Experiences in Building a Multi-University Testbed for Research in Multimedia Communications

Ram Dantu
Network Security Laboratory
Department of Computer Science & Engineering
University of North Texas
Denton, Texas 76203 USA
rdantu@unt.edu

Henning Schulzrinne
Department of Computer Science
Columbia University
New York, New York 10027, USA
hgs@cs.columbia.edu

Paul Sroufe
Network Security Laboratory
Department of Computer Science & Engineering
University of North Texas
Denton, Texas 76203 USA
prs0010@unt.edu

Abstract

The next generation Internet needs to support multimedia services such as Voice/Video over IP (VoIP) and IP-based television (IPTV) and media distribution. The goal of the project is to develop a testbed for understanding and analysis of vulnerabilities of IP-based multimedia networks. This is a collaborative project between University of North Texas, Columbia University, Purdue University, and University of California at Davis. This project was awarded in 2006 and in one year, we have developed a multi-university testbed with variety of PBX solutions including Asterisk, a multitude of voice and video IP phones, and multiple universities were connected through a secure VPN and Internet2.

As with any endeavor, we have many unique experiences and issues, which sometimes cause setbacks. We have dealt with issues concerning interoperability between phones and servers, Network Address Translation (NAT) connectivity issues, and many other collaboration issues concerning people and technology. An interworking of students from multiple universities, faculty, system administrators and support personnel has brought the testbed resources together for a working environment. In this paper we described our progress and experiences in more detail and how to fulfill our mission statement while supporting the various collaborative efforts involved with this project. In addition, we described the current research activities based on the testbed. Finally we described the next steps in the testbed development.

1. Introduction

IP-based multimedia such as Voice over IP (VoIP) and IP Television (IPTV) is being deployed aggressively in the telecommunications market. As this technology penetrates worldwide markets, advancements in performance, cost reduction, and feature support make VoIP a compelling proposition for service providers, equipment manufacturers, and end users alike. It is estimated that in a few years most enterprises and residences will be transitioning from circuit-switched to VoIP services. Such trends will result in what we can call *IP-based multimedia communications infrastructure*, encompassing the equivalent of conventional phone conversations, advanced communication and content distribution services.

In light of this growing interest, security in voice communications is evolving into a key requirement for VoIP solutions. Packet-based communication is particularly vulnerable to security risks including voice "tapping" by sniffing packets, unpaid service usage by falsification of network ID, and service disruption by packet manipulation. Because of the increased penetration of the new services, IP-based multimedia communication services will become *a critical infrastructure* for which high assurance security is crucial.

Although academic and commercial labs have been conducting studies on the security of next generation networks and VoIP, and these studies have offered fruitful preliminary results in understanding the threats and vulnerabilities, but the size and scope have been limited to the available resources at the respective labs. The goal of this *testbed* is conducting research, development, and testing of inter-domain security and QoS mechanisms for new services such as voice, multimedia, video, and 911 emergency services.

2. Research Activities

2.1. Preventing voice spamming

VoIP introduces a whole new set of problems for the network operators and service providers. We believe that one of the biggest risks with VoIP is its

978-1-4244-1694-3/08/$25.00 ©2008 IEEE

vulnerability to spamming attacks. The Internet is wide open for tapping and intrusion. In theory, anyone who can locate an IP phone via scanning the Internet, can call in, and with the cost of an Internet call near zero, this kind of vulnerability invites voice spamming. *The problem of spam in VoIP networks has to be solved in real time compared to e-mail systems. Compare receiving an e-mail spam at 2:00 AM that sits in the Inbox until you open it next day morning to receiving a junk voice call at the same time. Moreover, many of the techniques devised for e-mail spam detection rely upon content analysis. The same with VoIP calls is already late.*

2.2. VoIP Bots Development

With the advent of VoIP an user can always easily and cheaply be in touch with his community. As the scope of the VoIP deployment is growing as is the amount of security exploits being targeted at them. In order to design the defense mechanisms, we need suitable traffic generators based on VoIP *Bots*. VoIP *Bots* can exploit current and the future VoIP Networks. The *Bot's* are coded using the *reSIProcate* SIP Stack [7] and GNU-ccRTP RTP [6] Stack for sending out spam messages. *ReSIProcate* module consists of a protocol stack and collection of applications like the SIP Proxy Server and SIP Registration Server. We used *reSIProcate* Stack because it has a footprint of less than 1MB and is highly portable. The *Bot* module uses both the SIP and RTP stack's to mount attacks on the other SIP clients that are found on the network. This work can also be extended to exploit virtually any SIP client on the internet and spam them. Our project primarily deals with the types and methods of such an attack for maximum impact. We will be using API's from both *reSIProcate* for making a VoIP calls and *ccRTP* API's for handling the RTP data. It is also possible using the *Bots* to connect to a central 911 center and create Denial of Service (DoS). Therefore, a single *Bot* with multiple instances can literally saturate the link and fool the Proxy Servers to connect back the 911 servers.

The purpose is to research various VoIP spam filters and their performance in terms of false alarms, and conduct a sensitivity analysis of various parameters. VoIP Spam Algorithms VoIP spam differs from e-mail spam in that no real content analysis can be done from a call that hasn't taken place yet. E-mail spam can easily be checked for certain words or phrases, but VoIP spam needs a different algorithm to stop spam before the telephone rings. To meet this goal, we developed a five-stage process for determining whether an incoming call is spam. These stages include multivariable Bayesian analysis for computing and updating trust, and Bayesian Networks for inferring reputation. The results from each stage are fed back for collaboration between processes. [1]

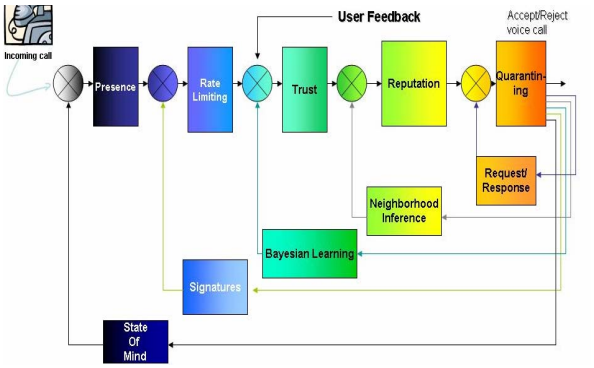

Figure 1: Feedback loop for detecting spam in VoIP calls.

2.3. Quality of Service (QoS) and security mechanisms

As multimedia services are real-time, it is important to ensure that the deployed security mechanisms do not impact the quality of service (QoS) of a session when the system is not under attack, while ensuring the QoS is maintained at an acceptable level when the system is under attack. The purpose of this research is to study the scalability (several thousands of sessions) of security mechanisms in terms of quality of service and performance degradation of the session.

2.4. Social Technical Issues of Video Phones (Security and Privacy)

Videophones, like other technologies, possess the potential for misuse. For instance, video phones may be abused for financial gain or as a way of conducting industrial espionage. Just as email, other Internet enterprises have become vehicles for criminal behavior, videophone services may offer the similar opportunities. Issues of compromise of privacy, security of residences, video phishing, identity theft and secured communications are included areas of research.

2.5. Video Phones for the Deaf and Hearing Impaired

Video Phones for the Deaf: Not all 911 or E911 operators will be able to communicate with the deaf,

for those who can't, we propose to develop protocol enhancements for video emergency calling, using our video development platform from *Wintech* Digital with all the latest hardware and software. [2] NG9-1-1 can make use of real time instant text messaging not currently supported in 911 centers. However, video phones offer a clear advantage to text messaging. We will be using the existing API's for video phones such as, pre-recorded audio and video playback, SIP instant text messaging, and facial movement recognition, to develop a more extensive library for others to use. [2] These enhancements include a button for conveying SOS (emergency) messages, recorded video playback for the deaf to understand, and other API's for SIP dialogs using video phones.

2.6. Video Phone Development Platform (VDP)

We are currently developing new library's and API functions for use in modern video phones. These functions will impact generally the NG911 research. The source development kit that we have is armed with a host of generic video API's. These API's include advanced audio and video stream control, including recording and playback of recorded and pre-recorded streams, full SIP message control, and facial and movement recognition. The platform uses the TI Davinci video chipset connected to an ARM9 core processor. The new API's will help people communicate with the deaf through various video playback and screen text scrolling options. We will be developing a set of 30 video clips in the American Sign Language (ASL). Sample questions including asking the disabled person to send pictures of his location, such as highway signs. Also, we will be developing measurement techniques for the performance of converged text, audio and video between the callers and E 911 operators. We plan to add additional messages to the session initiation protocol (SIP) to support the new API's for the deaf. [2]

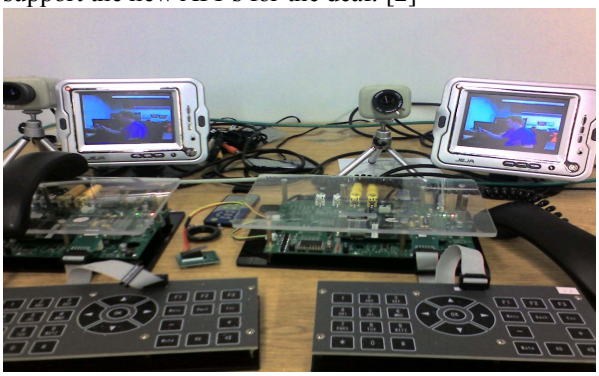

Figure 2: photo of VDP platform

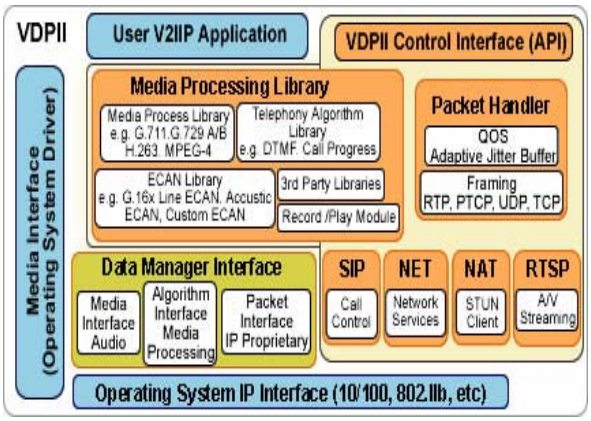

Figure 3: VDP architecture diagram

2.7. Testbed Layout

Our testbed is a multi-university collaboration. The University of North Texas (UNT), Purdue, and Columbia University are currently connected through a series of Cisco virtual private network (VPN) routers with local addressing schemes. (U.C. Davis is on course to join the group in the coming months.) This network allows for easy setup and execution of multiple development and research ideas.

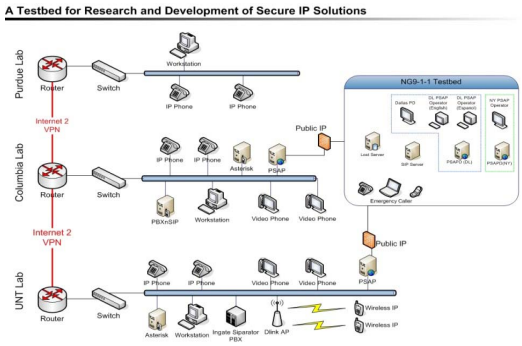

Figure 4: Basic diagram of the multi-university network scheme.

At the network security lab (NSL) in UNT we have several kinds equipment including public and private voice and video phone setups, voice spam test system using a modified reSIProcate session initiation protocol (SIP) stack, and a cross university VoIP calling system. The NSL lab is also supporting three graduate students including a recently graduated Ph.D. student who developed an algorithm for detecting spam in VoIP networks. There are two networks in the VoIP lab at UNT; the CRI testbed network and UNT's local area network (LAN). The video phones connected to the CRI network have public IP addresses. They serve as communication link between offices, labs, and homes

for the UNT personnel. The CRI network handles the other VoIP devices. A four digit numbering scheme was adopted to identify where a phone was calling from, denoted by 1--- is UNT' calling code, 2--- for Purdue, and 3--- for Columbia. Assignments of the individual UNT phones were also patterned. 0-49 are local test devices. 50's are video phones on the public network, and 100 and 101 are the two WiFi phones that we have.

3. System Integration Issues

To setup a working testbed takes time, people, and money. Also, in creating a working lab with multiple universities, hardware and software has a large list of issues and experiences which we will discuss. In the initial stage of the development, we had to acquire the equipment necessary for the different sites (i.e. VPN routes, IP phones, network infrastructure.) Many people, external to the project, were also needed to help create the testbed, including system administrators, IT employees and lab managers.

3.1. Test Bed Development

Some of the initial concerns we encountered were with deploying a multi-site environment and finding compatible equipment for interoperability. To develop a real-life multi-university network for VoIP, a software Private Branch Exchange (PBX) needed to be chosen. There are a variety of hardware and software solutions including Ingate SIParator (hardware), SIP foundry's *reSIProcate* (software) [7], PBXnSIP (software) [4], and Asterisk (software) [3] which we will be working with. To work as the main PBX for the testbed it would need to have video support, PBX trunking, NAT traversal, and custom dial plans. *PBXnSIP* comes with a web interface. However, it does not support video devices and did not have any techniques for supporting NAT traversal. The Ingate SIParator supports video and also supports IP phones behind a NAT. The SIParator is one of the most picky hardware devices when it comes to registering phones and routing SIP messages. Asterisk, on the other hand, was very easy to install and setup. It handles a variety of VoIP configurations, supports video devices (as well as the latest video codec H.264), and handles NAT traversal natively. Asterisk also comes with a SIP debug tool which was instrumental in setting up and configuring the network. We have also employed the use of SIP Foundry's *reSIProcate*. This PBX has a customizable SIP stack which is used for research in SPAM, DOS, and Bot related areas.

The next issue we encountered when working with NAT's is Real-time Transport Protocol (RTP) routing. An RTP port is, more often than not, randomly chosen from a high port range. This information stream is separate from the SIP signaling and will usually get blocked at the NAT entrance. A port and range of ports will need to be open to the IP device to allow of data connectivity (i.e. so you can hear/see the person despite the phone ringing). For example, our video phone connected remotely to UNT has a STUN client enabled and a chosen set of ports forwarded, through the remote firewall, for RTP video streams [5]. Our PBX server is configured to limit the range that a random RTP port could be selected. This allowed for an easier configuration of the remote firewall so that both RTP and SIP can pass through without opening the entire firewall to the remote device. This configuration is for a single phone to operate behind the remote NAT. Another issue we are currently working is to make a remote call to a CRI networked device through the PBX (connected to both networks through VPN). The SIP signaling is working correctly but are experiencing one-way and no-way calling. This is believed to be another NAT issue.

Once the network infrastructure was in place and the IP solutions were connected and working, interoperability will become then next major concern. As with any technology at the birth of its existence, not all devices will 'talk' to each other (or much less like each other). The CRI network has a large variety of VoIP equipment from different manufacturers. The PBX solutions posed the greatest portion of the interoperability concerns. IP devices use different identification methods such as username as the phone number and username is separate from the phone number. Asterisk was configured to allow either number or username authentications and a corresponding dial plan was created to handle the network. Once they are registered and able to make calls, SIP signaling is usually not a concern, however correct RTP establishment can be very moody.

4. Conclusion

Developing a testbed involves many procedures; multi-site issues concerning cooperative collaboration, interoperability between hardware and software, network address translation (NAT) issues involving remotely connected devices talking to inter-network devices, and research collaboration on several topics. We have developed a multi-university testing environment, which includes several different VoIP enabled hardware modules, and a VoIP call processing

system, which links the universities. We are also using Wintech Video Phone Development Kit to produce NG9-1-1 API's and to examine the socio-technical issues that come with video phones. In addition, we have a VoIP spam *Bot* to generate larger scale attacks for analysis and data gathering in spam research. This project has provided us with invaluable experience relating to VoIP and collaborative efforts. In addition, this project provided ideal setup for students and professors to research the fields relating to VoIP, including spam, denial of service and quality of service.

5. References

[1] R. Dantu, and P. Kolan, "Detecting Spam in VoIP Networks," *in Proc. of the Steps toReducing Unwanted Traffic on the Internet Workshop,* pp. 31-37, Cambridge, MA, July 2005.

[2] G. Gu, Wintech Digital Systems Technology Corp ,"Videophone Development Platform II Programmer Guide," May 2007, http://www.wintechdigital.com

[3] J. V. Meggelen, L. Madsen, and J. Smith, "Asterisk: The Future of Telephony," O'Reilly Media, Inc. 2005, 2007 pp. 37-144.

[4] pbxnsip Inc., "SIP-PBX User Manual" http://www.pbxnsip.com/documents, 2008.

[5] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," IETF-DRAFT rfc3489.txt, March 2003.

[6] GNU ccRTP Project, Available at: http://www.gnu.org/software/ccrtp/

[7] ReSIProcate Project, Available at: http://www.resiprocate.org/