Journal of Network and Computer Applications 34 (2011) 341–350

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Empirical tests of anonymous voice over IP

Marc Liberatore [b], Bikas Gurung [a], Brian Neil Levine [b], Matthew Wright [c,*]

[a] Qualcomm, Inc. 5775 Morehouse Drive, San Diego, CA 92121, USA
[b] Department of Computer Science, University of Massachusetts Amherst, Amherst, MA 01003, USA
[c] Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX 76019, USA

ARTICLE INFO

Article history:
Received 3 November 2009
Received in revised form
31 March 2010
Accepted 15 June 2010

Keywords:
Anonymity
Voice over IP
Privacy
Traffic analysis

ABSTRACT

Voice over IP (VoIP) is an important service on the Internet, and privacy for VoIP calls will be increasingly important for many people. Providing this privacy, however, is challenging, as anonymity services can be slow and unpredictable. In this paper, we propose a method for extending onion-routing style anonymity protocols for supporting *anonymous VoIP* (aVoIP) traffic with reasonable performance. We report the results of extensive experimentation across 210 globally placed PlanetLab proxies which shows that paths for reasonable aVoIP quality would need to be selected carefully. Our design includes an algorithm for the measurement and selection of paths for reasonable aVoIP performance and an analysis of the potential for attackers to take advantage of this algorithm to improve existing attacks. We show that aVoIP could be developed in an onion routing system with reasonable performance guarantees and a modest increase in risk to its users as compared to the standard path selection algorithm.

1. Introduction

Voice-over-IP (VoIP) is a tremendously popular and important application on the Internet. The popular Skype P2P VoIP service had over 28 billion minutes of phone calls in 2006 (Le Maistre, 2007). While calls over the Public Switched Telephone Network (PSTN) are secured by physical barriers to phone lines and equipment, VoIP calls are often routed through volunteer, intermediary peers that can easily inspect data. Although the call's data may be encrypted end-to-end, preventing third parties from linking participants in a call is more challenging. We define VoIP privacy as the protection of the knowledge of who is communicating from all parties except the two end-points of the call.[1]

In this paper, we introduce a method for *anonymous VoIP* (aVoIP) that is secure and has reasonable Internet performance. Techniques for proxy-based anonymous routing are well known; our contributions include a measurement study showing the feasibility of such a system on the Internet and a security analysis of threats posed by VoIP quality-of-service requirements.

End-to-end delays in voice communication greater than 100–150 ms are detectable by humans, and delays greater than 200 ms can become intolerable and impede interactive communication (Intl. Telecommunication Union, 2003). These performance requirements make it difficult to provide an anonymized end-to-end connection for VoIP using a series of proxies. We performed an extensive measurement study of about 210 globally placed proxies over a 10-week period. Our measurements demonstrate that aVoIP is currently possible on the Internet as a viable, robust, real-time service if we select paths carefully. Specifically, our measurements show that connections between a series of proxies located on the same continent could support aVoIP with one-way end-to-end delays of under 150 ms over 90% of the time. However, intercontinental paths of proxies could not support aVoIP traffic as well: of paths with one intercontinental hop, 35% show acceptable performance, while paths with two and three hops result in only 7% and 1% of the paths exhibiting acceptable performance, respectively.

These performance results dictate we build paths differently for aVoIP than for less delay-sensitive applications. As Kesdogan and Palmer point out, it is critical to consider the impact on network performance and user experience when building anonymity systems (Kesdogan and Palmer, 2006). We propose to conduct occasional measurements of the connection quality between pairs of nodes and use these measurements to help users select a path with sufficient quality of service (QoS) for phone calls. While intuitive, this method could help attackers to modify path selection by manipulating the measurements. For example, the attacker can attempt to remove some pairs of nodes to improve the odds of users selecting his nodes for their paths. This strategy in turn strengthens attacks such as the predecessor attack (Wright et al., 2004; Bauer et al., 2007).

* Corresponding author.
E-mail addresses: liberato@cs.umass.edu (M. Liberatore), brgurung@gmail.com (B. Gurung), brian@cs.umass.edu (B.N. Levine), mwright@cse.uta.edu (M. Wright).

[1] This definition is different from that typically used by anonymizing services that also protect the identity of the initiating user from receivers. Unfortunately, one-sided anonymous phone calls encourage harassment.

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.06.009