Background

Problem description: even with TLS, many identifiers in network traffic still reveal server identity, which enables network attackers to track user activity online

Our goal: leverage consolidation of web servers in clouds to hide from a network attacker the web server to which a client is connecting (server anonymity)
- Do not require extra browser extension or client software, and
- Hide web-server changes inside web programming frameworks, to minimize web developer effort
- Only minimally more expensive than HTTPS

Implementation

- Our design is realized as an OpenStack-based IaaS Cloud. We choose to use KVM as hypervisor, OpenvSwitch as SDN switch, and Nginx as web server.
- The backend of PoPSiCl store is implemented with 400 lines of C++ code.
- The SDN controller is implemented with 600 lines of C code.
- The TCP state migration module is implemented as a Linux kernel module.
- We also implemented traffic-analysis defenses within Ruby on Rails framework.

Evaluation

Our system was deployed and evaluated in the CloudLab testbed.

Scalability (1):

Scalability (2):

Scalability (3):

Scalability (4):

Design

PoPSiCl: a cloud service which offers user Personalized Pseudonyms for Servers in the Cloud.

Registration:

Access:

DNS query
Query name: www.example.com
IP: 111.111.111.111

PoPSiCl: Pseudo IP

Server Cert & Priv Key
PoPSiCl

Client Cert & Priv Key
PoPSiCl

Server Cert & Priv Key
PoPSiCl

Tenant Server ID

SDN Switch

DNS Server

PoPSiCl Store

PoPSiCl

Client Browser

(9) Client cert authentication

Server Cert verify

(1) DNS query (PopenSIC)

(3) DNS response (Pseudo IP)

(2) TLS (via SDN switch)

(4) Pseudo IP

(5) Establish TCP (via SDN switch)

(6) Rule update (PoPSiCl is SRB)

(7) TCP hand-off (PoPSiCl is SRB)

(8) Rule update (PoPSiCl is SRB)

(10) TLS (via SDN switch)

(11) TLS (via SDN switch)

(12) TLS (via SDN switch)

(13) TLS (via SDN switch)

(14) TLS (via SDN switch)

(15) TLS (via SDN switch)

(16) TLS (via SDN switch)

(17) TLS (via SDN switch)

(18) TLS (via SDN switch)

(19) TLS (via SDN switch)

(20) TLS (via SDN switch)

(21) TLS (via SDN switch)

(22) TLS (via SDN switch)

(23) TLS (via SDN switch)

(24) TLS (via SDN switch)

(25) TLS (via SDN switch)

(26) TLS (via SDN switch)

(27) TLS (via SDN switch)

(28) TLS (via SDN switch)

(29) TLS (via SDN switch)

(30) TLS (via SDN switch)

(31) TLS (via SDN switch)

(32) TLS (via SDN switch)

(33) TLS (via SDN switch)

(34) TLS (via SDN switch)

(35) TLS (via SDN switch)

(36) TLS (via SDN switch)

(37) TLS (via SDN switch)

(38) TLS (via SDN switch)

(39) TLS (via SDN switch)

(40) TLS (via SDN switch)

(41) TLS (via SDN switch)

(42) TLS (via SDN switch)

(43) TLS (via SDN switch)

(44) TLS (via SDN switch)

(45) TLS (via SDN switch)

(46) TLS (via SDN switch)

(47) TLS (via SDN switch)

(48) TLS (via SDN switch)

(49) TLS (via SDN switch)

(50) TLS (via SDN switch)

(51) TLS (via SDN switch)

(52) TLS (via SDN switch)

(53) TLS (via SDN switch)

(54) TLS (via SDN switch)

(55) TLS (via SDN switch)

(56) TLS (via SDN switch)

(57) TLS (via SDN switch)

(58) TLS (via SDN switch)

(59) TLS (via SDN switch)

(60) TLS (via SDN switch)

(61) TLS (via SDN switch)

(62) TLS (via SDN switch)

(63) TLS (via SDN switch)

(64) TLS (via SDN switch)

(65) TLS (via SDN switch)

(66) TLS (via SDN switch)

(67) TLS (via SDN switch)

(68) TLS (via SDN switch)

(69) TLS (via SDN switch)

(70) TLS (via SDN switch)

(71) TLS (via SDN switch)

(72) TLS (via SDN switch)

(73) TLS (via SDN switch)

(74) TLS (via SDN switch)

(75) TLS (via SDN switch)

(76) TLS (via SDN switch)

(77) TLS (via SDN switch)

(78) TLS (via SDN switch)

(79) TLS (via SDN switch)

(80) TLS (via SDN switch)

(81) TLS (via SDN switch)

(82) TLS (via SDN switch)

(83) TLS (via SDN switch)

(84) TLS (via SDN switch)

(85) TLS (via SDN switch)

(86) TLS (via SDN switch)

(87) TLS (via SDN switch)

(88) TLS (via SDN switch)

(89) TLS (via SDN switch)

(90) TLS (via SDN switch)

(91) TLS (via SDN switch)

(92) TLS (via SDN switch)

(93) TLS (via SDN switch)

(94) TLS (via SDN switch)

(95) TLS (via SDN switch)

(96) TLS (via SDN switch)

(97) TLS (via SDN switch)

(98) TLS (via SDN switch)

(99) TLS (via SDN switch)

(100) TLS (via SDN switch)