Understanding New Anonymity Networks From a User's Perspective

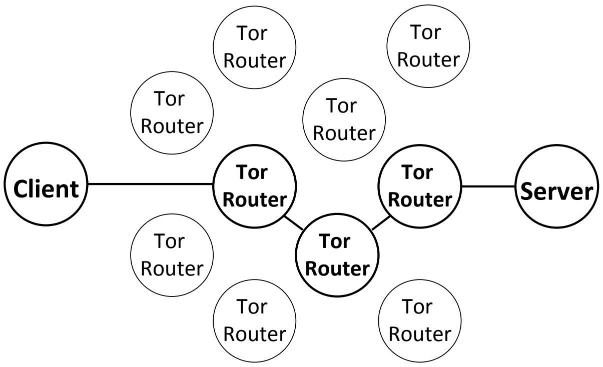
Erik Archambault and Craig A. Shue
Worcester Polytechnic Institute
archer@alum.wpi.edu, cshue@cs.wpi.edu

Introduction

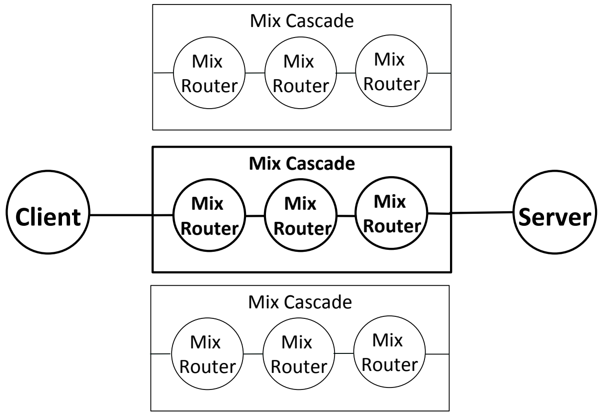
Anonymity networks have been studied for decades, both theoretically and practically. These systems allow users to access public services without fear of being identified or tracked. Several anonymity systems, such as Tor and Java Anon Proxy (JAP), have become popular enough for general Internet users. However, these systems constrain browsing performance are too complicated for some users. A new anonymity service, SurfEasy, has created a physical device that purports to provide easy, high performance anonymous network usage. However, the service does not readily describe the anonymity system it uses. In this work, we examine Tor, JAP, and SurfEasy from a performance and end-user perspective to characterize the tradeoffs in these systems and to provide a guide for analyzing future anonymity systems.

Anonymity System Architectures

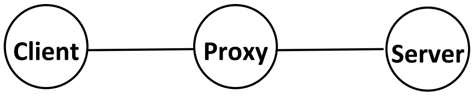
Tor (Onion Routing)



Java Anon Proxy (Web Mixes)



SurfEasy (Likely a simple proxy, may be like Anonymizer)



Methods

We examined Tor, JAP, and SurfEasy from a user's perspective, considering only properties that can be explored at the source and destination systems. In particular, we examined the latency and throughput of the systems, along with the observable IP address diversity.

We used PlanetLab to automate geographically distributed testing of Tor and the free version of JAP, though SurfEasy could only be tested from local machines due to its implementation. We used web sites which report the visitor's IP address as well as client-side packet capture to observe the IP addressing behavior of the systems while also measuring latency. We measured throughput by timing downloads from a well-connected server. SurfEasy's IP addressing behavior with regard to clients connecting from multiple geographically distributed locations was tested by using TorBox/Whonix as a transparent proxy, allowing us to connect to the SurfEasy network through multiple Tor nodes.

Relative Comparison

	SurfEasy	Tor	Java Anon Proxy
Latency	Best	Worst	
Throughput	Best		Worst
Observed Reliability	Best		Worst
Exit Node Rotation	Least (None)	Most	
Intermediate Nodes/Hops	One	Multiple	Multiple
Anonymous to Provider?	No	Yes	Yes
Estimated Anonymity	Worst	Best	
Estimated Ease of Use	Best		Worst
Pay to Use?	Yes	No	No (free version)

Findings

Our experiments show that SurfEasy currently offers superior Web browsing performance when compared to Tor and Java Anon Proxy. In our testing, it was also more reliable than either of the Tor or Java Anon Proxy systems. The system is still a new service and under development, and it may behave differently in the future as they expand the network.

SurfEasy offers superior performance, but the degree of anonymity it offers may be inferior to other modern approaches. We cannot determine the SurfEasy network's design with certainty, though substantial evidence suggests that it uses only a single proxy, possibly resembling the Anonymizer system. A single proxy server is weak against attacks and allows the server operator to trivially break a user's anonymity.