Secure Messaging Services using cloud

1.Prof. Pratik B. Kamble.
2. Mr.Umesh Chnadake.
3. Mr.Shekhar Pote.
4. Mr.Ghanshyam Chaudhari.
5. Mr.Rushabh Sarnaik.
6. Mr.Manoj Kulkarni.

Prof., Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India.
BE, Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India.
BE, Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India.
BE, Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India.
BE, Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India.
BE, Information Technology, Marathwada Mitra Mandal's College Of Engineering Karvenagar, Pune- 52,Maharashtra,India

ABSTRACT

Sanwad is a peer-to-peer text messenger built on the top of Tor network that provides authentication and end-to-end encryption, it also allows the users to stay anonymous during communication. In addition, it prevents third parties from even learning that communication is taking place.

The aim of this thesis is to document the protocol used by Sanwad and to analyze the security of Sanwad and its reference implementation. The work shows that although the design of Sanwad is sound, its implementation has several aws, which make Sanwad users vulnerable to impersonation, communication con rmation and denial-of-service attacks.

In Onion Routing a static tunnel through an overlay network is build via layered encryption. All traffic exchanged by its end points is relayed through this tunnel.

In this paper, we describe the design of our dynamic Multipath Onion RoutEr (MORE) for peer-to-peer overlay networks, and evaluate its performance. Furthermore, we integrate address virtualization to abstract from Internet addresses and provide transparent support for IP applications. Thus, no application-level gateways, proxies or modifications of applications are required to sanitize protocols from network level information. Acting as an IP-datagram service, our scheme provides a substrate for anonymous communication to a wide range of applications using TCP and UDP.

1. INTRODUCTION

In today's world, secure communication over the Internet is a challenging task. Recently it became known that the architecture of the most popular instant messenger Skype has been redesigned to enable communication surveillance on its users. The U.S. government is using secret warrantless requests to obtain personal information stored by service providers and is obtaining encryption keys from service providers by using legal means. Another aspect recently realized by society is that privacy cannot be achieved just by securing communication content. The communication metadata that shows the parties involved in the communication and their location might be even more sensitive as information than the content of communication and thus it must be protected as well. Therefore, in order to achieve communication privacy, we need a solution that would provide end-to-end encryption between communication parties and make collecting metadata very difficult. Sanwad messenger is a technology built on top of Tor which provides end-to-end encryption between Sanwad clients, but also hides the location of Sanwad users and prevents third parties from determining the parties with whom a Sanwad client is communicating.

Sanwad provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. A purpose of traffic analysis is to reveal who is talking to whom. The Sanwad is designed to be resistant to traffic analysis, i.e.,to make it difficult for observers to learn identifying information from the connection. Our implementation, Sanwad provides bidirectional and real-time communication similar to TCP/IP socket connections.

1.1 Literature survey

Sr.No.	Title	Author	Methodology	Year
1.	Performance and Security Analyses of Onion-Based Anonymous Routing for Delay Tolerant Networks	Kazuya Sakai; Min-Te Sun; Wei-Shinn Ku; Jie Wu; Faisal S. Alanazi	Delay tolerant network (DTN) routing provides a communication primitive in intermittently disconnected networks, such as battlefield communications and human-contact networks	2017
2.	Anonymous Communication in the Browser via Onion-Routing	Florian Burgstaller; Andreas Derler; Stefan Kern;	The goal of this work is to achieve anonymity within a network of communicating	2015

		Gabriel Schanner; Andreas Reiter	parties	
3.	Provably Secure and Practical Onion Routing	Michael Backes; Ian Goldberg; Aniket Kate; Esfandiar Mohammadi	The security and practicality of onion routing is measured	2012
4.	How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation	Robert Koch; Mario Golling; Gabi Dreo Rodosek	Explore strength and anonymity in the Tor network.	2016

1.2 System Architecture

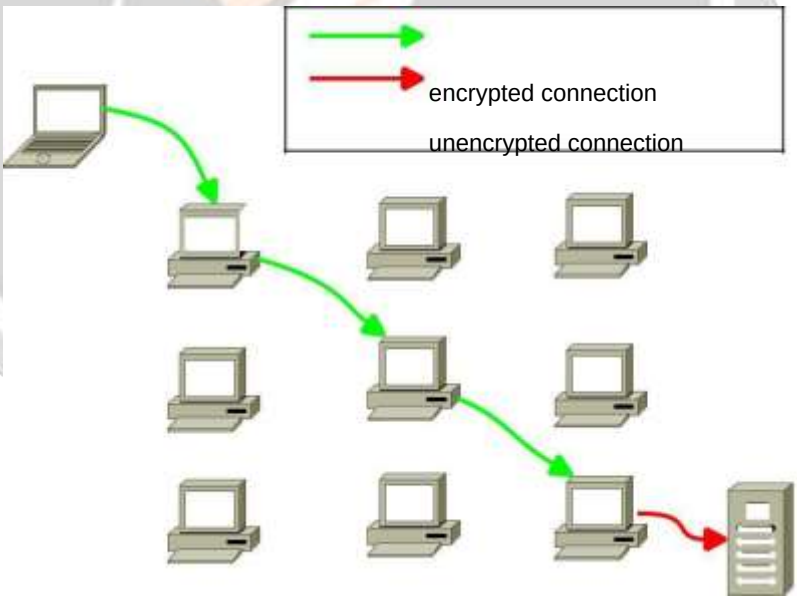

Fig1 System Architecture

The Tor client creates a private secure pathway called the Tor circuit through the Tor network to the destination. The circuit is made out of three Tor nodes. The circuit is extended one hop at a time and each node only knows where the data came from (the previous node) and where it should go (the next node). No single node knows all the nodes in the circuit. The client negotiates a separate set of encryption keys for each hop in the circuit to make sure that the connections could not be traced.

2. RELATED WORK

Study Paper:

1. Performance and Security Analyses of onion- Based Anonymous Routing for Delay Tolerant Network. Author: Kazuya Sakai, Min-Te Sun, Wei-Shinn Ku, Jie Wu, 2017

   Delay tolerant network (DTN) routing provides a communication primitive in intermittently disconnected networks, such as battlefield communications and human-contact networks.

2. Anonymous Is the Tor Network ? A Long – Term Black- Box Investigation.

   Author: Robert Koch, Mario Golling, Gabi Dreo Rodosek, 2016.

   Explore strength and anonymity in the Tor Network.

3. The TOR Data Communication System: A Survey.

   Author: Ramzi A. Haraty, Bassam Zantout, 2014.

   This paper thoroughly investigates one of the most communications for avoiding traffic analysis as well as assuring data integrity TOR. The paper also scrupulously present the benefits and drawbacks of TOR.

Methodoloy

This section presents the interface specification between the components in an onion routing system. To provide some structure to this specification, we will discuss components in the order that data would move from an initiating client to a responding server. There are four phases in an onion routing system: network setup, which establishes the longstanding connections between onion routers; connection setup, which establishes anonymous connections through the onion router network; data movement over a anonymous connection; and the destruction and cleanup of anonymous connections. We will commingle the discussion of these below.

Client Proxy

The interface between an application and the client proxy is application specific. The interface between the client proxy and the core proxy is defined as follows. For each new proxy request, the client proxy first determines if it will handle or deny the request. If rejected, it reports an application specific error message and then closes the socket and waits for the next request. If accepted, it creates a socket to the core proxy's well known port. In this we use protocol like RLOGIN, HTTP, SMTP which helps to respond proxy for connecting to the destination.

Core Proxy

If rejected, it sends an appropriate error code back to the client proxy, closes the socket, and waits for the next request. If accepted, it proceeds to build the anonymous connection to the responder proxy using the standard structure, sends the standard structure to the responder proxy over the anonymous connection, and then passes all future data to and from the client proxy and anonymous connection.

Onion and Onion Router Connection

To build the anonymous connection to the responder proxy, the core proxy creates an onion.An Onion is a multi-layered data structure that encapsulates the route of the anonymous connection starting from the responder proxy and working backward to the core proxy. During onion network setup (not to be confused with anonymous connection setup), longstanding connections between neighboring onion routers are established and keyed. The network topology is predefined and each onion router knows its neighbors and the RSA public keys of all nodes in the network. To remain connected to each of its neighbors, onion routers must both listen for connections from neighbors and attempt to initiate connections to neighbors. To avoid deadlock and collision issues between pairs of neighbors, an onion router listens for connections from neighbors with "higher" IP/port addresses and initiates connections to neighbors with "lower" IP/port addresses. "Higher" and "Lower" are defined with respect to network byte ordering. The protocol has two phases: connection setup and keying. The initiating onion router opens a socket to a well known port of its neighboring onion router, and sends its IP address and well known port (the port is included to allow multiple onion routers to run on a single machine) in network order to identify itself.

FUTURE WORK

In this paper, we present a novel approach to anonymous Internet communication: dynamic multipath Onion Routing. MORE routes each packet along a different path in an IP overlay. Compared to existing Onion Routers, MORE is not susceptible to pattern and timing based attacks and reduces the impact of overloaded relays. Its transparent architecture and name service allows a seamless integration of existing applications without changes to the applications or communi-cation protocols. MORE is implemented transparently in the network stack via virtual IP addresses.

CONCLUSION

The objectives set in the introduction were achieved. The Sanwad protocol has been documented, reference implementation has been audited, and as a result of security analysis, several security considerations were revealed that need to be considered when using Sanwad. The designer of Sanwad has made several smart design choices by exploiting the self-authenticating nature of Tor hidden services to provide authentication between Sanwad peers and by leaving the encryption and anonymity part to be handled by the well-tested and widely used Tor software.

However, several a ws were found in the implementation of Sanwad that make Sanwad users vulnerable to denial-of-service attacks and prevent Sanwad from achieving the privacy guarantees it could theoretically provide.

Despite the a ws found, the use of Sanwad might still be secure in a scenario where the peer's onion address does not became known to an adversary interested in attacking the person behind the Sanwad address.

Fortunately, the xes for the vulnerabilities found can be implemented in the code relatively easily and without needing to

change the design of Sanwad.

ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Pratik Kamble and Head of the Department Prof. Rupali Chopade for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of Marathwada Mitra Mandal's College of Engineering, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

1) Paul F. Syverson, David M. Goldschlag and Michael G.Reed, "Anonymous connection and onion routing",vol. 1.

IEEE, 1997.

2) Kazuya Sakai, Min-Te Sun, Wei-Shinn Ku, Jie Wu: "Performance and Security Analyses of onion-Based

Anonymous Routing for Delay Tolerant Network", IEEE, 2017.

3) Ina Jain, M. Choudary Gorantla and Ashutosh Saxsena, "An Anonymous Peer –to- Peer based Online Social

Network", Security and Privacy lab in Infosys Labs,IEEE,2011.

4) Ramzi A. Haraty and Bassam Zantout, " The TOR Data Communication System: A Survey", Department of Computer Science