Remotely-Accessible Dynamic Infrastructure for Students to Hack (RADISH)

David Broda  
School of Applied Technology  
Illinois Institute of Technology  
201 East Loop Road  
Wheaton, IL 60189  
+1 (630) 202-9373  
dbroda@hawk.iit.edu

Ben Khodja  
School of Applied Technology  
Illinois Institute of Technology  
201 East Loop Road  
Wheaton, IL 60189  
+1 (630) 815-9149  
bkhodja@hawk.iit.edu

Bill Lidinsky  
School of Applied Technology  
Illinois Institute of Technology  
201 East Loop Road  
Wheaton, IL 60189  
+1 (630) 682-6028  
lidinsky@iit.edu

ABSTRACT

This paper describes a remote teaching desktop infrastructure created for, and used by, the School of Applied Technology (SAT) at Illinois Institute of Technology (IIT). The Remotely-Accessible Dynamic Infrastructure for Students to Hack (RADISH) was developed in 2010 as a replacement for portable hard disk drives (HDDs) that were prepared with several pre-configured virtual machines (VMs) and handed out to students to complete in-class laboratories and home exercises. By attaching these HDDs to computers, students were able to determine information based on the structure of the HDDs. The physical existence aspect of the class was completely eliminated by this new system. Classes became 100% virtualized, and all the physical machines had their virtual correspondent with remote access. The system was designed to be an addition to the class’s computer infrastructure. Over the years RADISH has become the Forensics and Security Laboratory main system, and the class laboratory acts as an addition to RADISH.

This new infrastructure was originally used for the Vulnerability Analysis and Control class. The system transformed tremendously with many improvements made over the past few years which has allowed for the growth of the system and its utilization in other cyber forensics, cyber security, and steganography courses taught at IIT. This new system has eliminated many significant limitations. Students are now able to face real-life situations in the classroom by discovering, analyzing, and gaining control over computer network infrastructure they likely have never seen before. This transformation has not only improved the control and unreliability aspect of the class but has also created a platform to build new analytical skills.

Initially, students accessed RADISH through the use of a Virtual Private Network (VPN) system and a combination of the Microsoft Remote Desktop Connection and Virtual Network Computing (VNC) remote access protocols. Over time, the system’s connection quality was improved by making use of the PC over IP (PCoIP) remote access protocol.

Categories and Subject Descriptors

K.6 Management of Computing and Information Systems – System Management, Centralization/decentralization

General Terms

Security, Management, Reliability, Design

Keywords

Virtual Laboratory, Remote Laboratory, Virtualization, PCoIP, Remote Class, RDP

1. INTRODUCTION

RADISH was designed and developed as part of the Forensics and Security Laboratory (ForSec Lab) at IIT’s SAT by student assistants and their instructors. Students had an opportunity to build and experience a sophisticated computer infrastructure that they would later use in the classrooms. Over the years, an infrastructure that students and instructors could fully rely on was developed and continually improved upon. RADISH allows student class members to have full, unrestricted access to lab resources from any location and from nearly any Internet-connected device. Over time RADISH became the Infrastructure of the ForSec Laboratory due to its uniqueness and reliability. The laboratory applies lots of new technological innovations on daily basics. By creating a laboratory with the latest and advanced technology and software, students become more involved in the classes that use RADISH.

RADISH’s tested reliability and virtual capability meaningfully improves students’ research and lab work since new ideas can usually be tested without difficulty from remote computer devices. Currently RADISH supports three courses per semester as well as multiple student projects. RADISH’s 24/7 access enables students to work on their projects continuously with no logistic concern. Furthermore, RADISH’s remote capability allows for more involved and hands-on online courses because students are able to access their dedicated desktops in ForSec

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGITE/RIIT 2014, October 15–18, 2014, Atlanta, Georgia, USA.  
Copyright 2010 ACM 1-58813-000-0/00010 …$15.00.
library and work in the same setting as students in class. The university is able to meet students’ educational expectation though unlimited access to class laboratories. ForSec laboratory offers an exceptional online school experience that is focused not only on self-study/test basis but also on students’ involvement and in-class performance. Students who take courses online are able to experience a school desktop laboratory infrastructure from any location. Due to centralized computing, online students work at the same location and share the same resources.

2. HARDWARE INFORMATION

The reliability and functionality of the RADISH system are guaranteed by the combination of networking, computing, and storage equipment in use. This is one of the most important parts of the project as it provides outstanding performance and continuous work. The system consists mainly of reliable, enterprise-level components. All the equipment was chosen based on its scalability, performance and reliability. These components have been placed in close proximity to one another in order to improve the speed and reliability of the RADISH system. Therefore future expansion of the system can be done easily and quickly without significant downtime. All of this can boost RADISH’s performance at the equipment level with an exceptional user experience. This is the key to RADISH’s success. Over the course of three years, the system was unavailable for about two days, an uptime of approximately 99%. In addition, the system benefits from a 24/7 support team that is continuously on call. Those two factors are a part of RADISH’s fundamental strategy making it a reliable and trustable system.

2.1 Routers

RADISH is protected from the outside world by a Cisco RV042 Dual WAN VPN router which also acts as a firewall. This router is used to provide Internet access to users by two WAN ports. It is also configured to block all unsolicited requests made from the Internet to ports and services which have not been explicitly configured to be allowed through it. Other than HTTP, HTTPS, and PCoIP, the only services that have been configured to be allowed include the IPSec and PPTP VPN services which are provided by the router itself and used for backup maintenance purposes. The router supports two WAN network interfaces that help ensure continuous and uninterrupted access to the Internet. Additionally, the RADISH system has been equipped with a failover RV042 router for redundancy. Each router is equipped with 100Mbytes WAN interfaces as well as 100Mbytes LAN interfaces that are connected to 1Gbps Layer 2 switches.

2.2 Switch

A Juniper 1Gbps Layer 2, Ethernet switch is the RADISH system’s main connection to the rest of the ForSec Lab. Through the use of VLANs, this managed switch is configured to serve multiple networks alongside the system’s main network. Due to its high management capability, the traffic that passes through this switch can be monitored by an Intrusion Detection System (IDS). This IDS helps monitor RADISH traffic and protect it from unauthorized activity, a feature that is especially important as a variety of forensic and potentially malicious files may flood the RADISH network. Part of the system is to help students recognize and analyze viruses; therefore, their virtual machines on RADISH contain many “controlled” viruses that are spread over the network for analysis and control. For this purpose, switches are configured with virtual networks that help guard the rest of the system. In addition to the server integration, the switch connects computer laboratories accessible by students on a daily basis.

Every system is equipped with two 1Gbps Ethernet ports, one directly connected to the switch and the other dedicated to in-class exercises and projects.

2.3 Servers

Currently, five servers are used by the RADISH system. An IBM System x3690 X5 [2] is the main server that holds 90% of resources needed for classes and can serve hundreds of VMs. In addition, an older HP server acts as backup for the main server and also supports several less powerful VMs. Nevertheless, it can carry the load of the most significant VMs in case of main server failure. This failover feature is one of the most essential schemes of RADISH design. RADISH is designed to operate at least at the minimum level of functionality in case of any server failure. Other servers have minimal use in RADISH infrastructure and can be quickly substituted when needed. One of them is a primary DHCP server that shares about 50% of DHCP needs with the fourth physical server called the secondary DHCP server. Another server is a tower type server with two virtual machines running forensic software licenses such as EnCase (Guidance Software), FTK (AccessData), StegAnalyzer (WetStone) and MATLAB. RADISH servers are located in a separate room to which only administrators and class instructors have access.

2.4 Network Attached Storage

An IBM System Storage DS3512 [3] device is used as RADISH’s storage solution. It is equipped with 12 2TB 7200 RPM 1Gb Serial Attached SCSI (SAS) drives in RAID 10 configuration which gives excellent disk read and write performance and adequate storage capacity. The throughput of the six drives in RAID 0 configuration (part of RAID 10) can be utilized fully by the server through the use of a direct 10Gb SAS connection between the storage device and the server. All of this gives the RADISH system outstanding performance. The network storage supports an average of 200 virtual machines per semester with its maximum capacity of about 500 virtual machines.

3. LOGICAL AND SOFTWARE INFRASTRUCTURE

RADISH is a combination of physical machines and its virtual representatives. All of the virtual machines are divided into groups called “pools.” Each virtual machine is placed into a pool with appropriate resources and tasks. Pool restrictions are used to ensure RADISH performance and prevent server overload. The pool restrictions are based on the class needs and the number of users. The more users required per class, the more resources a pool will need. All pools are named according to their roles. Naming and descriptions are done in a self-explanatory manner so that future administrators can take over the management process without unnecessary pool reference manuals. Figure 6 represents the pool configuration for the RADISH main server.

Figure 6. Logical Infrastructure
3.1 Management Pool
The management pool (labeled “Manage” in Figure 6) contains all machines responsible for major RADISH operations such as:

3.1.1 Microsoft Active Directory
RADISH uses standalone authentication independent from IIT’s Active Directory system. This method of user authentication is used to increase the system’s security and reliability.

3.1.2 VMware vCenter
VMware vCenter is a centralized management point from which RADISH servers and VMs are managed. RADISH uses a single vCenter server with no failover options. If a vCenter server failure occurs, each host previously managed by the vCenter server can be managed individually and directly without the use of a vCenter server.

3.1.3 VMware View Composer
VMware View Composer is a part of the VMware View Horizon Suite [1]. View Composer allows a Network Storage device to store a hundreds of virtual machines by creating one parent virtual disk that can be then used with multiple VMs. This significantly reduces VM storage requirements. View Composer creates an entire fleet of VMs needed for students with one parent virtual disk. Additionally, the same parent machine can be improved over time and used to release or upgrade another set of VMs for different classes.

3.1.4 VMware View Connection
The View Connection Server is tightly integrated with the RADISH system’s Active Directory delivering authenticated users their dedicated desktop environment. Users of RADISH must connect to the View Connection server in order to obtain access to their desktop. The View Connection server acts as an agent delivering a dedicated virtual desktop to its user.

3.1.5 VMware View Security
The View Security Server acts as a safe bridge allowing students and instructors to connect to RADISH remotely from outside the school’s network. It was designed to protect the system from outside disturbances and only allows authorized users to obtain encrypted access to RADISH through the use of HTTPS.

3.1.6 Microsoft SQL Database
This database is used to support the vCenter and Composer servers with database needs.

3.1.7 License Servers
Several software license servers are used to centralize class specific software. Currently, these include FTK and EnCase forensic licenses, WetStone steganalysis licenses and MATLAB licenses. Sufficient licenses exist for concurrent use by multiple students without conflict.

3.1.8 Nagios Pro
The entire RADISH infrastructure is monitored by Nagios, which provides detail-oriented monitoring capability that helps keep RADISH up and running continuously. Nagios successfully prevents RADISH from any downtime or system malfunction. Every machine that is part of RADISH is being monitored 24/7 providing its administrators with detailed network status information and its problems. Nagios is also configured with logical and physical live diagrams that show all the devices in their physical location.

3.2 Administrators and Instructors
The system is managed by administrators who are also acting as a 24/7 support team. For security purposes, Instructor and Administrator roles have the same administrative privileges and share the ForSec Lab pool where every user has his/her own virtual machine. These virtual machines are accessible from any location through the use of the PCoIP and RDP remote access protocols over three different types of VPN. Multiple access points to these strategic machines is a crucial part of the system as it helps to maintain it at any circumstances.

In addition, ForSec Lab pool VMs are used for testing and class design. School staff can create and distribute students’ lab materials such as large capacity disk images for forensic examination or video/mp3 files used for steganography training. All class resources are distributed to students at the same time and speed regardless of the students’ locations. This creates no restriction for online classes and helps them keep up with live classes, which allows for a class to be comprised of online and regularly attending students. Consequently, online students experience the same class involvement as live students. Since students are working at the same remote location (RADISH) they can interact with each other and work on assignments without physically being in the same room.

3.3 Classes and Students
Classes are organized by their course code name such as ITMSxxx where ITMS represents an acronym from the department of Information Technology Management Security, and xxx is the number for the corresponding class number such as 543 - Vulnerability Analysis and Control. Class pools contain students’ VMs. Students have access only to dedicated VMs located at the class pool they are entitled to access. When a student requires access to use multiple VMs, he/she is assigned a personal sub-pool named with his/her username, which is placed under the main class pool. This solution provides more control over the user’s resources and his/her usage. All RADISH machines are carefully monitored by Nagios monitoring system and RADISH intrusion detection system.

3.4 Public
The Public pool is used for all machines with routable IP addresses and is a sub-pool of the Management pool. However, RADISH currently uses only 3 routable IP addresses where two addresses are assigned to the router and the third address is being used by VMware View Security.

4. NETWORKING
RADISH uses an average of 30 virtual computer networks per semester. All of them are divided into three categories: main, students, and public.

4.1 VM Network
The VM Network is the largest private network used for internal communication between the RADISH VMs and physical machines located inside the ForSec Lab. This is a primary and default network for all new devices inside the laboratories. The VM network is served by two DHCP servers and RADISH runs over the user’s resources and his/her usage. All RADISH machines are carefully monitored by Nagios monitoring system and RADISH intrusion detection system.

4.2 Students’ Networks
Students’ virtual networks are separated from all other virtual networks. Every student has a dedicated virtual network which he/she can use within a personal pool. Separate virtual networks
help students perform different kinds of vulnerability tests and analysis. This separation guarantees students’ precision in examination and future improvements.

5. SECURITY
RADISH puts an emphasis on its security because the system involves a large number of students every semester. At the Forensic and Security laboratories students have to deal with a variety of viruses or other software vulnerabilities as a part of class assignments. Other class requirements consist of experimenting with different kinds of hardware. Therefore, RADISH is equipped with a variety of security appliances that help keep it safe from its users.

5.1 vLANS
For security and reliability every student is provided with his/her own isolated vLAN where he/she can do a variety of network penetration tests using a range of tools. Students’ vLANs are purposely designed not secure to be used by students for their individual projects without any consequences of compromising a secure network. Unfortunately, RADISH’s main network sometimes experiences unwanted network intrusions when students unintentionally bypass their personal virtual networks. Consequently, VM network is highly monitored to prevent from intentional or unintentional malicious activity.

5.2 Intrusion Detection System (IDS)
An IDS is used to monitor and prevent the system from all network malicious activity. As mentioned in section 5.1 RADISH is experiencing a big number of internal unwanted network activities. Most of those activities are stopped before they have any effect on the main network.

5.3 Authentication
As mentioned in section 3.1.1 RADISH uses its standalone Active Directory authentication method. This protects its users from any disturbances of third party providers such as school global authentication mechanism.

5.4 Monitoring
The entire infrastructure is detail monitored by Nagios. All hosts and their services are being monitored 24/7. This helps RADISH achieve excellent reliability at 99%. Any monitoring alarm generates a notification action that helps its administrators resolve any issues within minutes, so end users can continue their work with minimal or no interruption.

5.1 Failover
Reliability is also ensured by duplicating the system’s core servers. Having failover servers on the infrastructure protects RADISH’s functionality from its servers’ failure. This commonly used enterprise solution helps administrators keep users connected with no interruption. This security feature improves class efficiency and creates an environment where RADISH’s end users are unaware that maintenance is being performed. Users and their instructors can fully rely on their machines with no worries of upcoming maintenance procedures that can limit them access to their work.

6. FUTURE WORK
There are several courses in the security and forensic technology area that are not yet supported. In some cases, such as forensic imaging with write blockers, virtualization has not been possible yet. Also some viruses and denial of service attacks cannot be virtually implemented. Our goal is to work toward supporting courses where issues are overcome. IIT serves students located in other continents. RADISH has the potential for use by these students because all interaction between virtual machines is local to virtual networks on RADISH; external networks are not involved.

7. References