RADICL

Design and Feasibility

Authors

Sergio Caltagirone Calt0563@uidaho.edu
Doug Shikashio Shik0526@uidaho.edu
David Manz Manz6595@uidaho.edu
Sean Melton Melt6173@uidaho.edu

Revision	Date	Description
1.0	9/21/04	Initial Draft

University of Idaho, Moscow, ID
Technical Report CSDS-DF-TR-05-29, 2005.

Contents

List of Figures

List of Tables

1 Introduction

Throughout this document, numbers are provided near the description of equipment. These numbers refer to Appendix F: Equipment List.

1.1 Purpose

The purpose of this document is two fold. First, the document will present the design for the RADICL lab. Second, the document will provide a feasibility study of the design that serves as a defense of the aforementioned design with an emphasis on the goals of RADICL and the pragmatic nature of an instructional computing laboratory.

1.2 RADICL Introduction

RADICL stands for reconfigurable attack and defend instructional computing laboratory. The purpose of RADICL is to provide hands-on computer and network security experience to undergraduate and graduate CS/IA students. Bookwork and classroom exercises are not sufficient to prepare IA professionals to adequately defend our computer networks and real-time control systems. We need to better prepare our IA professionals so they have the experience and tools needed to recognize emerging threats and take mitigating actions before serious damage is done. The only way this can be achieved is through hands-on laboratory experiences with a variety of network configurations under a multitude of attack-defend scenarios. By experiencing actual attacks – and implementing actual defenses – our CS/IA students will gain the knowledge and insights that will enable them to design and implement more secure and survivable systems. The broader impact of providing hands-on attack-defend laboratory experiences to CS/IA students would be twofold. First, both large complex IT systems and smaller real-time control systems used in our digital society would be better managed by experienced CS/IA graduates in the event of accidental or deliberate damage. This enables more stable and dependable infrastructures. Second, by better educating our upcoming IA professionals we move closer to a new generation of secure networks and computer systems. By giving them hands-on experience with today's IA tools we can increase the chance that they will develop tomorrow's security technologies.

1.2.1 Goals of RADICL

- Reconfigurable: The laboratory must have the ability to be extremely flexible with regard to physical layout, network layout, and software/operating system availability.
- Attack/Defend: The laboratory must have the ability to carry out basic attack/defend computer security scenarios as well as advanced computer security experiments. This includes: worm and virus research, intrusion detection research, hacker research, firewall research, operating system security research, and application security research.

- Instructional: The laboratory must meet the requirements of a classroom for the purposes of attack/defend instruction; this includes workspace for students and a presentational space for instructors.

2 RADICL Design

2.1 Usage Scenarios

In the design of RADICL, our first step was to enumerate some possible scenarios in which the laboratory was used. In this way, we could design RADICL such that it met both the stated RADICL requirements and the pragmatic needs of a teaching and experimentation environment.

Table 1. Usage Scenario 1

Usage:	Standard network attack
Notes:	Intruder attempts to gain access to a remote machine via network access
Computers Required:	A least 2 (Minimum 1 attacker and 1 server. Additionally, the attack can come directly from the intruders local machine or through intermediate computers).
Users:	>=1 (Administrator on target machine is only required for IDS scenarios)

Table 2. Usage Scenario 2

Usage:	Network Denial of Service Attack
Notes:	Network flood attack from compromised “zombie” client machines
Computers Required:	At least 2 (probably >6) (Minimum 1 attacker and 1 server. A more realistic scenario is many network zombies attacking a cluster of servers)
Users:	>=1

Table 3. Usage Scenario 3

Usage:	Network MiTM-type attack
Notes:	Malicious user inserts themselves into a network connection
Computers Required:	At least 3 (Alice, Bob, and Eve machines, more if necessary).
Users:	>=1

Table 4. Usage Scenario 4

Usage:	DNS Attack (DNS poisoning, etc)
Notes:	Malicious user attacks BIND (or other DNS software) as part of a MiTM or other network attack
Computers Required:	At least 2 (Need a DNS tree, as well as an attack computer).
Users:	>=1

Table 5. Usage Scenario 5

Usage:	Red Team/Blue Team Activities
Notes:	Group attack/defend exercises (Capture the flag, etc).
Computers Required:	2-n (The attack can come directly from the intruders local machine, or through intermediate computers).
Users:	>=2

Table 6. Usage Scenario 6

Usage:	Forensic Activities
Notes:	Live or Dead-disk forensic analysis of compromised machines/images
Computers Required:	At least 1 per team
Users:	Work in the Forensics class is performed in teams

The goal is to go from one scenario to another with only 50 minutes (or 1 class period) in between. This requires a very quickly reconfigurable lab.

2.2 Room Layout

Please refer to Appendix A: Room Layout Diagram and Appendix F: Equipment List for this section.

The room is laid out with two rows of 7 desks down the center and two desks on the end, facing the projector; and there is a one-foot channel between the rows of desks to provide space to run cable to the user stations. This provides 16 user stations (2x7 rows + 2 end desks). On each user station is a monitor (#1), keyboard (#2), mouse (#2), and Paragon II User Station (#21) that provides KVM capabilities. The servers (#3, 4, 5) are in two racks (#26) near the post in the room, below an air exhaust. Three power cables are run from the left-hand side of the room into the cable channel (#19); and the KVM cable (#17) is run from the servers on the right-hand side to the cable channel and then down the channel to each user station. All of the cable runs go under cable mats (# 27) to prevent walkway obstructions and to protect the cable from wear. This layout satisfies a number of requirements for the room.

1. It maximizes student workspace.
2. It satisfies ADA requirements for wheelchair accessibility.
3. It gives a generous presentational space in front of the whiteboard and projection screen.
4. It allows minimal movement by students to view the presentational space.
5. It allows, with little desk rearrangement, for the room to be divided into teams for red/blue teams.
6. It provides a central cable channel between the desks down the center of the room.
7. It minimizes the amount of cables crossing walk paths.
8. It places the servers in an easily accessible, yet out of the way location.

9. It places the servers in a location near an air exhaust for computer heat management.

2.3 Network Layout

Please refer to Appendix B: Network Layout Diagram for this section.

The networking needs of RADICL are met through the deployment of the Cisco Catalyst 3550-48 with SMI for wired networking needs and a Linksys WAP54g to facilitate wireless learning activities.

- Catalyst 3550-48 (#11)

The Catalyst 3550-48 is a Layer 3 switch, which when combined with 1 1000Base-T GBIC (#12), has 48 10/100 ports and 1 1000Base-T port. It features 13.6 Gbps switching fabric that can handle fully utilized, full duplex operation from every port simultaneously. Given the initial setup of RADICL requires 26 10/100 ports and the 1000Base-T port, the network should never see a loss of performance due to saturation at the switch.

The 3550 comes with either SMI (standard multilayer software image) or EMI (enhanced multilayer software image) installed. The hardware for both versions is the same, the only differences being the software installed and a couple of thousand dollars. EMI includes features deemed unnecessary for RADICL such as advanced Unicast and multicast routing protocols (SMI includes basic routing) and Web Cache Communication Protocol (WCCP).

The 3550 with SMI does include full VLAN support. A VLAN (Virtual LAN) is a switched network that is logically separated by function not physical location. Every VLAN on a switch acts like a physically separated LAN. Each VLAN is given its own broadcast and multicast domains.

No traffic is switched (at Layer 2) between separate VLANs. A router (Layer 3 device) is required for inter-VLAN communication. The configuration of each interface affects how it interacts with the switch and associated VLANs.

On the 3550 there are four main interface types, the first three are assignable to a physical port and the fourth is a virtual interface. The first of these is the switch port. Switch ports are Layer 2 interfaces and have three subtypes, access ports, trunk ports, tunnel ports.

An access port belongs to and carries the traffic of only one VLAN. Normally an access port does not use VLAN tags and it forwards non-tagged packets to the rest of its VLAN. Any tagged packets the port does receive will only be forwarded if they are tagged for the same VLAN, else they are dropped.

Trunk ports are members of multiple VLANs. They support ISL (Cisco proprietary protocol) and IEEE 802.1Q to allow traffic from multiple VLANs to be passed between two or more devices over a single physical link using VLAN tags.

Tunnel ports are mainly used by service providers to segregate traffic from multiple customers that exist in the same VLAN. Tunnels will most likely have limited use in RADICL.

The second main interface type on the 3550 is a routed port. They are Layer 3 interfaces that act like a port on a router. Routed ports are not associated with any particular VLAN and they are assigned an IP address and a Layer 3 routing protocol.

The third port configuration exists only for the purpose of analyzing network traffic. A SPAN, Switched Port Analyzer, configured port receives a copy of all traffic passing through another port or VLAN. Any of the 48 10/100 ports on the 3550 can be configured as a SPAN port.

SVI, Switch Virtual Interfaces, represent a VLAN of switch ports as one interface to the routing functions internally in the switch. Only one SVI can be associated with a VLAN, but they are only required for inter-VLAN routing. SVIs are assigned an IP address and do not become active until associated with at least 1 physical port.

To control packet flow across the ports of the switch, the 3550 support QoS and Layer 2 – Layer 4 ACLs. QoS, Quality of Service, is a capability of the network to provide better service to selected network traffic. ACL, Access Control Lists, provide basic traffic filtering capabilities. Both of these features facilitate a high degree of control over what traffic is allowed through the switch and at what rate.

- Linksys WAP54g (#13)

The WAP54g supports both 802.11b and 802.11g standards providing wireless connectivity up to 54Mbps. Supported security features are WPA, WEP (128 and 64 bit), MAC filtering, and BSID broadcast disabling. It also supports bridging to a wired network with one 10/100 Ethernet port.

- Cisco PIX 501 Firewall

The Cisco PIX 501 is a full-featured security appliance. The built in stateful inspection firewall can examine and filter packets based off Layer 2 through Layer 7, or full protocol and application inspection. Built in Virtual Private Networking (VPN) support in the PIX 501 can encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Lastly, the PIX 501 in-line intrusion protection can detect and stop more than 55 different popular network attacks with its built in DNSGuard, FloodGuard, FragGuard, MailGuard, and IPVerify protection mechanisms.

- Dual Network Interface Cards (NIC) (#8, 9)

Four of the machines (#3) will have dual NIC to allow for additional computer security experimentation such as firewalls and intrusion detection systems.

- Wireless PCI Cards (#8, 16)

Two machines will have wireless PCI cards to allow them to connect to the wireless access point. This allows us to run experiments with wireless attacks.

2.4 KVM Layout

Please refer to Appendix C: KVM Diagram for this section.

The KVM layout is simple. Each server (#3, 4, 5) in the rack has a CIM (Computer Interface Module) (#22, 23) connected to the keyboard, mouse, and video input. Cat5e cable (#17) is then connected to the CIM and run to the Paragon II KVM Switch (#20). Cat5e cable is then run from another port in the KVM switch to the Paragon II User Station (#21) sitting on the desks. The monitor, keyboard, and mouse (#1, 2) sitting on the desks are then connected to the Paragon II User Station (#21).

2.5 Rack Layout

Please refer to Appendix D: Rack Layout Diagram for this section.

Our design provides for two racks containing the servers, KVM, and networking equipment. The racks (#26) are freestanding telco (telecommunications) racks. These racks are two posts, with a bar across the top. The base is made to stand with no anchors, however, we would like to see the two racks somehow connected to provide greater stability. Each rack provides 30U of space, combining to give 60U of space. Our design requires a maximum of 44, allowing for 16U of unused space. This unused space will provide gaps for airflow and future expansion. There will also be two box fans (# 28) available near the server racks to provide even greater airflow during operation.

On one rack there will be the Cisco switch (#11), the image server (#4), and ten servers (#3). The image server will be connected to the switch via the GBIC adapter (#12) to provide gigabit throughput. On the other rack will be the Paragon II KVM Switch (#20), and the additional 10 servers (#3). Next to the racks will sit the Uninterruptible Power Supply (UPS) (#15) to provide power for the image server, and the Apple G5 (#5).

The DVD+R (#7) will also be available near the rack to provide backup for the servers. The DVD+R sits inside an enclosure (#10) that provides a USB interface so that it can be used on any of the machines.

3 RADICL Feasibility

3.1 Reconfigurable Capabilities

3.1.1 Room Layout

The room offers many reconfigurable options. Because the Paragon II KVM runs over Cat5 cable, the only limiting factor is that the user stations cannot be farther than 300m (1000') from the KVM switch. Additionally, the use of Cat5 means that the size and number of cables is minimal, and re-running the cable is easy. The only other limiting factor is that power must be run from an outlet to the user's monitor and KVM User Station.

With these factors, the room can be divided into four, four desk groups to facilitate a group atmosphere. Creating this layout would be easy and could be completed in 15 minutes.

3.1.2 Network Layout

RADICL requires rapid and multiple configurations. With simple SOHO networking equipment, topology changes require physically unplugging and re-plugging of cables between devices. Utilizing the enterprise class features of the Catalyst 3550, users of RADICL will never have to physically reconfigure the network; they will only have to edit settings through a remotely accessible administrative console.

Utilizing VLANs, the 3550 has a wide range of operation from acting as 49 non-interconnected switches to being 1 single unit. Some VLANs can remain totally isolated from the rest of the network, others can be interconnected using inter-VLAN routing. When combined with the dual NIC lab machines and the wireless AP, it is possible to construct almost any conceivable, both desirable and undesirable, network topology.

SPAN allows full network analysis of any part of the network. This solution is superior to investing in hubs, which will cost extra money and rack space in addition to the inconvenience of reconfiguring the network to include and remove hubs when needed.

The 3550 also supports IEEE 802.1x, or port based network access control. Beyond the intrinsic value of including support for security protocols in RADICL, IEEE 802.1x provides protection against uninvited physical and wireless (through WPA) connections to the network.

Packets can be filtered using the ACLs provided by the 3550. Router ACLs, Port ACLs, and VLAN ACLs are provided and together form a rudimentary firewall. Packets can be permitted or denied on router interfaces, VLAN interfaces, or port interfaces based on any information from Layer 2 through 4.

QoS is provided through congestion management, queue management, link efficiency, and shaping/policing tools. The ability to prioritize traffic helps prevent misbehaving or greedy devices from dominating the switch.

Initial configuration of the 3550 does have a steep learning curve, but that is inherent to any Cisco equipment. But after initial configurations are created, reconfiguring the lab in the future becomes a snap. The 3550 contains 16 MB of flash memory. The flash memory is a browsable file system from within the administrative interface. Multiple configurations can be loaded from or stored to the flash file system. Additionally, the 3550 can use a connected TFTP server to pull updates and configurations from.

The disk image server is provided a gigabit link between it and the switch. The rest of machines in the lab are connected over 100Mbps links. This arrangement should provide reasonable transfer speeds between any workstation and the image server for disk imaging operations. Other lab activity does not require a fast link and 100Mbps is more than sufficient.

3.1.3 Disk Imaging

One of the primary technologies used in the lab to make it as reconfigurable as possible is the use of disk imaging. This is a technology where a snapshot of a hard disk can be made and then reloaded in the future on any number of machines. In this way, only one image of each operating system/configuration can be created and then reloaded on demand on the machines.

First, we begin with a large capacity image server. Using RAID 5 for redundancy, and 200GB disks, we are able to have access to 600GB of usable disk space on our image server. With an estimated average of 5GB an image, this provides us with space to save 120 images. This will allow the laboratory to provide authorized students with the opportunity to save their work and experiments via image.

To actually image the disks, we will rely on open source software. Many imaging software tools are available. These include:

- dd/netcat
- Partimage: http://www.partimage.org/
- Mondo Rescue: http://www.microwerks.net/~hugo/
- In addition to others

However, in our decision we must be aware that some packages do not create forensic quality images and are not to be used for a forensic experiment. In this case we suggest the purchase of a commercial network-imaging package such as Norton Ghost, Altiris, or PowerQuest DeployCenter. These packages allow for central image management, and being able to push images to servers over the network.

Apple already has a package called Netboot and Network Install that allows cloning of partition and network booting.

3.2 Attack/Defend Capabilities

This design allows the lab to be reconfigured in a number of ways to support attack and defend research. First, the network capabilities of the design allow for a number of important attack and defend scenarios. This includes the ability to create virtual local area networks (VLANs) to separate the laboratory into several independent networks. The design also includes a Cisco PIX hardware firewall so that the laboratory has access to industry standard firewall technology. Four machines also include dual network interfaces that allow for the creation of our own firewalls and intrusion detection systems. The laboratory also includes a wireless access point and two wireless clients to experiment with wireless attacks.

The room layout, as described earlier also allows the room to be redesigned so that individual teams can be created for red/blue team scenarios. However, the greatest asset to the laboratory with respect to attack and defend experimentation is the ability to run almost any operating system. The only exclusions of major operating systems are SunOS, HPUX, and AIX. With our x86 processors we can run any Microsoft or Linux/UNIX operating system; and with the Apple server, we can run OSX.

Finally the KVM technology allows a single user station to control any of the 22 machines. This technology allows a person to be attacking a single server with multiple different attacks from multiple machines from a single user station and switching between them when necessary.

3.3 Instructional Capabilities

A primary purpose of the RADICL laboratory is to provide instructional facilities for computer security concepts and experiments. This design allows for this in three ways.

First, the room layout is such to facilitate lecture or directed experimentation through the creation of an instructional area and the placement of all the desks that minimizes user movement to view the instructional area.

Second, the KVM technology allows for any user to sit at any user station and control their machine(s). There is no need to reserve certain user stations, or to remember which user station they were sitting at in a previous class.

Third, the use of imaging and multiple platforms facilitates a wide range of security experiments. The hardware defined in this design allows for all x86 and any Apple operating systems. This means that an instructor is not limited to any particular operating system or hardware platform. Additionally, because of the use of imaging in the laboratory, an instructor can pre-create an image and then deploy it increasing the amount of instruction time and reducing the amount of setup time during class.

3.4 Laboratory Security

3.4.4 Physical Security

Considering the nature of the new lab, and its $40,000 price tag. Physical security should be an upper priority for the room planners as well. Given that previously there was a lab, we can rest assured that some forms of physical security have already been implemented. One egress/ingress facilitates our ability to lock down the room when it is currently not in use. But the problem lies in ascertaining who shall be allowed access to the room. Because it is NOT a general-purpose lab, the general student public nor, the general CS student should be allowed lab access without specific consent. Therefore we propose and a specific access policy be drawn up that would limit the number of people who can key into the room to a small subset of this class. One option would be to elect one or two members from each group. Alternatively and more restrictively we could rely on the largesse of full time faculty and staff to allow access.

Other than the keyed door the rest of the room should appear adequate for room security, the window could be boarded up to prevent eternal access but only at the great cost of losing all daylight.

3.4.5 Network Security

Because of the sensitive (and dangerous) nature of the experiments in the laboratory, it is necessary that there be no external network connection to the laboratory. The largest security concern for the laboratory is the use of the wireless access point. Policy and procedure need to put in place so that only authorized machines are able to connect and access our wireless point. This involves using MAC address filtering and 802.11x.

3.5 Laboratory Maintenance

3.5.6 Software Maintenance

There will be three primary sources of software in the laboratory: open source (freely available), Microsoft, and Apple. For the open source software, we will have to primarily rely on ourselves for maintenance, except for the cases where the open source project is in active development and provides new functionality and compatibility. For Microsoft, the University of Idaho owns a license for the Microsoft Developers Network (MSDN), which provides all of the Microsoft software the laboratory requires. The MSDN also provides updates to existing software. Apple computer will provide the operating system for our Apple server. Just like Microsoft, Apple provides timely updates of its software to its users for free.

There should be enough knowledge in the laboratory for the maintenance of the open source and Microsoft software. Additionally, there are two users in the laboratory that are familiar with Apple OSX. This should be sufficient for the laboratory to get started using this software.

3.5.7 Hardware Maintenance

All servers, routers, and KVMs have at least a one-year warranty. To that end any hardware failure in one year will be RMA for complete replacement or repair. After the warranty expiration all servers are capable of being repaired manually, the hard drive, memory, CPU, and even motherboard can be replaced. Given the prohibitive cost of extending the warranty, and the fact that most failures will crop up within the first year, the most cost effective venture will be to replace or upgrade machines on a case-by-case basis, in the future. As for upgradeability the machines can be fitted with at least a 3.0 gig Celeron, and 2 GB of DDR Memory.

3.5.8 File Backup/Recovery

In this design, there are two methods for file backup and recovery. The first is the image server. The image server is a RAID server, which allows for drive failures without loss of data. The second method is the inclusion of the DVD+R drive. This allows the laboratory to create 4.7GB DVD disks for backup purposes, and also allows the burning of dual-layer disks for over 8GB of disk storage.

3.6 Product Risk Mitigation

3.6.9 Operating System Compatibility

Throughout the design of RADICL, operating system interoperability has been stressed. All of the equipment in the lab is designed to work equally well with Windows as well as Linux and BSD variants. The primary components of concern are the 20 server machines, the wireless PCI cards, the network cards, the Paragon II KVM, the RAID server, and the DVD+R.

- Server Machines: the processors are x86 Celerons, and the website (http://www.tigerdirect.com/applications/searchtools/item-Details.asp?EdpNo=635298&sku=C122-1808) states the machine will work with Windows 2000/XP/Linux

- The SMC2802W wireless PCI cards have a Prism 54g chipset which is supported by Linux (see prism54.org)

- The network cards are Belkin 10/100 and the website (http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=162592&CatId=587) states the cards are supported by

Win3.1, WFW 3.11, 95, 98, Me, NT, 2000, FreeBSD, Linux, DOS, OS/2 Netware, SCO UNIX, Packet

- The Paragon II KVM is OS independent, however, the computer interface modules are platform dependent (e.g. Sun, Apple, PS/2). However, the Apple is supported with the USB CIM and the rest are supported with the PS/2 CIM. However, to control the KVM via web browser the requirements are:

Table 7. KVM Browser Requirements

PLATFORM	**BROWSER**
Netscape 7.0	Win 2K - SUN JRE 1.4.2
Netscape 7.1	Win 2K - SUN JRE 1.4.2
Mozilla 1.5	Win 2K - SUN JRE 1.4.2
Mozilla 1.6	Win 2K - SUN JRE 1.4.2
IE 6.0	Win XP - MS VM
Netscape 7.0	Win XP - SUN JRE 1.4.2
Netscape 7.1	Win XP - SUN JRE 1.4.2
Mozilla 1.5	Win XP - SUN JRE 1.4.2
Mozilla 1.6	Win XP - SUN JRE 1.4.2
Netscape 7.1	RedHat8
Mozilla 1.5	RedHat8
Mozilla 1.6	RedHat8
Netscape 7.1	RedHat9
Mozilla 1.5	RedHat9
Mozilla 1.6	RedHat9
IE 6.0, Netscape 7.0, Netscape 7.1, Mozilla 1.5, Mozilla 1.6	Win 2K - SUN JRE 1.4.2_3
IE 6.0, Netscape 7.0, Netscape 7.1, Mozilla 1.5, Mozilla 1.6	Win XP - SUN JRE 1.4.2_3

see (http://www.raritan.com/support/sup_faq.aspx#Dom52)

- The RAID Server, as stated in the website (http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=635323&CatId=1205) is supported by Windows 2000-2003 and Redhat 7.3

- The DVD+R hardware is Windows and Linux compatible since it is MMC complient. The software (Roxio EZ CD Creator) that comes with the DVD+R however is Windows only; but using CDRecord on Linux, we are able to interface with the drive.

3.6.10 Networking Equipment Compatibility

Since we are only purchasing one switch (#11), we just have to guarantee that the PIX firewall (#14) and Linksys Wireless Access Point (#13) are compatible with the switch. Because the PIX and Linksys conform to IEEE 802.3 Ethernet protocol, they will be compatible with the switch. Additionally, since the PIX and Switch are made by Cisco, and Linksys is a Cisco subsidiary then there is an added guarantee that they will work together.

3.6.11 KVM Latency

Those users who have experience with consumer level KVM products know KVM latency. It is the delay between user commands (e.g. key press or mouse movement) and the time it reaches the monitor. This obvious delay is very frustrating for the user because they do not have immediate feedback as to their actions. However, this delay does not exist in the Paragon II for local users (i.e. those not accessing the KVM over the Internet). Raritan, the engineer and manufacturer of the Paragon II KVM product, assure us that latency will not be an issue for their product when it involves local users. Although they have no data they did provide me with this statement via email, "…you will be extremely pleased with the performance of the system. I have folks working at over 600' away from their servers and its like they're working on the desktop at their desk."

3.6.12 Vendor Return Policies

- Tigerdirect
  - 15 days
  - See quote sheet

- Raritan
  - 15 days
  - See info sheet

- PCMallGov
  - 30 days
  - Called Account Rep. for information

- LanStreet
  - 30 days
  - http://www.lanstreet.com/customerservice.cfm

- CompuPlus
  - 30 days
  - http://www.compuplus.com/customerserv.php3?sid=m9mlxqz1419905c

3.6.13 Manufacturer Warranties

These numbers refer to the ID numbers provided in Appendix F: Equipment List.

1. IBM 17" CRT
   a. 3 Months Parts and Labor
   b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=615108&CatId=166

2. Keyboard/Mouse Combo
   a. Rely on vendor return

3. Cybertron Clients
   a. 1 year parts and labor
   b. http://www.tigerdirect.com/applications/searchtools/item-details.asp?EdpNo=635298&Tab=7&NoMapp=0
   c. http://www.cybertronpc.com

4. Vision Image Server
   a. 1 year parts and labor
   b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=635323&CatId=1205
   c. http://www.visionman.com/support/warranty.php

5. Apple G5
   a. 1 year parts and labor
   b. http://www.apple.com/legal/warranty/hardware.html

6. 200GB IDE Drives
   a. 1 year parts and labor
   b. http://www.maxtor.com/portal/site/Maxtor/?epi_menuItemID=a14629af82eff9461400585760b46068&epi_menuID=976d37cd478c5826433f226075b46068&epi_baseMenuID=976d37cd478c5826433f226075b46068&channelpath=/en_us/Support/Warranty%20Services/Warranty%20Periods

7. DVD+R

8. Riser Cards
   a. Rely on vendor return

9. Belkin 10/100 PCI
   a. Limited lifetime

10. USB to IDE Drive Enclosure
    a. 1 year parts and labor
    b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=1020410&CatId=1204
    c. http://www.kingwin.com/support_faq.asp#42

11. Cisco 3550 Switch
    a. Limited Lifetime
    b. http://www.cisco.com/en/US/products/prod_warranties_item09186a00800a4855.html

12. GBIC Adapter
    a. 90 day limited hardware

13. Linksys Wireless Access Point
    a. 1 year parts and labor
    b. http://www.tigerdirect.com/applications/searchtools/item-details.asp?EdpNo=628089&Tab=7&NoMapp=0
    c. http://www.linksys.com/rma/

14. Cisco PIX 501
    a. 90 day Limited hardware
    b. http://www.cisco.com/en/US/products/prod_warranties_item09186a00800a4855.html

15. UPS
    a. 1 year parts and labor
    b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=770423&Tab=7&NoMapp=0
    c. http://www.ultraproducts.com/images/CustomerSupport/UltraWarranty.pdf

16. PCI Wireless Card
    a. 3 months parts and labor
    b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=876249&CatId=368
    c. http://www.smc.com/index.cfm?sec=Support&pg=Warranty-Information&site=c

17. 1000’ Cat5e Cable
    a. Rely on vendor return

18. Cat5e Connectors
    a. Rely on vendor return

19. Surge Suppression Strips
    a. Lifetime Parts, Lifetime labor
    b. http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=557811&Sku=T105-5042%20P&Tab=7
    c. www.tripplite.com/about/contact/index.cfm

20. Paragon II KVM Switch

   a. 1 year parts and labor
   b. http://www.raritan.com/support/sup_services.aspx

21. Paragon II KVM User Station
    a. 1 year parts and labor
    b. http://www.raritan.com/support/sup_services.aspx

22. Paragon II KVM PS/2 CIM
    a. 1 year parts and labor
    b. http://www.raritan.com/support/sup_services.aspx

23. Paragon II KVM USB CIM
    a. 1 year parts and labor
    b. http://www.raritan.com/support/sup_services.aspx

24. Velcro Strapping
    a. N/A

25. Gigabit Patch Cable
    a. Rely on vendor return

26. 30U Telco Rack
    a.
27. Cable Covering Mat
    a. Rely on vendor return

28. Box Fan
    a. Rely on vendor return

3.7 Additional Issues

3.7.14 Environmental Systems

Again considering the significant investment in time and money that has and will go into this lab, ensuring a safe working environment for both the occupants and the machines should not be overlooked. To that end, temperature regulation is probably the single most important environmental factor. (Other factors include humidity and lighting that are quite hard to control and easy to control, respectively). The ideal operating temperature for humans varies considerably, but our core body temperature but our core body temperature cannot stray more than 9 degrees from the norm, or we die. Computers have much more resilience to temperature swings than a human. Of the ambient temperature can be kept below 107 degrees and above 32 degrees, a server, with proper ventilation should be able to function. However as temperatures increase the total life expectancy decreases.

Our serves are each equipped with one intake fan, two outtake fans, and one hard-drive cooling fan. After talking with a factory technician and learning how they cool their machines, the number one recommendation was ventilation. To further that goal, we are going with open sided racks that allow airflow. Two racks to ensure that less heat builds up, and the heat that does build up can dissipate easier. Lastly (just as Cybertron does) we have budgeted for two box fans ($10.87 at wall mart) to ensure maximal airflow. The machines are capable of dissipating enough heat, if there is sufficient airflow.

4 Suggestions

The design committee would like to put forth the following suggestions on how the lab can be made to better conform to the stated goals of RADICL.

- Add additional hardware and operating system platforms
  - Incorporating Apple, Sun, or other non-x86 hardware into the lab allows for additional experimentation and learning that would not be possible without them.

- Add additional machines
  - By adding additional computing resources to the laboratory, the number of possible configurations and experiments rises. The committee would like to see 32 total CPUs (excluding the RAID/File server) so that each student can have their own client and server with which to simulate attacks.
- Remove wireless capabilities

  - By adding wireless capabilities to the lab, we are removing the essential air-gapped nature of the laboratory because the signal from the wireless access points goes beyond the physical space of the room used to enclose RADICL. This element introduces serious liability to the lab where an external user may unknowingly connect to the access point that may cause the release of malicious code onto external networks.

- No external writeable media policy
  - It should be the policy of the RADICL laboratory that no external writeable media or computing devices (that can communicate on the RADICL network(s)) be allowed to enter or leave the laboratory, in order to protect external computing resources and limit laboratory liability.

- Air-gapped RADICL Network
  - The RADICL network should be disconnected from any external network so as to limit the liability with regard to the release and testing of malicious code. However, the committee understands the need to bring in software to the lab; this can be accomplished in two ways: via non-writable media (CD/DVD) burned outside the lab, or by connecting the image server to an external network for a short period of time while it is disconnected from the RADICL network. The second option is by far the most dangerous and should be discouraged.

- Laboratory Reservation System
  - There should be a method to reserve equipment and time in the lab. This will help guarantee the availability of necessary experiment equipment.

- Image Server Protection

- The image server needs to be protected at all costs. Policy should dictate that the image server will not be attacked and that due diligence will be performed with regard to the server. This could include disconnecting the server when not in use or putting the server behind the PIX firewall. Other methods of protection should be investigated and implemented.

Appendix A: Room Layout Diagram

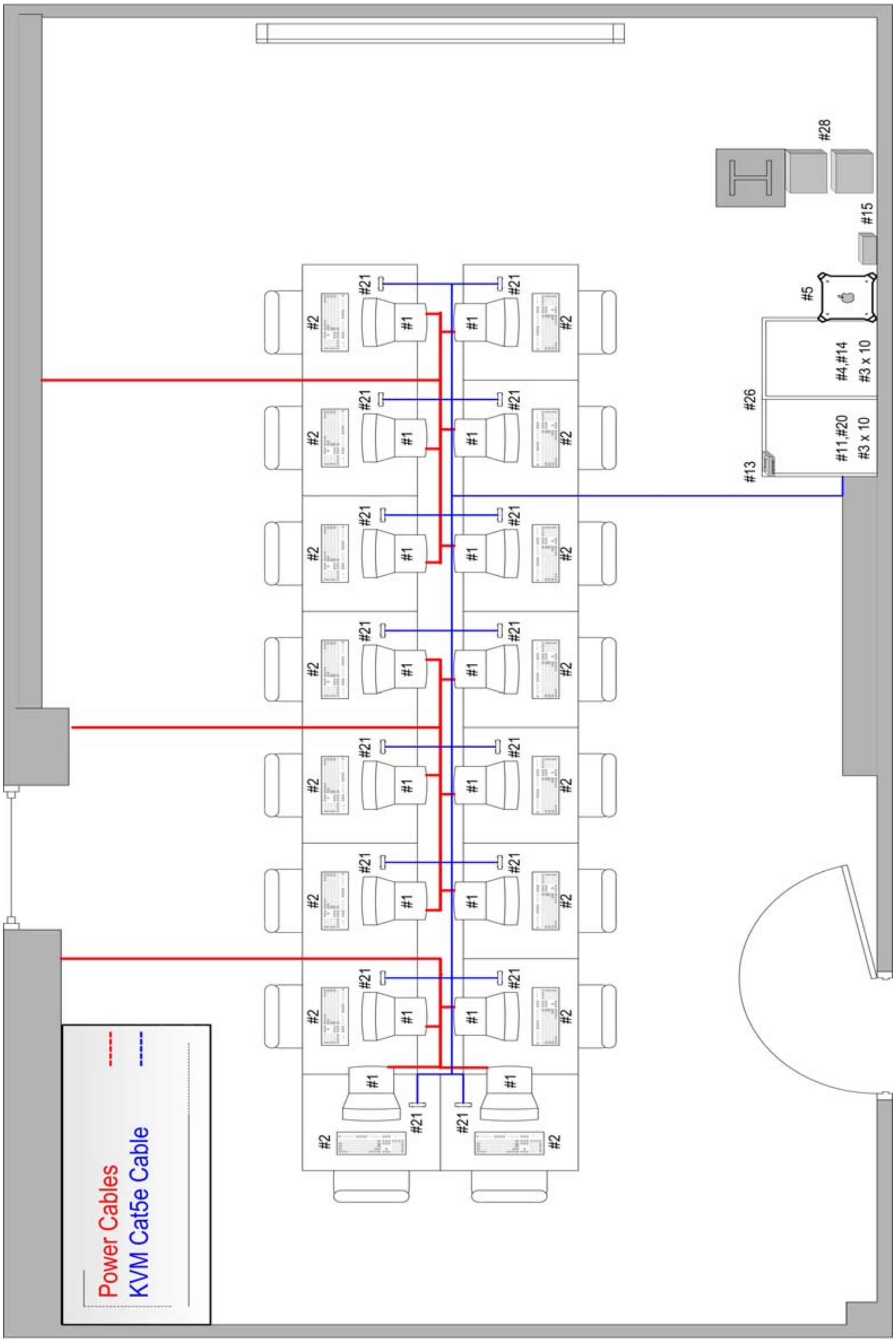

Figure 1. Room Layout Diagram

Appendix B: Network Diagram

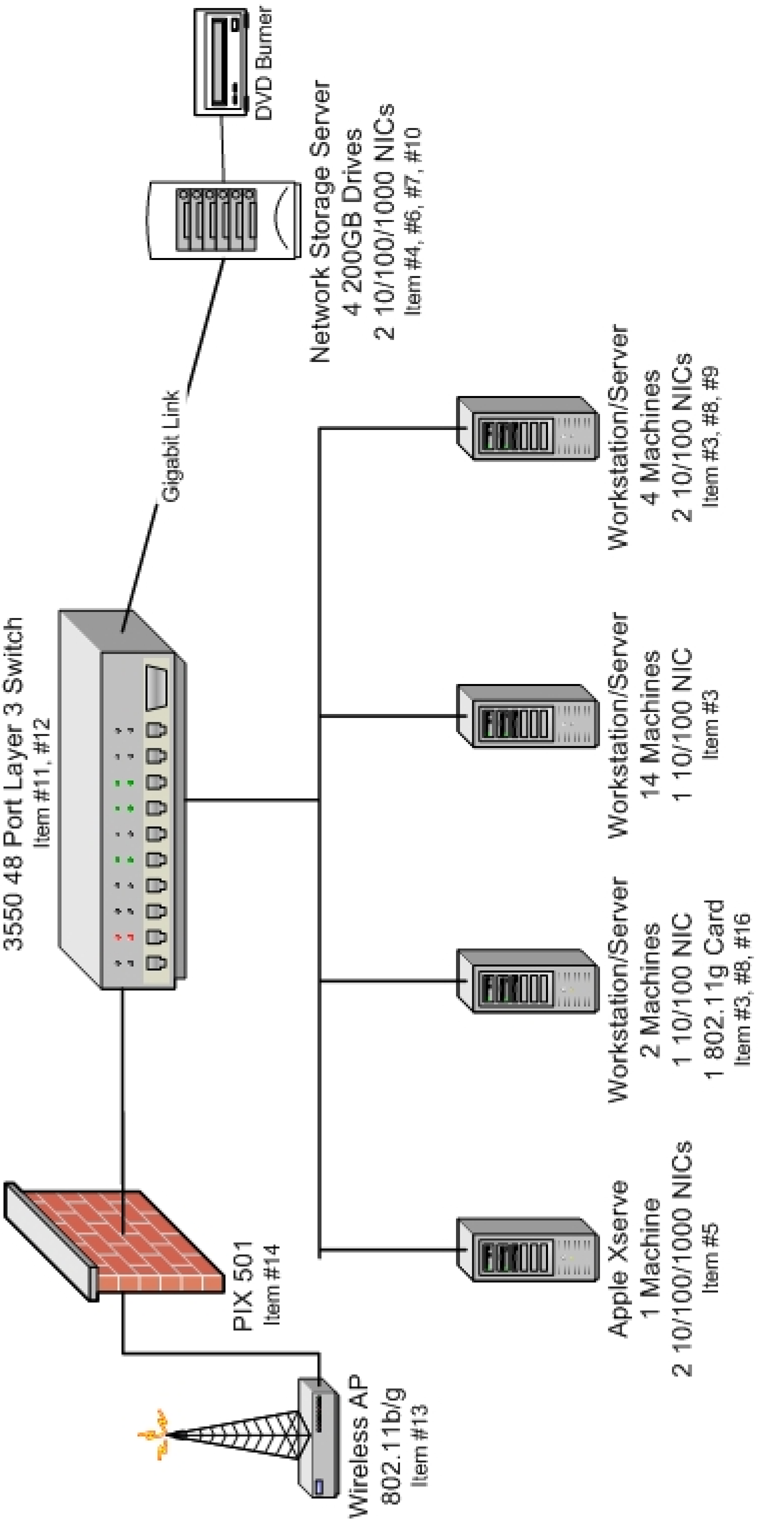

Figure 2. Network Diagram

Appendix C: KVM Diagram

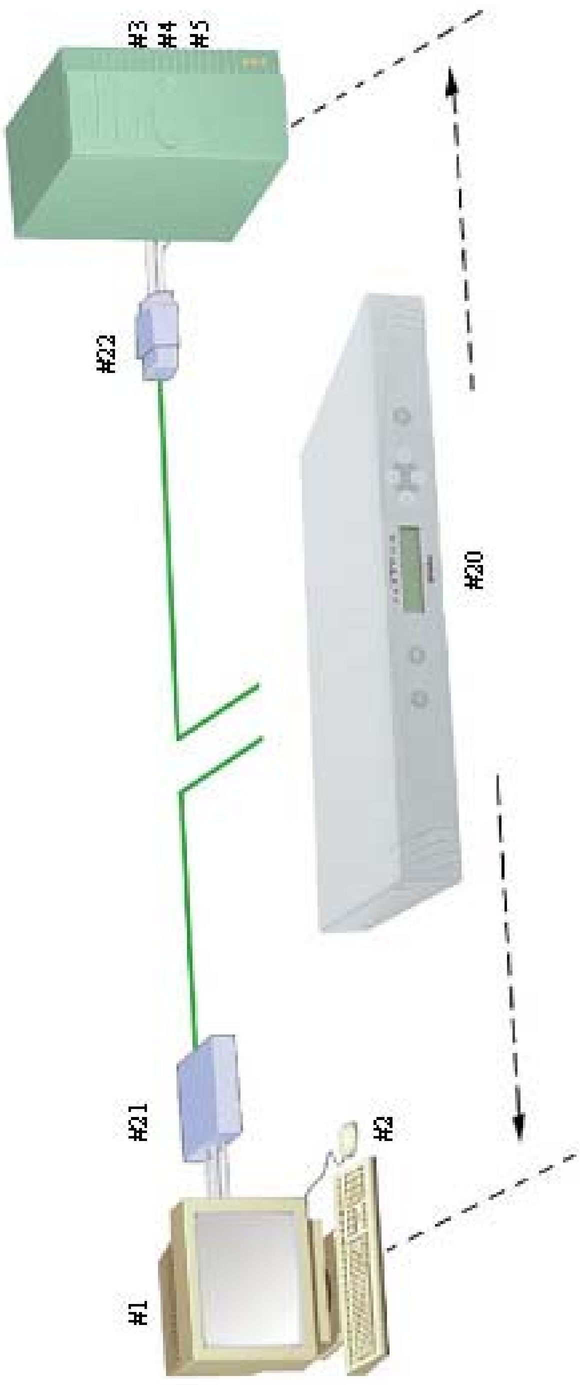

Figure 3. KVM Diagram

Appendix D: Rack Layout Diagram

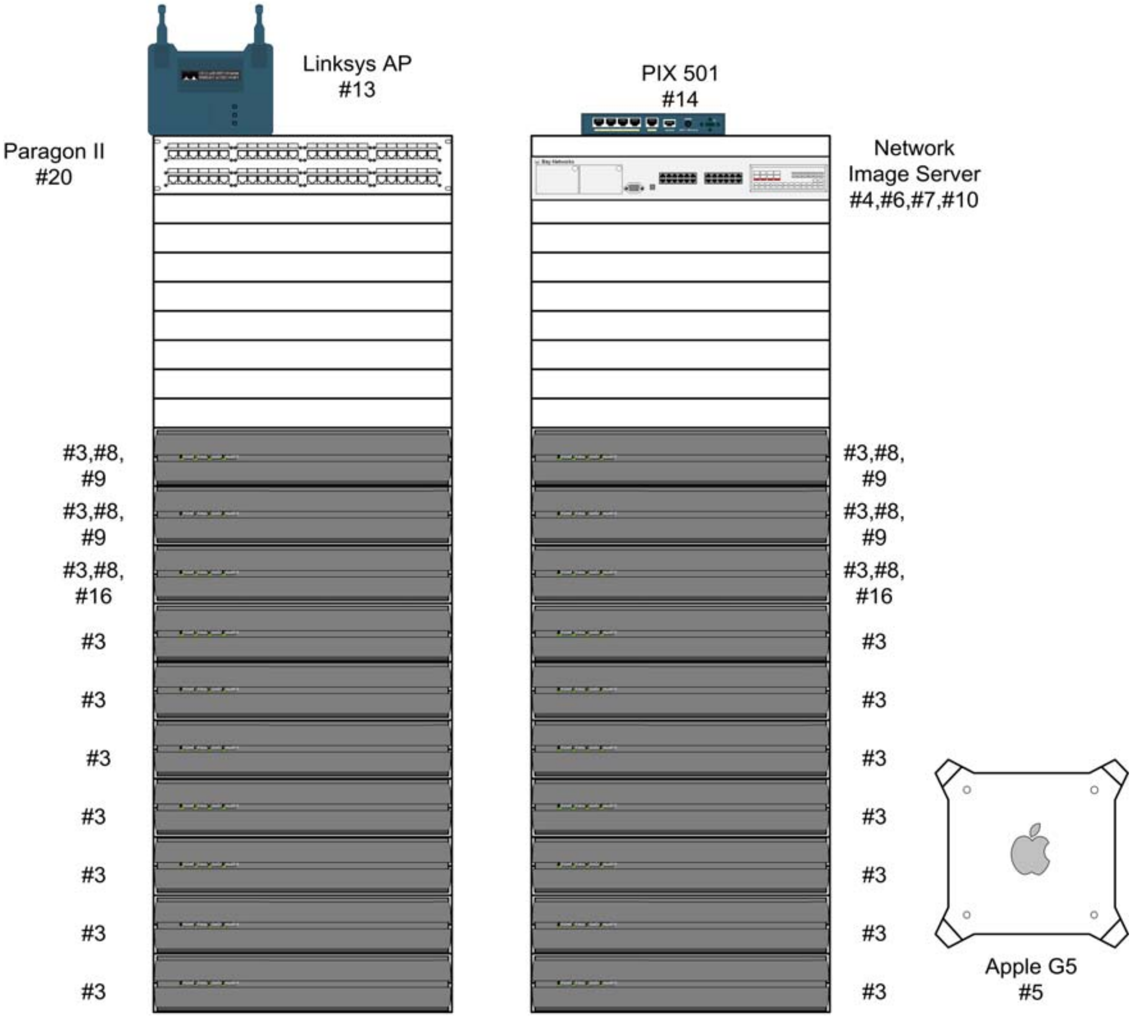

Figure 4. Rack Layout Diagram

Appendix E: Glossary

ACL

An acronym for Access Control List, it is a method of only allowing certain users or computers to access a service or resource (e.g. file, DHCP).

Air-gapped

Air-gapped is a term used to describe a stand-alone network. This is a network that is not connected to any other external network (like the internet). A network would be air-gapped for security reasons, either to keep people out, or keep malicious code (e.g. viruses and worms) from escaping accidentally.

IA

IA stands for information assurance, the area of computer science dedicated to security.

KVM

KVM is an acronym that stands for Keyboard, Video, and Mouse. It is a technology that allows one set of keyboard-monitor-mouse to control many computers by quickly and easily switching between them.

Red-Blue Team

This is a computer security exercise in which one team is actively attacking systems that another team is actively defending.

VLAN

An acronym for Virtual Local Area Network, it is a technology in most upper-end networking gear that allows the separation of computers into their own networks although connected to the same switch. Usually requires level 3 switches or routers to allow traffic to pass between the VLANs.

VPN

An acronym for Virtual Private Network, it is a technology that allows the creation of a private network over public networks using cryptography to secure the traffic between computers.

Appendix F: Equipment List

Equipment list is a spreadsheet in a separate file; it may be attached after this page.