Make use of Debian to fight againt censorship Alternaitve way other than Tor

Roger Shimizu

Debian Developer

August 10th, 2017
DebConf17, Montréal

Outline

Outline

About me

- ARM porter
  - Ported Debian Installer to Buffalo Linkstation NAS series
    - ★ Bits to Linux kernel, mainly device tree related
    - ★ Bits to Debian Installer
    - ★ Ported GNU/Screen to Debian Installer (DebConf16 talk)
- Package Maintainer
  - shadowsocks-libev and its dependency (below)
    - ★ libbloom
    - ★ libcork
    - ★ libcorkipset

Disclaimer

- I just do packaging of code from upstream. I'm not security expert.
- If you find any flaw in the protocol, or bug in the code, please kindly report it.

Outline

Problem to solve

- Connecting to public Wifi
  - Some sites are hijacked
  - e.g. Google
    - ★ maybe the cafe just wants to collect some trends from customers
- Travelling to certain countries in middle-or-far east
  - Some sites are inaccessible (blocked)
  - e.g. Google, G/Mail, Wikipedia, Facebook, Twitter, YouTube, etc.

Real problem to solve, from technical side

- DNS poisoning
  - Gateway redirects out-bounding port 53 traffic to local DNS server
    - ★ 53 is the famous port for DNS
  - So you got affected even you specify famous public DNS
    - ★ Such as 8.8.8.8, or 2001:4860:4860::8888
- IP address of certain sites are blocked / blacklisted

Why not Tor?

- Tor is a great tool to protect privacy, and bypass the censorship restrictions as well.

But ...

Status of Tor

Pros

- Anonymous
- No account registration required
- Free of charge

Cons

- Slow
  - Confirmed with Tor member, that there's only latency problem, but for bandwidth, streaming 1080HD should be OK.
  - But user real experience is still slow in some area. Maybe related to packet-loss by QoS.
- Tor IP addresses are blocked in some part of this planet
  - For this case: need to collect not-yet-blocked bridge node list and set it up by users on their own.

Scenario which Tor works well, and not

Works for Tor

- Wikipedia (view)
- Messaging (Telegram/Signal, etc)
- Email
- Google / DuckDuckGo

Cases that not working well for Tor

- Wikipedia (editing)
  - Blocked due to abuse[1]
- YouTube / TED / Coursera

[1] https://meta.wikimedia.org/wiki/Editing_with_Tor

Outline

Alternative ways to Tor

Once you have a VPS account, there will be many ways ...

- SSH tunnel
  - Server: Install squid (port 3128) and turn on transparent proxy
  - Client: ssh -L 8080:localhost:3128 <VPS host>
  - Client: set up browser to use HTTP proxy: http://localhost:8080
- OpenVPN
  - There's fingerprint in OpenVPN packet that can be detected by Deep Packet Inspection
  - Not decrypting the data, but just being detected it's a OpenVPN packet
- ShadowSocks-libev

Outline

ShadowSocks-libev

- It's a socks5 proxy server & client, with flexible modern ciphers support.
  - Server: on the VPS
  - Client: on your PC, or mobile devices, which connects to server
  - Browser: connect to client via socks5 proxy
- The cipher is pre-defined on both server and client side
- There's no handshaking to prevent being detected by DPI (deep packet inspection)
- Many implementations
  - Original in python
  - libev port, most widely used (PC, OpenWrt, Android)
  - golang port, runs even on Win32

Supported OS (as client)

- Linux: Yes, and under GPLv3+
- OpenWrt: Yes, and under GPLv3+
- Android: Yes, under GPLv3+
- iOS: Yes; there're a few proprietary Apps, depends on NEKit toolkit under Expat license.
  - Any volunteer to make the iOS client a total free one?
- Windows: Yes, under GPLv3+
- macOS: Yes, under GPLv3+

History of ShadowSocks

- Due to its effectiveness of bypassing network restrictions, the user base increases quickly, and cannot be detected and blocked easily, the project was almost killed by gov-backed agent.
- We can still see a message of "code removed due to regulation" on the github project page.[2]

[2] `https://github.com/shadowsocks/shadowsocks`

Thanks, Debian!

- And this gets much harder now since the package and its source are in Debian archive and mirrored all over the globe.
- Debian is not only a platform to include Tor and ShadowSocks to fight with censorship, but also a infrastructure to protect software itself.

Advanced usage

- script: ss-nat
  - Gateway mode under Linux. Use iptables rule to redirect all the out-going packet to shadowsocks port.
- plugin package: kcptun
  - Speed up in packet-loss prone circumstances such as mobile network
- plugin package: simple-obfs
  - Simple obfusacting, and also an example and good base when need to write a complex one.

Outline

Welcome to new contributors

Wishlist waiting for contributors

- Open source iOS client
- Source code auditing
  - Protocol flaw?
  - Any security hole?
  - Any pattern to be detected by DPI?
  - Other security tool ever got audited, such as truecrypt[3]

[3] https://www.schneier.com/blog/archives/2015/04/truecrypt_secur.html

Thanks for coming!

Any question or comment would be appreciated.

Roger Shimizu
rosh@debian.org
https://wiki.debian.org/RogerShimizu