Computer Communications 34 (2011) 1202–1212

Contents lists available at ScienceDirect

Computer Communications

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

# Traffic analysis attacks on Skype VoIP calls

Ye Zhu [a,*], Huirong Fu [b]

[a] Cleveland State University, 2121 Euclid Avenue, Cleveland, OH 44115, USA
[b] Oakland University, Rochester, MI 48309-4478, USA

ARTICLE INFO

*Article history:*
Received 11 February 2010
Received in revised form 2 December 2010
Accepted 18 December 2010
Available online 23 December 2010

*Keywords:*
Skype
VoIP
HMM

ABSTRACT

Skype is one of the most popular voice-over-IP (VoIP) service providers. One of the main reasons for the popularity of Skype VoIP services is its unique set of features to protect privacy of VoIP calls such as strong encryption, proprietary protocols, unknown codecs, dynamic path selection, and the constant packet rate. In this paper, we propose a class of passive traffic analysis attacks to compromise privacy of Skype VoIP calls. The proposed attacks are based on application-level features extracted from VoIP call traces. The proposed attacks are evaluated by extensive experiments over different types of networks including commercialized anonymity networks and our campus network. The experiment results show that the proposed traffic analysis attacks can greatly compromise the privacy of Skype calls. Possible countermeasure to mitigate the proposed traffic analysis attacks are analyzed in this paper.

## 1. Introduction

In this paper, we address on privacy issues of Skype calls. With the rapid growth of broadband Internet access services, the popularity of VoIP calls has grown significantly. As a competitor with traditional phone services provided over Public Switched Telephone Networks (PSTN), VoIP services are known for their lower cost and richer features. Skype is one of the most popular VoIP service providers.

Skype VoIP services are provided on a peer-to-peer structure. Skype peers form an overlay network. A Skype call may be routed through Skype peers during the call for better Quality of Service (QoS) [1,2]. One of the main reasons for the popularity of Skype VoIP services is its unique set of features to protect privacy of VoIP calls such as strong encryption [3], proprietary protocols [3], unknown codecs [4], and dynamic path selection[1] [1,2], and the constant packet rate [5]. To further protect privacy of Skype VoIP calls, advanced users are using anonymity networks to anonymize VoIP calls. For this purpose, low-latency anonymity networks such as Tor [6] and JAP [7] can be used.

In this paper, we propose a class of passive traffic analysis attacks to compromise privacy of Skype calls. The procedure of the proposed attacks is as follows: First an adversary collects Skype call traces made by a victim, say Alice. The adversary then extracts application-level features of Alice's VoIP calls and trains a Hidden Markov Model (HMM) with the extracted features. To test whether a call of interest is made by Alice, the adversary can extract features from the trace of the call and calculate likelihood of the call being made by Alice. The proposed attacks can identify speeches or speakers of Skype calls with high probabilities.

The contributions made in this paper are summarized as follows:

- We propose a class of traffic analysis attacks to compromise privacy of Skype calls. The attacks are passive and based on the HMM, a powerful tool to model temporal data. We also propose a method to extract application-level features from traffic flows for application-level traffic analysis attacks.
- We evaluate the proposed traffic analysis attacks through extensive experiments over the Internet and commercial anonymity networks. For most of Skype calls made in the experiments, the two parties are at least 20 hops away and the end-to-end delay between two parties is at least 80 ms. Our experiments show that the traffic analysis attacks are able to detect speeches or speakers of Skype calls with high probabilities.
- We propose intersection attacks to improve the effectiveness of the proposed attacks.
- We propose a countermeasure to mitigate the proposed traffic analysis attacks and analyze the effect of the countermeasure on quality of Skype calls.

The rest of the paper is organized as follows: Section 2 reviews related work. In Section 3, we formally define the problem. The details of proposed traffic analysis attacks are described in Section 4. In Section 5, we evaluate the effectiveness of the proposed traffic analysis attacks with experiments on commercialized anonymity

* Corresponding author. Tel.: +1 216 875 9749.
*E-mail addresses:* zhuye06@gmail.com, y.zhu61@csuohio.edu (Y. Zhu).

[1] Although the dynamic path selection is originally designed for QoS and bypassing restrictive NAT and firewalls, the technique is helpful for privacy protection.

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.12.007

networks and our campus network. Section 7 presents a countermeasure to mitigate the proposed traffic analysis attacks. Discussion and the outline of future work are given in Section 8. We conclude the paper in Section 9.

## 2. Related work

In this section, we review related work on low-latency anonymity networks and related traffic analysis attacks.

### 2.1. Low-latency anonymity networks

After Chaum proposed the anonymous communication for email in his seminal paper [8], many low-latency anonymity networks have been proposed or even implemented for different applications. The examples are *ISDN-mixes* [9] for telephony, *Web Mix* [7] for web browsing, *MorphMix* [10] for peer-to-peer applications, *GAP* base *GNUnet* [11] for file sharing. TARZAN [12], *Onion Router* [13], and *Tor* [6], the second-generation onion router, are designed for general usage by low-latency applications. Especially *Tor* has some desirable features for low-latency applications such as perfect forward secrecy and congestion control. In our experiments, we used the anonymity network managed by findnot.com to anonymize VoIP calls instead of the Tor network, because UDP traffic is not natively supported by Tor. The commercialized anonymous communication services provided by findnot.com can allow us to route VoIP packets through entry points located in different countries into the anonymity network.

Common techniques used in low-latency anonymity networks are encryption and re-routing. Encryption prevents packet content access by adversaries. To confuse adversaries, anonymity networks using re-routing techniques forward encrypted packets in a usually longer and random path instead of using the shortest path between the sender and the receiver. To attack an anonymity network using the re-routing technique, the attacker usually needs to be more powerful, for example, to be a global attacker.

### 2.2. Traffic analysis attacks

Traffic analysis attacks can be classified into two categories, network-level traffic analysis attacks and application-level traffic analysis attacks.

Network-level traffic analysis attacks target at disclosing network-level or transport-level information. Most privacy-related network-level traffic analysis attacks focus on traffic flow identification or traffic flow tracking. The examples are attacks by Levine et al. [14] on anonymity networks, the active attack proposed by Murdoch and Danezis [15] on the Tor network, our flow correlation [16], and our flow separation [17] attacks.

Application-level traffic analysis attacks target at disclosing application-level information. The examples are keystroke detection based on packet timing [18], web page identification [19], spoken phrase identification [20] with variable bit rate codecs.

The traffic analysis attacks proposed in this paper are at application-level. These attacks can detect speeches or speakers of Skype calls based on talk patterns, the application-level features which do not vary from call to call.

There are a number of research efforts focusing on traffic analysis of VoIP. Wang et al. [24] proposed to watermark VoIP traffic flows to trace VoIP calls through the Internet. In [21], Wright et al. showed that it was possible to recover spoken phrases from VoIP packet size information. Wright et al. [22] also showed the feasibility to detect languages used in VoIP conversations based on VoIP packet size information.

Similar as [21,22], our research in this paper focuses on disclosing application-level information from traffic analysis of VoIP. The traffic analysis attacks proposed in this paper aim to identify speakers of VoIP calls. Another difference is on the type of VoIP codecs and protocols. The researches in [21,22] focus on a variable bit rate (VBR) codec, more specifically the open-source Speex codec [23], and standardized VoIP protocols. We focus on the Skype VoIP service which uses codecs unknown to the public and its own proprietary protocols. Skype is also known for its strong encryption preventing packet content access. These privacy protection measures taken by Skype render traffic analysis on Skype VoIP traffic more difficult since (1) we have to treat the Skype software as a black box and (2) we are not even able to identify signaling packets so that these signaling packets can be completely removed before traffic analysis.[2]

## 3. Problem definition

In this paper, we focus on traffic analysis on Skype VoIP calls through anonymity networks to disclose sensitive information at application-level. More specifically, we are interested in detecting speeches and speakers of Skype VoIP calls by analyzing traffic patterns at the application-level.

A typical attack scenario focused in this paper is as follows: An adversary who has possession of traces of *previous* Skype VoIP calls made by a victim, say Alice, may want to detect whether Alice is talking to Bob *now* by collecting Skype packets on the link to Bob. The adversary may also want to detect the speech content, such as the repetition of a partial speech in previous Skype calls.

In this paper, we assume that traffic traces used in analysis can be collected at different time. This is the major difference between our research and the previous researches. Most of the previous researches assume that the adversary has *simultaneous* access to *both* links connected to Alice and Bob *during the Skype call* between Alice and Bob. By passively correlating VoIP flows at both ends or actively watermarking VoIP flows, the adversary can detect whether Alice is communicating with Bob. But for the typical attack scenario described above, both flow correlation and watermarking techniques do not work because traces to be compared are collected from different VoIP calls: (a) Correlation between different calls is low. (b) Watermarks used to mark traffic flows of Alice's VoIP calls can be different for different calls because of recycling watermarks or simply because Alice is making a call from a different location or with a different computer.

### 3.1. Network model

In the paper, we assume Alice makes VoIP calls by Skype. We are particularly interested in Skype VoIP calls because: (a) Skype is based on peer-to-peer structure. During a Skype call, VoIP packets may follow more than one path through different Skype peers or Skype supernodes [1]. The peer-to-peer structure and dynamic path selection make security attacks or eavesdropping on Skype calls more difficult. (b) Skype uses proprietary protocols so that attackers cannot differentiate media packets from signaling packets. (c) Skype uses unknown codecs that renders traffic analysis exploiting characteristics of voice codecs nearly impossible [4]. (d) Skype calls are encrypted and hard to decipher [3]. (e) Skype sends packets at the constant rate of 33 packet/s [5]. Due to the unique set of features listed above, Skype is known as secure voice

[2] In general, signaling packets are not affected by talk patterns so signaling packets are essentially "noise" in recovering talk patterns from Skype traffic. Signaling packets are not considered in [21,22] since these packets can be filtered out easily for standardized VoIP calls. In other words, patterns recovered from VoIP traffic in [21,22] are noise-free.