Zákonné odposlechy v SDN

83

Barbora Franková

xfrank08@stud.fit.vutbr.cz

Fakulta informačních technologií, Vysoké učení technické v Brně

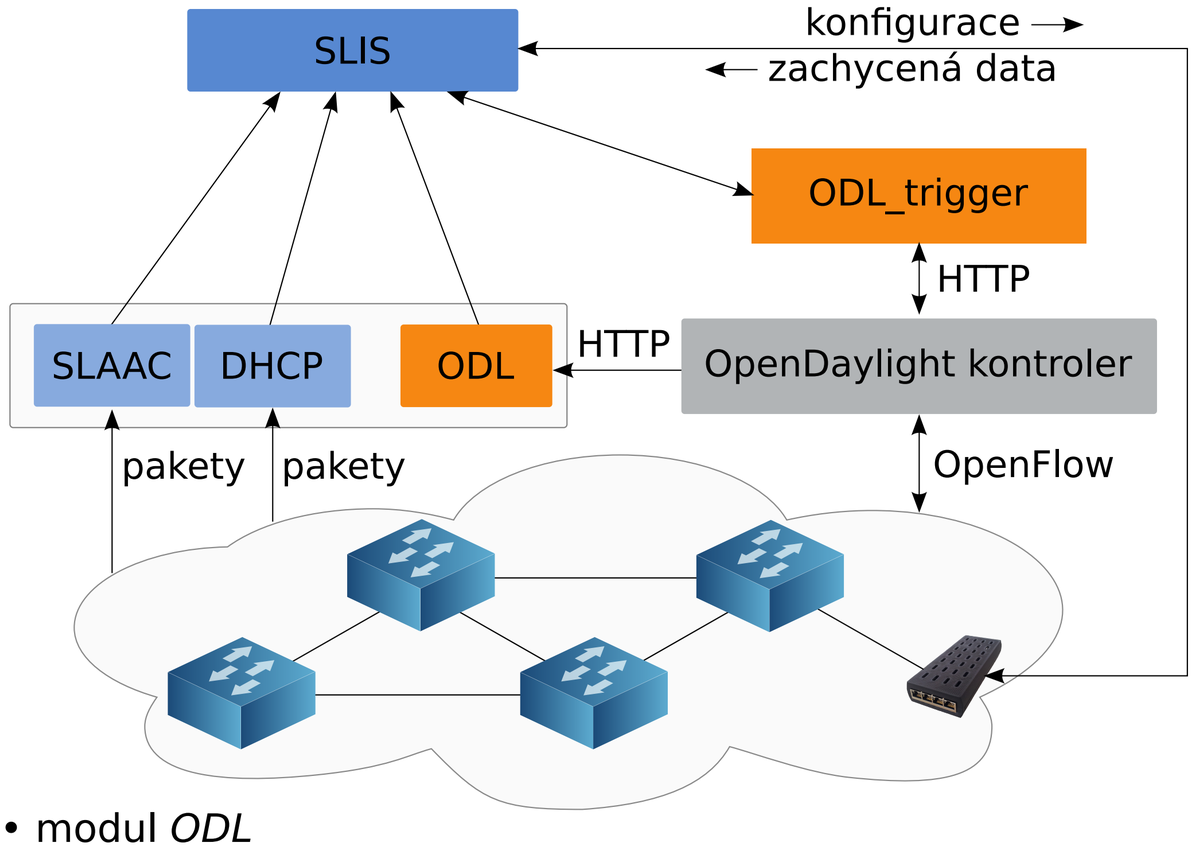
Motivace

- využití znalosti topologie ze softwarově definovaných sítí (SDN) v systému pro zákonné odposlechy (SLIS)
- cíle:
  - spolehlivější identifikace uživatelů
  - efektivnější využití sítě
  - dynamická rekonfigurace sond na základě aktuální topologie

Pojmy

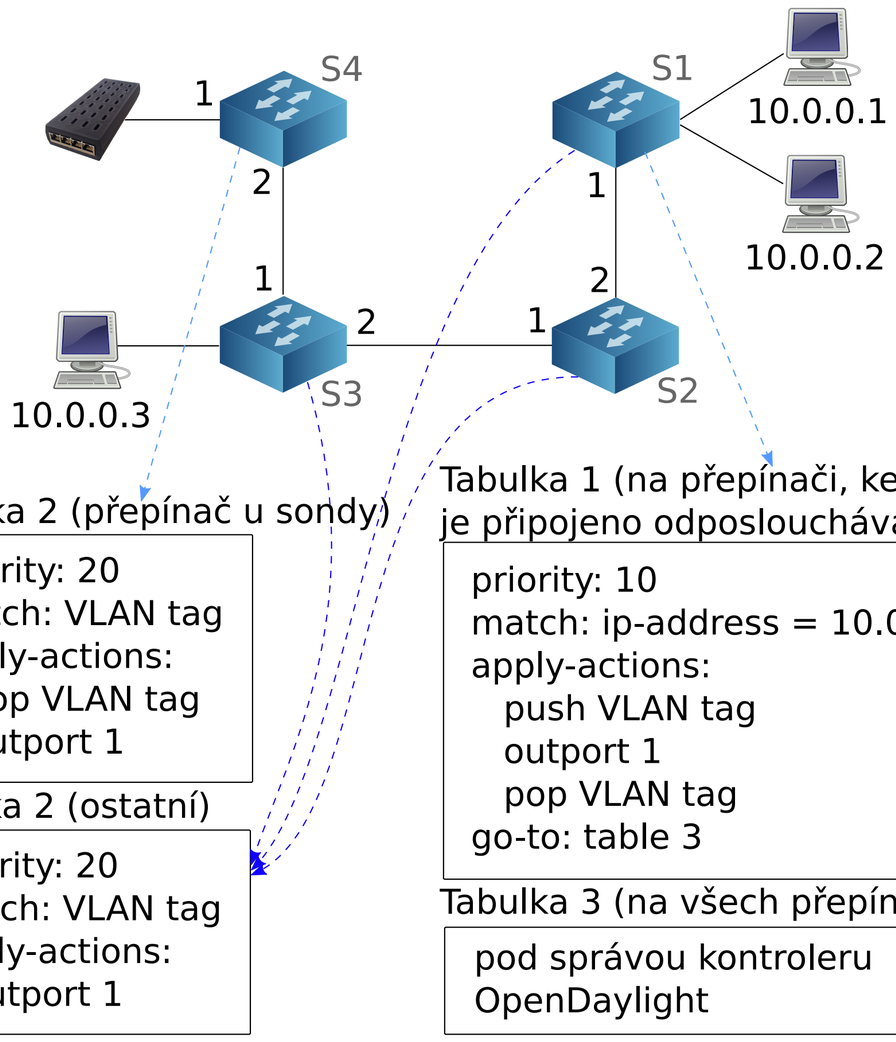
- Zákonné odposlechy
  - zákon o elektronických komunikacích (č. 127/2005 Sb.)
  - sytémy pro zákonné odposlechy umožují oprávněným orgánům sledovat komunikaci podezřených subjektů v počítačové či telefonní síti
- SLIS
  - implementace systému pro zákonné odposlechy, která vznikla v rámci projektu Sec6Net
- Softwarově definované sítě (SDN)
  - odděluje řízení sítě od samotného přeposílání paketů a umožňuje vytvářet programovatelné sítě
- OpenDaylight
  - opensource kontroler, který řídí síť a má přehled o topologii
- OpenFlow
  - rozhraní mezi kontrolerem a programovatelnými zařízeními
  - kontroler vytváří pravidla pro řízení sítě
  - pravidla identifikují datové toky a určují další zpracování (akce)

Řešení



- modul *ODL*
  - získávání identifikátorů koncových zařízení z kontroleru (IP adresa, MAC adresa, přepínač), které pak SLIS propojí a tím rozšíří informace o částečné identitě daného zařízení
- modul *ODL_trigger*
  - zjišťování topologie z OpenDaylight kontroleru
  - optimalizace konfigurace sond, které provádí odposlechy, podle jejich pozice v síti
  - dynamická rekonfigurace přepínačů k označování a přeposílání odposlouchávaných paketů k sondám, které neleží přímo na odposlouchávané lince

Ukázka konfigurace sítě



Tabulka 2 (přepínač u sondy)

priority: 20 match: VLAN tag apply-actions: pop VLAN tag outport 1

Tabulka 2 (ostatní)

priority: 20 match: VLAN tag apply-actions: outport 1

Tabulka 1 (na přepínači, ke kterému je připojeno odposlouchávané zařízení)

priority: 10 match: ip-address = 10.0.0.1 apply-actions: push VLAN tag outport 1 pop VLAN tag go-to: table 3

Tabulka 3 (na všech přepínačích)

pod správou kontroleru OpenDaylight

- konfigurace zařízení k označování a přeposílání paketů je postavena na využití tří tabulek toků
- každý přijatý paket se postupně porovává s pravidly od nejvyšší priority a je aplikováno první pravidlo, u kterého je nalezena shoda
- příklad vkládání pravidel na odposlech IP adresy 10.0.0.1:
  - do *první tabulky* zařízení S1 se vloží pravidlo, které bude porovnávat zdrojovou (cílovou) IP adresu, odpovídající pakety zduplikuje, označí VLAN tagem a odešle na port směrem k sondě
  - do *druhé tabulky* se na všech zařízeních vloží pravidlo, které bude odesílat pakety označené VLAN tagem k sondě
  - na zařízení S4 bude ve druhé tabulce pravidlo, které odstraní VLAN tag a předá paket sondě
  - *třetí tabulka* přeposílá původní pakety k cílovému zařízení
- výsledkem je dynamická konfigurace, která
  - konfiguruje sondy jednotlivě podle pozice v síti
  - konfuguruje zařízení tak, aby směrovaly označovaly zájmové pakety a směrovaly je k sondám
  - zabraňuje přetěžování některých sond

Závěr

- vytvořila jsem dva moduly, které využívají výhod SDN v systému pro zákonné odposlechy SLIS
- součástí navazující práce bude otestování systému v případě různých požadavků a omezení (kapacita sond, dostupnost sond, apod.)

Literatura

[1] L. Polčák, T. Martínek, R. Hranický, S. Bárta a další. Zákonné odposlechy v moderních sítích. Technická zpráva, FIT VUT v Brně, 2014

[2] European Telecommunications Standards Institute: TR 101 943: Telecommunications security; Lawful Interception (LI); Concepts of Interception in a generic Network Architecture, 2001, v1.1.1.

[3] L. Polčák, R. Hranický a T. Martínek. On Identities in Modern Networks. In *Journal of Digital Forensics, Security and Law.* 2014, roč. 2014, č. 2, s. 9-22.

Tato práce je součástí projektu VG20102015022 podporovaného Ministerstvem vnitra České republiky.