Secure asymmetry and deployability for decoy routing systems - Write-up*

Avishek Mondal

I. What has the paper contributed

The paper proposed a new protocol that supports asymmetric routing. This protocol can help previous end to middle (E2M) systems that only supported symmetric routing to support asymmetric routing, as well as provide newer systems that do support asymmetric routing with better security guarantees.

A. How does the Asymmetric Gossip Protocol work?

This section mainly summaries Section 3 of [1]. The authors' key insight is that a relay station in the upstream path only needs to observe one upstream handshake message to compute the TLS master secret (i.e. the ClientHello message), while those in the downstream route need to observe multiple messages. Relays that have observed tagged traffic in the upstream part of the route "gossips" the received ClientHello messages to other known relay stations to reach a relay station on the downstream path. To do this "gossiping", the asymmetric tagging is modified from that used in previous systems. The TLS key exchange parameters are computed from the shared secret of the user and relay, as well as a context string that depends onlyl on the server's IP and the first 4 bytes of the ClientHello random nonce (as compared to requiring a TLS session ID in the context string of previous systems). The process is outlined in Section 3 of [1] as -

1) Client tags a connection to the over site (NotBlocked.com in Telex's use) for a relay station in the downstream of the traffic flow
2) When a relay station sees a ClientHello message in an upstream flow for which it has not seen the downstream ACK packets, and dos not recognise a tag in the random nonce, they "gossip" this nonce (whit the server IP address) to nearby relays
3) Each relay checks the gossiped nonce for a tag using its own private key. If it was tagged for them, they observe the downstream half of the flow. To begin observing, the challenge-response protocol is used
4) When the user next makes a connection ot the same non-blocked site, new parameters are generated based on the old client-relay shared secret that the downstream relay can reconstruct
5) After seeing the server's handshake messages, the relay computes the TLS master secret and replaces downstream content

After this modified TLS handshake between the downstream relay station and the client, the station begins to become the man-in-the middle between a covert site and the client.

*Paper is [1]

II. Strengths

A. Thorough review of existing proposed systems

As a novice reader to the field of E2M systems, the first 2 sections, and the first subsection of the third subsection are very thorough and easy to understand in order to be brought up to speed with what the latest research is.

B. Backwards compatibility

The paper shows how the new protocol can be used with systems that have already been proposed and implemented. This system-agnostic property increases the deployability of such a proposal.

C. Support of asymmetric routing

In comparison to previous works, this protocol does account for the real-world behaviour of Internet routing protocols, and has incorporated it to build a robust system that supports asymmetric routing without trading off too much of the security properties of systems that only supported symmetric routing.

D. Resistance to active and passive attacks

The authors have shown how this protocol is resilient to both active and passive attacks. The "threshold value" that the authors used to justify the system's defence against latency attacks could be better elucidated however, and a more thorough consideration of sophisticated attacks that utilise deep-learning tools that better classify and identify differences between covert and over traffic could be a potential new field of work.

III. Weaknesses

This paper was very good, and what are described as weaknesses are possibly future scopes of work.

A. Requirement of more stations

Compared to Telex, this protocol requires the presence of more relays. The costs of deploying will have to be borne by the ISPs and "friendly" ASes. This could be a hurdle in its deployability

B. Requirement for friendly ASes and ISPs

As with the Telex paper and all other E2M systems, the requirement for friendly ASes and ISPs to participate remains a limitation. What happens if assumed "friendly ASes" are in fact colluding with the adversarial nation state and deanonymising/tracking users of this system? What guarantees the privacy of the users against a "friendly AS" turning rogue?

References

[1] Cecylia Bocovich and Ian Goldberg. "Secure asymmetry and deployability for decoy routing systems". In: *Proceedings on Privacy Enhancing Technologies* 2018.3 (2018), pp. 43–62.