Telex: Anticensorship in the Network Infrastructure - Write-up*

Avishek Mondal

I. How does Telex work?

Telex is an anti-censorship system and operates as what the authors describe as an "end-to-middle" proxy. In this system of proxying, a server redirects part of the connection payload to an alternative destination, and other systems such as Tor have some implementation of this. To quote the paper's summary of a Telex connection -

1) Telex client on user device chooses a popular website that the censor will not block (called NotBlocked.com)
2) User connects to NotBlocked.com via HTTPS, and Telex client includes an invisible tag that lookes like an encrypted nonce to the censor, but can be verified by a station
3) Traffic traverses a "friendly" ISP with a Telex station on one of its routers
4) Station detects tag, instructs router to block connection through it and diverts traffic to Blocked.com (on censor's blacklist)
5) This continues until either side terminates the connection.

The tagging uses the Diffie-Hellman key exchange implemented on elliptic curve groups, with slight modifications. For tagged flows, a modified TLS handshake is also used.

II. What are the strengths and weaknesses?

A. Strengths

1) Strong threat model: The threat model assumed in this paper is very strong, and the goals the authors are aiming for are high. They have demonstrated that given their assumptions, the system meets these goals. The low latency for such a protocol is a great advantage that will increase the base of users adn adoption of this technology

2) Consideration of both active and passive attacks: The authors have considered a wide range of active and passive attacks, and have shown for most likely scenarios Telex is likely to be robust. The authors note that there is a possibility that a handshake replay attack that could be successful, but go on to show that for a majority of the NotBlocked.coms of the world, replayed packets will not accept replayed packets anyway. This thorough an investigation of possible attacks is beyond what most papers consider.

3) Assumption that governments will not "unplug" the Internet: As [2] has noted, several governments during the Arab Spring and other political events did indeed "turn-off" the Internet. But this paper has made the reasonable trade-off in the sense that such events are unlikely (and when it does happen, a censor's priorities would very likely be diverted elsewhere, such as regime survival etc.) in order to ensure superior performance. While it is a reasonable assumption, governments may try other methods to enforce censorship. [2] notes, one way to deal with Telex would be to only allow unencrypted HTTP traffic into the country. Something similar like this was mentioned in [3] regarding the Iranian government blocking Internet protocols in 2013 in the run up to its controversial elections. However, over a third of internet traffic uses HTTPS [3], so this is also an unlikely mode of attack as the government would also be likely "turning off" the Internet.

B. Weaknesses

1) Overhead: In the real-world implementation, the authors note a median overhead of approximately 60%. This is not practical for large scale deployment. It makes it more difficult to convince ISPs to let Telex stations be kept near their routers, because the extra overhead costs will have to be borne by the ISPs.

2) Limitations of real-world implementation: There are several issues that have to be worked out before Telex becomes fully functional. The paper does not take into account the asymmetric routing inherent in the Internet and in BGP routing. Traffic takes one route upstream, and another downstream - the likelihood of the Telex station being on both the upstream and downstream route is very small. There has to be a sufficient number of Telex stations in order for this system to be widely usable by a large number of people. Friendly ISPs will need to block traffic to the NotBlocked.com site, which itself requires numerous resources whose costs the ISPs will have to bear. These are all summarised neatly in [3]. Additionally, the authors mention using the "sneakernet" as its initial way of distributing the Telex client, i.e. by having people physically distributing the code for the client. This is simply not a scalable way of distribution in a country as large as say, China, and poses an unnecessary risk to those carrying out such physical distribution.

3) Requirement for government level support in deployment: **What happens if governments collude?** What happens if an adversarial country requests the country in which the Telex stations are, to block these servers from reaching blacklisted websites? Or for example if a assumed "friendly" ISP router stops forwarding any kind of traffic to Telex stations? A very real-world possibility would be that of the US and Saudi Arabia for example. This would be the biggest weakness of this system, because it assumes "friendly" networks that allow unmitigated traffic to operate.

*Paper is [1]

REFERENCES

[1] Eric Wustrow et al. “Telex: Anticensorship in the Network Infrastructure.” In: *USENIX Security Symposium*. 2011.

[2] Zachary Weinberg et al. “StegoTorus: a camouflage proxy for the Tor anonymity system”. In: *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM. 2012, pp. 109–120.

[3] 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.