Progress Report: Voice-over-IP Security Vulnerabilities at UC Davis

Abdulhai Naqvi, Dixit Paudel, and Mark Weber
The University of California, Davis
{abdulhainaqvi, meondav, marweber}@ucdavis.edu

March 17, 2018

1 Problem statement

Information and Educational Technology (IET) of UC Davis has started to roll-out voice-over-IP (VoIP) for the whole campus. By enabling telephones to communicate over IP, one has to consider additional security risks. In order to evaluate the security and privacy concerns, this project performs an analysis regarding these issues. We identified three key properties for operating the VoIP network on the UC Davis campus:

1. Availability
2. Integrity
3. Confidentiality

Our project focuses on integrity and confidentiality of the VoIP network. We divided our research work into three parts: (I) Evaluate possible threats to the privacy of phone calls by using a network sniffer, (II) Analyze the risk of identity faking and social engineering and (III) Assess the security of the voice-over-IP network by performing man-in-the-middle attacks. During our work so far, we found out that initial assumptions about the network were false, which required us to adapt our plan. More details regarding this issue are given below.

2 Work Accomplished

The group submitted a research proposal for investigating UC Davis VoIP security vulnerabilities and also a literature review of VoIP security vulnerabilities.

The group co-ordinated with the Technical Director Mark Redican to order and set-up 6 Cisco Phones and established a test environment in the Security Lab at the Watershed Resources Building. Further, the group co-ordinated with the instructor to order a Netgear switch so that the phones could be connected to one NAM.

The group was able to set-up the phones and switch with the help of the Technical Director. The group further required IET's assistance in solving the Internet Connection Issues. The next step was to install wireshark and sniff packets. The group was able to sniff packets by port mirroring. This effectively is converting a switch to a hub. Detected

3 Work Remaining

4 Problems Encountered

The group encountered several impediments in the course of the project:

- Connecting the switch to NAM:
- Configuring 802.1q tagging on the switch:
- Configuring Internet Access in Lab: