Privacy-preserved Path Negotiation

Project Description

In source networking environments, the selection of routing paths is typically based on the sender's routing policy, without consideration for the receiver's intentions. To address this limitation, the concept of Consent Routing has emerged. Consent Routing involves sender and receiver collaboratively determining forwarding paths that align with their respective policies prior to communication. However, the process of path negotiation poses privacy concerns, particularly regarding the potential leakage of path policies. This project aims to mitigate such risks by developing a privacy-preserving path negotiation protocol that eliminates the explicit sharing of path segment sets. As a research-oriented endeavor, the participating student will contribute to designing the protocol, implementing a prototype, and evaluating its feasibility.

Main Tasks

Exploration of Path Negotiation Use Cases and Privacy Concerns:

- Analyze various scenarios where path negotiation is necessary and identify associated privacy risks.

Investigation of Existing Multi-Party Computation Frameworks:

- Explore and evaluate existing frameworks for multi-party computation to inform the design process.

Design and Implementation of Privacy-Preserved Path Negotiation Protocol:

- Develop a protocol that ensures privacy while facilitating path negotiation between sender and receiver.

Evaluation of Protocol in Real-World Environment:

- Conduct rigorous testing and evaluation of the protocol's effectiveness and efficiency in practical settings.

Preferred Qualifications

- Technical knowledge of cryptographic primitives, multi-party computation, and inter-domain networking
- General understanding of path-aware networking, e.g., SR-MPLS, IPv6-SR, or SCION
- Implementation experience in Go