SiegeBreaker : SDN based Decoy Routing System

Piyush Sharma(IIIT Delhi)
Chaitanya Kumar(IBM IRL)
Aneesh Dogra(Direct I)
Vinayak Naik(IIIT Delhi)
H.B. Acharya(RIT,USA)
Sambuddho Chakravarty(IIIT Delhi)
Background and Motivation

Decoy Routing [Karlin11]: an approach to anti-censorship

- Proxy servers are easy to blacklist
- Idea: use smart routers as proxy servers
  - The user does not explicitly connect to a proxy.
  - Instead, he sends packets to an “overt destination”. Their path crosses the decoy router.
  - The router acts as a Man-in-the-Middle and proxies the connection to its real destination.

- Problem: making real routers smart enough
  - To detect secret handshake on packets to proxy
  - To perform MitM attack
  - To act as a proxy and set up connection to real destination
- Idea: Build the system using SDN switches
Proposed Architecture

- 1-4: Set up normal HTTPS connection to Overt Destination
- 5-7: Signal to Controller that this flow is for Decoy Routing. Special rule pushed to Switch: “send client-OD traffic to proxy”
- 8-9: Send real (Covert) Dest. and key for TLS session to the proxy server, encrypted using public key of proxy
- 10-13: MitM attack by proxy, hijacking HTTPS connection and connecting client to Covert Destination

Note 1: switch just redirects – the MitM is done by a full server.

Note 2: SiegeBreaker located outside boundary of censor country.
Evaluation and Work in Progress

System implemented and tested on Deter lab [Deter].

Performance is comparable with regular TCP connections.

Work in Progress : Implementation on real SDN switches (HP, Zodiac fx).
