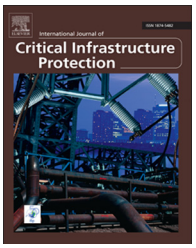
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Exploiting VoIP softphone vulnerabilities to disable host computers: Attacks and mitigation

*Ryan Farley, Xinyuan Wang**

Department of Computer Science, George Mason University, Fairfax, VA 22030, USA

ARTICLE INFO

Article history:
Received 10 March 2014
Accepted 31 May 2014
Available online 15 July 2014

Keywords:
VoIP telephony
Softphones
Security
Host attacks
Defense mechanisms

ABSTRACT

As increasing numbers of people run VoIP softphones on their laptops and smartphones, vulnerabilities in VoIP protocols and systems introduce new threats to the computer systems that run VoIP softphones. This paper investigates key threats that target VoIP hosts and techniques for mitigating the threats. In particular, this paper shows that crafted SIP traffic can disable a Windows XP host that runs a Vonage VoIP softphone or a Linphone by consuming almost all the free memory within minutes. While this "noisy attack" can be effectively mitigated by threshold-based filtering, the paper demonstrates that a "stealthy attack" can be launched to defeat threshold-based filtering and disable the host computer without ever ringing the softphone. To mitigate the stealthy attack, the paper describes a limited context aware filtering approach that leverages the context and SIP protocol information to ascertain the intentions of a SIP message on behalf of the client. Experiments demonstrate that limited context aware filtering can effectively defeat a stealthy attack while allowing legitimate VoIP traffic and calls to go through.

1. Introduction

The popularity of VoIP telephony has made it an attractive target for attackers [8]. Many of the known VoIP exploits stem from vulnerabilities in the de facto Session Initiation Protocol (SIP) [15], which is used for VoIP signaling. Previous research (see, e.g., [8,13,22,26]) has shown that SIP weaknesses make it possible for attackers to remotely monitor calls, modify billing control signals and even implement voice pharming attacks. As with any Internet-connected device, if a VoIP phone is vulnerable and unprotected, then an attacker can exploit it from anywhere in the world.

This paper takes a different perspective by focusing on stability and security threats exposed by VoIP softphones to the hosts that run them, and how these threats can be mitigated. As with most network-based applications, VoIP softphones expand the attack surface, which increases the chance that an attacker can find a weak point and pivot to compromise the host machine. This paper focuses on two SIP-based softphones: (i) Vonage softphone, which at one point had the largest residential VoIP market share in the United States and (ii) Linphone 3.7 [11], an open-source VoIP softphone.

This paper describes two attacks against a Windows XP host running an official Vonage softphone or a Linphone. The attacks use crafted SIP messages that can make the Windows XP host completely unusable until it is rebooted. Indirectly, these attacks also prevent softphones from receiving incoming calls and making outgoing calls within seconds. The first attack – called the noisy attack – can remotely disable a machine running the Vonage softphone or Linphone by taking up all the available physical and virtual

*Corresponding author.
E-mail address: xwangc@gmu.edu (X. Wang).

http://dx.doi.org/10.1016/j.ijcip.2014.07.001
1874-5482/

memory within minutes. The second attack – called the stealthy attack – takes longer to achieve the same effect, but it does not make the softphone ring. These attacks demonstrate that VoIP softphone vulnerabilities introduce grave threats to host systems. Indeed, the overwhelming majority of users are blissfully unaware that vulnerable VoIP applications can enable remote attackers to completely disable the host computers that are used for VoIP telephony.

This paper also discusses methods for mitigating the identified VoIP attacks at the network level. One technique uses threshold-based filtering to detect spikes in the arrival rates of `Invite` messages; experimental results demonstrate that this technique can effectively reduce the effects of noisy attacks by as much as 99.8%. However, threshold-based filtering is ineffective against stealthy attacks, which neither ring softphones nor use abnormally high SIP message rates. This problem is addressed by a novel limited context aware (LCA) approach, which buffers all incoming packets in a waiting queue while determining if they constitute attack traffic or legitimate traffic. The experimental results demonstrate that the limited context aware approach eliminates 100% of the stealthy attack packets without interfering with standard SIP operations.

The next section provides the foundation for discussing the two VoIP attacks by presenting signal flooding techniques that can disable the operation of softphones. Following this, the noisy and stealthy attacks are detailed along with the defense mechanisms that can combat the attacks. Next, the two attacks are empirically evaluated and the effectiveness of the proposed defense mechanisms is assessed. Finally, the implications of the attacks on softphone hosts are discussed, followed by a review of related research and the principal conclusions of the research effort.

2. Background

The Session Initiation Protocol (SIP) [15] is a general purpose application layer signaling protocol that is used to create, modify and terminate multimedia sessions such as VoIP calls between Internet endpoints known as user agents (UAs). To facilitate the location of user agents, all the users in a SIP network are identified by a SIP uniform resource identifier (URI), which typically includes a username and hostname in a format much like an email address.

Signaling between user agents is based on the request–response paradigm. A user agent client (UAC) sends requests to a user agent server (UAS), which sends the appropriate response and the corresponding status code. An endpoint can function as a user agent client and as a user agent server at the same time.

Fig. 1 illustrates the message flow of a normal SIP VoIP session between a user agent A and a user agent B without authentication. Initially, A only knows the URI of B. Since this does not provide the specific location information needed to complete the call, A must send an `Invite` message to its outbound proxy server http://atlanta.com. After http://atlanta.com resolves the URI, it forwards the `Invite` message to the appropriate next hop http://boston.com. Next, http://boston.com relays the `Invite` message to B and sends a `Trying` message back to http://atlanta.com, which is relayed to A. After B receives the `Invite` message, it sends a `Ringing` message to A. When B finally answers the call, it sends a 200 `Ok` message to A, to which A responds with an `Ack` message.

The packets sent during the exchange also contain Session Description Protocol (SDP) information. This establishes the

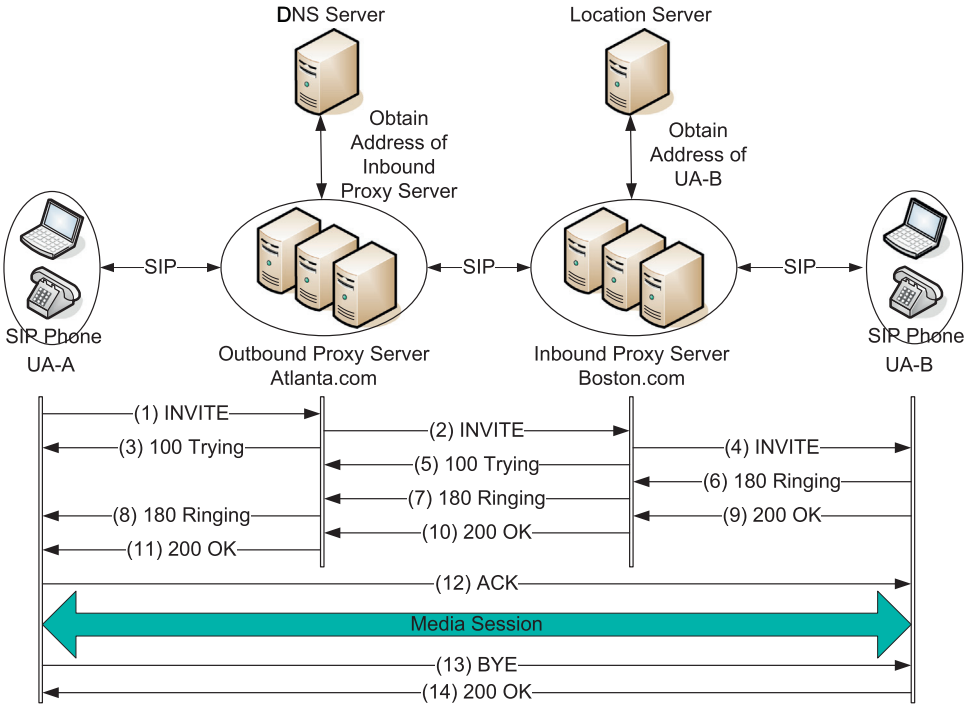


Fig. 1 – SIP message flow in a VoIP call.