Towards Secure Decoy Routing by Using SDN

Chaitanya Kumar   Vinayak Naik
IIIT-Delhi, New Delhi, India
chaitanya12031@iiitd.ac.in   naik@iiitd.ac.in

ABSTRACT

Software Defined Networking (SDN) is an emerging architecture, which allows networks to be centralized and programmable, aiding researchers in implementing complex network algorithms and policies. While SDN is widely used in LANs, it has also been deployed in WAN environments [2]. Like Tor, Decoy Routing [3] aids users to circumvent censorship on the Internet. While Tor uses onion routing, Decoy Routing uses some designated routers within the censored network, to divert traffic between the blocked destination and the client. Decoy Routing is faster than Tor as the former does away with multiple cryptographic operations.

As the traditional routers are not programmable, Decoy Routers are either servers with router software, or routers with proxy servers connected to them. In either case, such routers slow down traffic, nor is it scalable to manage them. We use SDN-based routers for Decoy Routing. In our work, we propose an SDN-based Decoy Routing protocol, without losing any of its Decoy Routing capabilities [1]. Our protocol is equally secure as the original Decoy Routing protocol.

Adversaries have used traffic analysis for attacking Tor and Decoy Routing. These routers have used traffic engineering to defend against these attacks. Thus, programmability of routers eliminates the need for servers or proxies, and the controller-based architecture gives us a consistent and centralized view of the Decoy Routing topology in the WAN. Although centralized, the SDN architecture and its implementation are robust. This central view of the network makes traffic engineering scalable [2].

BODY

Against existing censorship circumvention protocols, we propose SDN-based Decoy Routing that is faster and resilient to traffic analysis.

REFERENCES

[1] S. Chakravarty, V. Naik, H. B. Acharya, and C. S. Tanwar. Towards practical infrastructure for decoy routing (positional paper). In *Proceedings of the Workshop on Security of Emerging Networking Technologies (SENT) held in conjunction with 22nd Network and Distributed System Security (NDSS) Symposium.* Internet Society, 2015.

[2] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hölzle, S. Stuart, and A. Vahdat. B4: Experience with a globally-deployed software defined wan. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, pages 3–14, New York, NY, USA, 2013. ACM.

[3] J. Karlin, D. Ellard, A. W. Jackson, C. E. Jones, G. Lauer, D. P. Mankins, and W. T. Strayer. Decoy routing: Toward unblockable internet communication. In *USENIX workshop on free and open communications on the Internet*, 2011.