© 2014 IJIRT | Volume 1 Issue 7 | ISSN: 2349-6002

PRIVACY IN VOIP NETWORKS

Anirban Maitra, Arun Kumar, Akshay Kumar
Department of Electronics and Communication Engineering , Maharashi Dayanand University, Rohtak

***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.**

***Index Terms*- anonymzing , latency, packetization , route , telephony .**

I. INTRODUCTION

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 ([1][3][4]). 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 anonymzing network vulnerable to flow analysis attacks.Second, we develop practical techniques to achieve quantifiable and k-anonymity on VoIP networks ([5][7]).

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.

II. VOICE OVER INTERNET PROTOCOL (VOIP)

Voice over Internet Protocol (Voice over IP, VoIP) is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone. Internet telephony refers to communications services Voice, fax, SMS, and/or voice-messaging applications that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitizationof theanalog voic signal encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use IP protocols for voice communication while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codec‟s which encode speech allowing transmission over an IP network as digital audio via an audio stream. The codec used is varied between different implementations of VoIP (and often a range of codec‟s are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codec‟s. VoIP is available on many smart phones and internet devices so even the users of portable devices that are not phones can still make calls or send SMS text messages over 3G or Wi-Fi using this VoIP communication process.

Objectives

1) To Design Secure VoIP Protocol.

2) Route Setup and Route Maintenance Protocol. 3) To Find Out Shortest Path.

III. EXISTING PROCESS OF VOIP

Voice protocol is used to design the application without any security protocol has used and random route is select to transmit the information. Mix network provides good anonymity for high-latency communications by routing network. A 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. In Peer-to-peer VoIP networks neither provide personalization nor guarantee a quantifiable privacy level. To identify the caller-receiver pairs becomes a challenging problem. Random route for routing voice flows makes the anonymizing network vulnerable to flow analysis attacks. 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. The low-latency anonym zing networks are vulnerable to timing analysis attacks, especially from well-placed malicious attackers

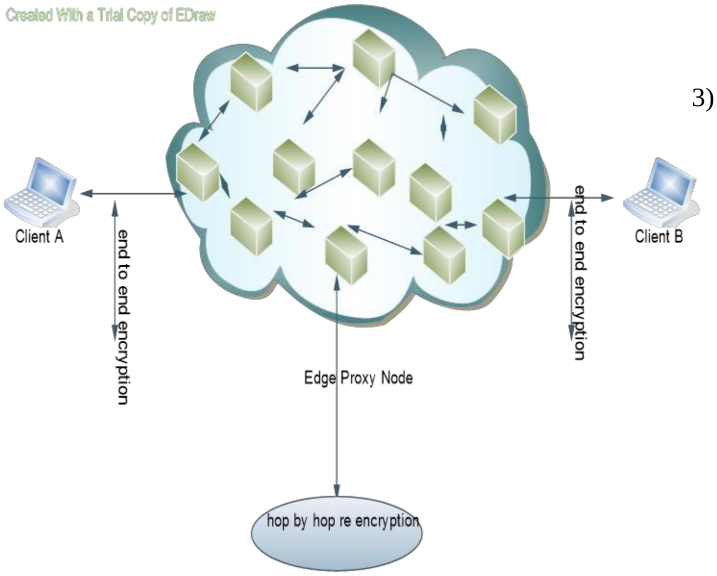
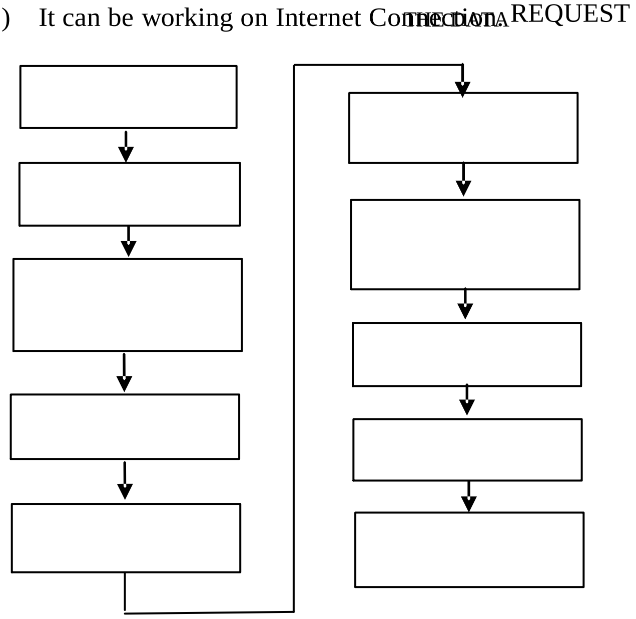


Fig 1.VoIP Communication process

Drawback Of Existing System

1) The network traffic through a number of nodes with random delay and random routes.

2) It can be working on Internet Connection.



3) Mix network have additional quality of service (QOS) requirements should be needed.

4) The quality of voice conversations is weakening. 5) Leaking the information to an external server easy.

IV. PROPOSED SYSTEM OF VOIP

We provide personalized privacy guarantees for VoIP clients that allow them to select privacy requirements on a per-call basis How to design VoIP protocol. A quantifiable k-anonymity metric and a privacy-aware VoIP route setup and route maintenance protocols. Qos sensitive applications on mix networks using peer-to-peer VoIP service. We make two important contributions. First, we show that using the shortest route (as against a random route) for routing voice flows makes the anonymzing network vulnerable to flow analysis attacks. Second, we develop practical techniques to achieve quantifiable and customizable k-anonymity on VoIP networks.

1) Cost advantage and richer call forwarding features than traditional public switched telephone networks.
2) No need to Internet connection and Privacy guarantees for VoIP clients.
3) A route setup protocol that sets up the shortest route on the VoIP network from a caller source to a receiver DST, So Quality of voice conversation.

RECEIVER DECRYPT THE

RECEIVER
RESPONSE

DATA ACCEPT THE

SEND BACK

CALLER
CALL ACCESS

SENDER ENCRYPT

Fig 2.VoIP Data flow process

V. TECHNIQUES USED

5.1 M2: Multicasting Mixes for Efficient and Anonymous Communication

We present a technique to achieve anonymous multicasting in mix networks to deliver content from producers to consumers. Employing multicast allows content producers to send (and mixes to forward) information to multiple consumers without repeating work for each individual consumer. In our approach, consumers register interest for content by creating paths in the mix network to the content‟s producers. When possible, these paths are merged in the network so that paths destined for the same producer share common path suffix to the producer. When a producer‟s ends content, the content travels this common suffix toward its consumers (in the reverse direction) and "branches" into multiple messages when necessary. We detail the design this technique and then analyze the unlink ability of our approach against a global, passive adversary who controls both the producer and some mixes. We show that there is subtle degradation of unlink ability that arises from multicast. We discuss techniques to tune our design to mitigate this degradation while retaining the benefits of multicast.

A mix is a routing element that attempts to hide the correspondences between its input and output messages, i.e., so an observer cannot determine which output message corresponds to a particular message that the mix received. To achieve this, a mix typically transforms each message it receives (e.g., by decrypting it) and then outputs messages in an order different from that in which it received them. If the compromise of a single mix is feared, then a message can be routed through multiple mixes (a mix network) to hide the correspondence between the message originator and destination (provided that at least one mix remain uncompromised), a property called unlink ability ([1][2][5]).

5.2 Tarzan: A Peer-to-Peer Anonymizing Network Layer

Tarzan is a peer-to-peer anonymous IP network overlay. Because it provides IP service, Tarzan is general-purpose and transparent to applications. Organized as a decentralized peer-to-peer overlay, Tarzan is fault-tolerant, highly scalable, and easy to manage.

Tarzan achieves its anonymity with layered encryption and multihop routing, much like a Chaumian mix. A message initiator chooses a path of peers pseudo-randomly through a restricted topology in a way that adversaries cannot easily influence. Cover traffic Tarzan imposes minimal overhead over a prevents a global observer from using traffic analysis to identify an initiator. Protocols toward unbiased peer-selection offer new directions for distributing trust among untrusted entities. Tarzan provides anonymity to either clients or servers, without requiring that both participate. In both cases, Tarzan uses a network address translator (NAT) to bridge between Tarzan hosts and oblivious Internet hosts. Measurements show that

Non-anonymous overlay route. The ultimate goal of Internet anonymization is to allow a host to communicate with an arbitrary server in such a manner that nobody can determine the host‟s identity. Toward this goal, we envision a system that uses an Internet-wide pool of nodes, numbered in the Thousands, to relay each others‟ traffic to gain anonymity([1][3]).

5.3 Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Manipulation of Interpacket Delays:

Network based intruders seldom attack directly from their own hosts, but rather stage their attacks through intermediate "stepping stones" to conceal their identity and origin. To identify attackers behind stepping stones, it is necessary to be able to correlate connections through stepping stones, even if those connections are encrypted or perturbed by the intruder to prevent traceability. The timing-based approach is the most capable and promising current method for correlating encrypted connections. However, previous timing-based approaches are vulnerable to packet timing perturbations introduced by the attacker at stepping stones. In this paper, we have developed a robust watermark correlation framework that reveals a rather surprising result on the inherent limits of independent and identically distributed (iid) random timing perturbations over sufficiently long flows. We also Sidentify the tradeoffs between timing perturbation characteristics and achievable correlation effectiveness. Experiments show that the new method performs significantly better than existing, passive, timing-based correlation in the presence of random packet timing perturbations ([8][9][10][11]).

5.4 Tracking Anonymous PeertoPeer VoIP Calls on the Internet

The key idea is to embed a unique watermark into the encrypted VoIP by slightly adjusting the timing of selected packets. Our analysis shows that it only takes several milliseconds time adjustment to make normal VoIP highly unique and the embedded watermark could be preserved across the low latency anonymizing network if appropriate redundancy is applied.Our analytical results are backed up by the real-time experiments performed on leading peer-to-peer VoIP client and on a commercially deployed anonymizing network. Our results demonstrate that tracking anonymous peer-to-peer VoIP calls on the Internet is feasible and low latency anonymizing networks are susceptible to timing attacks ([1][4][6][7]).

VI. SECURITY ISSUES

6.1 Voip Route Setup Protocol:

We describe a commonly used shortest route setup protocol in peer-to-peer VoIP networks. The protocol operates in four steps:

Init Search: initiates a route setup by source.

Process Search: process route setup request at some node. **Process Result:** process results of a route setup request at some node.

Fin Search :concludes the route set, One should note that flow analysis attacks exploit only the shortest path property and are independent of the concrete route setup protocol.

7.2 Observing user:

Observing user Module is the main module of this application to find out the how many users Are connected in local area network. Then only we will find out the caller and receiver. To get the host name. This module will operate the four steps:

1.Init Search
2.Process search
3.Process result
4.Fin Search

6.2 Flow Analysis Attacks

We describe flow analysis attacks on VoIP networks. These attacks exploit the shortest path nature of the voice flows to identify pairs of callers and receivers on the VoIP network. Similar to other security models for VoIP networks encodes the shortest path nature of the voice paths.

1) Naive Tracing Algorithm:

We describe flow analysis attacks on VoIP networks. These attacks exploit the shortest path nature of the voice flows to identify pairs of callers and receivers on the VoIP network. Similar to other security models for VoIP networks encodes the shortest path nature of the voice paths.

1)We observe that for low call volumes (<64 Erlangs) the shortest path tracing algorithm is about 5- 10 times more precise than the naive tracking algorithm.

2)The higher call volumes facilitate natural mixing of VoIP flows, thereby decreasing the precision of both the naive tracing and shortest path tracing algorithms.

3)The flow measurements to construct a probability distribution over the set of possible receivers

1) Init Search:

A VoIP client initiates a route setup for a receiver.

2) Process search:

Receiver search (search id) from its neighbor in search request.

3) Process result:

Receives res. Note that p has no knowledge as to where the search result was initiated.

4) Fin Search:

When source receives result to search id from q, it adds a routing entry to its routing table. The route setup protocol establishes the shortest overlay network route between source to and destination.

7.3 Call Acceptance:

Call acceptance allow to receive call from the Caller on your list .all other will hear on announcement that you are not accepting. Selective Call Acceptance allows you to screen incoming calls by creating a list of phone numbers from which you are willing to accept calls. Calls from phone numbers not contained on your list are sent to an announcement that informs the caller that you are not receiving calls at this time.

1) Enhances security and privacy by allowing only

2) Distance Prior and Hop Count Prior:

Hop count and distance it denotes (in terms of latency) between Source and Destination.

the most important calls to reach you.

2) Prevents unwanted interruptions, particularly solicitation calls.

VII. LIST OF THE MODULES

7.4 External Adversary:

1) Sign up module 2) Observing user 3) Call Acceptance

4) External Adversary

1) External Adversary is the main module to provide privacy in VoIP clients against defense, if external observer listening or trace out voice means to compromise our node.

7.1 Sign up:

1) The Client logins in the sin up module client register the(Name, Email, Address, Dob, Gender, city, photo, IP address) successfully register next access the sign in module (username ,IP address)

2) This information will be stored in xml. The user no needs to register sign up details.2) To give a secure link external observer call listening the voice conversation between caller and receiver. This module to provide a security in caller an and receicer.

VIII. 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.

[9] K. Yoda and H. Etoh, „Finding a Connection Chain for Tracing Intruders,‟ Proc. Sixth European Symp. Research in Computer Security (ESORICS), 2000.

REFERENCES

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

[2] G. Perng, M.K. Reiter, and C. Wang, „M2: Multicasting Mixes for Efficient and Anonymous Communication,‟ Proc. IEEE Int‟l Conf. Distributed Computing Systems (ICDCS), 2006.

[3] S. Saroiu, P.K. Gummadi, and S.D. Gribble, „A Measurement Study of Peer-to-Peer File Sharing Systems,‟ Proc. Multimedia Computing and Networks (MMCN) Conf., 2002.

[4] C. Shields and B.N. Levine, „A Protocol for Anonymous Communication over the Internet,‟ Proc. ACM Conf. Computer and Comm. Security (CCS), 2000.

[5] V. Shmatikov and M.H. Wang, „Timing Analysis in Low Latency Mix Networks: Attacks and Defenses,‟Proc. 11th European Symp. Research in Computer Security (ESORICS), 2006.

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

[7] X. Wang, S. Chen, and S. Jajodia,"Tracking Anonymous Peer-to- Peer VoIP Calls on the Internet," Proc. 12th ACM Conf. Computer and Comm. Security (CCS), 2005.

[8] X. Wang and D. Reeves, „Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Manipulation of Interpacket Delays,‟ Proc. 10th ACM Conf. Comp.2010.