Counter-RAPTOR - Write-up*

Avishek Mondal

I. What has the paper contributed

The paper is further fleshes out the counter-measures in [2] against the RAPTOR suite of attacks. It contributes the following -

1) A new measurement study on the resilience of the Tor network to active BGP prefix attacks
2) A new algorithm for guard relay selection that incorporates resilience to active BGP attacks in its selection
3) BGP monitoring system that can detect routing anomalies on the Tor network in real time

II. How does the defence work, and how strong is it?

A. Guard selection algorithm

The guard selection algorithm is defending is against a BGP hijack/interception attack. By incorporating prior knowledge of AS paths in BGP, the origin-source resilience of a given source AS being resilient to attacks on a true origin AS is calculated, and incorporated with the bandwidth of a potential relay path to calculate a "weight" for a all potential paths. The path with the highest weight is selected.

B. BGP monitoring system for Tor

Here are the steps -

1) Collect data on current running relays every hour that the Tor Project releases. Don't need to care about individual relay IP addresses, only care about /24 prefixes which contain Tor guard and exit relay.
2) Pull live stream of BGP announcements, and filter out to focus on IP prefixes collected in previous step, and map them to an Autonomous System number (ASN).
3) Carry out routing anomalies using the following checks:
    a) Origin AS check - Compare origin AS to the owner AS in the given database. **Leads to many false positives, needs further tuning and caching**
    b) Frequency analytic - Measures frequency of each AS that originates a given prefix and normalise it(i.e. total number of times a given prefix is announced by a given AS divided by the total number of times a given prefix is announced by all ASes). If this is below 0.0025, flag as a possible attack.
    c) Time analytic - Similar to point 3b, if the equivalent measure for time is below 0.065, flag as a possible attack

*Paper is [1]

III. What are the strengths and weaknesses of the attack adn the paper?

A. Strengths

1) Real world demonstration: The paper demonstrates how real world BGP attacks have affected Tor, how the countermeasures perform in a live BGP hijack scenario
2) The defence achieves what its aim was, i.e. higher resilience against hijacks and interceptions, with minimal overhead. If defence required more overhead, the resulting user-base could have reduced, which in itself reduces the overall anonymity and security of the system.
3) In the average case scenario, there is not a significant degradation of anonymity or privacy. If a user is static, it will take observations of multiple guard choices to erode privacy and anonymity significantly. Given that usually, once a guard relay has been chosen, it will remain the guard relay for a period in order of months, the erosion of entropy over time is acceptable. Even then, it is only information about a client's AS that is revealed, and not the client itself.

The main summary of the strength of this defence can be summarised as the fact that BGP resilience is gained, but corresponding "sacrifice" is not significant. Perhaps future work could look at metrics to quantify these trade-offs.

B. Weaknesses, and possible attacks that can be successful

1) [3] is a paper that looks at how the erosion of privacy in the Tor network can occur over time. In particular, it has noted that Counter-RAPTOR doesn't account for the possibility that clients move, i.e. "the guard selection is done based on the client's initial location, and the same guard is used for several months even though the clients may move across locations" [3]. The paper goes on to show how just a few moves by clients increases the chance of a successful attack, i.e. the probability of an AS being able to observe both client-guard and exit-destination traffic and carry out website fingerprinting to further deanonymise the client
2) Given that an AS level adversary is considered, there are more potential points of failure. In the resilience calculation, data from multiple roots of trust - for e.g. data published by the Tor project, AS topology from CAIDA etc. are used. These are vulnerable to pollution by an adversarial AS, that could force the algorithm to choose a path through a compromising AS. In a similar way, the detection system proposed can also be compromised. Possible mitigation steps could include

multiple roots of trust that cross-reference each other, that will set the bar higher for an adversary to defeat.

3) The entropy reduces quickly over multiple observations of guard relay selection. The paper here considers a static point in time, and does not consider the effects of network churn, such as for example, some guard relays going offline over time etc. that could increase the number of observations of a client's guard relay selection that erodes entropy quickly.
4) This defence could also be foiled by an AS-level adversary who can force the client to choose guard relays multiple times in a short period of time through active attacks, for example by making guard relays go offline. This is acknowledged in [1] and [3], and this possibility is seen as remote.

REFERENCES

[1] Yixin Sun et al. "Counter-RAPTOR: Safeguarding Tor against active routing attacks". In: *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE. 2017, pp. 977–992.

[2] Yixin Sun et al. "RAPTOR: Routing Attacks on Privacy in Tor". In: *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 271–286. ISBN: 978-1-931971-232. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sun.

[3] Ryan Wails et al. "Tempest: Temporal Dynamics in Anonymity Systems". In: *Proceedings on Privacy Enhancing Technologies* 2018.3 (2018), pp. 22–42.