802.1X WLAN NETWORK SECURITY

Lukáš Antal

Master Degree Programme (2), FIT BUT

E-mail: xantal02@stud.fit.vutbr.cz

Supervised by: Michal Drozd

E-mail: idrozd@fit.vutbr.cz

Abstract: Wireless networks in large organizations often use 802.1X authentication via EAP protocol. There are several EAP methods that can be used. This paper describes widely used method published by Cisco System called LEAP and its vulnerabilities and presents tool used for EAP method identification.

Keywords: 802.1X, WLAN, EAP, LEAP

1. ÚVOD

Bezdrátové WiFi sítě jsou v současné době součástí síťové infrastruktury téměř každé společnosti a organizace. Z důvodu dostupnosti WiFi signálu i mimo vyhrazené prostory je nutné věnovat bezpečnostnímu nastavení bezdrátové sítě náležitou pozornost, zejména pokud je bezdrátová síť součástí síťové infrastruktury organizace či společnosti, jejíž kompromitace by s sebou nesla finanční, reputační či jiná rizika.

2. 802.1X WLAN

Autentizační standard IEEE 802.1X byl původně vytvořen pro drátové LAN sítě, avšak s nástupem WiFi technologie našel uplatnění i u bezdrátových sítí. V architektuře WiFi sítě založené na tomto standardu vystupují tři entity: klient, autentizátor a autentizační server. Klientem může být jakékoliv zařízení podporující standard 802.1X. Autentizátorem je obvykle přístupový bod, fungující jako prostředník mezi klientem a autentizačním serverem. Autentizační server na základě údajů dodaných klientem rozhoduje o jeho připojení k síti.

Standard 802.1X využívá pro vlastní autentizaci protokol EAP. Existuje množství metod tohoto protokolu, které se navzájem liší požadavky na nasazení tak i svoji bezpečností. Tento článek se zabývá bezpečností jedné z nejrozšířenějších metod, a to metodou LEAP.

2.1. LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL

EAP metoda LEAP je proprietární metoda publikovaná společností Cisco Systems. V případě jejího použití se klient k síti hlásí svým uživatelským jménem a heslem. Heslo není přenášeno v otevřeném tvaru, ale je využit modifikovaný protokol MS-CHAPv1 implementující autentizaci typu Challenge-Handshake[1].

2.2. POPIS ZRANITELNOSTI

Na bezpečnostní nedostatky metody LEAP bylo poprvé upozorněno na konferenci DEFCON 1. srpna roku 2003. Výzkumník v oboru bezpečnosti bezdrátových sítí Joshua Wright zde prezentoval náchylnost metody na offline slovníkový útok[4]. Na tomto místě je nutné podotknout, že téměř každá autentizační metoda založená na zadávání hesla je v případě zvolení slabého hesla náchylná na tento útok. V případě metody LEAP však zranitelnost spočívá v markantním snížení časové náročnosti tohoto útoku. Pro úspěšné vykonání slovníkového útoku musí nejdříve útočník od-

chytit LEAP komunikaci autorizovaného klienta. Autentizace v rámci metody LEAP funguje na principu challenge-handshake a je založená na autentizačním algoritmu společnosti Microsoft MS-CHAPv1[2]. Následuje popis činnosti tohoto protokolu:

1. Autentizátor zašle klientovi 8B dlouhý challenge řetězec.
2. Klient vytvoří 16B dlouhý NT hash hesla, který použije k vygenerování 3DES klíčů (Algoritmus 3DES používá klíč o celkové délce 21B.) následujícím způsobem:
   - Klíč 1 = NT1 – NT7
   - Klíč 2 = NT8 – NT14
   - Klíč 3 = NT15 – NT16 + "\0\0\0\0\0"
3. Každým z klíčů je zašifrován challenge řetězec, výstupem jsou tři 8B dlouhé řetězce.
4. Klient zašle konkatenaci těchto řetězců (24B) autentizátoru jako challenge-response řetězec.
5. Autentizátor na základě přijatého challenge-response řetězce rozhodne, zda bude klient úspěšně autentizován.

Bezpečnostní problém spočívá v postupu vytvoření třetího DES klíče. Klíč je 7 bajtů dlouhý, avšak posledních 5 bajtů je vždy konstantních (bajty s hodnotou nula). Útok hrubou silou na algoritmus DES s klíčem dlouhým 16 bitů spočívá v projití pouhých 65536 možností. Prolomením třetího šifrovacího klíče je tak téměř v konstantním čase možné získat poslední dva bajty (výše označené jako NT15 a NT16) NT Hashe hesla.

V další fázi je nutné převést slovník s hesly na slovník obsahující pouze NT hashe těchto hesel. Jelikož použitý NT hash neobsahuje žádný salting materiál, je možné mít tyto slovníky předgenerované. Z tohoto souboru jsou poté vyfiltrovány NT hashe končící dvěma znaky, které byly zjištěny v přechozí fázi. Tím dojde k enormnímu snížení možných shod tak, jak zachycuje tabulka 1. Z každého ze slovníků byl náhodně vybrán jeden záznam a podle posledních dvou bajtů jeho NT hashe byl slovník vyfiltrován.

Slovník	Počet záznamů	Po filtrování
darkC0de.lst[1]	1707659	24
Ispell English Wordlist[2]	74158	2
AlphaNum 6char[3]	308915776	267

Tabulka 1: Redukce stavového prostoru pro hledání hesla.

V poslední fázi je proveden klasický slovníkový útok na MS-CHAPv1 algoritmus pouze s použitím hesel ze slovníku, jejichž NT hashe končí zjištěnými dvěma znaky. Pokud dojde ke shodě, je na základě NT hashe vyhledán odpovídající řetězec v původním slovníku, který je zároveň heslem uživatele bezdrátové sítě. Uživatelské jméno je v otevřené podobě obsaženo v EAP-Identity-Response paketu a útočník může tímto způsobem získat platné přihlašovací údaje uživatele.

2.3. IMPLEMENTACE

Spolu se zveřejněním popisu zranitelnosti metody LEAP byly zároveň uvolněny nástroje sloužící k automatizaci útoku vůči této metodě. Balík nástrojů Asleap[4] obsahuje aplikace pro převod slovníku na seznam NT hashů a také nástroj implementující výše popsaný slovníkový útok vůči zachycené

[1] http://static.hackersgarage.com/darkc0de.lst.gz

[2] http://downloads.sourceforge.net/wordlist/ispell-enwl-3.1.20.zip

[3] Veškeré šestiznakové permutace malých písmen anglické abecedy a číslic

[4] http://wirelessdefence.org/Contents/AsleapMain.htm

LEAP autentizaci. Vstupem nástroje je zachycená komunikace ve formátu pcap anebo specifikace challenge a response řetězce prostřednictvím parametrů. Tyto nástroje nemusí sloužit pouze útočníkům, ale také penetračním testerům provádějícím audit bezdrátové sítě.

Prvním krokem takového auditu 802.1X WLAN sítě je identifikace použité EAP metody. V současné době neexistuje automatizovaný nástroj provádějící tuto detekci. V rámci své diplomové práce jsem proto navrhnul a implementoval nástroj EAPtool. Jednou z jeho funkcionalit je právě tato detekce, která může být provedena ve dvou režimech.

Při použití pasivního režimu aplikace naslouchá síťovému provozu a v případě zachycení EAP autentizace jsou z této komunikace extrahovány informace o AP, klientovi, jeho uživatelském jméně a použité EAP metodě. Pokud je touto metodou právě LEAP, je komunikace uložena pro použití v rámci nástroje asleap. Výhodou tohoto režimu je jeho nedetekovatelnost prostředky WIDS. V aktivním režimu dochází přímo ke komunikaci s autentizátorem za účelem vylistování všech podporovaných EAP metod. Výhodou tohoto režimu je jeho rychlost, kdy není nutné čekat na zachycení autentizace klienta.

Dalším módem, který aplikace EAPtool v souvislosti s metodou LEAP podporuje, je tzv. penetrační režim. Vstupem aplikace je pak kromě názvu síťového rozhraní i slovník s hesly. Tento slovník je po spuštění aplikace předpřipraven, tedy převeden na seznam odpovídajících NT hashů. Penetrační mód je založen na pasivním módu s tím, že pokud aplikace detekuje probíhající LEAP autentizaci, jsou z ní extrahovány hodnoty challenge a response. Ty jsou následně předány aplikaci asleap spolu s připraveným slovníkem. Pokud se hledané heslo nachází v zadaném slovníku, jsou výstupem programu přihlašovací údaje uživatele, a to téměř okamžitě po jeho autentizaci. Tento mód slouží k usnadnění auditu uživatelských hesel.

3. ZÁVĚR

Na výběru vhodné metody protokolu EAP závisí zabezpečené celé síťové architektury. V tomto článku bylo poukázáno na fakt, že jedna ze stále často používaných metod obsahuje závažnou bezpečnostní chybu usnadňující útok hrubou silou na zachycenou autentizaci uživatele, který může vést ke kompromitaci uživatelských přihlašovacích údajů. Dále byla stručně představena aplikace EAPtool a její funkcionalita detekce použité EAP metodu, a to v aktivním i pasivním režimu.

PODĚKOVÁNÍ

Příspěvek vznikl v rámci výzkumného záměru Výzkum Informačních technologií z hlediska bezpečnosti (MSM0021630528). Práce byla podporována operačním programem Výzkum a vývoj pro inovace v rámci projektu Centrum excelence IT4Innovations (CZ.1.05/1.1.00/02.0070) a projektem Pokročilé bezpečné, spolehlivé a adaptivní IT (FIT-S-11-1).

REFERENCE

[1] Sankar, K.; Sundaralingam, S.; Miller, D.; aj.: Cisco Wireless LAN Security. Cisco Press, 2004, ISBN 1587051540.

[2] Schneier, B.; Wagner, D.; Mudge: Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). In Proceedings of the International Exhibition and Congress on Secure Networking - CQRE (Secure) '99, London, UK: Springer-Verlag, 1999, ISBN 3-540-66800-4, s. 192–203.

[3] Cisco Response to Dictionary Attacks on Cisco LEAP. [online], [cit. 2.3.2012]. URL http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

[4] Wright, J.;Weaknesses in LEAP Challenge/Response. [online], [cit. 19.3.2012]. URL http://asleap.sourceforge.net/asleap-defcon.pdf