Vtalk: Secure Deployment of VoIP over LAN'S

Ms.Sassirekha.S.M[1], Ms. J.R.Thresphine[2]

[1]*(Student, Department of CSE, PRIST University, Tamil Nadu)*
[2]*(Assistant Professor, Department of CSE, PRIST University, Tamil Nadu)*

ABSTRACT: *Peer-to-peer VoIP (voice over IP) networks, exemplified by Skype, are becoming increasingly popular due to their significant cost advantage and richer call forwarding features than traditional public switched telephone networks. One of the most important features of a VoIP network is privacy (for VoIP clients). Unfortunately, most peer-to-peer VoIP networks neither provide personalization nor guarantee a quantifiable privacy level. In this paper, we propose novel flow analysis attacks that demonstrate the vulnerabilities of peer-to-peer VoIP networks to privacy attacks. We then address two important challenges in designing privacy-aware VoIP networks: Can we provide personalized privacy guarantees for VoIP clients that allow them to select privacy requirements on a per-call basis? How to design VoIP protocols to support customizable privacy guarantee? This paper proposes practical solutions to address these challenges using a quantifiable k-anonymity metric and a privacy-aware VoIP route setup and route maintenance protocols. We present detailed experimental evaluation that demonstrates the performance and scalability of our protocol, while meeting customizable privacy guarantees.*

IndexTerms: *VOIP,SSH,QOS,ITU,RSP,AARSP,FCC,PSTN*

I. INTRODUCTION

Peer-to-peer ("P2P") technology became widely deployed and popularized by file-sharing applications such as Napster and Kazaa. In this context, P2P technology allowed users to share, search for and download files. The mix network provides good anonymity for high-latency communications by routing network traffic through a number of nodes with random delay and random routes. The Peer-to-peer VoIP network typically consists of a core proxy network and a set of clients that connect to the edge of this proxy network. This network allows a client to dynamically connect to any proxy in the network and to place voice calls to other clients on the network.

VoIP uses the two main protocols: route setup protocol (RSP) for call setup and termination, and real-time transport protocol (RTP) for media delivery. Common solution used in peer-to-peer VoIP networks is to use a route setup protocol that sets up the shortest route on the VoIP network from a caller source to a receiver dst.1 RTP is used to carry voice traffic between the caller and the receiver along an established bidirectional voice circuit. First, we show that using the shortest route (as against a random route) for routing voice flows makes the anonymizing network vulnerable to flow analysis attacks. Second, we develop practical techniques to achieve quantifiable and k-anonymity on VoIP networks.

II. VOIP OVERVIEW

This paper will address the problems in most peer to peer VoIP networks Most WiFi networks provide a tempting entry point for hackers and other unauthorized users. Many enterprises are discovering the cost and productivity benefits wireless VoIP provides. As a result, a growing number of enterprises are installing wireless hotspots inside office buildings, warehouses, shipping yards, corporate campuses and various other facilities, allowing employees with wireless IP handsets and other compatible devices to talk to each other, as well as the outside world, without relying on desktop phones. Yet wireless VoIP technology is not without risk. Unsecured voice packets can be intercepted and WiFi networks provide a tempting entry point for hackers and other unauthorized users.

Having a VOIP requires a broadband connection, which may be (a little bit) expensive. Still, having all these costs in mind, the benefits of VOIP are not to be neglected when deciding what you should do for your long distance calls. But using your VOIP connection for local phone calls may turn to be a disadvantage

The main objective is to provide secure voice communication within any wired/wireless networks . We facilitate the transport of objects through networks using XML serialization in visual c#.NET , Since the XmlSerializer class is part of the .NET framework rather using servers and all the voice signals have been compressed using G.711 standard before transmission so that the signals can be quickly transmitted and standard encryption algorithm TRIPLE-DES to conceal our information is used and so that lack of synchronization is avoided and even though any adversary who knows the flow rate and VoIP topology cant interrupt our call or hack our data by any means.

III. RELATED WORK

Peer to Peer Voip technology such as skype uses overlay peer to peer network. There are two types of nodes in this overlay network, ordinary hosts and super nodes (SN). An ordinary host must connect to a super node and must register itself with the Skype login server for a successful login.

VOIP denial of service attacks (DoS attacks) overwhelm IP telephony devices with call requests and registrations. This flooding can create resource exhaustion, long term busy signals, and force disconnects of in session calls.

Identifying the caller receiver pair becomes the challenging problem. Random route for routing voice flows makes the anonymizing network vulnerable to flow analysis attacks.The low-latency anonym zing networks are vulnerable to timing analysis attacks, especially from well-placed malicious attackers.

IV. PROPOSED SYSTEM

XML serialization provides a simple and efficient set of techniques to transfer object states between multiple software platforms. The following are the basic advantages of XML serialization:

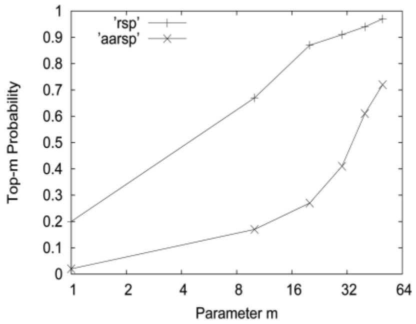
1) Facilitate the transportation of an object through a network
2) Create a clone of an object

The algorithm of the proposed system is as follows:

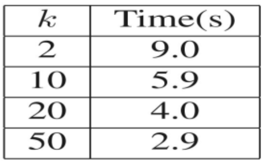
AARSP accepts an anonymity parameter k as an input for the route setup protocol, on a per-client per-call basis AARSP modifies the basic route setup protocol such that it simultaneously satisfies three conditions:

1) We have at least one node p €route (src,dst) such that in(p)≥k (kanonymity)
2) The end-to-end one-way latency on the route from src to dst is smaller than maxLat (typically set to 250 ms)
3) The total call volume on every node p €route (src,dst) is smaller than its capacity maxFlow(p)

V. EVALUATION AND RESULTS



Observe that at low and moderate call volumes, AARSP offers significantly improved protection against flow analysis attacks. The top-m probability for both AARSP and RSP for varying m and a call volume of 128 Erlangs. We also observe that AARSP consistently out performs RSP for all values of m



k	Time(s)
2	9.0
10	5.9
20	4.0
50	2.9

AARSP tolerating compromised proxies
Attack cost versus anonymity level (k)

A secure communication between caller and sender in both wired and wireless networks using a standard advanced encryption algorithm called TRIPLE DES unlike other VoIP technologies that use AES (advanced encryption standard)

1) Cost advantage and richer call forwarding features than traditional public switched telephone networks
2) Privacy guarantees for VoIP clients.
3) A route setup protocol that routes the shortest path from src to dest
4) Quality of voice conversation.

VI. FUTURE WORK AND CONCLUSION

In this paper, we have addressed the problem of providing privacy guarantees in peer-to-peer VoIP networks. First, we have developed flow analysis attacks that allow an adversary (external observer) to identify a small and accurate set of candidate receivers even when all the nodes in the network are honest. We have used network flow analysis and statistical inference to study the efficacy of such an attack. Second, we have developed mixing-based techniques to provide a guaranteed level of anonymity for VoIP clients. We have developed an anonymity-aware route setup protocol that allows clients to specify personalized privacy requirements for their voice calls (on a per-client per-call basis) using a quantifiable k-anonymity metric. We have implemented our proposal on the Phex client and presented detailed experimental evaluation that demonstrates the performance and scalability of our protocol, while meeting customizable privacy guarantees.

Acknowledgement

The author would like to thank the anonymous rewiewers for their valuable comments and suggestions.

References

[1]. Mudhakar Srivatsa, Arun Iyengar, Ling Liu and Hongbo Jiang, “Privacy in VoIP Networks : Flow Analysis Attacks and Defense,” IEEE Trans.Parallel and distributed systems, pages 621-633, 2011.

[2]. M.J. Freedman and R. Morris, “Tarzan: A Peer-to-Peer Anonymizing Network Layer,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), 2002.

[3]. Stoeckigt, K.O. , Vu, H.L. , VoIP Capacity—Analysis, Improvements, and Limits in IEEE 802.11 Wireless LAN,” IEEE Transaction,pages 4553 – 4563,2010.

[4]. M. Srivatsa, A. Iyengar, and L. Liu, “Privacy in VOIP Networks: A k-Anonymity Approach,” Technical Report IBM Research RC24625, 2008.

[5]. Chacon, Sergio University of Houston, USA, Benhaddou, Driss ; Gurkan, Deniz ,” Secure voice over Internet Protocol (voIP) using virtual private networks (VPN) and Internet Protocol Security (IPSec),”IEEE conference,2006.

[6]. M.J. Freedman and R. Morris, “Tarzan: A Peer-to-Peer Anonymizing Network Layer,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), 2002.