There and Back Again – IT Provisioning for IT Students

Ryan Clarke

Nelson Marlborough Institute of Technology

ryan.clarke@nmit.ac.nz

Abstract

The purpose of an IT infrastructure in an academic institute is to provide a resource to facilitate and enhance the ability of the student to undertake successful study and research. The purpose of the IT infrastructure support service should be to provide the service described above, but to also provide reliable and secure services to the other institutional stakeholders. All too often, the needs of one group of users must be sacrificed to accommodate the needs of the other. The situation is exacerbated when the students are studying applied IT courses, as this user group typically has high demands with regard to flexibility and the breadth of software and services required.

This discussion paper will describe the solution that the School of Business and Computer Technology of the Nelson Marlborough Institute of Technology uses to work around this fundamental IT provisioning issue. Additionally it attempts to define a better solution based on currently accepted best/good security practices.

Keywords: Computing education, IT Provisioning, quality assured 6-8 pages.

1 Introduction

This paper has three primary purposes. The first is to highlight the issues associated with the provision of IT for the education of IT students.

The second purpose is too highlight the struggle that NMIT has had in trying to provide IT services to a student group with diverse and demanding requirements in a wireless environment.

The third objective is to provide a flexible and secure solution for tertiary providers considering a move to a wireless network infrastructure.

2 The Inherent Issue – The Fundamental Security Trade-off

Security is a state of mind, not an absolute. The security of an IT system can only be implemented to a degree that is considered "good enough" given the organisations resources and security goals. There is no such thing as a secure network.

"Unlike corporations, higher education cannot take a draconian approach to protecting the network." (Q1 Labs)

Unfortunately, all too often the relationship between security and the flexibility/usability of an IT infrastructure are impossibly intertwined.

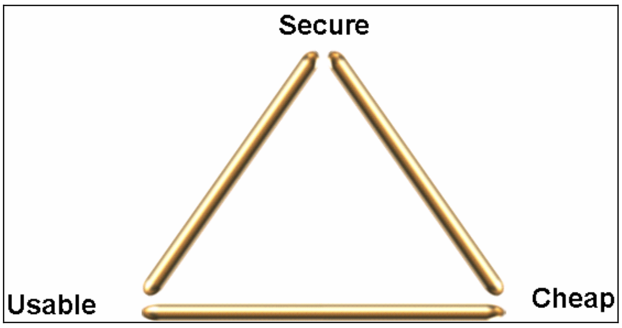
Microsoft and in particular Jesper Johansson touts the idea of the "Fundamental Tradeoffs" which adds a third parameter to the equation:

1. Secure
2. Usable
3. Cheap

He states:

"This fundamental trade-off between security, usability, and cost is extremely important to recognize. Yes, it is possible to have both security and usability, but there is a cost, in terms of money, in terms of time, and in terms of personnel. It is possible to make something both cost efficient and usable, and making something secure and cost-efficient is not very hard. However, making something both secure and usable takes a lot of effort and thinking. Security takes planning, and it takes resources." (Johnansson, 2004)

The Fundamental Tradeoff



(Johansson, 2004)

In 2002 it became apparent to the staff of the School of Business and Computer Technology (SBCT) at NMIT

This quality assured paper appeared at the *19th Annual Conference of the National Advisory Committee on Computing Qualifications* (NACCQ 2006), Wellington, New Zealand. Samuel Mann and Noel Bridgeman (Eds). Reproduction for academic, not-for profit purposes permitted provided this text is included. www.naccq.ac.nz

that the security mechanisms in place on both student and staff workstations was hindering the activities required to ensure a successful and viable Bachelor of Information Technology program.

3 IT Student IT Provisioning Requirements

Due to the fundamental trade-off issue described above, a solution to the situation was not likely to occur in the short term, if at all. As a pragmatic approach to the situation, the tutors developed a list of basic requirements that were considered essential for the successful delivery of IT courses. These requirements come with both an institutional and security cost however:

3.1 Local administrative control of the desktop operating system.

When reviewing the IT related problems faced by staff and students at NMIT, it was quickly realised that providing the users with Local Administrative control of the client operating systems would resolve the majority of these complaints. It was also considered important that students learn the art of maintaining a desktop operating system during their studies so as not to grow dependent on an IT services department. Basic trouble shooting skills could be learnt, and this was considered to be of particular importance to our mature students who were relatively new to computer systems. Students would be able to install alternative operating systems, server software, or application software provided it did not interfere with lab sessions. This would give students the freedom to explore and research in a way that was previously impossible, other than on home computer systems.

This freedom of course comes with a cost. Staff can no longer guarantee that any particular student will have a working computer system at any particular time. Additionally, the security of the desktop computer systems can no longer be controlled. Automatic software updating of the operating system and virus scanner can be disabled by the determined student. The student will often install software with little regard to the potential security vulnerabilities inherent in untested software. Finally, it is far easier for staff or student to accidentally or maliciously launch attacks against other computer systems

.

3.2 Unfettered Access to the Internet

As the Internet begins to assert itself as the primary research tool, it is imperative that high speed and unrestricted access is provided to both the student and staff. Students and staff should be considered mature enough to responsibly use this resource. Students and staff now expect to be able to download the software that they require at their institute of study, and in reasonable time. Digital natives in particular appear to expect the IT infrastructure to deliver the resources necessary from the Internet when they need it. Simply, they expect a service as good, or better than the one they have at home.

The problems with the provision above are significant from an institutional perspective. Modern Internet applications such as download managers, or Google Earth are very aggressive in their consumption of Internet bandwidth. This often leads to crude bandwidth shaping to contain these aggressive applications. Secondly, as users start running new Internet services, the network administrator must open holes in the firewall systems in place in the organisation. This exposes the organisation to risk via potentially insecure publicly accessible server applications. Finally it is possible that there is a legal requirement to protect the student from access to inappropriate content. Current algorithmic approaches to this problem often to lead to false positive results and add significant frustration in a teaching environment.

3.3 Staff and Student Involvement in a Production Network

Student and staff involvement in a production system was determined to be a mutually beneficial arrangement. Firstly both staff and students are able to gain experience and knowledge of working on a production system with real problems, something that is notoriously difficult in a “sterile” lab environment. In a lab environment, known problems can intentionally be introduced, however these are often common situations with well documented solutions. In a production system rarely are the issues so forgiving, and as such genuine problem solving approaches are required rather than a quick Google search. The second benefit of direct involvement is that there is significant motivation for continual improvement. Both the staff and students feel compelled to continually improve the system, and add features as they stand to directly benefit in the classroom from these improvements. In contrast an engineer in a network administrator or management role generally only sees the improvement as a cost in terms of time, money, and or security. Instantly the mind set is positive rather than negative, ensuring an exceptionally agile IT infrastructure for its users.

Careful consideration must be given to the delegation of rights to student users as the potential for abuse is significant. Secondly, a “constantly improving” system is not always the most stable system. Features are often added “ad-hoc” with little planning or consideration. This can obviously result in unintended negative consequences.

4 Implementation

Having identified these three fundamental requirements for providing an acceptable IT service to students, the School of Business and Computer Technology staff began the process of proposing to NMIT management that the school provides a standalone IT network for its IT students.

The basis for this proposal was as follows:

1. It would be fundamentally undesirable given the available security techniques employed at the time to connect potentially dangerous machines to the core NMIT infrastructure.

2. The SBCT was the only teaching department in the institute dependent on an external (external to the school) body to provide the key resource for its students.

   Therefore, it was the only department that was fundamentally at the mercy of the external body's priorities and resources. Without a service level agreement in place, the school was in an extremely vulnerable position.

   Being responsible for the management of its own infrastructure would allow the school to prioritise issues for itself, significantly increasing the schools agility and hence student satisfaction.

3. A series of very critical student programme evaluations left the SBCT with very little option but to radically change how IT was provided to its higher level IT students.

   To be unresponsive likely result in a severe decline in student numbers enrolled on the NMIT IT programmes. Due mostly to the impact of negative comments made by disgruntled students.

   Nelson is a small town and as such our enrolments are very susceptible to negative commentary.

4. Our BIT external monitor's report for 2002 stated that NMIT should provide a small "sand box" network so that BIT students could study and conduct research at the level required by a degree programme.

Our petition was successful and the staff were given the right to conduct a small pilot for the 2003 academic year. This provided immediate benefit to our IT service department, as their most demanding customer disconnected itself.

5 Implementation Phase 1: 2003-2005 Academic Years

The first solution to the problem was one of a completely separated IT network, The only connection to core NMIT systems was into the NMIT DMZ switch which provided the school with unfettered Internet access The school maintained it's own Windows domain, file servers, database servers, firewall and proxy server and all other essential network services. The NMIT IT department had no control over the system, but this came at the cost of no support from facilities like the IT help desk The initial pilot was for third year BIT students only, and consisted of one classroom lab of 20 end of life workstations fitted with removable disc caddies and CD burners (prior to this, there were only two CD burners accessible to students in the entire campus). The entire network was designed and built by three students who had completed two years of study, and the project was managed by a staff member of the school.

This proved a successful model, and the students worked hard to create a network that they would be happy to use for their own study. Whilst the desktop hardware was far from modern, the newly found freedom more than made up for it. Instantly the students felt empowered and began studying with their computer systems in ways that had not been previously possible The success of the first year found the school wanting to markedly increase the size of the network from one to three rooms, and from one student group to three. The school planned to run its BIT year 2, BIT year 3, and DICT Level 6 programmes through the network.

In 2004, two new rooms were added to the pool, and again the network was designed and built by a new group of enthusiastic students eager to impress an even larger group of their peers. The desktop hardware specification was raised to an acceptable level which culled the only negative comment associated with the pilot.

2005 saw the network maintain the same physical space but added 20 brand new machines built by the schools DICT Level 5 students in their Build Your Own Computer course. This topped off the number of courses supported by the network to 4 and a workstation count of 72.

For the three years that the SBCT network ran, only a 0.1 salary was assigned to design, implementation and maintenance of the systems. The network servers ran on desktop class hardware (although student data was saved on one occasion by the onboard IDE based RAID chip).

Network performance was never mentioned which can only be considered a resounding success.

Students were allocated 1GB of network storage to use as a backup point. The primary storage location for students was to be their individual hard disc caddy which contained their operating system, applications and user data. Over these three years numerous student hard disc drives failed, yet not one student lost a significant amount of work, due in part to the constant reinforcement of the message to backup often. Despite these successes and very low cost of ownership, it was strongly signalled to the school that 2005 would be the last year that it would be able to maintain its own network. The rationale for this was that the duplication of resources, lack of consistent helpdesk support, and inability to access key NMIT IT based services was detrimental to our students and the institute as a whole.

This decision was viewed as a disappointment for both staff and students involved with the stand-alone network, particularly given that the justification described above was of little significance to the majority of the stakeholders, and secondly was not reinforced with any objective data such as a cost benefits analysis.

6 Implementation Phase 2: The 2006 Academic Year

The schools standalone network it was decided, would be reintegrated as part of an institute wide IT system upgrade from a Novell to a Windows Server 2003 directory service. The intention was that NMIT's corporate network would provide a directory service and other key network services like DHCP, DNS, Web Printing, Web Proxy and Web File Access, whilst the school itself could provide other services as necessary with a new VMWare GSX server running on genuine Hewlett Packard server hardware. During the planning for this significant project, the staff at the school made a firm commitment to providing laptops for all Level 5 and above IT students. The laptops were to be connected using a wireless networking infrastructure and specifications were drawn up by the school to support this initiative.

This initiative provided a considerable institutional security concern.

The security conscious corporate network was now required to wirelessly support a large number of uncontrolled and untrusted laptops.

The solution involved a hardware firewall/virus scanner, and required the use to type the same user name and password up to four separate times just to read NMIT webmail. In short, NMIT had navigated to the least desirable (from an academic perspective) position in the Johansson "Fundamental Tradeoff" triangle. NMIT had implemented an expensive, unusable, but highly secured environment. This implementation was considered a failure by our student group due to excessive Internet restrictions, and excessive authentication requirements. Within three weeks of starting the new academic year, the schools network servers were restored in a virtualised environment.

The system as it stands is now semi-integrated, in that the school no longer maintains its own Internet proxy/firewall server, but runs through the Firewall/Virus Scanning hardware Internet servers. Since moving the laptops back to the schools directory service, the laptops have ceased to be a cause for complaint, and have instead assumed the intended role of flexible/mobile tool for student learning. This solution of course does not solve the institutional issues that prompted the move to an integrated solution.

7 Possible Solution to the IT Education IT Provisioning Dilemma

Caveat Emptor: The following security solution should provide a single integrated environment that is "secure enough" to support the academic needs of higher level IT education in the same network as the corporate line of business systems. It is important to understand that determining appropriate levels of security is something only possible when considering your own organisations needs and objectives. These recommendations were produced in accordance with the guidance provided by (Microsoft Solutions for Security Group, 2005) Server and Domain Isolation Using IPSec and Group Policy, and (Microsoft, 2005) Deployment of Secure 802.11 Networks Using Microsoft Windows guides.

7.1 Summary

The solution makes use of a concept known as packet authentication. Packet authentication forces each and every packet of data received to be checked to ensure that the sending computer is authorised to send to the recipient. This allows core line of business computer systems to completely ignore traffic from untrusted computers such as student laptops. The second and considerably important aspect of the solution is the implementation of currently accepted strong wireless authentication. This ensures that only authorised devices can communicate with the wireless infrastructure. These two practices are strongly suggested by Microsoft as being best practice for securing Windows based networks.

7.2 Possible Solution

Microsoft has for some time been touting the use of IPSec for "Server and Domain" isolation in corporate networks. In this scenario, IPSec is used to authenticate each packet that reaches a destination computer system. If further security is required, IPSEC provides encryption for the payload of each packet providing very strong security in a network environment.

Using careful planning, IPSec policies can be introduced that prevent untrusted machines such as student laptops from initiating a dialog with corporate line of business systems. Furthermore authorised desktop systems would encrypt and authenticate traffic between the local system and NMIT line of business systems. This would subvert any kind of active or passive "sniffing" of network traffic.

Student laptops would now authenticate to a single organisation wide domain, as domain controllers are part of the IPSec exclusion group, but from that point on, the laptops may only communicate with designated computers on the network.

For Internet access, the student laptops would still use NMIT's primary proxy server, however it would now have an IPSec policy and only allow traffic from machines that are actually joined to the domain. This prevents users external to NMIT from connecting to physically unsecured labs and utilising NMIT's Internet bandwidth.

Printing would fall into the category above, and only allow domain joined computers would be able to communicate with the shared print servers.

Real-time anti-malware and intrusion prevention could be provided for untrusted network devices by an appliance such as a WatchGuard Firebox, or a Trend Micro anti-malware appliance.

802.1x EAP-TLS would be used to authenticate wireless devices and users to the wireless access points. This ensures that only authenticated devices and users can wirelessly communicate with the system.

This solution is now becoming a Microsoft standard solution for isolating corporate servers from untrusted, devices. This particular solution was designed in partnership with a prominent network infrastructure solution provider, and guidance provided through the Microsoft Patterns and Practices web site.

Whilst this solution provides significant institutional benefit, it does neglect to provide for the considerations of 2.3 above, staff and student involvement in a live network.

8 Observations

During the past three years the School of Business and Computer Technology has observed the following when considering IT provisioning for IT education.

1. IT educational requirements and corporate line of business systems do not easily mix. During a question and answer session after his presentation on Server and Domain isolation at Microsoft's TechEd 2005, Steve Riley, Senior Program Manager for the Microsoft Security Business and Technology Unit stated that he probably would not attach educational systems to corporate systems, the risk is too great.

   Whilst this goes against the recommendation listed above, it must be accepted that the small size of organisations in New Zealand prohibit the duplication of significant infrastructures such as IT.

2. IT systems designed, built and maintained by the user base are extremely reactive to adversity and the inherent rapid pace of change in the industry.

   For IT tutors the desire to provide the best possible environment for students is significant.

3. Students benefit significantly from an unconstrained IT environment. The sense of academic freedom liberates the student and easily enables research into new technologies.

9 References

(Q1 Labs)
Lessons in Threat Management: Lowering Security Risks in Campus Networks
Accessed 20th March 2006 from
http://www.packeteer.com/resources/partners/Q1Labs_Education.pdf

(Johansson, 2004)
Security Management – The Fundamental Tradeoffs – Microsoft TechNet Column
Accessed 20th March 2006 from
http://www.microsoft.com/technet/community/columns/secmgmt/sm0104.mspx

(Microsoft Solutions for Security Group, 2005)
Server and Domain Isolation Using IPSec and Group Policy
Accessed 20th March 2006 from
http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/default.mspx

(Microsoft, 2005)
Deployment of Secure 802.11 Networks Using Microsoft Windows
Accessed 20th March 2006 from
http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx