REPUTATION SYSTEMS IN WIFI NETWORKS

Petr Blahák, Magister Degree Programme (2)
Dept. of Intelligent Systems, FIT, BUT
E-mail: xblaha11@stud.fit.vutbr.cz

Supervised by: Ing. Daniel Cvrček, Ph.D.

ABSTRACT

This document describes usage of reputation system in WiFi networks. Although it seems to be safe enough to activate WEP protection, in case when the key is compromised reputation system based on evaluation of metrics gathered from clients is used to distinguish valid users and attackers.

1 ÚVOD

Tento příspěvek pojednává o možnosti použití reputačního systému ve WiFi sítích. Zavedením reputačního systému se snažíme ověřit oprávněnost přístupu jednotlivých klientů k WiFi síti. Z přístupových bodů sítě jsou získávány informace o každém připojeném klientovi a následně je vyhodnocena jeho reputace.

2 CHARAKTERISTIKA KOMUNITNÍ BEZDRÁTOVÉ SÍTĚ

V České republice během posledních pěti let vzniklo několik desítek komunitních bezdrátových sítí. Sítě vznikly za účelem distribuce a sdílení dat a také především jako levná varianta připojení k síti Internet. Struktura komunitních sítí je většinou podobná. Několik přístupových bodů, propojených s centrálním serverem a jednou sdílenou bránou k internetu. Pro získání reálných dat pro reputační systém byla použita bezdrátová síť o následující topologii:

1. Přístupové body postavené z PC + operační systém Linux + WiFi karta xi626 + ovladače HostAP;
2. do bezdrátové sítě se připojují uživatelé, kteří mají pevnou privátní IP adresu, předem známou MAC adresu a používají zabezpečení WEP 128bitů;
3. síť obsahuje jednu Internetovou bránu;
4. síť obsahuje centrální server, kde běží reputační systém.

2.1 ODŮVODNĚNÍ POUŽITÉ TOPOLOGIE

Vycházel jsem z nejvíce používaného a rozšířeného zařízení v komunitních WiFi sítích v České republice. Přístupové body postavené z běžného nebo průmyslového PC mají velkou výhodu v možnosti použití standardní distribuce operačního systému Linux. Bezdrátová karta Z-com xi626 obsahuje zřejmě jeden z nejlepších chipsetů pro 802.11b - Prism 2.5. Ovladače HostAP umožňují přepnutí karty xi626 do módu MASTER, ve kterém karta funguje jako klasický bezdrátový přístupový bod. Pro zabezpečení je použit WEP 128b, lepší stupeň zabezpečení (WPA, 802.11i) není dosud příliš rozšířen v běžných WiFi zařízeních. V síti RepuNET nebudu řešit zabezpečení spojení mezi jednotlivými přístupovými body nebo spojení mezi přístupovými body a centrálním serverem. Budu předpokládat, že zabezpečení těchto linek je na dostatečné úrovni a mohu přes tyto linky přenášet data potřebná k nastavení přístupových bodů a k hodnocení reputace uživatele.

2.2 PROČ POUŽÍT REPUTAČNÍ SYSTÉM VE WIFI SÍTI?

Zabezpečení přístupového bodu pomocí 128bitového klíče WEP můžeme považovat za bezpečné. Proč tedy nasazovat další systém na zvýšení bezpečnosti? Důvod je jednoduchý, na přístupový bod se připojuje několik uživatelů se stále stejným WEP klíčem. WEP klíč je statický a při větším počtu připojených uživatelů je prakticky nemožné klíč rychle změnit v případě jeho prozrazení. Klientská zařízení nemají vždy možnost dálkové správy, takže jediná možnost, jak klíč operativně změnit, je každého uživatele kontaktovat (ať již e-mailem, dopisem nebo telefonem) a sdělit mu nový klíč. V okamžiku prozrazení klíče se síť stává nezabezpečenou a to je moment pro nasazení reputačního systému. Reputační systém by měl být schopen rozpoznat, jestli se jedná o řádného uživatele nebo o útočníka, který zjistil WEP klíč. Většina přístupových bodů umožňuje filtraci připojených klientů podle MAC adresy. Tento mechanismus povolí asociaci klientů, kteří mají zadanou svoji MAC adresu na přístupovém bodě. Filtrací MAC adres nedokážeme rozpoznat uživatele od vetřelce. Pouze víme, že dané WiFi zařízení má správnou MAC adresu, která byla uvedena při registraci. Útočník však může odposlechnout platnou MAC adresu a následně ji použít pro svoje zařízení, bude tedy bez problému asociován na přístupový bod.

3 NÁVRH SENZORU

Identifikace uživatele a útočníka je velmi složitá a riskantní. Při špatném vyhodnocení můžeme odpojit korektního uživatele nebo naopak povolit přístup útočníkovi. Základní data, která známe o klientovi jsou jeho IP a MAC adresy. Další informace, které mohou posloužit k jednoznačné identifikaci uživatele jsou: síla signálu, rychlost připojení, chybovost linky, ale také množství přenesených dat, doba připojení nebo nejčastěji používané služby (HTTP, FTP, ...).

3.1 ZÍSKÁVÁNÍ DAT

Registrace uživatele O každém uživateli máme základní informace, které jsou uloženy v databázi. Tyto údaje uvedl uživatel při registraci. Základní údaje jsou: jméno, příjmení, datum narození, adresa, email, telefonní číslo. Každému uživateli je vygene-

rováno identifikační číslo a následně přidělena IP adresa. Při přidělení IP adresy je požadována MAC adresa koncového WiFi zařízení uživatele.

Data z přístupových bodů Základní data, která můžeme získat z přístupového bodu, kde je klient asociován, jsou IP a MAC adresa koncového WiFi zařízení klienta. Většina WiFi klientů bohužel není plně transparentní a nedovoluje tak průchod MAC adres počítačů přes ně připojených.

3.2 VYHODNOCENÍ REPUTACE

Vyhodnocení, zda připojený uživatel je právoplatný nebo vetřelec, provádíme v několika krocích.

- Porovnání MAC a IP adresy - jedná se o porovnání záznamů získaných při registraci klienta se záznamy, které jsme získali z daného přístupového bodu. Tímto základním porovnáním jsme schopni zjistit, jestli si klient svévolně nezměnil IP adresu nebo nevyměnil WiFi zařízení. Případný rozdíl v porovnaných údajích může značit neoprávněného uživatele v síti.

- Síla signálu a úroveň rušení - tato data jsou dlouhodobě uchovávána v databázi ke každému klientovi. Náhlá změna síly signálu může být způsobena různými příčinami. Prudkou změnu signálu u skupiny klientů může způsobit např. špatné počasí, námraza na anténách, výskyt lokálního rušení. Náhlá změna síly signálu může ovšem značit i výskyt vetřelce, který se snaží vydávat za právoplatného uživatele.

- Množství přenášených dat - pomocí těchto dat získáme statistické údaje o tom, kolik dat uživatel přenesl.

Po vyhodnocení všech kritérií už můžeme s určitou pravděpodobností označit klienta za právoplatného uživatele nebo za vetřelce.

4 ZÁVĚR

Reputační systém v bezdrátových sítích dokáže usnadnit práci administrátorům, protože umí identifikovat uživatele a následně nastavit příslušná protiopatření ve spolupráci s dalšími aplikacemi (jako jsou iptables, snmp). Výstupním formátem dat z reputačního systému byl zvolen formát WEKA, což je formát používaný u nástrojů pro dolování dat. My jsme ho zvolili pro možnost dalších experimentů a vývoj algoritmů založených právě na dolování dat.

REFERENCE

[1] Jon Edney,William A. Arbaugh: Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004