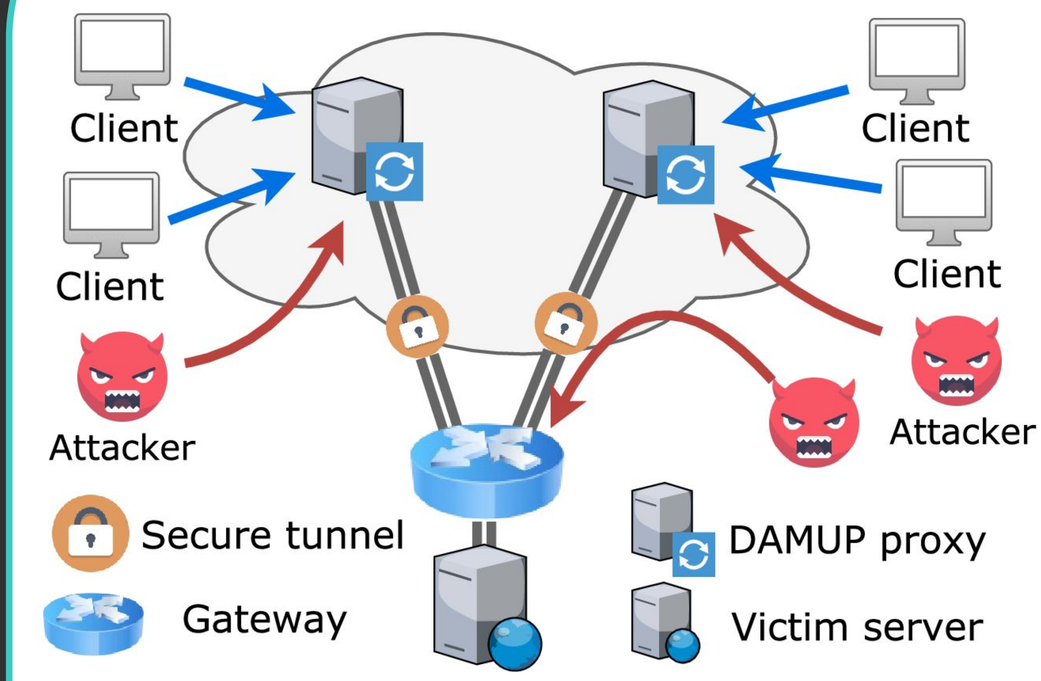
Challenges in Realizing Privacy-aware Cloud-based DDoS Mitigation Mechanism

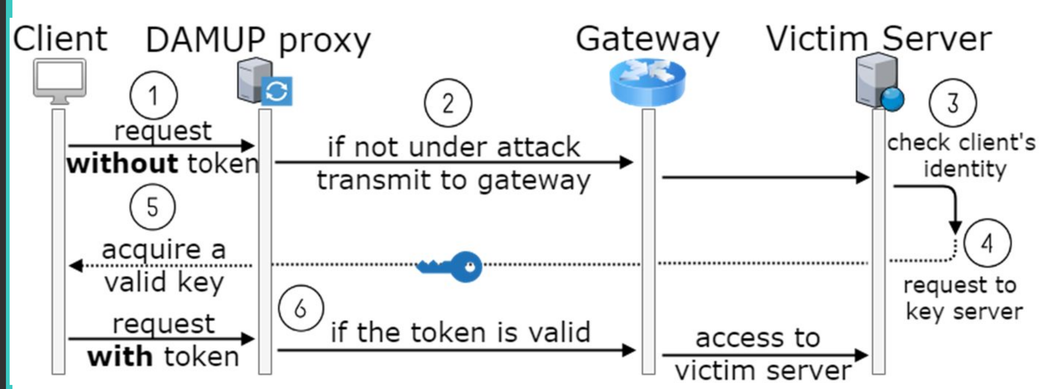
Su-Chin Lin, Wei-Ning Chen * and Hsu-Chun Hsiao*†
*Department of Computer Science and Information Engineering, National Taiwan University, Taiwan
†Research Center for IT Innovation, Academia Sinica, Taiwan

Introduction

- Current cloud-based DDoS mitigation service breaks the end-to-end security guarantee
- Privacy violation due to TLS private key sharing to third-party cloud
- Our previous work, DAMUP, proposed a privacy-aware architecture DDoS mitigation utilizing secure tokens

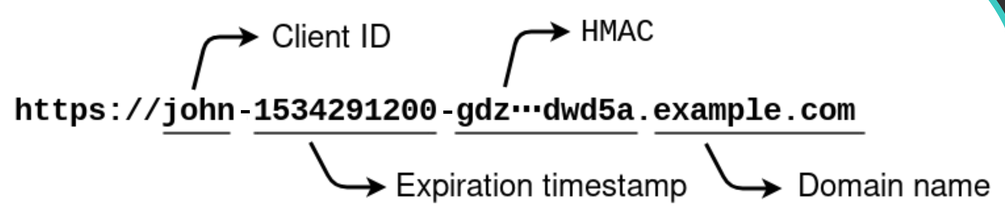
Architecture





- Victim Server will check their identity (e.g. 2FA), and grant the secret key
- Client requires a token to access Victim Server via the DAMUP proxy
- For clients without the token, they can access origin server if not under attack

Implementation



Secure Token

- Embedded in the Server Name Indication (SNI) field in the TLS handshake
- client ID, expiration timestamp, HMAC
- Implementation: open-source *sniproxy* library

Secure Tunnel

- IPsec IKEv2 VPN tunnel
- Origin IP protection
- Implementation: open-source *strongSwan* IPsec

Challenges

Token Tracking

- ISP may abuse the token for tracking
- Shorten the token life
- Rotate the client ID

Traffic Limit

- Adversary may acquire a few tokens
- Encoding the traffic limit information in the token leads to substantial overhead
- Leverage efficient flow monitoring approaches

SNI encryption

- Several IETF drafts discussing about SNI encryption
- TCP encapsulation with proxy
- Other TLS extension field

NSLAB

https://github.com/bookgin/damup