has several benefits, including:

- Charging provides departmental administrators with an overview of Internet usage by their colleagues. This provides a realistic estimate of the actual costs incurred, which is needed when budgeting research projects.
- Users have little incentive to use the Internet for non-work-related activities (e.g. downloading large files), since this will impinge upon their departmental budgets.

Our usage metering system provides summary data for each user's Internet usage. From time to time ITSS gets requests from departmental staff asking for details of an individual's usage. Releasing such information would, of course, breach New Zealand's Privacy Act, so instead we suggest that the problem should be resolved by discussion with the individual concerned. This situation is a good example of our approach to managing the network; ensuring proper usage of university systems is a

'management' issue, and one which is best viewed as a community responsibility.

B. The Student Environment: NetAccount

Once the Internet and the World Wide Web became ubiquitous, i.e. since the mid-90s, we have been using the web as a teaching resource, using e-mail as a common means of communication with students, and providing Internet access for students. Our Computer Science Department developed a system called NetAccount, which provides control of, and charging for

- Printing,
- E-Mail, and
- Internet access

ITSS recognised NetAccount as the most effective Internet environment for students; ITSS and Computer Science made it available campus-wide in the late 90s. Today NetAccount is managed by ITSS, with technical support provided by Computer Science.

As part of NetAccount's campus-wide implementation, we established a unique NetID for each member of the University. This is essentially a single usercode which can be used network-wide, i.e. as a usercode on any system the user needs to work with. Extending this notion, other widely-used systems, such as the Library's LEARN information service and CECIL, our on-line teaching support system, have been extended to use NetAccount's NetIDs as their usercodes.

NetAccount also maintains a ledger; each user has dollar amounts for printing and for Internet access. As a user prints pages or downloads Megabytes, NetAccount decrements the appropriate balances. Departments can allocate 'printing' or 'Internet' dollars for use by students in a particular course. When a user's balance reaches zero, no further use is allowed until that user has put some more money into NetAccount, by paying real dollars at one of many NetAccount cash stations around the campus.

The NetAccount system maintains a database that keeps track of which users are logged in to the network, and associates their NetID with the network (IP) Address of the machine they are working on. In this way, accounting is done on a per-user basis, rather than per-computer.

One area of concern was that early on we had some problems with users sending harassing e-mail, using forged 'from:' addresses to disguise the sender's identity. The student e-mail system uses a `sendmail` mail forwarder which has been modified to rewrite mail's 'from' headers. Since `sendmail` knows the IP address of the sender, it can simply look up the sender's NetID in the NetAccount database. In this way users are prevented from forging their e-mail 'from:' addresses. This has greatly reduced e-mail harassment among NetAccount users.

IV. SUPPORT FOR SYSTEM ADMINISTRATORS

As mentioned above, ITSS operates the University's DMZ, i.e. its gateway to the Internet. We have always kept usage logs for Internet Accounting purposes, which was sufficient in the early- to mid-90s. Since then, as the Internet became more widespread and commercial, there has been an increasing tide of network-borne exploits of various kinds. To cope with such exploits, we have established an IP Auditing regime, i.e. we now

keep Internet traffic logs in fine detail, allowing IT staff to go back through the logs so as to determine exactly how an exploit developed on the network.

This kind of monitoring – riding shotgun on the network – is time-consuming, requiring attention to minute detail as well as a strong sense of duty. We have been able to automate much of this work, nonetheless it remains important that someone checks the incident logs on a daily basis. We see a steady stream of incidents. In an average week these include hundreds of attacks from worms, two or three ‘manual’ attacks, set against a steady background of ‘reconnaissance activity,’ i.e. network scans.

V. NETWORK SECURITY: TOOLS AND TECHNIQUES

This section discusses some of the risks which threaten our campus network, together with some of the tools we use to minimise those risks.

A. Network Administration, Firewalls

ITSS’s network supportgroup maintains *Rincewind*, a database of network configuration data which we have developed in-house over the last few years. *Rincewind* holds IP configuration data for a large proportion of the computers on campus; from this data it automatically generates configuration files for various IP-based network services, e.g. our Domain Name System resolvers.

Since all traffic to and from the Internet passes through our network’s De-Militarised Zone (DMZ), we have a firewall within the DMZ. The firewall is a Unix machine running *Drawbridge*, an open-source firewall system. Configuration files for *Drawbridge* are generated by *Rincewind*; these files specify which computers on campus have access to the Internet, and for which IP services (e.g. web, ftp, etc.). Staff needing Internet access for any machine register with ITSS, and we make the appropriate entries in *Rincewind*. This allows that staff member to access the Internet through the firewall, and adds their computer to the list of those appearing on the department’s monthly Internet usage accounts.

B. Viruses, Worms and Trojans

These three types of program are usually discussed together, under the generic name of *viruses*. Viruses are programs which make copies of themselves and propagate the copies to other computer systems. These days the most common example of viruses are e-mail worms, recent examples include ‘Code Red,’ ‘Nimda’ and ‘Goner.’ They can propagate very quickly, usually by e-mailing themselves to everyone in an infected computer’s e-mail address book. In addition, viruses can carry a potentially destructive payload, usually some code to be executed at a given time.

From the user’s point of view, a virus can infect many files on the user’s computer. Worse, it may require a significant amount of work to remove a virus, and repair the damage done to the user’s files. From the system administrator’s point of view, viruses can cause serious network congestion, increasing network traffic as they send copies of themselves as fast as they are able.

Within our university we deal with viruses at several levels. First, we have a site license for Symantec’s Norton Anti-Virus

software. All users are expected to have the current version of this software installed on their computers, and we distribute updates to the list of virus signatures automatically via a server within ITSS.

Second, IT staff who administer systems providing service to staff and students are expected to install anti-virus software on their servers, and to perform regular scans of files on those servers.

In the last few years we have experienced many virus outbreaks. In most cases these have been limited to a few machines. Occasionally we have suffered serious loads on our network caused by viruses. Overall, though, we cope reasonably well with viruses. We are strongly supported in this by our users, most of whom understand viruses and the way they propagate, and are well aware of the need to maintain effective anti-virus systems on their computers.

C. Junk E-Mail, Spam, etc.

Junk e-mail is a problem which has developed over the last few years, coinciding with the rapid commercialisation and popularisation of the Internet since the late 90s. Most users deal with junk e-mail by simply deleting messages from people they don’t know, especially mail addressed to ‘undisclosed recipients.’

Several departments provide help for users who want to set up e-mail filters. Such filters allow one’s e-mail program to recognise mail from frequent correspondents, and place it into appropriately labelled in-trays. Other mail goes into the default in-tray, where it can be easily checked, or simply deleted.

Recently, however, junk e-mail has grown to the point where it is a campus-wide irritation, both because there is so much of it, and because some of it is objectional to many of our users.

ITSS is an planning e-mail screening service, which will check incoming e-mail for viruses. When this is well-established, we will also offer users a junk e-mail screening service. Note, however, that although we may decide that by default we will filter out junk e-mail, our users will be able to specify that they don’t want their e-mail to be filtered in this way.

D. Network-borne attacks

Our *Drawbridge* firewall provides reasonably good protection for computers within our campus network. However, the ‘per-service’ screening it provides cannot protect our network against newly-emerging attacks launched against computers within our network.

To cope with this we run an IP Auditing tool called *Argus*, which produces fine-detail logs of all network packets reaching our network. As well, we run Intrusion Detection tools such as *snort*. These tools allow us to detect very low-level attacks, where only a few probe packets are sent, followed hours later by a few more packets, and so on.

When we detect an attack, we attempt – when this is feasible – to report it to the site from which it originates. If it is a new attack we may discuss it on one of the security mailing lists in which we participate. From our various logs we can determine which computers have been compromised; we contact their sys-

tem administrators and provide advice and support for them as they proceed to repair any damage.

Although we occasionally see new (i.e. previously unreported) security attacks, most of the attacks come from 'script kiddies.' Script kiddies are individuals who have obtained attack software from an Internet distribution site and proceeded to run it, launching indiscriminate attacks on the Internet. These attack packages are written to exploit known security weaknesses in various types of software, most often operating systems utilities or web browsers.

Since new security weaknesses are continually being reported, it is absolutely essential that vendor-supplied software updates which correct such weaknesses are installed as soon as they become available. Ideally, updates can be distributed and installed before new attack software exploiting such weaknesses. Within our university our strongest message to systems administrators is "*keep your system up-to-date with all security updates as soon as they become available.*"

VI. CONCLUSION

Sensible use of computing and networking at The University of Auckland is viewed as a shared responsibility for all members of the University. Although ITSS (supporting the campus network and Internet connection) and other IT staff use a wide variety of technology and tools in their security work, such technology is most useful for detection and overall monitoring.

Ensuring that the University's network commons continues to be an effective, safe and efficient working environment, free from attacks on systems – or worse, on individuals – remains as a management and oversight responsibility for everyone involved. We continue to improve our policies, as well as our ability to implement them and to audit their effectiveness.

REFERENCES

- [1] IT Systems & Services (ITSS) policies website, <http://www2.auckland.ac.nz/itss/Policy/itpolicies.html>
- [2] The University of Auckland, *Anti-Harassment Policy and Procedures*, http://www.auckland.ac.nz/cir_visitors/index.cfm?action=display_page&page_title=antiharassment
- [3] Nevil Brownlee and Erik Guttman, *Expectations for Computer Security Incident Response*, RFC 2350 (BCP 21), June 1998
- [4] Nevil Brownlee, *Internet Pricing in Practice*, pp 77-90 of *Internet Economics*, Lee W McKnight and Joseph P Bailey, MIT Press, 1997