Review of

How China Detects and Blocks ShadowSocks

By Alice, Bob, Carol, Jan Beznazwy, Amir Houmansadr

What is the problem?

Shadowsocks is a protocol for internet censorship circumvention popular especially in china. Since May 2019 there have been numerous reports of blocking of shadowsocks servers in China especially during sensitive times. This paper attempts to discover the techniques used by the great firewall of China to achieve this real time blocking of shadowsocks.

Strengths

- The paper is data driven and follows from experiments. They conduct 3 experiments.
    1. Shadowsocks server experiment. They setup shadowsocks clients in China and servers in US and UK(along with a control host) and record the probes sent by GFW
    2. Random data experiment. Based on the result of the initial experiment and their observations they conduct another experiment where now they do not use a real shadowsocks client, but are able to trigger active probing by GFW by just sending random data. They implement a TCP server with 2 operating modes: sink mode(server accepts TCP connections but does not respond with any data, and closes the connection in 30 seconds) and responding mode(server responds with random data to the GFW probes)
    3. Prober simulator experiment. Now they themselves send the probes to shadowsocks servers and record their responses. Based on this they claim that an attacker **can identify a Shadowsocks server with high confidence using statistical analysis of random probes.**
- They publish code so one can conduct the experiments themselves: https://gfw.report/talks/imc20/slides/

Limitations/Weaknesses

- They do not publish the actual pcap files or recorded probes. So the only way to verify these results is by conducting the experiment yourself

Summary of Key Results

- **GFW** detects shadowsocks in a 2 phase process: **1. Passive Traffic Analysis:** Based on **size** and **entropy** of the first data packet in each connection the GFW takes a list of suspected targets. **2. Active Probing: Active probing to confirm suspected targets:** The probes are partial replays of past legitimate connections, and random probes of varies length

- It designs active probes and based on the response of suspected shadowsocks server's responses it confirms it's guess. A lot of probes are required to confirm shadowsocks and it's based on statistical analysis, as opposed to confirming tor relays where only one active probe is enough.
- GFW probes from a lot of IPs with high churn. The 51,837 active probes were sent from 12,300 unique source IP addresses, all located in China
- However the probes are generated by just 7 unique processes(based on TSval of the packets), and most of them come form just 2 autonomous systems **: AS4837 (CHINA169-BACK-BONECNCGROUP China169 Backbone) and AS4134 (CHINANET-BACK-BONE No.31, Jin-rong Street)**.
- To protect against passive detection of shadowsocks traffic, the paper recommend the use of Brdgrd (bridge guard) is software that can be run on a Shadowsocks server that causes the client to break its Shadowsocks handshake into several smaller packets. Brdgrd was originally intended to disrupt the detection of Tor bridges by forcing the GFW to do complicated TCP reassembly, but here we take advantage of its ability to shape client packet sizes.
- To protect against active probing the paper recommends **1. PROPER AUTHENTICATION, 2. REPLAY FILTERING, 3. BEING CONSISTENT WITH SERVER'S REACTIONS**

Open Questions?

- In the random data experiment, 2 new types of probes were observed which were not observed on legitimate shadowsocks servers. If they were not directed towards shadowsocks, what protocols were they directed towards?
- In June 2020, VMess was discovered to be vulnerable to active probing. We want to test is this vulnerability has actually been exploited by the GFW