The Tor network is a widely-used system for anonymous communication. It protects users’ anonymity by bouncing traffic through a network of relays between the client and the destination server. The Tor client initiates the circuit by selecting three relays, one of each type: guard, entry relay, middle relay and exit relay.

However, Tor is known to be vulnerable to network-level attacks (i.e., Autonomous Systems) who can observe both ends of the communication path. The traffic entering and leaving Tor are highly correlated, and thus are vulnerable to traffic correlation attacks.

The underlying Internet paths between a client and guard relay vary over time due to changes in the physical topology (e.g., failures, recoveries and the rollout of new routers and links) and AS-level routing policies (e.g., traffic engineering and new business relationships). These changes give a malicious AS surveillance power that increases over time.

Asymmetric traffic analysis inspects TCP headers in the observed transmission time, each requesting a 100MB image file from one of the 50 web servers, respectively. We use tcpdump to capture data for 300 seconds at the time, enabling the malicious AS to exactly deanonymize the client via asymmetric traffic analysis.

We successfully performed a BGP attack on an existing Tor relay. Note that our experiments did not compromise the privacy or safety of real Tor users. We attacked our own traffic and our own relay. We hosted an entry relay at Princeton, and advertised the covering IP prefix via GATECH. We setup a Tor relay node and advertised the prefix as its own. The attack causes a fraction of Internet traffic destined to the prefix to be captured by the adversary. Tor relay nodes can observe a large amount of client traffic. For example, a Tor guard relay observes information about client IP addresses. Thus, the IP prefixes corresponding to Tor guard and exit relays presents an attractive target for BGP hijack.

Right: Example of uncorrelated client/server pair using TCP ACKs.