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 19, 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 to order and set-up 6 Cisco Phones (only 2 used for initial set-up) 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 just one NAM.

The group was able to set-up the phones and the switch with the help of the Technical Director. The group was able to install Wireshark (a program to capture network packets) and sniff VoIP packets on a test computer. The group was able to sniff packets directed to and from the phone cables by port mirroring. This process effectively converts the switch to a hub.

The group was able to identify and detect the VoIP SIP packets directed to and from the phones, but contrary to the group's and Technical Director's expectations the SIP packets were encrypted and were displayed as TLS 1.2 packets. The group was also able to detect the RTP packets carrying voice data, which were displayed as unencrypted UDP datagrams. Finally, the group also identified certificate/key exchange between a central server and the phones when the phones booted up.

3 Work Remaining

4 Problems Encountered

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

- **Connecting the switch to NAM**: The group encountered two problems while connecting the up-link cable from the switch to the NAM port in the wall. One of the NAM's was not configured properly, and the one that was configured for usage caused the switch to recycle power when connected to the Power Over Ethernet port on the switch. The group with the help of the Technical Director were eventually able to resolve the problem by communicating with the appropriate IET channel, and by trial and experiment.

- **Configuring 802.1q tagging on the switch**: The next problem the group faced was with configuring the switch settings so that 802.1 tagging was enabled for the VLAN with ID 200 (the VoIP VLAN). The group initially wanted to configure the switch settings through a console cable, but upon reading the switch manual, the group concluded that the switch could only be configured through the switch software that came with it. The group installed a fresh copy of windows on our test computer and was able to install the switch software. After trial and error, the group eventually configured some ports on the switch to support 802.1q tagging.

- **Configuring Internet Access in Lab**: After, the group had set-up the switch and the phones, the next step was to install Wireshark, a network sniffer program. But unfortunately, the group had no Internet connection on the test computer. IET helped the group register the test PC and provided an IP address. However, the IP address provided was diagonsed as a duplicate address by the Networking Interface on the test computer. After a physical visit by an IET technician, the issue was conceded and the group was provided a new IP address, and finally a working Internet connection.