REMOTE PROTOCOLS AND SECURITY (REPAS) LABORATORY AND ITS APPLICATIONS

Fatih Alagöz
e-mail: alagoz@gwu.edu
Harran University, Chairman, Department of Electrical Engineering, Sanliurfa, Turkey

Robert Daniel
e-mail: rqdaniel@seas.gwu.edu
George Washington University, School of Engineering and Applied Science, Washington D.C., USA

Alina Koos
e-mail: akoos@verisign.com
Member IEEE
Washington, D.C., USA

Key words: Distance learning, telecommunications, security, protocols

ABSTRACT

This paper discusses the use of the Remote Security and Protocols Laboratory (REPAS) in a telecommunication protocols class as well as a telecommunication security class. The REPAS Lab allows researchers and graduate level students to study, analyze, test and debug different types of protocols and security approaches. This allows the class to focus on applications of lectured topics, emphasizing hands-on projects. The class is divided into teams where each team has a dedicated server in the REPAS lab with full administrator privileges. The REPAS lab gives the students remote access to their server, while protecting the outside networks. Implementing protocols requires kernel modifications and as such, LINUX on an Intel platform is chosen since the source code is freely available for any OS modifications. It will be shown that the REPAS Lab makes it possible to conduct a distance-learning class over large distances, between locations as far apart as George Washington University in Washington, D.C., in the United states and Harran University in Sanliurfa, Turkey.

I. INTRODUCTION

Need for Hands-on Projects

Protocols being developed within the IETF benefit from an implementation as a proof-of-concept before Request For Comment (RFC) documents become accepted in any forum. In academia, security theory covered in lectures cannot be experienced by the student without hands-on assignments. These assignments help students understand the severity and implications of the possible security infringements, as well as the importance of appropriate level of security implementation. In addition, students experience performance and verify calculations implied by overhead of security protocols.

Need for a Laboratory

Although the university has a computer lab available to classes and students, it falls short regarding proper isolation, support, access and flexibility needed for learning.

The REPAS Laboratory requires contained chaos. The design and management of the lab needs to strike a balance between full system access and total network isolation. The lab needs Internet access since a large portion of the required drivers, programs, software patches, upgrades, and resources are on-line. Communication with developers of the on-line resources via message boards, chat rooms and email is also critical.

At the same time, network isolation is required to enable full ownership and administrative privileges of the network and individual servers. More importantly, the need for isolation is critical to protect the student's research from outside attackers as well as outside networks from run-away student experiments.

Need for REPAS Laboratory

The student body of more and more graduate-level classes consist of mature students that are undertaking part-time studies, have full-time employment and spend a significant amount of time commuting to a university location. As such, they require remote 24-hour access for laboratory work, as well as the support and infrastructure implied by such a lab.

In addition, the full-time students that have not yet garnered working experience, have an opportunity to

experience real-world problems from the support of their more experienced teammates.

Need for REPAS Laboratory Isolation
The REPAS Lab provides a one-way function in a security sense. It is easy for the students and researchers to do work on the REPAS Lab, but hard for their experimentations, such as attacks, to get out of the Lab network.

The new state-of-the-art protocols and bleeding edge security mechanisms actively studied may have unintended security holes that compromise network security, or other bugs that affect the entire network, such as crashing or thrashing the network. The REPAS Lab one-way function is an essential feature when studying these new protocols and security mechanisms.

Need administrative support for REPAS Lab
Proper implementation of security and protocols requires kernel modifications. Therefore, students needed full administrative access. Traditionally, system administrators do not allow kernel modification on a live network, let alone super-user access. This however, this is a major hindrance to the implementation freely available source code for any OS modifications. The REPAS Lab gives super-user access to individual students, while proving administrative support in the event of server or network crashes. Student super-user access is limited to the REPAS Lab, but not the firewall isolating the network from the Internet. For proper support, the REPAS Lab administrator requires notification for changes to root passwords.

Given the remote access requirements as well as the implementation of open source software and COTS hardware, outsourced administrative support and the operation and maintenance of the Lab may be ideal. Since the inception of the REPAS Lab, the instructor was the REPAS Lab administrator.

Administrative and project-related support of the instructor is available real-time and interactively for guidance on usage of tool sets as well as topical questions on the projects. The support was given using several applications.

Need for applications that enable distance learning
The tools enabling real-time and Internet accessible communications are critical to learning the materials outlined in the class syllabus within the REPAS Lab environment. Such tools may include multimedia applications or communication methods such as instant messaging and team webboards

Since the entire class was using compatible instant messenger applications, online students could communicate with each other and the instructor, while the instructor was supervising their overall activities. IM allows the flexibility of providing support and supervision, while allowing unfettered online intra-class interaction.

Policy, mathematics, and hacking
The constant adjustment to the balance between security policy, mathematics and hacking makes up the fabric of the REPAS Lab.

Security policy follows laws that are being revised constantly with changing technologies as well as security methods. Since the REPAS Lab is used across political boundaries, knowledge of the local laws is required. Specifically, export laws of cryptography systems need to be adhered to. Security policy is changing faster than the Internet and therefore requires constant reading. The REPAS website maintains up-to-date links relating to policy topics. There is self-interest in keeping up with security policies. The instructor and students need to read the fine print of online notices, since they do not want to find themselves in the position of not being able to publish their work because of an online agreement that they have inadvertently agreed to.

Mathematics is an integral part of security. The students are taught how to code mathematical algorithms and how to analyze code for weaknesses. As such, students need to gain the skill of reading code to check for weakness and incorporate that skill into their projects. OpenSSL libraries are resources used in teaching cryptographic algorithms. It is helpful to join the online development email systems for both code and security alterations.

Students in this class do not necessarily have extensive experience in system administration or programming. Therefore they hack – with a basic understanding of the tools available to them, they implement, mostly through trail and error, security and protocols. Hacking in this sense is the component for the online class and also the most time consuming. There are daily upgrades to patches, as well as interoperability problems between different types of software applications and the different LINUX distributions. These issues are in addition to the work required to reassemble servers and configurations after or during an attack from another team.

Requirements for REPAS Laboratory
This Graduate level class was designed to have minimal academic requirements. Graduate students of all levels are allowed in the class since the required skills are hard to acquire in a structured class or working environment. It is suggested that students successfully complete the protocols class before the security class. However, students that don't have an UNIX, mathematics, and programming background are warned that they may have to dedicate more time than students with some of the background. In general, students of all skill levels are

looking forward to being given full access to their own machines on the network. Some students find that because of the fun, war-game atmosphere of the class, they are dedicating more time to the class than anticipated.

The one true requirement for this class is access to a computer that has a continuous Internet connection with Secure Shell. As noted earlier, the class is in effect online 24x7 and network attacks on team systems may happen anytime of the day. Given individual students' work and familial commitments, students take time when available to do class work, i.e. crack passwords and sniffing information about the other teams.

...

II. PROJECTS

Team makeup and interaction

The teams are determined through self-selection with intervention from the instructor when appropriate. This method encourages a sense of healthy competition between the teams as well as team responsibility. Teams help each other via the class webboard and team members come to each other's aid on team webboards and through instant messaging, when schedules permit. Help comes in different forms, but mainly as guidance on where patches can be found or where fixes to the kernel are available. Also, there is some prestige of being the first to post an answer.

Some teams meet at the university in a university computer lab with team member that not available in person accessing the REPAS Lab from home. After each project the teams are required to submit a team report and an individual report, and give a 5-minute summary of their experiences. Some projects are team assignments as well as individual assignments.

Team Projects

The projects required for the protocols class have a different style than those required by the security class.

In the protocols class the each team chooses different protocols to research, simulate and implement on the REPAS Lab network. The team is given the whole Lab to accomplish this task. At the end of the semester each team is required to teach a class on their protocol and give an online assignment pertaining that protocol. To capture the knowledge of the learning examples of the protocols covered, a CD with all working examples of all protocols studied is distributed to the students. Protocols chosen by teams as subjects include Mobile Agents using IBM's Aglets, Peer-to-Peer Networks using Jabber Instant Messenger System

In the security class the projects have relatively vague descriptions to allow the team's creativity to add to the project's design, implementation and troubleshooting. The teams are given the same project description. The teams are given administrative guidance and the resources of the Lab. The help available does not include project-related support. The Lab administrator supports the teams' needs of physical modifications to the topology of the network. The instructor is a silent partner on each team and is aware of the teams' activities. Grades are based on creative team collaboration as well as degree of difficulty and their success or failure. Examples of projects topics are malicious codes, sniffers and scanners, computer security, and building a VPN network.

Individual assignments

While team projects are new topics, individual assignments are designed to emphasize the basic principles and theories discussed in class. The instructor monitors these assignments for individual student progress and grasp of the topic. The student will do the assignments using the REPAS network.

The protocols class assignments emphasize throughput and latency measurements based on link-to-link and end-to-end measurements. These metrics are critical for evaluating several protocols as they relate to performance and scalability.[2]

The security class assignments concentrate on how to implement a system with a given security service requirement. The assignments emphasize requirements regarding confidentiality, integrity, availability, authentication, accountability access control.[1]

...

III. SYSTEM DESCRIPTION

To meet the minimal requirements for a REPAS Lab, at least two machines and a network connecting them are required. This configuration is depicted in Figure 1.

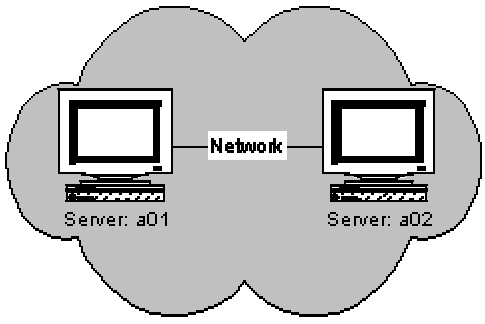

Figure 1. Simple Network

To enable the machines to communicate, two networking approaches were implemented. The configuration of Figure 1 can be implemented in several different ways. The REPAS Lab used two methods for interconnection.

One implementation consisted of Ethernet cards and a switch or a hub, while the second used point-to-point connections. Using both methods enables a scalable implementation of the REPAS Lab. Although only two machines may be needed for client/server work, implementation of routing protocols or IPSec would require at a minimum five machines.

Connecting the REPAS lab to the Internet requires a firewall and an Internet connection as seen in Figure 2.

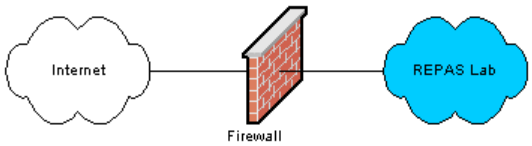

Figure 2. The REPAS Lab

The Firewall software for the LINUX operating system includes applications such as ipchains and iptables.

Now the REPAS lab is connected to the Internet and remote users can start developing on the network. Figure 3 shows the REPAS lab with desired users including students, researches, and guests. Connecting to the Internet may bring undesired users such as crackers.

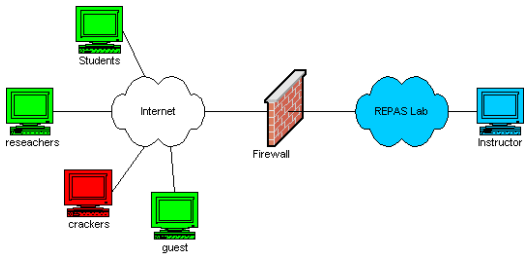

Figure 3. The REPAS Lab with users

The firewall adds flexibility to the REPAS lab. And we can visit the two extreme scenarios. The firewall could be a brick wall filter by not allowing any entity to enter or leave the network. This would completely isolate the lab, disallowing remote access, and the user of the network would have to be physically located with the equipment. The other extreme is essentially turning off the firewall such that every machine in the REPAS Lab is connected straight to the Internet. The firewall may be configured to allow communication with security anywhere between the two extremes mentioned. Thus when just starting with the implementation of a security protocol such as IPsec, the initial configuration would be a strict one, but still allowing remote access. As testing progresses and the confidence level increases, external VPN connections to the internal RESAP lab may be allowed. The next section discusses examples from the classes including required adaptations of the REPAS Lab network.

...

IV. LAB TOPOLOGIES AND FIREWALL SETTINGS

Case study I: The REPAS Lab and attack software.

The class used the REPAS Lab to test the network and servers under various network attacks and defense mechanisms. Each team's goal is to attack other servers while defending their own. Figure 4 shows the REPAS Lab network with six servers, one server per team. Each team has super user access to their server. Team01 server is therefore a01.

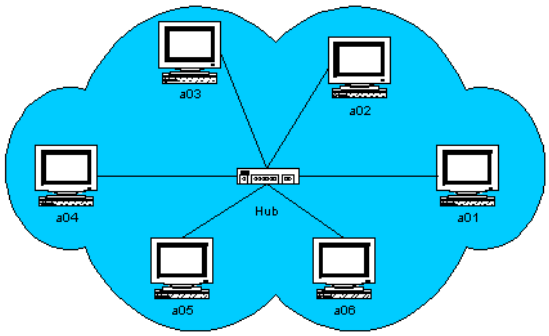

Figure 4. LAN using 10/100 MB Ethernet Hub

All machines are connected using a 10/100 MB Ethernet Hub. To connect to their servers, the students need to first secure shell to the firewall machine and then connect to their servers to install their intrusion detection software, malicious code, port scanner and packet sniffers. Each team invokes various attacks on each other, and at times teams may joined together to do IP spoofing.

Case study II: Using Mobile Agents routing protocols

Studying routing protocols required changing the REPAS Lab network form a Local Area Network (LAN) to a Wide Area Network (WAN) by transforming the host machine into routers and connecting them using the point-to-point connections, as in Figure 5.

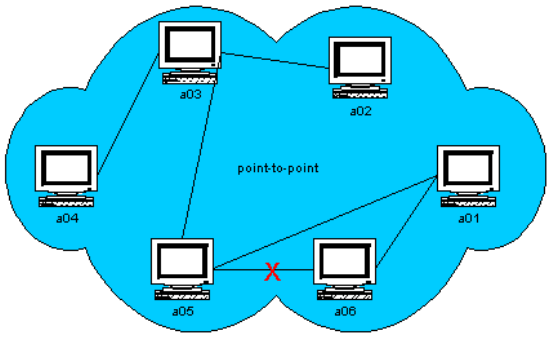

Figure 5: WAN using point-to-point

As in Figure 5, the network is setup as a WAN to test OSPF and RIP. It is possible to remotely bring up and down links as needed, to test the protocols ability to adapt to the new network topology. This testing requires total class cooperation because if a05 kills the link to a03 the three servers above are disconnected from the network

and form an isolated network with no possibility of reconnecting to the network. The administrator may have a mechanism in place to safeguard against such eventualities. Implications would be much harsher if the servers are in geographically dispersed locations. Reconnecting the servers may be a long trip away.

Mobile Agents are used to generate traffic in this network, as well as to collect network data on under various loads. The mobile agents are configured to jump from machine to machine using different patterns.

For example, a mobile agent may be configured to travel from node a03 to node a06. Assuming all links have equal costs of one, the shortest path would be a03-a05-a06. The Mobile Agent logs time and locations as it travels across the WAN. If to test the routing protocol, the link between a05 and a06 is disconnected, the Mobile Agent can no longer find its route for a03 to a06 and will stay at its current location until the routing tables are updated.

Case study III: Mobile Agents and VPN networks
To test the Mobile Agent routing protocol in a more realistic WAN environment, which would have a larger number of nodes as well as latency issues, students implement VPNs from their remote locations. Figure 6 illustrates the new configuration.

The VPN implementation introduces latency into the REPAS Lab that inherently does not have latency, since all servers are at the same geographic location. This implementation also increases the number of nodes by a factor of six. Implementing VPNs from remote locations also redefines the REPAS Lab such as to include these remote locations.

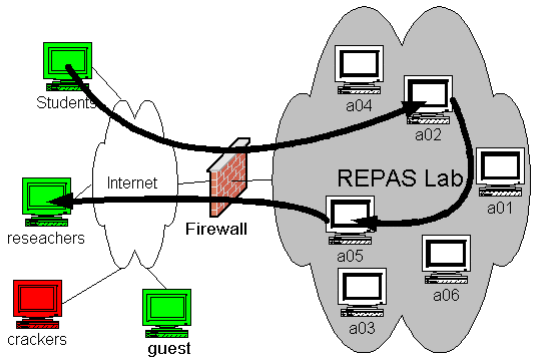

Figure 6. Mobile Agents in a VPN environment

...

V. FUTURE STUDIES

The next topic of research will apply the REPAS Lab to a distance-learning course taught at the University of Harran, Sanliurfa, Turkey. This study will include observations of the performance and functionality of the network across very large area network.

...

VI. CONCLUSION

It has been shown that the Remote Protocols and Security (REPAS) Laboratory fills a critical gap in today's university operated computer facilities. On the one hand, universities are furiously advancing with wireless access to online course registration, while on the other hand they seem to regress by limiting scope and access to computer research facilities that used to provide 24x7 student access to much more comprehensive computer systems. The REPAS Lab offers the proper and stimulating environment to allow students and researchers to do their work with as much ease and confidence as online banking.

The REPAS Lab is easily adapted to meet various needs for different environments and topologies, which are a must in protocol and security studies. As such, the REPAS Lab lends itself to distance-learning programs, as well as university-independent operation and maintenance.

By using the REPAS Lab model presented in this paper, universities could completely outsource their research facilitates and avoid the costs of administration and maintenance, while providing the remote access needed by a growingly mobile and time-constrained student body.

REFERENCES

1. Larry L. Peterson and Bruce S. Davie, "Computer Networks: A Systems approach Second Edition", Morgan Kaufmann, 2000
2. William Stallings, "Cryptography and Network Security Principles and Practice", Second Edition, Prentice Hall, New Jersey, 1999.
3. Internet Engineering Task Force (IETF) www.ietf.org
4. Internet Assigned Number Authority (IANA) www.iana.org
5. GNU Not Unix (GNU) www.gnu.org/software/
6. Shift from Protocol to Agents, Bill Joy, Sun Microsystems