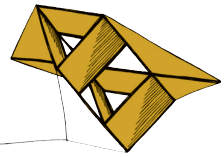


Analyzátor VPN komunikace

Aneta Koldovská[1]

1 Úvod

Koncept virtuálních privátních sítí (VPN) spočívá v zajištění určité míry soukromí přenášených informací (IP adres i dat) mezi komunikujícími stranami. Cílem tedy je zajistit dostatečnou formu privátnosti dat a odstínění probíhající konkrétní komunikace od mezilehlých nebo okolních uzlů sítě s využitím privátního spojení. Jak zmínil Heinzman (2019), při použití VPN může být veškerá komunikace posílána přes vzdálený server, tudíž poskytovatel internetového připojení nemůže vidět aktivitu uživatelů z důvodu jejího šifrování a tunelování. Stejně tak například webové stránky, které uživatel navštíví, nemohou odhalit skutečnou IP adresu používaného zařízení, protože je maskována adresou výše zmíněného vzdáleného VPN serveru.

VPN bývají také často využívány k obcházení internetových pravidel institucí, jako jsou například vysoké školy. V rámci Západočeské univerzity v Plzni (ZČU) bylo žádoucí detekovat uživatele VPN zejména v prostředí kolejní sítě, což byl hlavní důvod vzniku této bakalářské práce.

2 Popis aplikace

Jedná se o konzolovou aplikaci, která umí v současné době detekovat tři VPN služby. Konkrétně se jedná o *IPSec*, *OpenVPN* a *WireGuard*. Aplikace zpracovává soubor se zachycenou síťovou komunikací (například z kolejní sítě) tak, že nejprve vyfiltruje části dat, které s VPN komunikací nemají nic společného (jedná se například o protokoly ARP, DNS nebo ICMP a všesměrové nebo skupinové zprávy, tj. *broadcast* či *multicast* pakety) a následně po tomto předzpracování provádí podrobnější analýzu informací obsažených v hlavičkách jednotlivých paketů.

Celý program je strukturován do modulů (například pro každou VPN je implementován jeden modul). Uživatel analyzátoru si při spuštění programu prostřednictvím vstupních parametrů zvolí konkrétní protokoly, které chce v zachyceném provozu detekovat, a na základě této volby dojde ke spuštění vybraných modulů.

U každého paketu jsou zkoumány jednotlivé byty v hlavičkách, případně další charakteristické vlastnosti dané komunikace (například v případě IPSec detekce se zkoumají také standardně využívané porty této služby). U OpenVPN probíhá zpřesnění detekce s využitím stavového automatu dané komunikace. K tomuto doplnění se přistoupilo z důvodu zvýšeného výskytu falešně pozitivních výsledků u této VPN, což bylo způsobeno množstvím různých zpráv, které si mezi sebou zařízení vyměnila na počátku své komunikace.

Když analyzátor detekuje paket, který by mohl patřit VPN službě, pak jej přesune do připraveného slovníku, který je po dokončení hlavní analýzy dále zkoumán. Data ze slovníku projdou automatickou kontrolou na přítomnost kontrolních a datových paketů v rámci jedné

[1] studentka bakalářského studijního programu Inženýrská informatika,
obor Informatika, e-mail: anetkold@students.zcu.cz

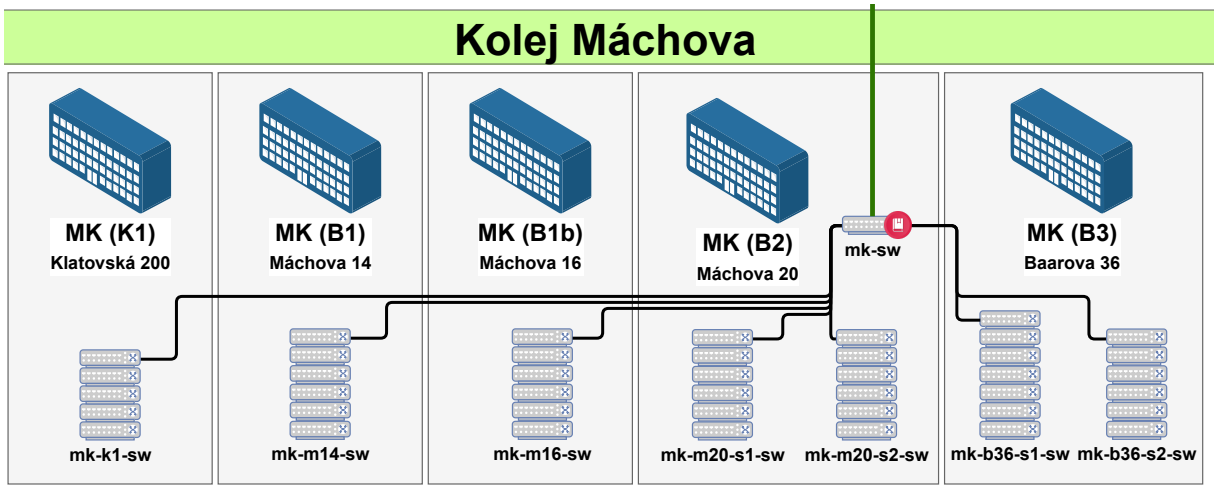
VPN komunikace. Pokud by chyběla jedna z těchto složek, tak je daný záchyt vyhodnocen jako falešně pozitivní a z výsledků detekce je odstraněn. Na základě obsahu slovníku se vytvoří *CSV* soubor, který se zapíše na disk a uživatel po jeho zobrazení vidí výsledky provedené analýzy komunikace.

3 Závěr

Spolehlivost výsledného analyzátoru byla porovnána s běžně dostupnými programy na detekci síťového provozu (do srovnání byly zahrnuty programy *WireShark* nebo *EtherApe*). Ukázalo se, že obě aplikace využívají k detekci zejména čísla portů daných protokolů. V případě, že bude konfigurace služeb změněna (například se změní standardní čísla portů), výše uvedené programy tyto protokoly v ostatním síťovém provozu nerozpoznají. Implementovaný analyzátor tento nedostatek řeší porovnáváním struktury hlaviček paketů, díky čemuž tyto aplikace překonává a jeho detekce je tedy přesnější.

Kvalita analyzátoru byla ověřena prostřednictvím testovacích dat z připravených scénářů, a také byla ověřena přesnost detekce VPN v zachycené síťové komunikaci, pocházející z reálného provozu. Místo, ve které se zaznamenával síťový provoz pro testování aplikace, je na obrázku 1 označeno červeným bodem.

V současné době je výsledný analyzátor využíván k analýze zachyceného provozu z kolejní sítě ZČU.



Obrázek 1: Schéma kolejní sítě Máchova ZČU.

Poděkování

Ráda bych poděkovala vedoucímu bakalářské práce Ing. Martinovi Šimkovi, Ph.D. za jeho rady, ochotu a čas, který mi věnoval při konzultacích. Dále bych ráda poděkovala Ing. Antonínovi Vrbovi za věcné připomínky a praktické rady při implementaci.

Literatura

Heinzman, Andrew. *Why do some websites block VPNs?* [online]. www.howtogeek.com, 2019 [cit. 2022/29/05]. Dostupné z: https://www.howtogeek.com/403771/why-do-some-websites-block-vpns/