Performance and Incentives in Anonymity Networks

Joan Feigenbaum, Aaron Johnson, and Paul Syverson

www.cs.yale.edu/homes/jf/econsecurity.html

NSF Grant CNS-0428422

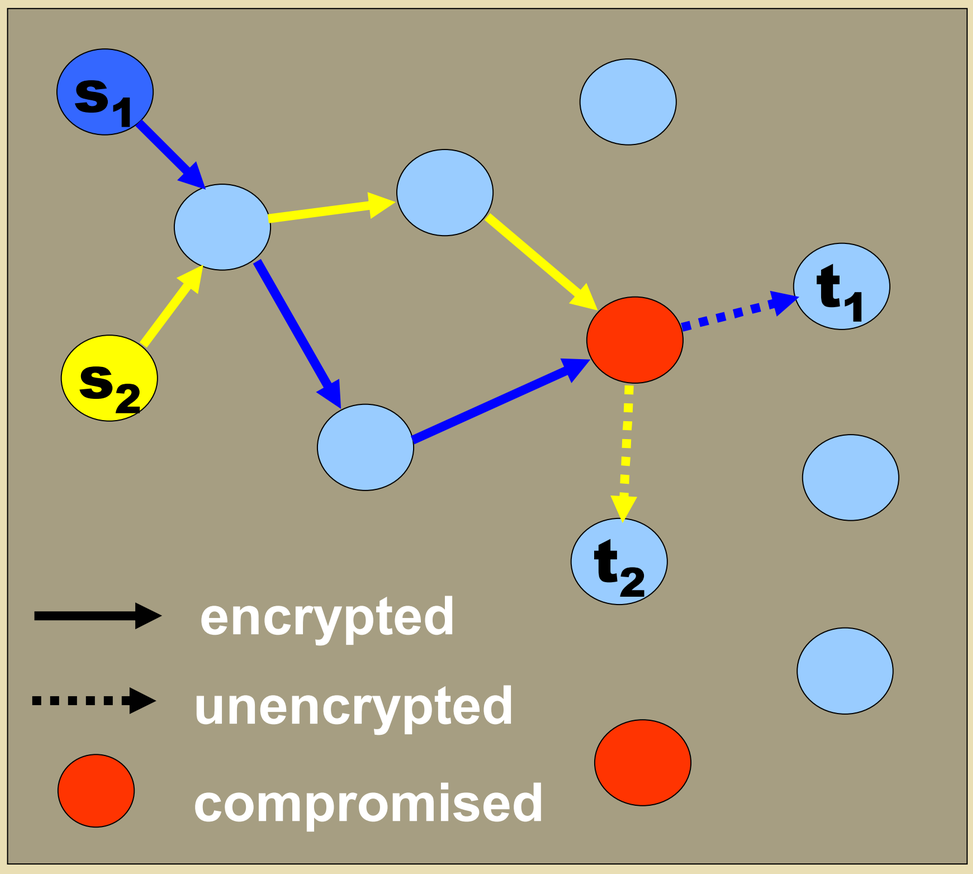
Problem

Onion routing is a practical scheme for anonymous communication. However, it does not offer formal privacy guarantees, and in practice users do not provide enough resources for good performance.

Approach

We formally model and analyze an onion-routing protocol. For various anonymity metrics, the anonymity lost is quantified as the amount the metric changes after observing parts of the system.

We assume agents are selfish and rational. Incentives for desirable behavior can be offered through good service or payments.



Approach and Impact

New approach	Research Impact
• Formally model the onion-routing protocol	• New anonymity guarantees in a practical and popular service (Tor)
• Give agents preferences over whole outcomes	• Suggestions for improved participation in onion routing

Technical Description

We model an onion-routing system using IO-automata. The network in the model provides asynchronous communication. The protocol we use is based on Tor, a real-world onion-routing network running on more than 750 routers. The adversary that we analyze is local and active in that he controls only a subset of the routers but can program them arbitrarily.

We incorporate probability into our model by assuming that users choose their actions from probability distributions. After observing the network, the adversary can infer a posterior distribution on the user responsible for a given action, such as sending a particular message or communicating with a given destination.

Results

- Anonymity is provided when the first or last router in a user's circuit is uncompromised.
- Expected increase in probability of discovery tends to **b*p**.
- Expected entropy preserved is at least $(1-b)^n$.

b is the fraction compromised. **p** is the prior probability. **n** is the number of users.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
January 28-30, 2007
Atlanta, Georgia

LUX ET VERITAS