Abstract

The Tor anonymous network uses self-reported information measure ethics to pick out routers
for building tunnels. Since tunnels square measure assigned in proportion to the current information measure, this enables a malicious router operator to ask tunnels for compromise. Though Tor bounds the self-reported information measure, it uses a high most price, effectively selecting performance over high namelessness for all users. The router alternative algorithmic rule that permits users to manage the compromise between performance and secrecy. During this associate timeserving information measure measuring algorithmic rule to exchange self-reported values that's a lot of sensitive to load and a lot of perceptive to dynamic network things. This mechanism will effectively mergers the traffic from users of various preferences, creating partitioning attacks tough. And might additionally defensible to the antecedently printed low-resource attacks on Tor.

Refernces

- Robin Snader and Nikita Borisov, Member, IEEE, Improving Security and Performance in the Tor Network through Tunable Path Selection, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.

Index Terms

Computer Science

Networks
Keywords
Tor  Security  Privacy  anonymous Communication  Traffic Analysis  Path Choice  Information Measure Estimation.