# Demonstration of Rebound: Decoy Routing on Asymmetric Routes Via Error Messages

Daniel Ellard, Christine Jones, Victoria Manfredi,
W. Timothy Strayer, Bishal Thapa, and Megan Van Welie
Raytheon BBN Technologies
10 Moulton Street
Cambridge, MA 02138
Email: {dellard,cej,vmanfred,strayer,bthapa,mvanweli}@bbn.com

***Abstract*—We propose to demonstrate *Rebound*, a decoy routing protocol that tolerates asymmetric routes without modifying the route taken by any packet that passes through the decoy router, making it more difficult to detect or disrupt than previous decoy routing protocols. We will demonstrate that Rebound can be used to browse the web and access other web services, such as Twitter.**

**Decoy routing [13], [15], [16], [17] is a powerful circumvention mechanism intended to provide secure communications that cannot be monitored, detected, or disrupted by a third party who controls the user's network infrastructure. Current decoy routing protocols have weaknesses, however: they either make the unrealistic assumption that routes through the network are symmetric (i.e., the router implementing the decoy routing protocol must see all of the traffic, in both directions, for each connection it manages), or they require forging packets and/or modifying the route taken by packets in connections that use the protocol, and these actions are detectable by a third party. Rebound is the first protocol that addresses both of these weaknesses.**

## I. Scope

We propose to demonstrate our implementation of Rebound, a decoy routing protocol. We will demonstrate using Rebound to browse the web and access other network services, such as Twitter, using a protocol that is secure and cannot be monitored, blocked, or tampered with by a third party who controls the user's network.

A full paper describing the details of Rebound will be presented at IEEE LCN'15. This demonstration will augment this paper and illustrate Rebound in a practical setting.

## II. Significance

Rebound is a novel decoy routing protocol that only needs to observe packets from the client to the decoy host, and does not forge packets from the decoy host. Rebound conveys *all* messages to the client, securely and privately, via the decoy host; the decoy router never sends messages directly to the client. Because Rebound tolerates asymmetric routes and never forges packets addressed to the client, it is able to work in a wider variety of network settings and withstand more types of attacks than any other decoy routing protocol.

### *A. An Introduction to Decoy Routing*

Decoy routing [13], [15], [16], [17] is motivated by the desire to mitigate developments in network infrastructure that enable network operators or other third parties to filter or monitor access to portions of the Internet.

Users of decoy routing establish ordinary connections to *decoy hosts* that the third party does not block or tamper with, and signals are encoded within those connections. Note that the decoy hosts are ordinary destinations on the Internet, such as popular web sites; these web sites are oblivious to decoy routing and are unwitting participants in the protocol.

If a decoy routing connection transits a *decoy router*, the router decodes the signal and uses a handshake protocol embedded in the ordinary traffic of the connection to validate that the connection was initiated by an authorized user. Once validated, the connection is redirected to a *decoy proxy*, which can be used to reach any service, using any protocol desired, regardless of the protocol used for the original connection. Meanwhile, a third party anywhere on the network between the user and the decoy router only sees what appears to be ordinary traffic to and from the original, unblocked destination.

The key difference between decoy routing and conventional proxy services [2], [3], [4], [5], [6], [9], covert channels [1], [7], [8], [11], or anonymization tools such as Tor [10], is that decoy routing uses real connections to *allowed* (or *decoy*) hosts and services outside of the filtered area as a conduit for clients within the filtered area to exchange information with *disallowed* hosts and services outside of it. A third party who wishes to block use of a conventional proxy service only needs to block the address of the proxies, but a third party who wishes to block use of decoy routing must block the addresses of all possible decoy hosts, which includes *every* web site that might be reached by the client via a route that includes a decoy router.

### *B. The Advantages of Rebound*

Previous decoy routing protocols have taken one of two approaches. The first approach makes the simplifying assumption that the decoy router observes all messages between the client and decoy host [13], [17]. This assumption is unreasonable because the route from the client to the decoy host is often different than the route in the reverse direction. He *et al.* observed that 65% of sampled routes between public traceroute servers have some degree of asymmetry at the AS level [12]. John *et al.* found that asymmetry increases dramatically as the routes use networks closer to the core of the Internet: on two Tier1 ISP backbone links, as many as 96% of the routes were asymmetric because of hot-potato routing [14].

The second approach taken by previous decoy routing protocols does not require observing messages in both directions, but instead forges messages, addressed to the client, that appear to be from the decoy host [15], [16], which introduces critical vulnerabilities to the protocol. There are a number of pitfalls that a protocol that forges packets can fall into, including timing analyses (if the timing of the packets is different from the timing of the packets created by a typical connection to the decoy host), stack fingerprinting (if the behavior of the decoy router does not precisely mimic the behavior of the decoy host), and connection state probes (if a third party can bypass the decoy router and directly query the connection state of the decoy host, it can detect that the decoy host is ”out of sync” with the apparent connection state of the client).

Rebound is a novel decoy routing protocol that only needs to observe packets from the client to the decoy host, and never forges packets from the decoy host. Rebound conveys *all* messages to the client, securely and privately, via the decoy host; the decoy router never sends messages directly to the client. All packets received by the decoy router are forwarded immediately to the decoy host, although in some cases their contents are modified by the decoy router.

In terms of flexibility of placement within the network and resistance to analyses based on latency analysis or the detection of forged packets, Rebound is an important addition to the family of decoy routing protocols.

## III. Required Equipment

We were not sure from the call for demos whether these will be presented serially (one demo at a time) or as a sort of ”poster session” of concurrent demos as was done last year. We list our requirements for both scenarios.

- Connection to the Internet. Preferably wired Ethernet, but wireless is is acceptable
- If presented serially, connection to a projector. Setup time: two minutes. Teardown time: one minute.
- If presented concurrently:
  - A table that can support two laptops and two 24” monitors (approximately 60-by-30” or larger).
  - Power for two laptops and two 24” monitors.
  - Setup time: five minutes. Teardown time: five minutes.

## References

[1] Analogbit: Tcp-over-dns tunnel software howto. http://analogbit.com/tcp-over-dns_howto

[2] Freegate. http://www.dit-inc.us/freegate

[3] Global pass. http://gpass1.com/gpass/

[4] Guardster. http://www.guardster.com

[5] Proxify web proxy. https://proxify.com

[6] Ultrasurf. http://www.ultrareach.com

[7] Baliga, A., Kilian, J., Iftode, L.: A web based covert file system. Proceedings of the 11th USENIX workshop on Hot topics in operating systems HOTOS (2007)

[8] Burnett, S., Feamster, N., Vempala, S.: Chipping away at censorship with user-generated content. USENIX Security Symposium (2010)

[9] Deibert, R.: Psiphon. http://psiphon.civisec.org/

[10] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. 13th USENIX Security Symposium (2004)

[11] Feamster, N., Balazinska, M., Harfst, G., Balakrishnan, H., Karger, D.: Infranet: Circumventing Web Censorship and Surveillance. In: 11th USENIX Security Symposium. San Francisco, CA (August 2002), http://wind.lcs.mit.edu/papers/

[12] He, Y., Faloutsos, M., Krishnamurthy, S., Huffaker, B.: On Routing Asymmetry in the Internet. In: IEEE GLOBECOM 2005 (November 28–December 2, 2005)

[13] Houmansadr, A., Nguyen, G.T.K., Caesar, M., Borisov, N.: Cirripede: circumvention infrastructure using router redirection with plausible deniability. In: Proceedings of the 2011 ACM Conference on Computer and Communications Security (CCS). pp. 187–200 (October 2011)

[14] John, W., Dusi, M., claffy, k.: Estimating Routing Symmetry on Single Links by Passive Flow Measurements. In: The 6th International Wireless Communications and Mobile Computing Conference (IWCMC 2010) (June 28–July 2, 2010)

[15] Karlin, J., Ellard, D., Jackson, A.W., Jones, C.E., Lauer, G., Mankins, D.P., Strayer, W.T.: Decoy routing: Toward unblockable internet communication. In: Proceedings of the 2011 USENIX Workshop on Free and Open Communications on the Internet (FOCI) (August 2011)

[16] Wustrow, E., Swanson, C.M., Halderman, J.A.: Tapdance: End-to-middle anticensorship without flow blocking. In: 23rd USENIX Security Symposium (2014)

[17] Wustrow, E., Wolchok, S., Goldberg, I., Halderman, J.A.: Telex: Anticensorship in the network infrastructure. In: Proceedings of the 20th USENIX Security Symposium (August 2011)