Towards an Analysis of Onion Routing Security

Paul Syverson[1], Gene Tsudik[2], Michael Reed[1], and Carl Landwehr[3]*

[1] Center for High Assurance Computer Systems, Code 5540, Naval Research Laboratory, Washington DC 20375, USA.
{lastname}@itd.nrl.navy.mil

[2] Information and Computer Science Dept., University of California, Irvine CA 92697-3425, USA.
gts@ics.uci.edu

[3] Mitretek Systems, Inc., 7525 Colshire Drive, McLean VA 22102, USA.
Carl.Landwehr@mitretek.org

Abstract. This paper presents a security analysis of Onion Routing, an application independent infrastructure for traffic-analysis-resistant and anonymous Internet connections. It also includes an overview of the current system design, definitions of security goals and new adversary models.

Keywords: Security, privacy, anonymity, traffic analysis.

1 Introduction

This paper presents a security analysis of Onion Routing, an application independent infrastructure for traffic-analysis-resistant and anonymous Internet connections. It also includes an overview of the new system, definitions of security goals and new adversary models. Although the conceptual development and informal arguments about the security of Onion Routing have been presented elsewhere [9,15,16,10], we have not previously attempted to analyze or quantify the security provided against specific attacks in detail. That is the primary contribution of this paper.

The primary goal of Onion Routing is to provide strongly private communications in real time over a public network at reasonable cost and efficiency. Communications are intended to be private in the sense that an eavesdropper on the public network cannot determine either the contents of messages flowing from Alice and Bob or even whether Alice and Bob are communicating with each other. A secondary goal is to provide anonymity to the sender and receiver, so that Alice may receive messages but be unable to identify the sender, even though she may be able to reply to those messages.

An initial design has been implemented and fielded to demonstrate the feasibility of the approach. This prototype, which uses computers operating at the Naval Research Laboratory in Washington, D.C., to simulate a network of five

* Work by Carl Landwehr was primarily performed while employed at the Naval Research Laboratory.

H. Federrath (Ed.): Anonymity 2000, LNCS 2009, pp. 96–114, 2001.

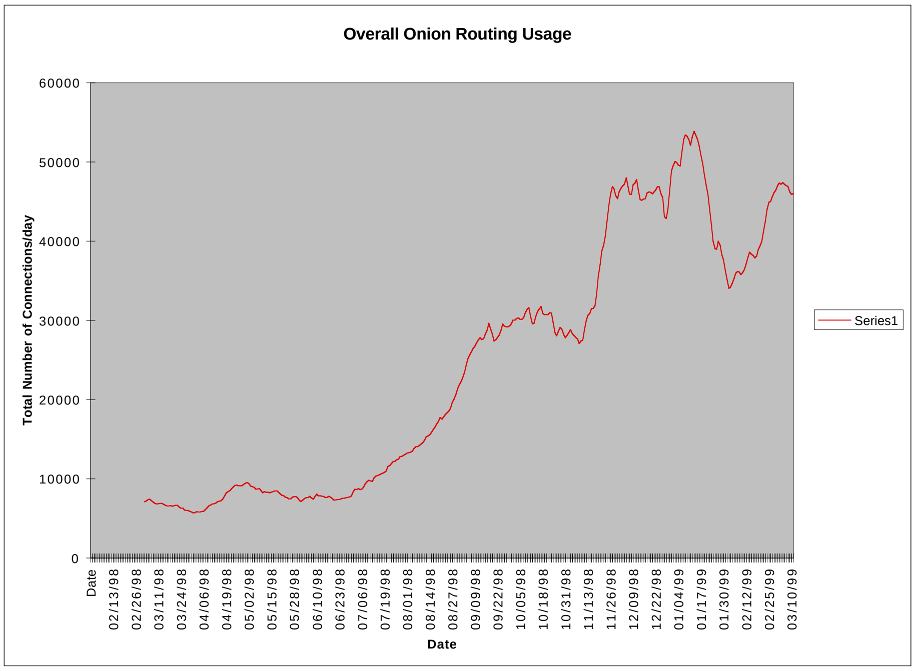

Fig. 1. 30 Day Rolling Average of Onion Routing Usage: 3/1/98 – 3/1/99

Onion Routing nodes, attracted increasing use over the two years it was available. While in operation, users in more than sixty countries and all seven major US top level domains initiated up to 1.5 million connections per month through the prototype system; cf. also Figure 1, which shows connections per day averaged over the preceding 30 days. This demand demonstrates both an interest in the service and the feasibility of the approach. However, the initial prototype lacked a number of features needed to make the system robust and scalable, and to resist insider attacks or more extensive eavesdropping. A design for a second generation system that addresses these issues is complete, and the processes required to release the source code for public distribution have been initiated. Several companies have contacted NRL to with intent to commercially license Onion Routing.

This paper analyzes the protection provided by the second generation design. We start by describing, briefly, the architecture and features of the second generation system relevant to our analysis. In section 3 we define security goals for anonymity and/or traffic-analysis-resistance. In section 4 we give some assumptions about the configuration of our network. In section 5, we set out our adversary model. In section 6, we present a security assessment based on the definitions and assumptions made in earlier sections. Finally, we compare Onion Routing to systems with similar goals, most specifically with Crowds [17].