THE UNIVERSITY OF CALIFORNIA, DAVIS

PROPOSAL

Analyzing Voice-over-IP at UC Davis

Abdulhai Naqvi
(Hardware & Programming)
abdulhainaqvi@ucdavis.edu

Dixit Paudel
(Hardware & Programming)
meondav@ucdavis.edu

Mark Weber
(Organization & Programming)
marweber@ucdavis.edu

supervised by
Professor Matt BISHOP

with support of
Mark Redican

This project will analyze threats to privacy and security of Voice-over-IP (VoIP) users at UC Davis. These threats are not specific to the campus, but are of interest for any large network operator and the security research community. The total budget for this project is $80,506.07 and the deliverables include a final written report, a poster and a publication.

Keywords— VoIP Security, Telephone Security, Internet Telephony, Computer Security

February 11, 2018

1 Executive Summary

Analyzing Voice-over-IP at UC Davis
Abdulhai Naqvi
Dixit Paudel
Mark Weber
The University of California, Davis
February 11, 2018

The goal of the project is to explore possible security flaws with the UC Davis Voice-over-IP (VoIP) implementation. The Information and Educational Technology (IET) department at UC Davis will oversee and provide technical support for this project. Currently, there are about 1500 VoIP clients on the campus and the security risks assocated with them is unknown. The VLAN is susceptible to potentially any kind of attack through access points spread throughout the campus. The project will specifically evaluate possible threats to privacy, analyze risks of identity faking, and assess the security of the VOIP network through commonly known attack techniques.

2 Motivation

Information and Educational Technology (IET) of UC Davis has started to roll-out voice-over-IP (VoIP) for the whole campus. Currently, there are 1,500 VoIP clients on the campus. By the end of this year, most clients should be upgraded from the traditional telephone network to VoIP. By enabling telephones to communicate over IP, one has to consider additional security risks. In order to evaluate the security and privacy concerns, IET would like this team to perform an analysis regarding these issues. This report will help IET to harden the VoIP network further and protect thousands of students and employees of UC Davis.

The VoIP network has to meet specific user requirements to increase the acceptance of this new system. Two significant properties are security and privacy. Users have to be able to trust the network that their conversations will be private. This is particularly important for institutes like Student Health and Counseling Services (SHCS), which offer service via phone and will deal with very sensitive details.

Furthermore, our research will also apply to others. Since most networks use the same standard for VoIP, our possible findings will be important to other infrastructure providers. Hence, our project is of interest to the security research community as well.

3 Previous Work

Two papers and several RFC's are cosnidered here. The first paper discussed is **On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers** by Zhang et al.

This paper discusses launching remote attacks to gain MITM access to the VoIP system. For our project, this would be a moonshot since it requires a lot of testing and probing to show vulnerabilities within the hardware/software clients to hijack them

Given the time limit, its easier for us to do MITM attacks non-remotely. An example of registration hijacking, which is very practical for our purposes, is shown here (from Symantec: https://www.symantec.com/connect/articles/two-attacks-against-voip):

The first paper discusses how to launch a MITM attack remotely. The remote access is gained through a vulnerability in the user client. It uses DNS spoofing to launch the actual MITM attack. This attack has two distinct parts: 1) finding a client vulnerability and 2) launching a MITM attack. For this reason, this approach is considered more of a moonshot in that our goal is to achieve 2) within the timeframe (1 quarter or two and half months) and tacking 1) if time permits.

The second source, an article by Symantec: Two attacks against VoIP, which describes registration hijacking to gain MITM access is actually closer to what we think we can achieve within the time period. Our goal is to follow a similar technique to gain MITM access.

We are assuming that not implementing SIPS (SIP with TLS) is going to be a major shortcoming for the campus VoIP system. As such, we believe RFC 3830 (MIKEY Multimedia Internet Keying), which describes different methods of key sharing (such as pre-shared key, Diffie-Hellman, Public Key Cryptography, etc), is also an important previous work. In addition, the ZRTP protocol, described in RFC 6189 is also a good alternative, requiring Diffie-Hellman key exchange; however, it is more computationally expensive but guarantees perfect forward secrecy. In addition, the overarching RFC for SIP with TLS, RFC 5630, is also important as it gives the general overview of implementing TLS with SIP.

One should keep in mind, however, that TLS only provides security between nodes. It doesnt provide security against a malicious node. For that, IPSec (RFC 6071), which secures the underlying IP layer as opposed to the transport layer in TLS, is better suited. In addition, one could also implement tunneling of SIP over SSH or any such secure end to end protocol.

4 Specific Aims

The goals of this project are to:

- evaluate possible threats to the privacy of phone calls by using a network sniffer to listen to unencrypted SIP

packets.

- analyze the risk of identity faking and social engineering by using CallID spoofing.
- assess the security of the voice-over-IP network by performing man-in-the-middle and DoS attacks.

5 Plan

We will follow the steps listed below in that order to reach the goals given in section 4.

1. We will build a test environment which is close to the real one and in which we can conduct our research with as few consequences for other users as possible.
2. We will install an ethernet packet sniffer to listen for SIP packets. We will record all these packets, pseudonymize them and build communication profiles from them which includes: Who speaks to who and how long is each conversation. We hope to build a social graph from this data.
3. We will modify SIP packets to hide our identity (CallID spoofing).
4. We will impersonate a PBX (man-in-the-middle) to redirect calls and listen on fully encrypted conversations by performing a timing attack.

Further steps and directions of this research project will be decided on the basis of the results of above experiments and in close reconciliation with the technical director.

6 Deliverables

1. Project Progress Report: This report will be delivered at the end of the Winter Quarter and will contain the research project progress.
2. Biweekly Progress Update: We will update the technical director, Mark Redican, about our progress through email on a biweekly basis.
3. Research Paper: Voice-over-IP Vulnerabilities At UC Davis. This report will be delivered at the end of the Spring Quarter and will specifically layout results of our research.

7 Data Management Plan

Network traffic data collection is essential for this project. We will use UC Davis computing resources to perform network sniffing, and will store the data on the campus systems. If during data collection we happen to collect information not private to our test set-up, we will not store such information.

8 Issues

We face three issues chiefly: a shorter than desired time window to finish the project, potential team attrition over the next quarter and, on the technical side, how to provide security when dealing with non-secure or legacy telephony networks.

The best solution for our team would be to prioritize gaining MITM access and to build a logical network topology from the intercepted traffic.

9 Biographies

Dixit Paudel is a Master's student at UC Davis with a strong interest in the field of security and networking engineering. He earned his Bachelors in Electrical Engineering during the course of which he worked on several projects involving network communication. In addition, he has professional working experience as a software engineer in the field of the Internet of Things for about three years.

Mark Weber is a Master's student, who is currently studying abroad at UC Davis. He got his Bachelor's degree in 2026 at RWTH Aachen University. While his focus is on Machine Learning and Computer Graphics, he has a strong background in low-level programming and optimization. Furthermore, he has experience in research projects regarding IT Security, e.g. security of neural network based speech-recognition-systems.

Abdulhai Naqvi is a PhD student at Davis. He is interested in security in general. His B.S in Computer Science was also obtained at UC Davis.

10 Timeline

Table 1 presents the approximate timeline for completion of our project goals. The aims are distributed proportionately among 2 Quarters and we expect each of them to be completed in two weeks.

11 Budget

Table 2 lists all costs for this project. This team consists of three members, who will work on this project for two quarters. Therefore, most of the items are needed in the quantity of $3 * 2 = 6$ units. The salaries and benefits ensure that we will be able to follow our schedule and finish this project in time. Since one of our deliverables is a written report that will be published, the travel costs are

Table 1: Project Timeline

Activity	Feb 15-28	Mar 01-15	Mar 16-31	Apr 01-15	May 01-15	May 16-31
Project Approval & Equipment Setup	X					
Build Communication Profiles		X				
Final Progress Report & Presentation			X			
Call ID Spoofing & Man-in-the-middle attack				X		
Network Subversion & Network Disruption					X	
Final Report & Presentation						X

necessary to present our work at a conference. For our research, we will need six CISCO IP phones of model 7800 costing $120 each and a TP-Link 16-Port Gigabit Desktop/Rackmount Switch of $60. The tuitions for all team members are necessary costs to make sure the team can focus on this project. Additionally, UC Davis requires an indirect costs rate of 56.5%.

12 Broader Impact

Overall, regrettably, our project will likely not add anything to the state of the art in VoIP security. However, we intend to demonstrate shortcomings in the UC Davis campus-wide VoIP network and by extension in similar setups elsewhere. In addition, it is our goal to find solutions to these shortcomings where possible and to improve general security for the campus VoIP network. This will help ensure privacy of the calls made through the campus VoIP network.

In general, the weaknesses of the campus VoIP system and the strengthening of it through works such as ours, can be seen as a growing national trend to secure the nation's cyber infrastructure. As such, our research will help raise awareness of some common security pitfalls and security-aware best practices

Table 2: Items and Costs

Item	Costs	Units	Total
Salaries	$4,813	6	$28,787
Benefits	$63	6	$378
Travel Costs	$1,250	3	$3,750
Equipment	$780	1	$780
Fees	$12,130	6	$72,780
Indirect Costs	$2,789.28	1	$2,789.28
Total			**$80,506.07**

A Research Conference

The **ACM Asia Conference on Computer & Communications Security** is a respectable conference in this area. One of the papers discussed in this proposal was published in this conference in 2009.

The paper is titled **On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers** by Zhang et al. A link to the paper can be found here.