Mendelova univerzita v Brně
Provozně ekonomická fakulta

Bezpečnostní rizika domácích bezdrátových sítí

Bakalářská práce

Vedoucí práce:
Ing. Jiří Balej

Lucie Kaplanová

Brno 2017

Provozně ekonomická fakulta

Ústav informatiky
Akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zpracovatelka: **Lucie Kaplanová**

Studijní program: Inženýrská informatika

Obor: Automatizace řízení a informatika

Název tématu: **Bezpečnostní rizika domácích bezdrátových sítí**

Rozsah práce: cca 40 normostran

Zásady pro vypracování:

1. Nastudujte problematiku zabezpečení bezdrátových sítí, podrobně se zaměřte na bezpečnostní mechanizmy pro autentizaci a šifrování v bezdrátových sítích standardu 802.11.
2. Proveďte rešerši publikací a závěrečných prací zabývajících se útoky na bezdrátové sítě.
3. Vyberte vhodný software k provedení analýzy odolnosti často používaných typů zabezpečení a zvolte vhodnou hardwarovou konfiguraci pro testování prolomení zabezpečení.
4. Sestavte scénář testu odolnosti zabezpečení bezdrátových sítí, který bude sloužit k systematickému prověření různých druhů zabezpečení s rozdílnou složitosti použitého klíče.
5. Na základě vytvořeného scénáře proveďte analýzu jednotlivých typů zabezpečení bezdrátových sítí. Ve výsledcích srovnejte odolnost jednotlivých typů zabezpečení a také časovou náročnost prolomení daného zabezpečení. Pokuste se porovnat teoretickou výpočetní náročnost se zjištěnou časovou náročností.
6. Zhodnoťte dostupná zabezpečení bezdrátových sítí standardu 802.11 a sestavte doporučení k jejich použití.

Mendelova univerzita v Brně

Seznam odborné literatury:

1. HUCABY, D. *CCNA Wireless 640-722 Official Cert Guide .* : Cisco Press, 2014. 600 s. ISBN 1-58720-562-9.
2. KIM, P. *Hacking: praktický průvodce penetračním testováním.* Brno: Zoner Press, 2015. 184 s. ISBN 978-80-7413-313-8.
3. KIZZA, J M. *Guide to Computer Network Security.* Londýn: Springer, 2015. 545 s. ISBN 978-1-4471-6653-5.
4. NAJERA-GUTIERREZ, G. *Kali Linux Web Penetration Testing Cookbook.* Birmingham: Packt Publishing, 2016. 296 s. ISBN 978-1-78439-291-8.

Datum zadání bakalářské práce: říjen 2016

Termín odevzdání bakalářské práce: květen 2017

L. S.

Lucie Kaplanová
Autorka práce

Ing. Jiří Balej
Vedoucí práce

Ing. Petr Jedlička, Ph.D.
Vedoucí ústavu

doc. Ing. Arnošt Motyčka, CSc.
Děkan PEF MENDELU

Poděkování patří především mému vedoucímu Ing. Jiřímu Balejovi za odborné vedení, vstřícnost při konzultacích a za cenné rady při zpracování této práce. Dále bych ráda poděkovala Ing. Tomášovi Koubkovi za poskytnutí virtuálního počítače prostřednictvím univerzitního serveru. Děkuji také své rodině za podporu při psaní této práce i během celého studia.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Bezpečnostní rizika domácích bezdrátových sítí**
vypracovala samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*
Jsem si vědoma, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.
Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 8. května 2017 .....

Abstract

Kaplanová L. Security threats of home wireless networks. Bachelor thesis. Brno, 2017.

This bachelor thesis describes the problem of home wireless networks security and is divided into two parts. The first part of this thesis is dedicated to authentication and encryption mechanisms according to the standard IEEE 802.11, attacks, methodologies, and tools of penetration testing. The second part of the thesis deals with the design of hardware configuration and creation of a test scenario used for systematic verification of security standards, using various complexity of the key. According to the results drawn from the performed analysis, the recommendation of home wireless networks security is presented.

Keywords: IEEE 802.11, Wi-Fi, wireless networks, security, penetration testing, Kali Linux, WEP, WPA, WPA2, WPS.

Abstrakt

Kaplanová L. Bezpečnostní rizika domácích bezdrátových sítí. Bakalářská práce. Brno, 2017.

Tato bakalářská práce se zabývá problematikou zabezpečení domácích bezdrátových sítí a je rozdělena do dvou částí. První část práce je věnována autentizačním a šifrovacím mechanismům spadajících do standardu IEEE 802.11, útokům, metodikám a nástrojům penetračního testování. Ve druhé části práce je navržena hardwarová konfigurace a vytvořen scénář testu, jenž slouží k systematickému ověření bezpečnostních standardů s využitím různé složitosti klíče. Z provedené analýzy jsou prezentovány výsledky, které odhalují bezpečnostní rizika jednotlivých typů zabezpečení, na základě kterých je sestaveno doporučení pro zabezpečení domácích bezdrátových sítí.

Klíčová slova: IEEE 802.11, Wi-Fi, bezdrátové sítě, zabezpečení, penetrační testování, Kali Linux, WEP, WPA, WPA2, WPS.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AES	Advanced Encryption Standard
Anonce	Authenticator's pseudo-random number
AP	Access Point
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CPU	Central Processing Unit
CRC-32	Cyclic Redundancy Check
EAP	Extensible Authentication Protokol
EAPOL	EAP over LAN
GTK	Group Transient Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
MAC	Media Access Control
MIC	Message Integrity Code
NIST	National Institute of Standards and Technology
Nonce	Pseudo-random number
OSSTMM	Open Source Security Testing Methodology Manual
PIN	Personal Information Number

PKE	Enrollee Public Key
PKR	Registrar Public Key
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTES	The Penetration Testing Execution Standard
PTK	Pairwise Transient Key
QSS	Quick Security Setup
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
SNonce	Supplicant's pseudo-random number
SSID	Service Set Identifier
TK	Temporary Key
TKIP	Temporal Key Integrity Protokol
TMK	Temporary Message Integrity Code Key
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup
XOR	Exclusive OR

1 Úvod

S rozvojem přenosných počítačů a chytrých telefonů neustále roste i množství bezdrátových sítí, které jsou v posledních letech velmi oblíbené. Hlavním důvodem rozvoje je volnost pohybu, kdy uživatel v prostředí pokrytém bezdrátovou sítí není nijak limitován, nízká pořizovací cena potřebného hardwaru s jeho snadnou konfigurací a možnost připojení vyššího počtu klientů.

V dnešní době jsou bezdrátové sítě nezanedbatelnou součástí mnoha domácností, restaurací, kaváren, obchodních center a dalších veřejných prostor. Za svého působení prošly několika vylepšeními, mezi která lze zařadit postupné zvyšování přenosové rychlosti a bezpečnější šifrovací i autentizační mechanismy.

Právě bezpečnost je v tomto typu počítačových sítí nejdůležitější, neboť data se šíří vzduchem a je nutno je zabezpečit tak, aby nemohla být odhalena. Probíhající komunikace mezi klientem a přístupovým bodem lze třetí stranou odchytit, avšak při uplatněném zabezpečení je obsah skryt. Pokud by komunikace nebyla zabezpečena, bylo by z odposlechu sítě možné získat informaci o uživatelských heslech, obsahu zasílaných zpráv a adres webových stránek, jež si připojený klient prohlíží.

2 Cíl práce

Cílem bakalářské práce je otestovat typy zabezpečení určené pro domácí bezdrátové sítě za použití klíčů s rozdílnou složitostí. K provedení testu poslouží sestavený scénář a zvolená softwarová a hardwarová konfigurace. Na základě získaných výsledků ze zrealizované analýzy bude vytvořeno vhodné doporučení pro zabezpečení domácích bezdrátových sítí.

3 Zabezpečení bezdrátových sítí

V této kapitole jsou popsány existující metody zabezpečení určené pro bezdrátové sítě, jejich principy ověřování vstupujících klientů a metody pro šifrování komunikace. Taktéž jsou představeny základní principy existujících útoků určených proti jednotlivým typům zabezpečení.

3.1 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP), uveden do provozu roku 1997, byl první protokol zabezpečující ověřování totožnosti vstupujících klientů do bezdrátové sítě a šifrování komunikace mezi klientem a přístupovým bodem. Šifrování dat probíhá pomocí sdíleného symetrického klíče a šifrovacího algoritmu RC4 (Rivest Cipher 4).

WEP bohužel neposkytuje přesně definovanou metodiku správy klíčů, která by jednoznačně určovala, jakým způsobem by mělo docházet k předání klíče mezi klientem a přístupovým bodem. Tento proces tedy zůstává na správci sítě, jenž sám určí postup distribuce klíčů (Broad, 2014, s. 50).

3.1.1 Princip autentizace

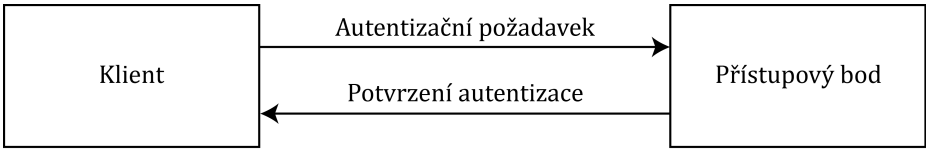
Standard WEP nabízí dva způsoby ověřování totožnosti, kdy je možné využít autentizaci pomocí otevřeného systému (Open system) nebo pomocí sdíleného klíče (Shared-Key).

Otevřený systém

Při autentizaci pomocí otevřeného systému klient vyšle autentizační rámec obsahující informace o síti, na který přístupový bod pouze odpovídá potvrzením, ve kterém klientovi povoluje přístup do sítě.

Jedná se o dvoucestný handshake neboli výměnu (obrázek 1), při které je autentizován každý klient žádající o připojení. Klient je asociován bez ověření, poněvadž nemusí přístupovému bodu poskytnout žádné přístupové údaje.

Tato metoda je hojně využívána veřejnými přístupovými body, u nichž je úmyslem zajistit klientům volný přístup (Carroll, 2011, s. 330–331).



Obrázek 1: Autentizace pomocí otevřeného systému

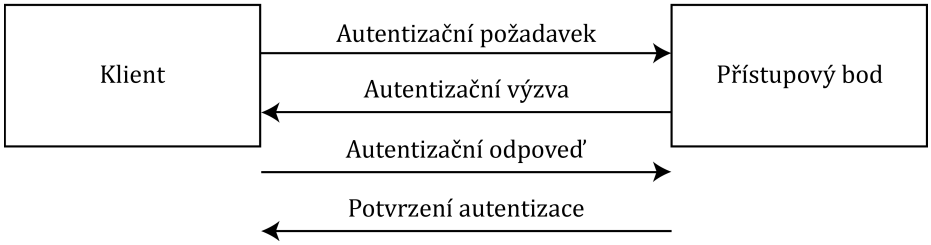
Sdílený klíč

Autentizace se sdíleným klíčem je prováděna ve čtyřech krocích (obrázek 2), při kterých je pouze ověřována správnost zadaného bezpečnostního klíče.

V prvním kroku klient zasílá autentizační požadavek přístupovému bodu, kdy žádá o ověření a vpuštění do sítě. Přístupový bod na požadavek odpovídá autentizačním rámcem s odpovědí, ve kterém je obsažena nešifrovaná náhodně vygenerovaná 128bitová hodnota Nonce představující autentizační výzvu.

Klient přijatou hodnotu zašifruje pomocí sdíleného WEP klíče a pomocí autentizačního rámce ji zasílá zpět přístupovému bodu. Ten ji dešifruje pomocí stejného klíče a získanou hodnotu od klienta porovná s původní vygenerovanou hodnotou.

Pokud dojde ke shodě, přístupový bod vytvoří poslední autentizační rámec, kterým klienta informuje o úspěšné autentizaci (Kurose, 2014, s. 558).



Obrázek 2: Autentizace pomocí sdíleného klíče

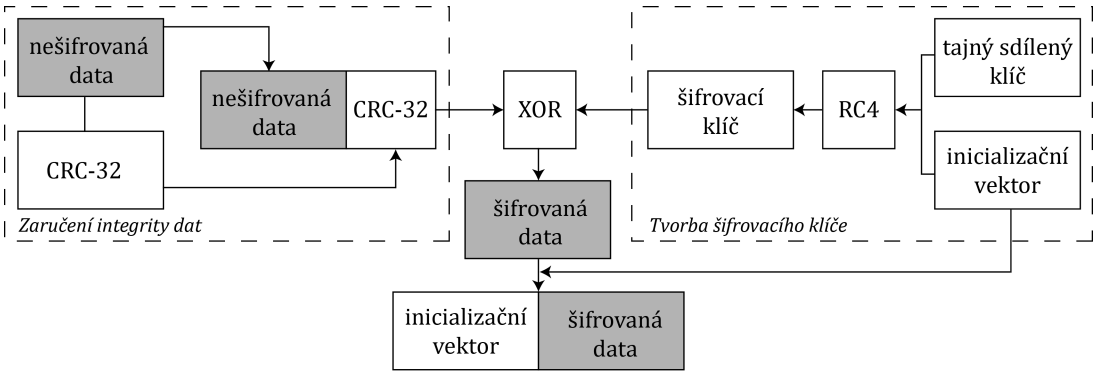
Z rozdílů autentizačních metod by se dalo říci, že verze sdíleného klíče je mnohem bezpečnější. Avšak při čtyřcestné výměně má útočník možnost zachytit autentizační výzvu i její následnou odpověď a kvůli nezašifrované komunikaci se pokusit o prolomení sdíleného klíče (Carroll, 2011, s. 331).

3.1.2 Princip šifrování

Protokol WEP aplikuje na datové vrstvě symetrickou proudovou šifru RC4 k šifrování a kontrolní součet CRC-32 (Cyclic Redundant Check) pro zajištění integrity dat a ověření při dešifrování, kdy je výsledná hodnota pojmenována ICV (Integrity Check Value).

Průběh šifrování začíná u prostého textu, ze kterého musí být v první řadě vypočten 32bitový kontrolní součet, který je připojen do rámce prozatímních nešifrovaných dat. Následně dojde k vygenerování inicializačního vektoru (IV) o pevně určené délce 24 bitů, který je využíván k inicializaci generátoru pseudonáhodných čísel RC4. Tím je zajištěno, že inicializační hodnota tohoto generátoru bude pro šifrovací klíč vždy jedinečná, což je hlavní pravidlo šifry RC4, která nedovoluje znovupoužití stejného klíče (Kizza, 2015, s. 413).

Inicializační vektor je následně spojen s tajným 40bitovým či 104bitovým sdíleným klíčem, z něhož je pomocí generátoru pseudonáhodných čísel RC4 vytvořen šifrovací klíč, jehož délka nabývá 64 nebo 128 bitů.



Obrázek 3: Průběh šifrování standardu WEP

Po vytvoření šifrovacího klíče je možné provést operaci XOR (exkluzivní logický součet) se zprávou doplněnou o kontrolní součet ICV. Touto operací vznikne konečný šifrovaný text, jehož prefix je doplněn o vygenerovaný inicializační vektor, který je přenášen spolu s šifrovanou zprávou kvůli možnosti dešifrování paketu příjemcem (Sosinsky, 2011, s. 387–388). Proces šifrování je zobrazen na obrázku 3.

3.1.3 Útoky na WEP

Standard WEP byl za dobu své existence vystaven mnoha typům útoků, které byly vytvořeny na základě odhalených nedostatků. Jak bylo řečeno, princip šifrování je založen na sdíleném klíči, který je využíván pro šifrování i dešifrování. Je nutné, aby všichni klienti v síti tento klíč znali a drželi jej v tajnosti.

Před šifrováním je sice vytvářen kontrolní součet pomocí CRC-32, který by měl zajišťovat integritu dat, ovšem žádným způsobem není ošetřena integrita vůči úmyslné modifikaci dat útočníkem.

Kritickým nedostatkem je generování inicializačních vektorů, které má podstatný vliv na šifrování pomocí RC4. V první řadě není přesně definován způsob, jak by mělo ke generování vektorů docházet, a není ani ošetřeno, co se stane při vyčerpání všech možností. Inicializační vektor je dlouhý 24 bitů, což znamená, že při vysoké přenosové rychlosti bude prostor rychle vyčerpán a poté bude přistoupeno k opakovanému použití stejného inicializačního vektoru, čímž ovšem dojde k porušení základní myšlenky šifry RC4.

Pokud k opakovanému použití IV dojde, nastane kolize, při které je vygenerován stejný šifrovací klíč, jenž může být odhalen odposlouchávajícím útočníkem (Kurose, 2014, s. 559).

Cafe Latte

Útok Cafe Latte umožňuje získat klíč WEP pomocí klienta, kdy je využito odchytávání ARP paketů. K tomuto jednání je aplikován falešný přístupový bod označený

jako Evil Twins, který má stejné SSID jako přístupový bod, ke kterému je vybraný klient momentálně připojen.

Klient je donucen se k falešnému bodu připojit a vyslat ARP pakety zašifrované WEP klíčem. Po přijetí jsou pakety útočníkem modifikovány a odeslány zpět pro vynucení dalšího provozu, kvůli odchycení co největšího množství těchto paketů a možnosti dešifrování sdíleného klíče (Aircrack-ng, 2009–2017).

FMS útok

Typ FMS, jehož název je odvozen od tvůrců Fluhrer, Mantin, Shamir, byl publikován v roce 2001 pod názvem *Weaknesses in the Key Scheduling Algorithm of RC4*.

Útok využívá chybu v generování inicializačního vektoru, kdy může dojít k částečné bitové shodě mezi inicializačním vektorem a šifrovacím klíčem. K útoku přispívají i hlavičky výsledných šifer, jejichž hodnota se vždy opakuje.

K odhalení klíče je nutné odchytit značné množství inicializačních vektorů, na základě kterých je početně určen výsledný bezpečnostní klíč (Vaudenay, 2001, s. 9–12).

KoreK chopchop

Tento útok byl navrhnut pro dešifrování datových paketů i bez nutnosti sdíleného klíče. K dešifrování jsou využity nedostatky protokolu WEP a chyby v algoritmu CRC-32, kdy je zapotřebí odchytit minimálně jeden datový paket.

Cílem není odhalit klíč WEP, ale dešifrovat či upravit probíhající komunikaci. Tento útok je pojmenován po autorovi s pseudonymem KoreK (Aircrack-ng, 2009–2017).

PTW

Posledním publikovaným útokem z roku 2007 je PTW, který je pojmenován po svých tvůrcích Pyshkin, Tews a Weinmann. K úspěšnému nalezení sdíleného klíče stačí nižší počet zachycených inicializačních vektorů než při útoku FMS, čímž dochází ke znatelnému zkrácení času.

Vzorem pro zhotovení tohoto útoku byl objev nových slabin šifrovacího algoritmu RC4, které byly roku 2005 zjištěny Andreasem Kleinem (Alamanni, 2015, s. 45).

3.2 Wi-Fi Protected Access

Protokol WPA, celým názvem Wi-Fi Protected Access, byl vytvořen v roce 2003 jako náhrada za protokol WEP, který byl v roce 2001 prolomen a uznán společností Wi-Fi Alliance za bezpečnostně nedostatečný.

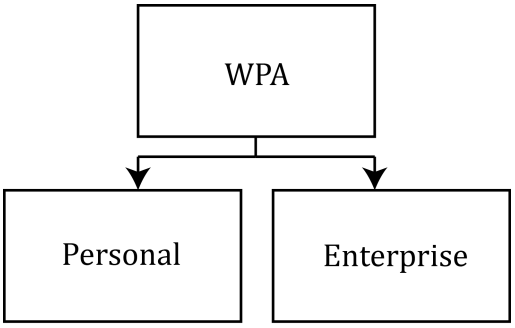
WPA byl navrhnut pouze jako dočasné řešení před úplným dokončením nového standardu IEEE 802.11i, známým spíše pod označením WPA2. K ochraně komunikace je aplikován protokol TKIP (Temporal Key Integrity Protocol), který stále využívá šifru RC4 s využitím inicializačních vektorů.

Motivací pro zavedení byla udržitelnost zabezpečené komunikace v rámci bezdrátové sítě a možnost zpětné kompatibility s dosud využívaným hardwarovým zařízením s případnou softwarovou aktualizací (Broad, 2014, s. 50–51).

3.2.1 Princip autentizace

Protokol WPA nabízí dvě možnosti autentizace. Pro domácí a malé podnikové sítě je využívána autentizace pomocí předsdíleného klíče, zkráceně PSK (Pre-Shared Key). Většinou je tato metoda nazývána jako WPA Personal.

Pro komerční a rozsáhlejší bezdrátové sítě je určen standard IEEE 802.1x využívající protokol EAP (Extensible Authentication Protocol) pro komunikaci klienta s přístupovým bodem a protokol RADIUS (Remote Access Dial In Users Service), jenž slouží jako autentizační server zajišťující ověřování vstupujících klientů. Označení pro tento typ autentizace je WPA Enterprise (Carroll, 2011, s. 341–342). Jelikož je práce zaměřena na domácí bezdrátové sítě, nebude standard IEEE 802.1x dále představován.



Obrázek 4: Autentizační metody standardu WPA

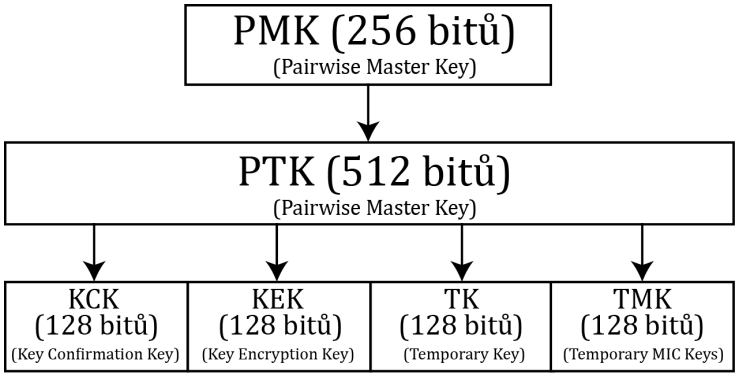
Předsdílený klíč

Autentizace pomocí předsdíleného klíče je prováděna pomocí čtyřcestné výměny, avšak za pomoci jiné bezpečnostní politiky než u standardu WEP. Ačkoli se stále jedná o nešifrovanou výměnu čtyř autentizačních zpráv, ani v jedné nefiguruje předsdílený klíč, který je ovšem základem pro odvození klíčů pomocných. Předsdílený klíč má stejnou hodnotu pro všechny autentizované klienty.

Před zahájením autentizace, je za pomoci předsdíleného klíče nabývajícího osm až šedesát tři znaků a SSID bezdrátové sítě vytvořen 256bitový klíč PMK (Pairwise Master Key) neboli hlavní klíč relace. Klíč je vypočten a udržován zvlášť na klientovi i na přístupovém bodě.

Poté je na přístupovém bodě, na základě PMK a aktuálního času, vygenerována náhodná hodnota ANonce (Authenticator's pseudo-random number) dlouhá 256 bitů, která je posléze zaslána klientovi první EAPOL (EAP over LAN) zprávou, jež je zapouzdřená v ethernetovém rámci (Odom, 2009, s. 631–633).

Klient po přijetí zprávy vygeneruje svoji náhodnou hodnotu SNounce (Supplicant's pseudo-random number) dlouhou taktéž 256 bitů, kterou odešle druhou EAPOL zprávou přístupovému bodu. Na základě těchto získaných hodnot je s využitím PMK a MAC adresy klienta a přístupového bodu vytvořen unikátní 512bitový klíč PTK (Pairwise Transient Key). Ten slouží pro zajištění šifrované jednosměrové (unicast) komunikace, z něhož je první 128bitová část (KCK – Key Confirmation Key) využita pro vygenerování klíče MIC (Message Integrity Check), který slouží ke kontrole integrity dat v probíhající komunikaci (obrázek 5). Klíč PTK je udržován na klientovi i přístupovém bodě k určení dočasných šifrovacích klíčů.

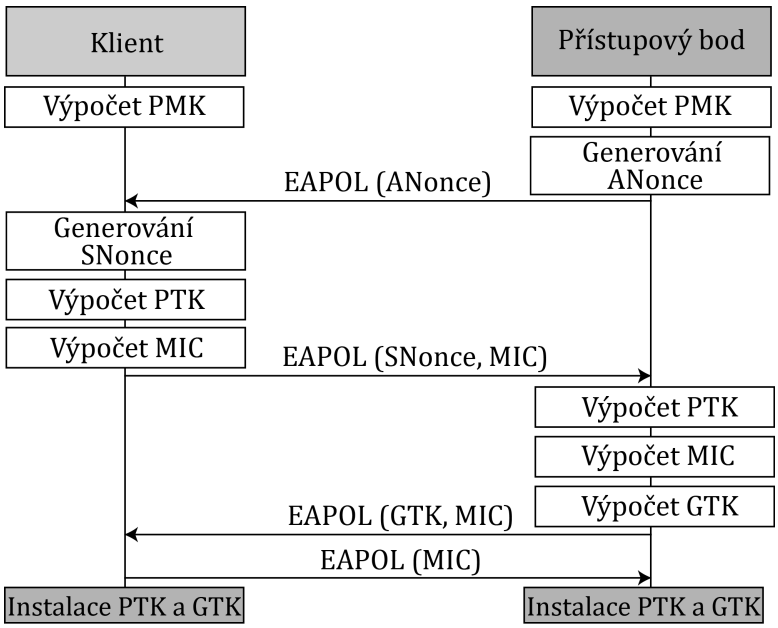


Obrázek 5: Proces tvorby klíčů na základě předsdíleného klíče

Pro zajištění všesměrové (broadcast) a vícesměrové (multicast) komunikace je posléze přístupovým bodem vypočten skupinový klíč GTK (Group Transient Key) dlouhý 256 bitů, který je vytvořen na základě GMK (Group Master Key).

Klíč GTK je společný pro všechny klienty v dané bezdrátové síti a klientovi je předán ve třetí zprávě čtyřcestné výměny. Poslední zpráva je zasílána klientem a obsahuje pouze hodnotu MIC, která uzavírá výměnu a informuje o instalaci vyměněných klíčů a začátku šifrované komunikace. Jakmile přístupový bod přijme poslední zprávu a ověří přijatou hodnotu MIC, nainstaluje si i své vytvořené klíče (Gast, 2005, s. 164–166).

Jelikož je PTK i skupinový klíč GTK použit pro zabezpečení probíhající komunikace mezi klientem a přístupovým bodem, jsou oba klíče po odeslání deseti tisíc rámců nově vytvořeny (Gast, 2005, s. 167). Úplný průběh EAPOL zpráv při autentizaci pomocí předsdíleného klíče je na obrázku 6.



Obrázek 6: Čtyřcestná výměna při autentizaci s předsdíleným klíčem

3.2.2 Princip šifrování

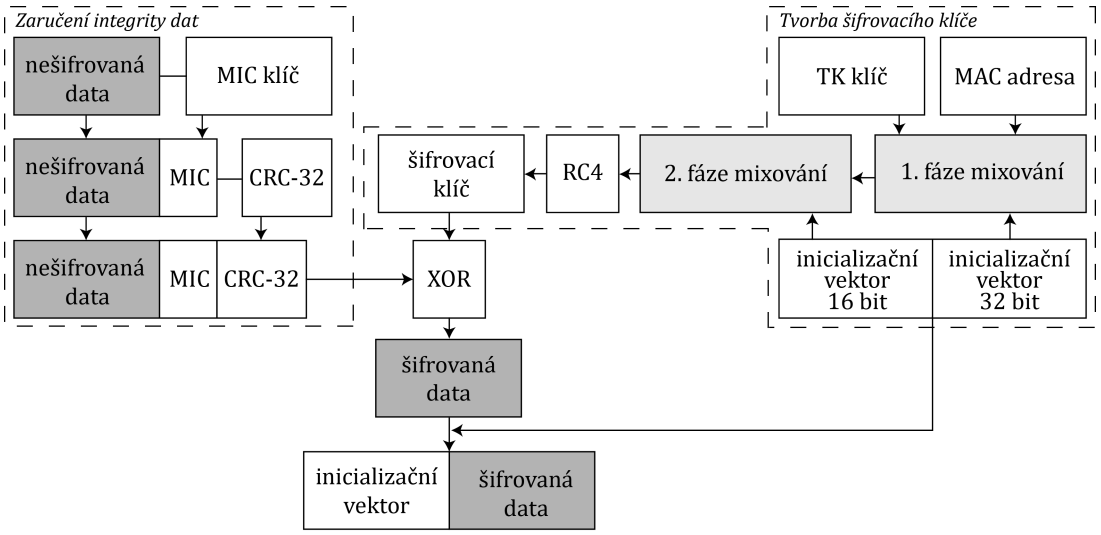
K šifrování dat je využita proudová šifra RC4, stejně jako u standardu WEP, ovšem výraznou změnou u protokolu WPA je způsob generování inicializačních vektorů a použití dynamických klíčů, k čemuž je využit protokol TKIP. K zajištění integrity dat je aplikován protokol MIC (Message Integrity Code), jenž data chrání proti záměrné úpravě a mnohonásobnému odesílání (Lammle, 2010, s. 704–705).

Proces šifrování (obrázek 7) začíná u prostého textu zprávy, kterému musí být v prvé řadě zajištěna integritní ochrana pomocí protokolu MIC. Datový rámec je spolu s MAC adresou klienta a přístupového bodu a s 64bitovým MIC klíčem, vygenerovaným z PTK v průběhu autentizace, předán do jednocestné hashovací funkce nazvané Michael. Výsledná MIC hodnota o délce 64 bitů je připojena na konec datového rámce, kdy je po sloučení ještě vypočten kontrolní součet pomocí CRC-32, který se taktéž stává součástí výsledného rámce (Hucaby, 2011, s. 296).

Po této části dochází k vygenerování inicializačního vektoru prodlouženého na 48 bitů, kdy protokol TKIP předepisuje generování začínající na nule s postupnou inkrementací. Inicializační vektor je logicky rozdělen do dvou částí, z nichž první je dlouhá 16 bitů a druhá 32 bitů. Obě části se podílejí na tvorbě šifrovacího klíče, která má dvě fáze zvané mixování.

V první fázi probíhá mixování 48bitové MAC adresy zdroje s druhou částí inicializačního vektoru (32 bitů) a 128bitového Temporary Key (TK), jež je součástí PTK. Výsledkem první fáze je mezilehlý klíč. Ten vstupuje s první částí inicializačního vektoru (16 bitů) do druhé fáze mixování, jehož výstup je vložen do generátoru RC4, z něhož vzejde výsledný paketový šifrovací klíč dlouhý 128 bitů.

Při posledním procesu je použita operace XOR mezi vytvořeným šifrovacím klíčem a daty doplněnými o kontrolní součty. Tímto vzniká zašifrovaná zpráva, která je před odesláním doplněna o nešifrovaný 48bitový inicializační vektor (Gast, 2005, s. 151–153).



Obrázek 7: Princip šifrování dat protokolu TKIP

3.3 IEEE 802.11i

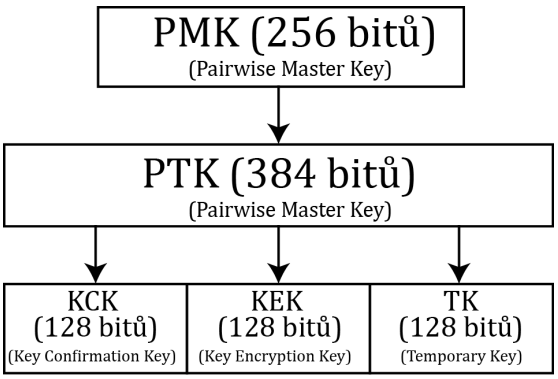
Wi-Fi Protected Access druhé generace (WPA2) je komerční pojmenování pro plnohodnotný standard IEEE 802.11i, jenž byl schválen a uveden na trh v roce 2004. WPA2 k šifrování komunikace již nevyužívá proudovou šifru RC4, ale nově implementuje šifrovací algoritmus AES (Advanced Encryption Standard) za použití protokolu CCMP (Cipher Block Chaining Message Autentication Code Protocol).

Na rozdíl od standardu WPA, kdy při přechodu z WEP byl pouze aktualizován firmware, muselo v tomto případě dojít k výměně celého přístupového bodu, jelikož WPA2 s použitím šifry AES není zpětně kompatibilní (Sosinsky, 2011, s. 388–389).

3.3.1 Princip autentizace

Autentizační metody obsažené ve standardu WPA2 mají stejný princip jako v předešlém WPA, které byly objasněny na straně 23. Hlavní rozdíl je pouze v používaném protokolu, kdy u WPA byl využit TKIP a novější WPA2 implementuje protokol CCMP. Změna protokolu se projevila pouze v bitové délce klíčů PTK a GTK (Hucaby, 2011, s. 296).

Jelikož protokol CCMP neimplementuje funkci Michael, není potřeba v klíči PTK ukládat informaci o TMK klíčích, a proto je PTK zkrácen z předešlých 512 bitů na pouhých 384 bitů. To stejné platí pro klíč GTK, který byl zkrácen na 128 bitů (Gast, 2005, s. 164).

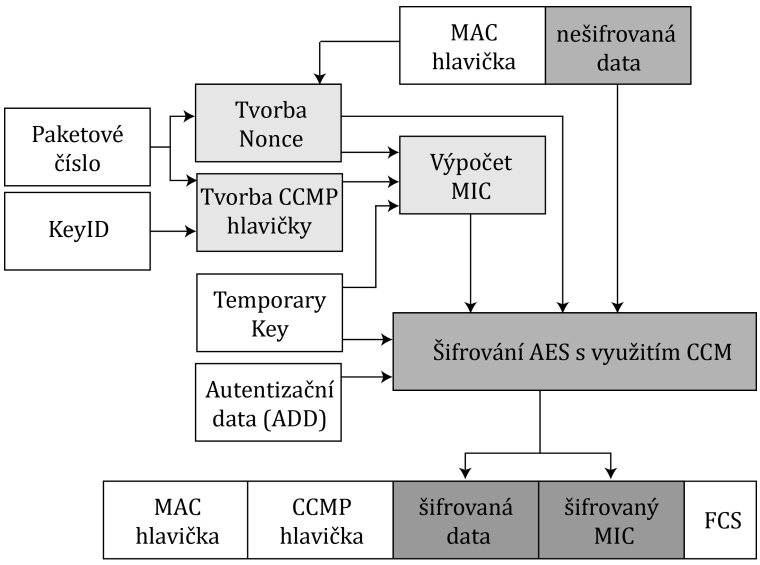


Obrázek 8: Proces odvozování klíčů protokolu CCMP

3.3.2 Princip šifrování

Pro šifrování a kontrolu integrity dat je použit protokol CCMP, který využívá blokovou šifru AES a čítač CCM (Counter with CBC-MAC) pracující s 128bitovými bloky, jejichž průběh je vyobrazen na obrázku 9.

V první fázi šifrovacího procesu dochází k určení 128bitové hodnoty Nonce, zajišťující správnost a unikátnost vstupních dat, která je vypočtena na základě MAC adresy obsažené v datovém rámci a 48bitového paketového čísla (Packet Number), který zajišťuje jedinečnost výsledné Nonce hodnoty.



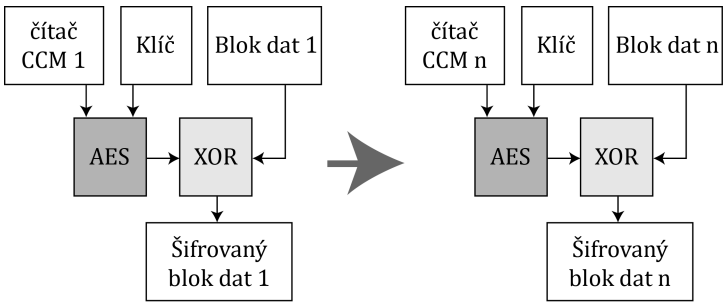
Obrázek 9: Průběh šifrování dat protokolu CCMP

Při použití stejného Temporary Key (TK) nesmí dojít ke znovupoužití stejné Nonce hodnoty, a proto je paketové číslo při každé transakci zvýšeno. Poté je vytvořena CCMP hlavička dlouhá 64 bitů, která obsahuje paketové číslo rozdělené na šest oktetů a identifikátor skupinového klíče (KeyID) (Gast, 2005, s. 161–163).

Ve druhé fázi je vypočten autentizační kód MIC, určený pro zajištění integrity dat, pomocí čítače Cipher Block Chaining (CBC-MAC), jehož vstupem je 128bitový Temporary Key sloužící pro šifrování i ověřování rámce, dále Nonce hodnota a CCMP hlavička.

Poslední fází je samotné šifrování řešené pomocí blokové šifry AES. Do této šifry vstupují data sloučená s kódem MIC, hodnota Nonce, dynamický klíč Temporary Key a Autentizační data (ADD) zajišťující správné pořadí bitů a korektní hlavičku MAC.

Vstupní data jsou rozdělena na bloky dlouhé 128 bitů, které jsou spolu s nově vytvořenými výstupy předány do operace XOR (obrázek 10). Tento proces skončí až po zašifrování všech dat. Výsledkem jsou šifrovaná data o minimální délce 64 bitů a zašifrovaná 64bitová hodnota MIC (Edney, 2004, s. 264–274).



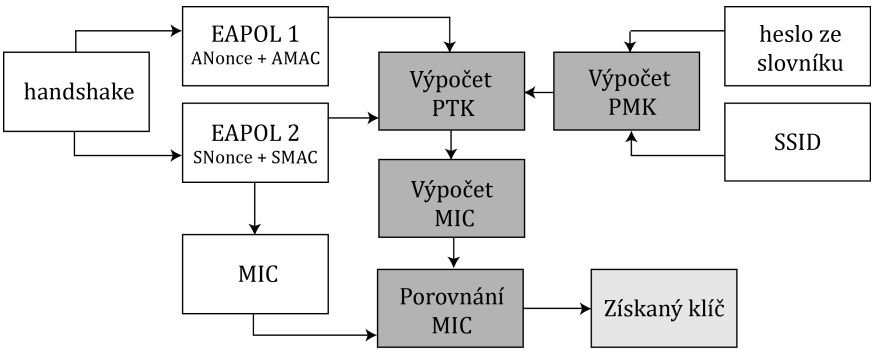
Obrázek 10: Princip blokové šifry AES

3.3.3 Útoky na WPA/WPA2 Personal

Pro získání předsdíleného klíče zabezpečení WPA a WPA2 je nutné zachytit první dvě EAPOL zprávy, které jsou zasílány mezi klientem a přístupovým bodem při čtyřcestné výměně. Je tedy zapotřebí získat informaci o náhodné hodnotě klienta (SNonce) i přístupového bodu (ANonce), které se podílejí na tvorbě klíče PTK.

Teprve po získání těchto hodnot je možné přistoupit k samostatnému útoku, který může být řešen pomocí hrubé síly nebo slovníku. Při útoku hrubou silou dochází k postupnému generování všech kombinací hesel ze zadané množiny znaků či číslic o vymezené délce. Nevýhodou tohoto útoku je obrovská časová náročnost, která se odvíjí od využité hardwarové konfigurace. Naopak při použití slovníkového útoku jsou testována pouze hesla obsažená v daném slovníku, což je značnou nevýhodou, jelikož nemusí dojít k úspěšnému nalezení předsdíleného klíče.

Na základě odchycených náhodných hodnot a hesla ze slovníku je útočníkem vytvořen vlastní PTK klíč. Z něho je pomocí KCK klíče vypočten kontrolní součet MIC, který je porovnán s odchyceným kontrolním součtem (obrázek 11). Tento proces je opakován do doby, dokud se vypočtená a odchycená hodnota nerovnají nebo nejsou vyčerpána dostupná hesla ze slovníku (Ramachandran, 2015, s. 80–82).



Obrázek 11: Průběh slovníkového útoku

3.4 Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) byl v roce 2006 vyvinut společností Wi-Fi Alliace pro snadnější přístup do bezdrátové sítě. WPS ovšem není součástí standardu IEEE 802.11. Inspirací pro jeho tvorbu bylo zvětšující se množství domácích bezdrátových sítí, u kterých by konfiguraci zabezpečení zvládl i nezkušený uživatel. WPS nabízí automatické nastavení sítě a zajištění bezpečnosti pomocí standardu WPA či WPA2 (Alamanni, 2015, s. 79).

3.4.1 Princip autentizace

Nastavení ochrany sítě se nejčastěji provádí pomocí dvou metod. První možností je PBC (Push-button configuration), kdy je spárování přístupového bodu a klienta provedeno pomocí stisku tlačítka. Nejdříve je stisknuto tlačítko umístěné na přístupovém bodě, čímž dojde k aktivaci naslouchání a očekávání nového klienta ve vymezeném časovém úseku. Poté je tlačítko stisknuto na klientovi. Tlačítko je buď součástí externí síťové USB karty nebo desktopové aplikace dodané výrobcem.

Druhou možností je zadání osobního identifikačního čísla, které je vygenerováno přístupovým bodem o délce osmi číslic. Metoda je zkráceně nazývána PIN (Personal Information Number).

Klientem je vložen PIN kód a odeslán přístupovému bodu, který ověří jeho správnost a klientovi vrátí zprávu o výsledku. Pokud byl PIN zadán správně, je přístupovým bodem dodán předsdílený klíč (PSK) pro zajištění šifrované komunikace (Coleman, 2010, s. 233–235).

3.4.2 Útoky na WPS

Na WPS lze aplikovat útok hrubou silou, kdy jsou postupně testovány různé řetězce kódu PIN. PIN je tvořen osmi číslicemi, nicméně poslední číslice obsahuje kontrolní součet, a proto se počet kombinací vypočte jako 10^7. PIN kód tedy může nabývat deseti milionů různých kombinací (Ramachandran, 2015, s. 175).

Ovšem v roce 2011 byla odhalena implementační chyba, která značně snižuje celkový počet kombinací. PIN kód není odesílán v celém rozsahu, ale je rozdělen na dvě části, které jsou přístupovému bodu odeslány postupně. Nejdříve je poslána první část obsahující čtyři číslice, na kterou přístupový bod odpovídá. Pokud je kombinace správná, je klientovi zaslána zpráva o úspěchu a požadavek na zaslání druhé části obsahující tři číslice.

Při rozdělení identifikačního čísla na dvě části dojde ke snížení celkového počtu kombinací na pouhých 11 000, čímž dochází ke snížení časové náročnosti (Alamanni, 2015, s. 80).

4 Penetrační testování

Jak uvádí Patrick Engebretson (2013, s. 19), penetrační testování je soubor metod a procesů, který vede ke zhodnocení stavu zabezpečení. Testování probíhá podle vymezené strategie představující životní cyklus, který se skládá ze čtyř hlavních fází, jež jsou zobrazeny na obrázku 12.

Obrázek 12: Životní cyklus penetračního testování, zdroj: (Engebretson, 2013, s. 19)

Penetrační testování spadá do kategorie etického hackování, které se zabývá hledáním bezpečnostně slabých míst nejen v počítačové a bezdrátové síti, ale i v podnikovém systému či webové aplikaci, za účelem odhalení podnikových hrozeb. Cílem je nalézt řešení a doporučení kvalitního zabezpečení, která vyplývají z výsledků provedeného testu (Baloch, 2015, s. 8).

4.1 Metodiky penetračního testování

V rámci penetračního testování existuje mnoho standardizovaných příruček stanovujících detailní postupy. Cílem bylo nalézt metodiku, která by sloužila jako podpora pro vykonání penetračního testování domácí bezdrátové sítě.

Příručka NIST SP800-115

Speciální publikace 800-115 je metodikou od společnosti NIST (National Institute of Standards and Technology), která byla vydána v roce 2008. Dokument definuje obecné strategie pro údržbu a kontrolu stavu technického zabezpečení organizace.

V části bezdrátové bezpečnosti je pojednáno o všeobecně známých znacích bezdrátových sítí. Následně jsou představeny techniky pasivního a aktivního skenování provozu a odposlechu bezdrátové komunikace (NIST, 2017).

Metodika OSSTMM

Open Source Security Testing Methodology Manual, zkráceně OSSTMM, je komplexní metodika zaměřená na testování bezpečnosti a zlepšení zabezpečení ve větších podnicích. Zahrnuje širokou škálu modulů představujících jednotlivé oblasti pro testování, do kterých lze zařadit telekomunikační a technologické testování a metody pro skenování zranitelnosti a bezpečnostní analýzy.

Modul zaměřený na bezdrátové sítě je velmi rozsáhlý a definuje ověřování bezpečnosti v několika krocích. Dále popisuje jednotlivé fáze životního cyklu, do kterého jsou zahrnuty právní aspekty, monitoring, testování a spousty dalších složek (ISECOM, 2017).

Standard PTES

Penetration Testing Execution Standard definuje způsoby penetračního testování, jež mohou pomoci méně zkušeným testerům. Standard byl vytvořen etickými hackery, kteří mají s testováním mnohaleté zkušenosti a metody jimi definované jsou reálně využívány.

Součástí postupů je i doporučení nástrojů s praktickou ukázkou použití. Standard je volně přístupný ve formě webové stránky s poslední modifikací z roku 2014 (PTES, 2014).

4.1.1 Shrnutí

Pro splnění cíle práce byla vybrána metodika PTES, která nabízí obsáhlé postupy řešení a doporučené nástroje. Metodika posloužila jako podpora při výkonu penetračního testování domácí bezdrátové sítě.

4.2 Nástroje pro testování

K dispozici je obrovské množství nástrojů určených k penetračnímu testování bezdrátových sítí, a proto pro snazší výběr posloužila metodika PTES doporučující ověřené a více využívané nástroje.

Klíčovým parametrem hledaného nástroje je možnost prolomení zabezpečení WEP, WPA i WPA2-PSK a skenování všech dostupných bezdrátových sítí s výpisem detailních informací. Mezi další požadavky patří schopnost prolomení PIN kódu funkce WPS a podpora operačním systémem Linux.

Aircrack-ng

Komplexní balíček zahrnující řadu nástrojů určených pro penetrační testování bezdrátových sítí. Využívá se ke zjištění klíče zabezpečení WEP i WPA/WPA2-PSK za pomoci analýzy odchycených paketů.

Primárně je navrhnut pro operační systém Linux a pro práci v příkazové řádce. Součástí webových stránek nástroje Aircrack-ng je rozsáhlá dokumentace prezentující jednotlivé nástroje a postupy práce (Aircrack-ng, 2009–2017).

Airmon-ng

Slouží k přepnutí síťové karty do monitorovacího režimu, při kterém je zachytávána veškerá probíhající komunikace dostupných bezdrátových sítí. Monitorovací režim je klíčový pro sledování provozu a odchyt paketů, aniž by muselo dojít k asociaci s přístupovým bodem (Aircrack-ng, 2009–2017).

Airodump-ng

Využívá se k zachytávání datových paketů okolních bezdrátových sítí. Při použití filtrace lze odchytávat pakety jen vybraného přístupového bodu. U zabezpečení WEP jsou shromažďovány jedinečné inicializační vektory, které poslouží ke snazšímu odhalení bezpečnostního klíče. Při zabezpečení WPA/WPA2-PSK je odchycen čtyřcestný handshake (Aircrack-ng, 2009–2017).

Aireplay-ng

Aireplay-ng je používán ke generování vlastního bezdrátového provozu za pomoci využití injekce paketů. Tím dochází k urychlení procesu odchytávání a dosažení většího množství paketů pro získání inicializačních vektorů u standardu WEP nebo čtyřcestné výměny u standardu WPA/WPA2-PSK (Aircrack-ng, 2009–2017).

coWPAtty

Slouží k automatickému prolomení zabezpečení typu WPA/WPA2-PSK pomocí slovníkového útoku. Výchozí slovník obsahuje tisíce předem definovaných hesel a pro úspěšné prolomení sítě je nezbytné, aby hledané heslo bylo v seznamu obsaženo.

Nevýhodou je rychlost testování klíčů, která je oproti nástroji Aircrack-ng značně snížena. Průběžný výpis je bohužel příliš strohý a během hledání hesla nemá útočník žádné informace o uplynulém čase ani průměrné rychlosti procházení klíčů. Tyto informace jsou prezentovány až po ukončení testu (Offensive Security, 2017a).

Fern Wifi Cracker

Jedná se o nástroj, který automaticky vykonává penetrační test bezdrátových sítí. Funkcionalita vychází z nástroje Aircrack-ng a je doplněná o přívětivé grafické rozhraní. Je schopen prolomit zabezpečení WEP, WPA/WPA2 i WPS za použití známých útoků, jako jsou KoreK, Cafe Latte či slovníkového útoku při online přístupu. Dostupný je pro operační systém Linux, Windows i macOS (Fern Pro, 2017).

Reaver

Nástroj na prolomení klíče při zabezpečení WPA/WPA2-PSK za pomoci nalezení WPS pinu. Útok je proveden pomocí hrubé síly a je úspěšný pouze tehdy, když je funkce WPS na cílovém přístupovém bodu spuštěna. Čas pro uhádnutí PIN kódu a následného WPA/WPA2-PSK klíče je stanoven od čtyř do deseti hodin, v závislosti na použitém přístupovém bodě (Offensive Security, 2017a).

Wash

Zobrazuje všechny dostupné bezdrátové sítě a informaci o tom, zda má přístupový bod zapnutou funkci WPS či nikoli. Wash je součástí nástroje Reaver, který se stará

o prolomení WPS. Některé přístupové body mají automatickou detekci na opětovné zadávání chybných PIN údajů, kdy se brání uzamknutím funkce WPS. Nástroj Wash dokáže toto uzamknutí zachytit a útočníka upozornit (Offensive Security, 2017a).

Wifite

Wifite slouží pro automatický útok na zabezpečení WEP, WPA/WPA2 a WPS. Součástí útoku je detekce a analýza okolních bezdrátových sítí. K těmto procesům jsou využívány výše zmíněné nástroje, čímž se z Wifite stává spíše zjednodušený zprostředkovatel nežli plnohodnotný nástroj s vlastní funkcionalitou (Offensive Security, 2017a).

Operační systém Kali Linux

Operační systém Kali Linux je speciálně vyvinut pro potřeby bezpečnostním specialistům, kteří se zabývají analýzou zabezpečení a penetračním testováním.

Systém obsahuje nepřeberné množství nástrojů a utilit navržených pro penetrační testování různých oblastí. Kali Linux je volně dostupný a nabízí kvalitně zpracovanou dokumentaci (Offensive Security, 2017b).

Obrázek 13: Operační systém Kali Linux

4.2.1 Shrnutí

Na stroj útočníka byl nainstalován operační systém Kali Linux z důvodu otestování bezdrátové sítě. Kali Linux zahrnuje veškeré výše zmíněné nástroje a je uzpůsoben pro potřeby penetračního testování. Nástroje jsou v systému nainstalované v nejnovějších verzích, a proto jsou po spuštění stroje ihned plně funkční.

Pro skenování, odchyt a následné prolomení zabezpečení WEP a WPA2-PSK byl vybrán komplexní balíček Aircrack-ng, který umožňuje vlastní konfigurace, detailní náhledy a informativní výpisy. Při odchytu datových paketů je umožněno

ukládání průběhu do souboru, k němuž je možné se později vracet v takzvané offline verzi, která dovoluje lámání hesla bez nutnosti dosahu testované sítě.

Pro otestování standardu WPS byl vybrán nástroj Reaver, který využívá útok hrubou silou. Současně s ním byl aplikován nástroj Wash pro skenování stavu WPS a informování o případném uzamčení služby.

4.3 Legislativa

Při penetračním testování se provádí lámání sítě či systému a v případě nevědomosti majitele dochází k trestné činnosti. Před započetím testování je nutné vytvořit závaznou smlouvu s přesným stanovením rozsahu mezi bezpečnostním specialistou a zákazníkem, aby nemohlo dojít k porušení zákona.

Pokud se organizace či osoba stane obětí kybernetického útoku skrze nedovolenou činnost, je útočníkem porušen trestní zákoník č. 40/2009 Sb. a podle povahy útoku některý z následujících paragrafů:

- *„§ 182 Porušení tajemství dopravovaných zpráv*
- *§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací*
- *§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*
- *§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti“* (Zákon č. 40/2009 Sb., 2009)

Obecně se pro páchání trestných činů za pomoci informačních technologií využívá termín kybernetická kriminalita, která pokrývá veškeré protiprávní jednání v kybernetickém prostoru (informační a komunikační prostředí) a může být dále dělena do kategorie internetové kriminality či kyberterorizmu.

Pro pojem kybernetická kriminalita neexistuje zcela přesná definice, která by rozsah termínu stanovila, ovšem Jan Kolouch ve své knize CyberCrime (2016, s. 31–35) definoval kybernetickou kriminalitu jako čin mířený proti počítači či systému nebo čin, při kterém jsou informační technologie využity v kyberprostoru jako prostředek k vykonání trestné činnosti.

Tato problematika je detailně rozebrána ve výše zmíněné knize CyberCrime, která je věnována právním aspektům nezákonného chování v kybernetickém prostoru a prezentuje možné hrozby v počítačových a sociálních sítích (Edice CZ.NIC, 2017).

Podle dostupných zdrojů Policie České republiky (2017) je odposlouchávání bezdrátových sítí, získávání citlivých informací o síti a zachytávání komunikace označeno jako sniffing, čímž může dojít k odchycení hesel a jejich zneužití. V tomto případě dochází k porušení § 182 trestního zákoníku. Tato technika je nejčastěji využívána v nezabezpečených veřejných bezdrátových sítích, které jsou dostupné v restauracích, obchodech a dalších veřejných prostorech.

5 Publikace související s tématem práce

Před započetím vlastní práce bylo vhodné provést rešerši odborných publikací a závěrečných prací, které se zabývají stejným tématem, to jest bezdrátovými sítěmi, jejich možnostmi zabezpečení a penetračním testováním těchto sítí.

Tímto rozborem byly získány informace o četnosti publikací a bylo zjištěno, zda stanovený cíl práce nekoresponduje s již vytvořenou prací.

5.1 Závěrečné práce

Vyhledání závěrečných prací bylo provedeno v národní databázi theses.cz a ve veřejně dostupném katalogu závěrečných prací Vysokého učení technického v Brně.

K nalezení publikací byla použita klíčová slova jako bezdrátové sítě, bezpečnost bezdrátových sítí, penetrační testování, Wi-Fi, WEP, WPA, WPA2 i jejich anglické ekvivalenty wireless networks, wireless networks security, penetration testing a další.

Z množství vyhledaných prací lze usoudit, že oblast bezdrátových sítí je rozsáhlá a dosti populární, a proto pro další selekci byly zvoleny práce vydané po roce 2012.

Bezdrátové sítě a jejich zabezpečení – Miroslav Sajvera

Bakalářská práce pojednávající o celé oblasti bezdrátových sítí, kdy jsou popsány standardy, zapojení, přenosy dat a přístupové metody. Nejobsáhlejší kapitola je věnována bezpečnostním mechanismům a možným hrozbám, kdy je pro ukázku provedeno prolomení zabezpečení typu WEP s využitím injekce ARP paketů a WPA pomocí slovníkového útoku (Sajvera, 2015).

Bezpečnost WiFi sítí – Tomáš Skovajsa

Diplomová práce, která je věnována bezpečnosti bezdrátových sítí. Líčí bezpečnostní a šifrovací metody, správu klíčů a autentizační mechanismus 802.1x. Ve druhé části práce jsou prezentovány útoky na bezpečnostní mechanismy, kdy k zabezpečení typu WEP, WPA-PSK a WPS jsou představeny základní nástroje s příkazy pro provedení útoku (Skovajsa, 2012).

Moderní trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11 – Tomáš Lieskovan

Bakalářská práce se obecně zaměřuje na bezdrátové sítě, popis principů, koncepce a metody zabezpečení. Po teoretickém rozboru jsou jednotlivá zabezpečení otestována ve virtualizovaném prostředí s ukázkou nástrojů a základního nastavení (Lieskovan, 2015).

Nástroje a metody pro prolamování bezdrátových sítí norem IEEE 802.11 s použitím virtualizace – František Pecha

Obsáhlá bakalářská práce, která seznamuje s bezpečnostními standardy a útoky vedenými proti šifrovacím metodám. V praktické části je provedeno penetrační testování jednotlivých bezpečnostních metod pomocí několika typů útoků, které jsou vedeny ve virtualizovaném prostředí (Pecha, 2015).

Nástroj pro analýzu zabezpečení bezdrátových sítí - Jakub Šenovský

Práce Jakuba Šenovského (2012) se zabývá zabezpečením bezdrátových sítí a síťovými útoky. Praktická část práce popisuje implementaci vlastního nástroje zahrnující útoky na klienty a komunikační provoz. Součástí je porovnání s existujícími nástroji a prezentace dosažených výsledků na základě implementované aplikace.

Předcházení útokům na standard 802.11 – Filip Štefanec

Tato bakalářská práce je zaměřená na zabezpečení bezdrátových sítí a šifrovací procesy, které jsou v práci i prakticky otestovány. Hlavní náplní je ovšem simulace útoku proti zabezpečení WPA2 typu Enterprise za pomoci serveru RADIUS a protokolu EAP (Štefanec, 2015).

Využití penetračního testování v bezdrátových sítích – Jan Rydlo

Autor ve své bakalářské práci seznamuje s problematikou penetračního testování a obecnými principy. V práci je navrhnuta bezdrátová síť, která je podrobena penetračnímu testování za pomoci nástrojů Metasploit a Nessus (Rydlo, 2016).

Zabezpečení bezdrátových sítí proti pokročilým útokům – David Glevický

Práce se soustředí na všeobecný popis bezdrátových sítí, architektur, jednotlivých standardů a zabezpečení. Prakticky popisuje útok na bezdrátovou síť pomocí útočníkem vytvořeného falešného přístupového bodu (Glevický, 2016).

5.2 Vlastní práce

Po výběru a prostudování většího počtu závěrečných prací zaobírajících se problematikou bezdrátových sítí a jejich zabezpečením nebyla nalezena žádná podobná práce, která by při testování a útocích brala v potaz složitost použitého hesla, případně která by řešila vztah mezi časovou náročností a hardwarovou konfigurací.

Z tohoto důvodu bylo ve vlastní práci testování bezpečnostních metod doplněno o měnící se složitost bezpečnostního hesla. V případě zabezpečení WPA2 bylo testování provedeno na několika hardwarových konfiguracích.

6 Metodika práce

Testování zabezpečení bezdrátových sítí je rozděleno do tří částí. V první části dojde k otestování zabezpečení WEP s použitím 64 a 128bitového klíče, k čemuž bude aplikován útok PTW. Druhá část je zaměřena na standard WPA2-PSK, k jehož otestování poslouží slovníkový útok. Třetí a poslední část je určena standardu WPS. Veškeré části budou otestovány na navržené laboratorní bezdrátové síti s podporou postupů metodiky PTES a za pomoci nástrojů vybraných v kapitole 4.2.

Aby bylo možné jednotlivé typy zabezpečení vyhodnotit z hlediska odolnosti, budou navrhnuta a použita hesla se vzrůstající procentuální složitostí, která je dána délkou řetězce a kombinací znaků a číslic.

Pro systematické otestování zabezpečení WEP je sestaveno pět kategorií s lišící se složitostí. Každé kategorii se přidělí pět hesel, která se vyberou z mezinárodního seznamu obsahujícího deset milionů těch nejpoužívanějších. Ta budou následně přeložena do českého jazyka a modifikována pro konkrétní kategorii. Seznam je volně dostupný z webové stránky bezpečnostního specialisty Daniela Miesslera (2016). Vybraná hesla jsou uvedena v příloze B.

Sestavené kategorie pro otestování zabezpečení WEP:

- Kategorie 1: číslice 0–9
- Kategorie 2: malá písmena anglické abecedy
- Kategorie 3: malá písmena anglické abecedy a číslice 0–9
- Kategorie 4: malá a velká písmena anglické abecedy a číslice 0–9
- Kategorie 5: malá a velká písmena anglické abecedy, číslice 0–9, speciální znaky

Pro otestování zabezpečení WPA2 bude aplikován slovníkový útok, ke kterému se využije volně dostupný slovník českého jazyka Extra Dictionaries (2016), který je zbaven diakritiky, ale obsahuje duplicitní slova. Pro odstranění duplicit se aplikuje příkaz `cat [slovník] | sort | uniq > [nový slovník]`, čímž vznikne základní slovník českého jazyka zahrnující 232 849 slov.

Kvůli testu s různou složitostí klíče musí dojít k modifikaci základního slovníku podle postupu definujícího tvorbu uživatelských hesel. Postup je vytvořen s pomocí výzkumu Troye Hunta, který v roce 2011 analyzoval používaná hesla zaměstnanců společnosti Sony. Způsob tvorby slovníků je uveden v příloze A.

Sestavené kategorie pro slovníkový útok na zabezpečení WPA2:

- Kategorie 1: Slovo ze slovníku
- Kategorie 2: Slovo ze slovníku začínající velkým písmenem
- Kategorie 3: Slovo ze slovníku, na konci číslice 0–9
- Kategorie 4: Slovo ze slovníku, na začátku číslice 0–9
- Kategorie 5: Zdvojení stejného slova
- Kategorie 6: Zdvojení slova, na konci číslice 0–9
- Kategorie 7: Zdvojení slova, na začátku číslice 0–9

Pro každou kategorii bude z vytvořených slovníků vybráno pět hesel, k čemuž se využije generátor náhodných čísel. Generátor se spustí příkazem `shuf -i 1-[počet možností] -n 5`, kde parametr `-i` definuje množinu hodnot a parametr `-n` udává počet vygenerovaných čísel. Veškerá vybraná hesla pro testování zabezpečení WPA2 jsou součástí přílohy B.

Měření zabezpečení WPA2 bude vykonáno i pomocí útoku hrubou silou. Ovšem kvůli velké časové náročnosti bude útok hrubou silou proveden pouze matematicky pro řetězce dlouhé osm znaků s použitím stejných kategorií jako u standardu WEP.

Po tvorbě slovníků a výběru hesel může být uveden do provozu přístupový bod, jehož konfigurace bude provedena v internetovém prohlížeči po zadání adresy `tplinklogin.net` či IP adresy `192.168.0.1` s výchozími přístupovými údaji `admin/admin`. Pro uložení nastavení musí být přístupový bod restartován.

Nastavení přístupového bodu:

- Název sítě (SSID): `testWIFI`
- Kanál a šířka pásma: `Auto`
- Mód: `standard 11g`
- Heslo: `závislost na zabezpečení a kategorii`

Scénář testu bezdrátové sítě:

1. Pro generování většího počtu datových paketů mezi klientem a přístupovým bodem bude na klientském stroji spuštěno stahování ISO souboru operačního systému Kali Linux z oficiálních webových stránek výrobce (Offensive Security, 2017c). Průměrná rychlost stahování je 10 Mbps s mírným kolísáním (otestováno na www.dsl.cz/test-mereni-rychlosti), kvůli rušení způsobeným okolními bezdrátovými sítěmi. Po celou dobu testování bude k bezdrátové síti `testWIFI` připojen pouze jeden klient.
2. První fází útoku je skenování, při kterém budou sbírány informace o dostupných bezdrátových sítích. Před tím musí nástrojem Airmon-ng dojít k přepnutí síťového adaptéru do monitorovacího režimu a poté může být použit nástroj Airodump-ng pro odchyt datových paketů.
   a) Při testování zabezpečení WEP budou z datových paketů evidovány inicializační vektory a k zaznamenání času budou použity ruční stopky.
   b) Pro otestování standardu WPA2 musí být zachycena čtyřcestná výměna mezi klientem a přístupovým bodem. K vynucení opětovného zaslání této výměny bude aplikován Aireplay-ng s jehož pomocí bude připojený klient deautentizován. Po odchycení bude handshake uložen do souboru pro otestování zabezpečení na více hardwarových strukturách.
3. Po odchycení dostatečného množství inicializačních vektorů (WEP) nebo zachycení čtyřcestné výměny (WPA2) dojde ke spuštění nástroje Aircrack-ng,

který provede lámání hesel. Při zabezpečení WPA2 je nutné přidělit slovník. Na základě získaných hodnot při testování standardu WPA2 bude vytvořen matematický odhad pro útok hrubou silou vedený na toto zabezpečení.

4. Posledním typem na otestování bude WPS, u něhož je cílem odhalit bezpečnostní PIN kód. Aplikován bude nástroj Reaver využívající útok hrubou silou a nástroj Wash pro detekci aktivních funkcí WPS. Při tomto útoku stroj komunikuje pouze s přístupovým bodem, a není proto nutné získávat informace o připojených klientech.

5. Po provedených útocích bude porovnána časová náročnost a zhodnocena odolnost vybraných typů zabezpečení. Na základě provedené analýzy budou doporučeny metody pro zajištění ochrany domácí bezdrátové sítě.

7 Test odolnosti bezdrátových sítí

V této kapitole jsou prezentovány ukázky postupu penetračního testování jednotlivých bezpečnostních metod a následně jsou porovnány získané výsledky.

7.1 Hardwarová konfigurace

Odposlech síťové komunikace v bezdrátových sítích i jejich exploitace bez souhlasu vlastníka se zákonem trestá, a proto musela být vytvořena laboratorní bezdrátová síť, která sestává z několika komponent.

Přístupový bod

Přístupovým bodem, určeným pro domácí bezdrátovou síť, se stal model TL-WR741ND, jenž vyrábí společnost TP-LINK. Výrobce udává maximální rychlost přenosu dat až 150 megabit za sekundu. Směrovač je rozšířen o odnímatelnou anténu a podporuje standard 802.11b/g/n, kdy vysílá ve frekvenčním pásmu 2,4 GHz.

Bod poskytuje autentizaci pomocí WPS standardu, který byl firmou TP-LINK pojmenován jako QSS (Quick Security Setup). Pro zabezpečení komunikace lze nastavit 64, 128 nebo 152bitový WEP, WPA/WPA2 typu Personal i Enterprise.

Stroj klienta

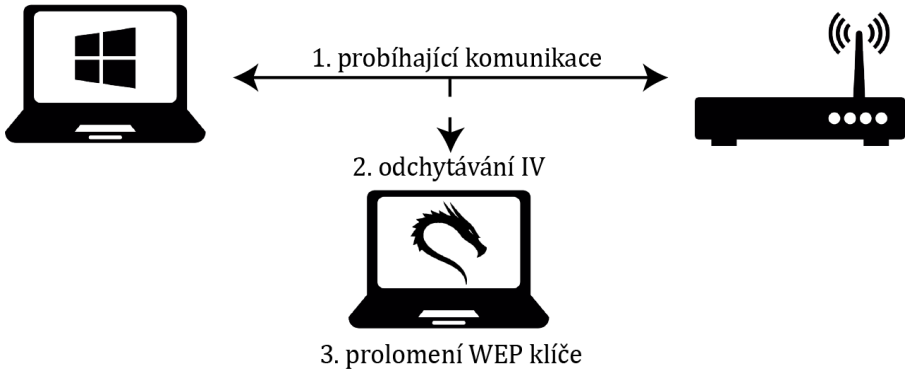
Jako klientský počítač byl použit notebook HP ProBook 455 G2, který disponuje čtyřjádrovým procesorem řady AMD A8-7100 Radeon R5 s frekvencí 1,8 GHz, při zapnutí Turbo režimu frekvence dosahuje až 3 GHz. Operační paměť stroje nabývá 4 GB. Integrovaná síťová karta určená pro bezdrátovou komunikaci je značky Realtek s podporou standardu 802.11b/g/n. Na stroji je nainstalován operační systém Windows 8.1 od společnosti Microsoft.

Tento stroj byl využit pro komunikaci s přístupovým bodem, čímž útočníkovi umožnil lepší detekci a odchyt datových rámců.

Stroj útočníka

Primárním strojem útočníka byl přenosný počítač od firmy Toshiba s produktovým označením Satellite C855-1QG, který posloužil k otestování zabezpečení WEP, WPA2 i WPS. V počítači je osazen čtyřjádrový procesor Intel Core i5-3210M, jehož frekvence v normálním režimu nabývá 2,5 GHz a až 3,1 GHz při zapnutí technologie Intel Turbo Boost.

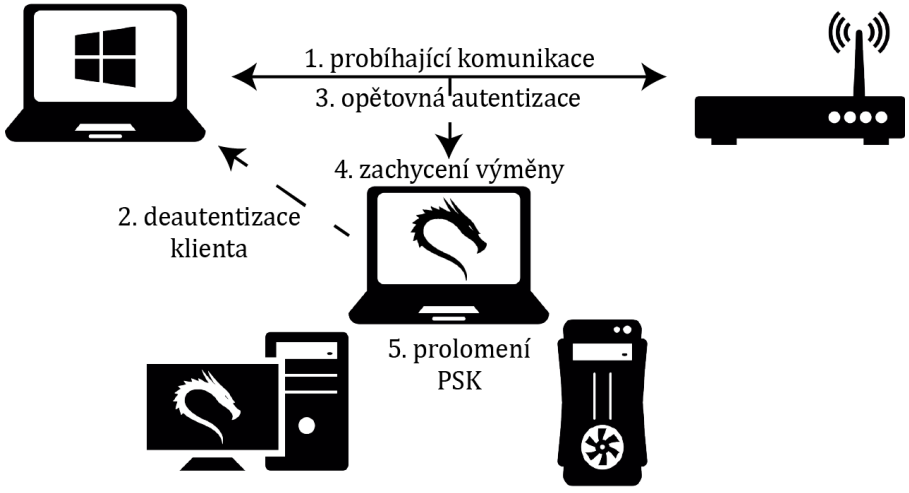
Operační paměť obsahuje 4 GB a integrovaná bezdrátová síťová karta Realtek podporuje standard 802.11b/g/n. Pro pohodlnější testování a snazší přístup k vybraným nástrojům byl výrobcem předinstalovaný operační systém nahrazen za volně dostupný Kali Linux. Konfigurace pro otestování zabezpečení WEP je zobrazena na obrázku 14.



Obrázek 14: Hardwarová konfigurace pro testování WEP, zdroj ikon: autor Freepik na www.flaticon.com/packs/computer-icons

Aby bylo možné provést lámání hesla standardu WPA2 při různém výkonu počítače, byl vytvořen virtuální stroj emulující systém Kali Linux s využitím zdrojů hostitelského počítače. K tvorbě stroje posloužil nástroj Oracle VM VirtualBox verze 5.1, který byl nainstalován na stroj klienta. Při testování bylo stroji nejdříve přiděleno jedno jádro, posléze dvě a čtyři jádra procesoru o frekvenci 1,8 GHz a operační paměť 1 GB.

Po konzultaci s vedoucím práce a pracovníkem Mendelovy univerzity spravujícím výpočetní techniku, byl virtuální stroj i se získanými čtyřcestnými výměnami přenesen na univerzitní počítače. Nejdříve byl použit počítač umístěný v síťové laboratoři Provozně ekonomické fakulty, který obsahuje procesor Intel Core i5-3470 s frekvencí 3,2 GHz (3,6 GHz při Turbo režimu), operační paměť 16 GB a systém Windows 8.1 Pro. Procesor nepodporuje funkci Hyper-Threading, a proto mohly být virtuálním strojem využity pouze čtyři logické jednotky.



Obrázek 15: Hardwarová konfigurace pro testování WPA2, zdroj ikon: autor Freepik na www.flaticon.com/packs/computer-icons

Poté došlo k nainstalování virtuálního Kali Linuxu na univerzitní server, ve kterém jsou osazeny procesory řady Intel Xeon typu X5660 o výkonu 2,8 GHz v normálním režimu a 3,2 GHz při využití Turbo Boost technologie. Virtuálnímu stroji bylo nastaveno 6 GB operační paměti, osm a následně i šestnáct jader procesoru. Přístup k tomuto stroji byl umožněn prostřednictvím univerzitního serveru Akela za použití ssh klienta. Schéma konfigurace pro otestování standardu WPA2 je zobrazena na obrázku 15.

Síťový adaptér

Útočníkův stroj obsahuje integrovaný síťový adaptér, který nenabízí možnost přepnutí do monitorovacího režimu. Tento režim, jenž má za úkol odposlouchávat bezdrátový provoz bez nutnosti asociace, je ze strany útočníka nepostradatelný, a proto byl použit externí síťový adaptér. Operačním systémem útočníka je Kali Linux verze 2016.2, a proto bylo potřeba vybrat adaptér plně kompatibilní s tímto systémem.

Byl použit typ TP-LINK TL-WN722N s čipem Atheros AR9271, jehož ovladače jsou v operačním systému již předinstalovány, což znamená, že po zapojení do sběrnice je adaptér plně funkční a připraven k provozu.

Síťový adaptér obsahuje odnímatelnou anténu a tlačítko WPS pro usnadnění připojení. Pracuje pouze ve frekvenčním pásmu 2,4 GHz a podporuje standard 802.11b/g/n. Podporuje 64 nebo 128bitový WEP a WPA/WPA2 s využitím PSK.

7.2 Nastavení monitorovacího režimu

Prvotním nutným krokem před započetím testu bylo připojení síťového adaptéru ke stroji útočníka. Po připojení byl adaptér ihned připraven k provozu, neboť ovladače jsou již součástí operačního systému Kali Linux. Ověření funkčnosti bylo provedeno příkazem `iwconfig`, který vypsal všechna dostupná bezdrátová rozhraní.

```
root@testPC:~# iwconfig
wlan1   IEEE 802.11 ESSID:off/any
        Mode:Managed    Access Point:Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off  Power Management:off

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed    Access Point:Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off  Power Management:off
```

Jak je patrné z výpisu, v počítači byla dostupná dvě bezdrátová rozhraní v režimu `Managed` neboli režimu řízeném, který značil připravenost k připojení do sítě. `Wlan0` je rozhraní patřící integrované bezdrátové kartě, která je primárně určena na komunikaci s přístupovým bodem. `Wlan1` je bezdrátové rozhraní náležící připojenému externímu adaptéru, jež muselo být přepnuto do režimu monitorovacího.

Na přepnutí režimu byl využit nástroj Airmon-ng, jenž režim přepnul pomocí příkazu `airmon-ng start [rozhraní]`. Adaptéru náleželo rozhraní `wlan1`, a proto se užil příkaz ve tvaru:

```
root@testPC:~# airmon-ng start wlan1
Found 2 processes that could cause trouble.
PID  NAME
618  NetworkManager
700  wpa_supplicant

PHY  Interface Driver     Chipset
phy0 wlan0     rtl8723ae  Realter Semiconductor Co.,
                          RTL8723AE PCIe Wireless Network Adapter
phy1 wlan1     ath9k_htc  Atheros Communications, Inc. AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
(mac80211 station mode vif disabled for [phy1]wlan1)
```

Po zadání příkazu byl zobrazen výpis, který upozorňoval na dva procesy, které mohly mít negativní vliv na prováděné testování. Bylo proto nutné je ukončit příkazem `airmon-ng check kill`, který rušivé procesy zobrazil a ukončil.

Z výpisu lze dále vyčíst možná využitá rozhraní, ovladače a čipové sady bezdrátových karet. Poslední dva řádky výpisu informují o tom, že monitorovací režim byl úspěšně zapnut a je dostupný na rozhraní `wlan1mon`, čímž ovšem došlo k vypnutí rozhraní `wlan1`. Nově vytvořené rozhraní lze zkontrolovat výše použitým příkazem `iwconfig`.

```
root@testPC:~# iwconfig
wlan1mon    IEEE 802.11 ESSID:off/any
            Mode:Monitor    Access Point:Not-Associated Tx-Power=20 dBm
            Retry short limit:7 RTS thr:off Fragment thr:off
            Encryption key:off  Power Management:off

wlan0       IEEE 802.11 ESSID:off/any
            Mode:Managed    Access Point:Not-Associated Tx-Power=20 dBm
            Retry short limit:7 RTS thr:off Fragment thr:off
            Encryption key:off  Power Management:off
```

Rozhraní `wlan1` bylo vypnuto a nahrazeno za logické rozhraní `wlan1mon`, jehož režim je momentálně nastaven na `Monitor`. Přepnutí rozhraní do monitorovacího režimu proběhlo úspěšně a síťový adaptér byl připraven na odchytávání paketů.

Pro navrácení režimu zpět do řízeného stavu je možné taktéž aplikovat nástroj Airmon-ng, pouze s využitím příkazu `airmon-ng stop [rozhraní]`. Jelikož při zapnutí monitorovacího režimu došlo k deaktivaci síťového správce, není možné se přihlásit k jakékoliv síti. Je nutné správce opětovně ručně aktivovat pomocí příkazu `service network-manager start` a až poté je přihlašování k bezdrátovým sítím opět dostupné.

7.3 Útok na WEP

První zabezpečení, jež se stalo předmětem testování, byl WEP s 64 i 128bitovým klíčem. Vybraným typem útoku byl PTW, popsán na straně 22, který je primárně implementován v nástroji Aircrack-ng. Cílem bylo odchytit potřebný počet paketů obsahující inicializační vektory, které byly potřeba pro odhalení sdíleného klíče.

Před útokem bylo nutné analyzovat síť, respektive nalézt vysílající a dostupné přístupové body. K tomuto účelu posloužil nástroj Airodump-ng, který odhalil veškeré dostupné sítě, dokonce i ty se skrytým SSID.

```
root@testPC:~# airodump-ng wlan1mon

CH 11 ][ Elapsed: 42 s][ 2017-02-01 12:17]
BSSID              PWR Beacons #Data,#/s CH MB  ENC  CIPHER AUTH ESSID
A0:F3:C1:XX:XX:XX -43   67    446   0   11 54e WEP  WEP         testWIFI
AC:A2:13:XX:XX:XX -53   47      0   0    1 54e WPA2 CCMP   PSK  Klara
1C:BD:B9:XX:XX:XX -59   79     10   0    8 54e WPA2 CCMP   PSK  LadaM
04:8D:38:XX:XX:XX -70   68      0   0    1 54e WPA2 CCMP   PSK  Andrlikovi
50:46:5D:XX:XX:XX -69   85     53   0    6 54e WPA2 CCMP   PSK  Palenikovi
00:02:72:XX:XX:XX -73   64     76   0    6 54  WEP  WEP         NET_MJ
00:02:72:XX:XX:XX -81   29      0   0    4 54e WPA  CCMP   PSK  NET_NED
00:02:72:XX:XX:XX -82   45      0   0    3 54  WPA2 CCMP   PSK  NET_C
94:0C:6D:XX:XX:XX -82   32      6   0   10 54  WPA2 CCMP   PSK  MOTOR
C8:3A:35:XX:XX:XX -82   45      0   0    5 54e WPA2 CCMP   PSK  Honda
32:CD:A7:XX:XX:XX -82    9      0   0   11 54e WPA2 CCMP   PSK  DIRECT
C0:4A:00:XX:XX:XX -84   27      0   0    6 54e WPA2 CCMP   PSK  Penzion
00:1C:F0:XX:XX:XX -87   20      0   0    6 54  OPN              dlink
00:0C:42:XX:XX:XX -88    0     87   0   13 -1  OPN              [length: 0]
00:15:6D:XX:XX:XX -89    1      1   0    1 54  WPA2 CCMP   PSK  UBNT
90:A4:DE:XX:XX:XX -91    2      0   0   13 11  OPN              [length: 0]

BSSID              STATION            PWR Rate    Lost Frames Probe
A0:F3:C1:XX:XX:XX 2C:33:7A:XX:XX:XX -33 54e-54e  0      446
1C:BD:B9:XX:XX:XX 58:82:A8:XX:XX:XX -92  0 - 1   0       12
50:46:5D:XX:XX:XX 54:27:1E:XX:XX:XX -87 54e- 1   0       55
00:02:72:XX:XX:XX 80:13:82:XX:XX:XX -58 54 -54   0       81
```

Ve výpisu jsou zobrazeny veškeré dostupné přístupové body poskytující přístup do domácí bezdrátové sítě. V jednotlivých sloupcích jsou zobrazeny podrobné informace o přístupovém bodu. V prvním sloupci je uvedeno `BSSID` zobrazující fyzickou MAC adresu přístupového bodu, která posloužila pro specifikaci při útoku.

Sloupec `PWR` uvádí sílu signálu jednotlivých AP, kdy vyšší hodnota znamená lepší kvalitu signálu a dostupnost připojení. Pro lepší přehlednost jsou identifikované sítě pomocí této hodnoty seřazeny. `Beacons` informuje o přijatém počtu oznamovacích rámců, kterými přístupové body ohlašují svou přítomnost. Dalším sloupcem je `#Data`, který zaznamenává počet zachycených datových paketů a při zabezpečení WEP definuje počet inicializačních vektorů.

Sloupec `#/s` zobrazuje průměrné množství zachycených paketů v posledním desetisekundovém intervalu. `CH` definuje číslo vysílajícího kanálu a `MB` nejvyšší možnou

přenosovou rychlost. Následující sloupce `ENC`, `CIPHER` a `AUTH` určují využívaný šifrovaný algoritmus a ověřovací protokol. Posledním sloupcem v horní části výpisu je `SSID`, které pouze zobrazuje identifikační jméno dostupné sítě. V dolní části výpisu jsou zobrazeni připojení klienti, kde je uvedena MAC adresa přístupového bodu (`BSSID`), MAC adresa stroje (`STATION`) a počet přijatých (`Frames`) a ztracených (`Lost`) datových rámců.

Dostupná bezdrátová síť určená speciálně pro vykonání útoku byla nazvána `testWIFI`, jejíž přístupový bod má BSSID ve tvaru `A0:F3:C1:XX:XX:XX` (MAC adresa je částečně skryta z důvodu důvěrnosti). Jak je zřejmé z výpisu, k této síti byl připojen jeden aktivní klient s fyzickou adresou `2C:33:7A:XX:XX:XX`. Jelikož při útoku na zabezpečení WEP závisí na počtu odchycených inicializačních vektorů, bylo na klientském počítači spuštěno stahování většího množství dat při průměrné rychlosti 10 Mbps. Pro odchyt rámců vybrané laboratorní sítě byl využit příkaz:

```
root@testPC:~# airodump-ng --channel 11 --bssid A0:F3:C1:XX:XX:XX --write testWEP
               wlan1mon
```

Parametr `--channel` konkretizuje využívaný kanál, `--bssid` určuje odchytávaný přístupový bod a `--write` ukládá odchycené inicializační vektory do souboru s názvem `testWEP`. Pro útok s úspěšným výsledkem, tedy odhalením sdíleného klíče, bylo zapotřebí dostatečné množství inicializačních vektorů. Dokumentace nástroje Aircrack-ng (2009–2017) specifikuje minimální počty inicializačních vektorů pro úspěšné odhalení klíče, jejichž hodnoty jsou uvedeny v tabulce 1.

Tabulka 1: Doporučený počet inicializačních vektorů, zdroj: (Aircrack-ng, 2009–2017)

Délka WEP klíče	**Počet inicializačních vektorů**
64 bitů	20 000
128 bitů	40 000

Po nasbírání dostatečného množství inicializačních vektorů je nutné proces ukončit klávesovou zkratkou CTRL+C. Poslední fází je zjištění použitého hesla, k jehož úkonu je využit nástroj Aircrack-ng s následujícím příkazem.

```
root@testPC:~# aircrack-ng -a 1 testWEP.cap
```

Parametr `-a` určuje typ útoku, kdy jednička definuje zabezpečení WEP, po níž následuje soubor obsahující získané inicializační vektory. Po tomto příkazu bylo spuštěno čtení paketů a zahájen PTW útok.

Pokud je počet inicializačních vektorů dostatečný, heslo je nalezeno a zobrazeno jak v hexadecimálním, tak i v ASCII tvaru. V případě selhání útoku a nenalezení hesla, nástroj vypíše zprávu s doporučením o opětovné odchytávání.

```
                        Aircrack-ng 1.2 rc4
            [00:00:01] Tested 31984 keys (got 20101 IVs)

KB  depth byte(vote)
0   23/26 E3(22784) 1C(22528) 31(22528) 37(22528) 51(22528) A2(22528) F9(22528) FD(22528)
1    0/ 1 32(34560) 87(27136) 58(25344) 36(25088) 43(24576) 7B(24320) 0D(24064) C6(24064)
2    2/25 33(25600) 8B(25600) 00(25344) DA(25088) 93(25088) AC(24576) B4(24576) CF(24576)
3    0/ 1 34(33792) DE(25344) 31(24576) C4(24576) D0(24576) 15(24320) 34(24320) 14(24064)
4    5/51 35(24832) 7E(24576) CB(24576) 4E(24064) 50(24064) AB(24064) B6(24064) C4(24064)

                    KEY FOUND! [ 31:32:33:34:35 ] ( ASCII: 12345 )
    Decrypted correctly: 100%
```

7.4 Výsledky testování WEP

Testování standardu WEP bylo zaměřeno na lámání bezpečnostního hesla a zjištění, zda má složitost klíče vliv na prováděný útok. Bylo definováno pět kategorií definujících politiku klíčů, z nichž každá obsahovala pět různých hesel. Při testování tak bylo předpokládáno dvacet pět pokusných měření.

Při každém testovaném hesle byly shromažďovány informace o celkovém počtu zachycených datových rámců, z nich získaných inicializačních vektorů, celkový čas potřebný na odchycení paketů a potřebný čas ke zjištění sdíleného klíče. Získaná data jsou kvůli své rozlehlosti uložena na přiloženém CD, které je součástí přílohy.

V průběhu útoku byl čas měřen pomocí ručních stopek, poněvadž nástroj Airodump-ng zobrazuje pouze čas orientační, zaokrouhlený na celé minuty, čímž by vznikly velmi zkreslené výsledky.

Při použití 64bitového klíče byl pro jeho úspěšné prolomení stanoven minimální počet 20 000 inicializačních vektorů a při 128bitovém klíči bylo potřeba odchytit 40 000 těchto vektorů. Nástroj Airodump-ng bohužel nenabízí možnost automatického zastavení síťového skenu, a proto muselo dojít k ručnímu vypnutí, čímž ovšem mohlo dojít ke zpoždění způsobeným lidskou chybou. Počet zachytávaných paketů nevzrůstal o konstantní hodnotu, a proto nebylo možné zastavit měření na přesně vymezené hodnotě.

Při testování došlo k několika selháním, kdy nástroj Aircrack-ng nebyl schopen ze získaných vektorů vypočítat správný sdílený klíč, což mohlo být způsobeno nedostatečným počtem podstatných inicializačních vektorů a chybějící bitovou shodou mezi inicializačním vektorem a šifrovacím klíčem.

Výpisem informujícím o selhání bylo doporučeno provést odchyt komunikace znovu, ovšem s o pět tisíc vyšším počtem inicializačních vektorů než při předešlém útoku, jelikož nástroj se po vyzkoušení pěti tisíc inicializačních vektorů sám restartuje. Při opětovném útoku na stejné heslo byl zaznamenán nový čas odchytávání, který byl sečten s předešlým časem naměřeným při neúspěšném pokusu.

Jak je vidět v tabulce 2, u varianty s 64bitovým klíčem došlo ke třem neúspěšným měřením, která musela být opakována, a proto bylo měření celkem provedeno 28krát. Selhání tedy nastalo ve dvanácti procentech pokusů měření.

Tabulka 2: Výsledky testování WEP s použitím 64bitového klíče

	Celkový čas	Počet IV
Min	0:00:21	20 005
Max	0:01:26	25 348
Medián	0:00:32	20 095
Průměr	0:00:36	20 754
Počet testů	28	
Počet selhání	3	
Procento selhání	12 %	

Na základě použité hardwarové konfigurace a podpůrné komunikace mezi klientským strojem a přístupovým bodem stačilo odchytávat provoz zhruba třicet dva sekund. Takto krátký časový interval postačil k zachycení potřebného počtu rámců sloužících k úspěšnému odhalení klíče. Samotné prolomení nástrojem Aircrack-ng bylo provedeno v řádech milisekund.

U druhé varianty měření se 128bitovým klíčem (tabulka 3), docházelo k častějšímu selhávání, tudíž muselo být 88 % měření vykonáno znovu. Ve většině případů došlo k několikanásobnému opakování testu. Celkově bylo provedeno sedmdesát pět měření. Čas za každý neúspěšný pokus byl sečten s předešlým testem, a proto průměrná doba odchytu dosáhla čtyř minut a jednadvaceti sekund.

Tabulka 3: Výsledky testování WEP s použitím 128bitového klíče

	Celkový čas	Počet IV
Min	0:01:08	40 080
Max	0:10:06	65 144
Medián	0:04:22	50 143
Průměr	0:04:21	50 378
Počet testů	75	
Počet selhání	50	
Procento selhání	88 %	

Nejvíce selhání prodělalo heslo `Pen*zePen*ze8` spadající do páté kategorie, které bylo úspěšně nalezeno až na šestý pokus s odchycením 65 144 inicializačních vektorů s celkovým časem deset minut a šest sekund.

Pouze ve třech případech bylo heslo úspěšně prolomeno při zachycení doporučených čtyřiceti tisíc inicializačních vektorů, kdy byla nalezena dvě hesla spadající do první kategorie a pouze jediné heslo z druhé kategorie. U dalších klíčů muselo být nasbíráno minimálně 50 000 vektorů, což bylo množství na úspěšné prolomení 48 % hesel. Z výsledků provedeného měření je zřejmé, že odhadnutý minimální

počet inicializačních vektorů nástroje Aircrack-ng byl pro většinu testovaných hesel nedostatečný a jedná se spíše o orientační hodnotu.

Ze získaných výsledků 64bitového klíče lze usoudit, že rozdíly ve složitosti klíče nemají na prolomení zásadní vliv. Většina hesel byla úspěšně prolomena po nasbírání minimálního doporučeného množství ve zhruba stejném čase.

Stejný závěr neplatí pro 128bitovou variantu, neboť s průchodem jednotlivých kategorií docházelo k postupnému zvyšování potřebného množství inicializačních vektorů a kvůli opakujícím se měřením i k nárůstu celkového času. Sdílený klíč 128bitové varianty nabývá třinácti znaků, čímž je složitost značně ovlivněna a s využitím obsáhlé množiny znaků se složitost dále zvyšuje. I přes komplikace při odchytu paketů ve výsledku došlo k odhalení veškerých stanovených hesel.

Při útoku na zabezpečení WEP má složitost hesla vliv pouze na množství inicializačních vektorů, které je nutno odchytit. Ať už je v síti zajištěna dostatečná probíhající komunikace či nikoli, s minimálně jedním přihlášeným klientem lze sdílený klíč úspěšně prolomit bez ohledu na jeho složitost.

7.5 Útok na WPA2 Personal

Pro otestování zabezpečení WPA2 typu Personal byl využit slovníkový útok, k němuž byla v kapitole 6 vybrána hesla a předem vytvořeny slovníky. Slovníkový útok byl použit na prolomení předsdíleného klíče, zkráceně PSK, který lze dopočítat ze získaných hodnot obsažených v EAPOL rámcích při čtyřcestné výměně mezi klientem a přístupovým bodem. Proto muselo v prvé řadě dojít k zachycení této výměny a až poté mohl být spuštěn útok na zjištění klíče.

Pro zachycení EAPOL rámců bylo spuštěno skenování sítě pomocí již známého nástroje Airodump-ng s využitím stejného příkazu jako na straně 48. Jelikož mělo být otestováno a prolomeno několik hesel v různých kategoriích, byly zachytáváné čtyřcestné výměny ukládány do souborů s názvem `verze[číslo kategorie]_[číslo hesla]` pro lepší přehlednost. Pro skenování sítě za využití prvního hesla z první kategorie byl proveden příkaz:

```
root@testPC:~# airodump-ng --channel 11 --bssid A0:F3:C1:XX:XX:XX --write verze1_01
               wlan1mon
```

Čtyřcestná výměna probíhá pouze při připojování klienta do sítě a existují dvě metody, jak ho získat. V prvním případě se vyčkává na nově připojovaného klienta a automatické odchycení výměny. Při druhé metodě je zapotřebí, aby byl v cílové bezdrátové síti minimálně jeden aktivní klient, který by mohl být násilně odpojen kvůli vynucení opětovného připojení. Pro tento test byla využita druhá metoda, to jest odpojení komunikujícího klienta.

Při provedení deautentizace klienta muselo být stále spuštěno skenování sítě, pomocí kterého byla výměna uložena. Proto musely být na útočníkově stroji otevřeny dva terminály. V prvním terminálu tedy probíhalo skenování sítě a odchytávání komunikace a ve druhém terminálu bylo provedeno vynucené odpojení. Odpojení

klienta se provedlo nástrojem Aireplay-ng, který je součástí balíčku Aircrack-ng, za pomoci příkazu:

```
root@testPC:~# aireplay-ng --deauth 1 -a A0:F3:C1:XX:XX:XX -c 2C:33:7A:XX:XX:XX
               wlan1mon
```

Parametr `--deauth` definuje typ útoku, tedy deautentizaci klienta, s následným počtem zaslaných deautentizačních paketů. Parametr `-a` upřesňuje fyzickou adresu přístupového bodu a `-c` fyzickou adresu klienta, jenž má být odpojen.

```
Waiting for beacon frame (BSSID: A0:F3:C1:XX:XX:XX) on channel 11
Sending 64 directed DeAuth. STMAC: [2C:33:7A:XX:XX:XX] [47 | 64 ACKs]
```

Po provedení příkazu proběhl výpis, ve kterém bylo uvedeno, že nástroj vyčkal na příchozí Beacon rámec od přístupového bodu, který vysílal na kanále číslo jedenáct. Následně byla klientovi zaslána sada deautentizačních rámců, které mu sdělily odpojení od sítě a potřebu opětovného připojení. Na tuto výzvu klient ihned zareagoval a výsledkem byl zachycený čtyřcestný handshake, který byl odchycen skenováním.

```
CH 11 ][Elapsed: 12 s ][ 2017-02-03 15:52 ][ WPA handshake: A0:F3:C1:XX:XX:XX
BSSID              PWR Beacons #Data,#/s CH MB  ENC  CIPHER AUTH ESSID
A0:F3:C1:XX:XX:XX -53   118   216   36  11 54e WPA2 CCMP   PSK  testWIFI

BSSID              STATION           PWR Rate    Lost Frames Probe
A0:F3:C1:XX:XX:XX 2C:33:7A:XX:XX:XX -29 54e-54e  0      421
```

Z pohledu klientského stroje došlo ke krátkému odpojení v případě zapnutého automatického připojování, které se v operačním systému Windows projevilo probliknutím ikony znázorňující odpojení od sítě, jež je umístěna v pravé části hlavní lišty, a současně s tím došlo k úplnému pozastavení přenosu dat. Tento úkon není nikterak rychlý a uživatel má možnost tuto změnu stavu zpozorovat.

Po získání výměny bylo možné provést slovníkový útok, pro který byl specifikován slovník podle aktuálně testované kategorie. K útoku byl aplikován nástroj Aircrack-ng, který vyžaduje určení typu útoku pomocí parametru `-a`, kdy číslice `2` určuje útok na WPA2. Dále bylo potřeba přiřadit konkrétní slovník za parametr `-w` a nakonec uvést soubor obsahující zachycený handshake.

```
root@testPC:~# aircrack-ng -a 2 -w slovnik1.txt verze1_01.cap
```

Nástroj zkouší slova ze slovníku postupně, dokud nenalezne shodu či nedojde na konec slovníku. Testovaná bezpečnostní hesla byla ovšem vybrána z konkrétních slovníků v různém pořadí, a proto by mělo vždy dojít k úspěšnému nalezení klíče.

V průběhu testování i po nalezení hesla je útočníkovi k dispozici výpis zobrazující strávený čas, celkový počet otestovaných hesel a aktuální rychlost, definovanou jako počet vyzkoušených hesel za sekundu. Průměrná rychlost prolomení, jež je podstatná z hlediska výsledků, byla vypočtena pomocí získaného času prolomení a pořadí hesla v odpovídajícím slovníku.

```
                    Aircrack-ng 1.2 rc4
[01:01:29] 1330028/1974460 keys tested (415.81 k/s)
Time left: 25 minutes, 52 seconds           67.36%
                 KEY FOUND! [ 4pujcime ]

Master Key      :35 6A 24 0C 8B 61 24 CB CC 80 A2 73 51 87 4A 1C
                 35 71 38 52 1F AF 00 EE D2 64 A6 21 1B 50 51 A6

Transient Key   :E5 18 1E 6E DB 40 56 38 B5 74 8D 3E 22 EA C8 7A
                 06 85 A0 5B 92 5A CA 0D 80 C9 2F AF 98 30 DA 60
                 A4 10 BE 54 35 A9 03 8D 59 CB A6 4A 10 F7 56 C1
                 36 6F AF 43 B5 B1 CE 73 DA 37 13 7E E9 AB 63 88

EAPOL HMAC      :03 CD 50 D3 EF B7 3D BD 6D 5A C4 6B 15 46 B9 55
```

7.6 Výsledky testování WPA2

K měření standardu WPA2 typu Personal byl aplikován slovníkový útok, který byl použit na otestování třiceti pěti klíčů s různou složitostí i délkou. K testu sloužila různorodá hardwarová konfigurace (tabulka 4) s měnícím se počtem jader procesorových jednotek, která posloužila k vykonání testu.

Tabulka 4: Konfigurace pro otestování standardu WPA2

Počet jader	**Frekvence [GHz]**	**RAM [GB]**	**Hardwarová konfigurace**
1	1,8–3,0	1	virtuální stroj na počítači klienta
2	1,8–3,0	1	virtuální stroj na počítači klienta
4	1,8–3,0	1	virtuální stroj na počítači klienta
4	2,5–3,1	4	stroj útočníka
4	3,2–3,6	2	virtuální stroj na univerzitním počítači
8	2,8–3,2	6	virtuální stroj na univerzitním serveru
16	2,8–3,2	6	virtuální stroj na univerzitním serveru

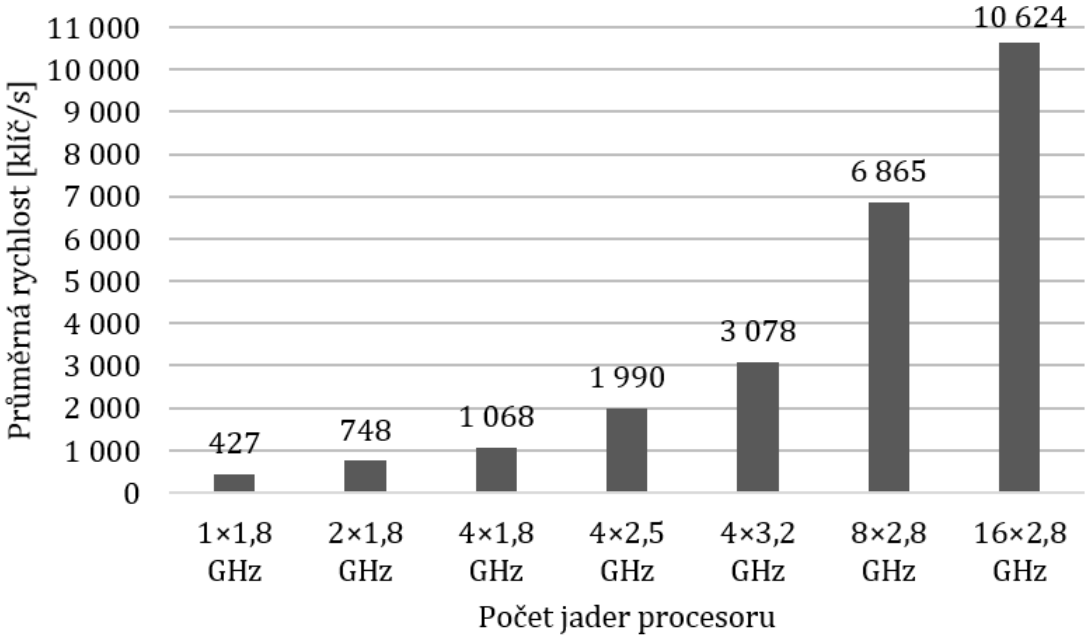
Před útokem bylo ze základního slovníku českého jazyka vytvořeno sedm modifikovaných slovníků, které podléhaly nadefinovaným kategoriím ze sekce 6. Jelikož klíč zabezpečení WPA2 musí minimálně nabývat osm znaků, musela být při modifikaci slovníků brána v úvahu politika jednotlivých kategorií. Celkové počty slov obsažené v konkrétních kategoriích jsou uvedeny v tabulce 5.

Tabulka 5: Obsáhlost jednotlivých slovníků

Kategorie	Počet slov
1	168 418
2	168 418
3	1 974 470
4	1 974 470
5	231 442
6	2 314 420
7	2 314 420

Po odchycení všech čtyřcestných výměn jednotlivých hesel mohlo být provedeno měření v offline podobě, při kterém byl zaznamenáván pouze celkový čas útoku. Do výsledků bylo nutné zahrnout i průměrnou rychlost, která ovšem ve výpisu testování nebyla uvedena, a proto byla vypočtena ze získaného času a pořadí slova ve slovníku.

Vypočtené průměrné rychlosti měření, se závislostí na počtu použitých jader procesorové jednotky, jsou vizualizovány na obrázku 16. Rychlost testování je ovlivněna nejen počtem jader, ale i frekvencí, jak je zřejmé z porovnání použitých čtyřjádrových procesorů.

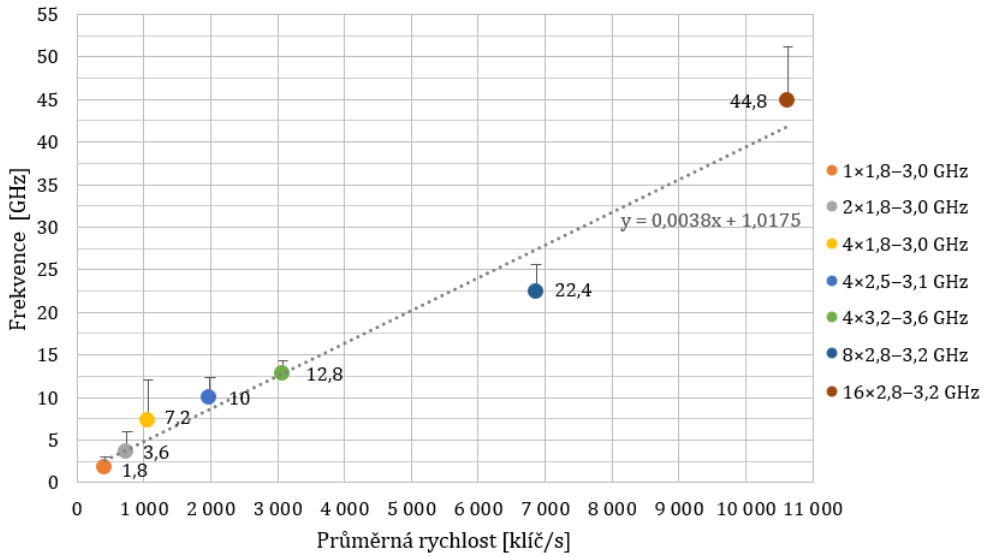


Obrázek 16: Průměrná rychlost určená počtem jader procesoru

Procesorové jednotky jsou schopny v případě potřeby spustit turbo režim, při kterém je provozní frekvence na vymezený čas zvýšena. Při testování pomocí virtuálního počítače nemohla být využita celková kapacita zdrojového stroje, neboť musela

být zajištěna jeho samostatná činnost a udržovatelnost virtuálního rozhraní, a proto mohou být naměřené výsledky mírně zkresleny. Taktéž nebylo přesně známo, jaký výkon byl při testování využit a přidělen emulujícímu systému. Nicméně vytvoření a porovnávání kontrolních součtů je výpočetně dosti náročné a systém pro výpočet využívá veškerou přidělenou kapacitu.

Na obrázku 17 je znázorněn vztah mezi rychlostí testování a celkovou frekvencí procesoru, která byla vypočtena pomocí počtu jader a frekvence určené pro jedno jádro, kdy byly tyto dvě hodnoty vynásobeny. Při nárůstu jader procesoru i zvýšení frekvence dochází k lineárnímu nárůstu průměrné rychlosti, která ovlivňuje celkový čas prováděného testování. Všechny použité procesory podporují funkci turbo režimu, a tak byla do výsledků zahrnuta i frekvence spadající pod tento režim.

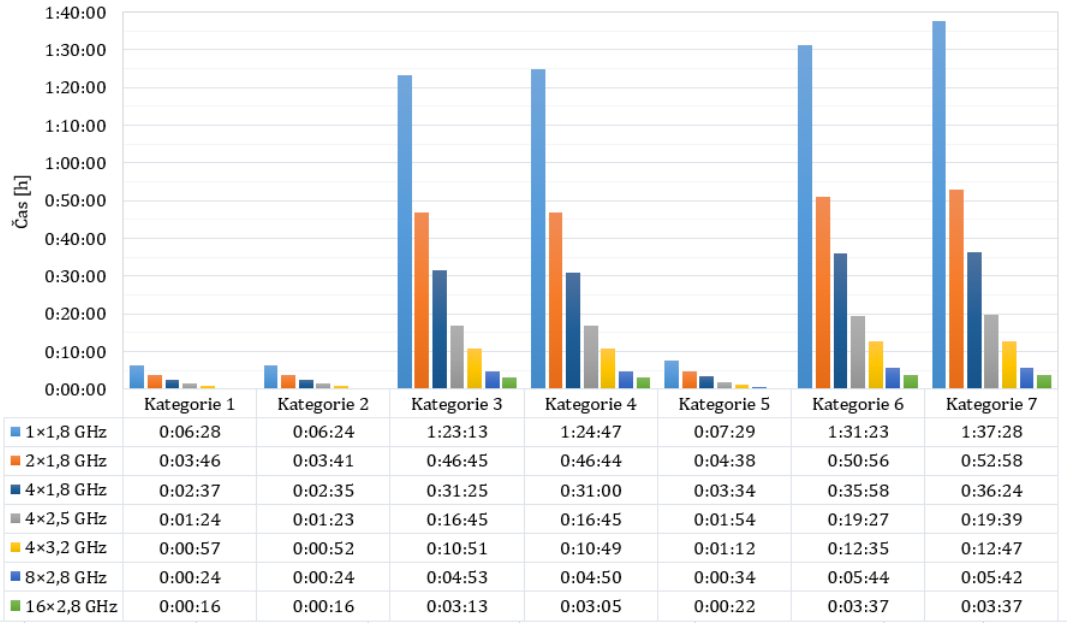


Obrázek 17: Průměrná rychlost se závislostí na frekvenci procesoru

Na základě zjištěných rychlostí byly dopočítány maximální časy potřebné k prolomení hesel z jednotlivých kategorií, které jsou zobrazeny na obrázku 18. Již na první pohled je jasné, že vyšší počet jader použitých při hledání hesla sníží celkovou časovou náročnost. V případě první, druhé a páté kategorie, jejichž slovníky jsou v řádech stovek tisíc, nejsou časové rozdíly až tak patrné. Odlišnost mezi měřením s využitím jednoho jádra a šestnácti jader se liší o zhruba šest minut.

Heslo, které je sestaveno ze základního českého slova bez použití diakritických znaků, není žádným způsobem komplikované na prolomení. I s pouhým jedním jádrem procesoru je možné heslo prolomit do maximálně deseti minut.

Naopak v dalších kategoriích, které obsahují miliony hesel, je maximální náročnost daleko vyšší. Při testování s využitím šestnácti jader bylo heslo z posledních dvou kategorií nalezeno v maximálním čase tři minuty a třicet sedm sekund. Ovšem při použití pouze jednoho jádra trvalo prolomení jednu hodinu a třicet sedm minut. Při takovémto časovém rozdílu je již vidět zásadní vliv vícejádrových procesorů.



	Kategorie 1	Kategorie 2	Kategorie 3	Kategorie 4	Kategorie 5	Kategorie 6	Kategorie 7
1×1,8 GHz	0:06:28	0:06:24	1:23:13	1:24:47	0:07:29	1:31:23	1:37:28
2×1,8 GHz	0:03:46	0:03:41	0:46:45	0:46:44	0:04:38	0:50:56	0:52:58
4×1,8 GHz	0:02:37	0:02:35	0:31:25	0:31:00	0:03:34	0:35:58	0:36:24
4×2,5 GHz	0:01:24	0:01:23	0:16:45	0:16:45	0:01:54	0:19:27	0:19:39
4×3,2 GHz	0:00:57	0:00:52	0:10:51	0:10:49	0:01:12	0:12:35	0:12:47
8×2,8 GHz	0:00:24	0:00:24	0:04:53	0:04:50	0:00:34	0:05:44	0:05:42
16×2,8 GHz	0:00:16	0:00:16	0:03:13	0:03:05	0:00:22	0:03:37	0:03:37

Obrázek 18: Časová náročnost odhalení hesel

Celkový průběh testování na jednotlivých procesorech má lineární charakteristiku. To znamená, že zvětšující se množství hesel ve slovníku je přímo úměrný celkovému času trvání. Ovšem pouze za předpokladu, že rychlost procházení hesel se nemění. S rychlostními výkyvy dochází k většímu nárůstu potřebného času na dokončení testu a úspěšného nalezení hesla.

Další možností odhalení hesla je metoda známá jako útok hrubou silou, při které jsou generovány náhodné řetězce znaků. Účinnost tohoto útoku je velmi vysoká, avšak se značnou časovou náročností. Pro představu bylo vytvořeno pět kategorií, které jsou uvedeny v tabulce 6, obsahující různý počet kombinací, které byly vypočteny pro řetězce dlouhé osm znaků.

Tabulka 6: Sestavené kategorie pro útok hrubou silou

Kategorie	**Politika hesla**	**Počet znaků**	**Počet variant**
1	Číslice	10	$1,00 \cdot 10^{8}$
2	Písmena anglické abecedy	26	$2,09 \cdot 10^{11}$
3	Písmena a číslice	36	$2,82 \cdot 10^{12}$
4	Malá a velká písmena, číslice	62	$2,18 \cdot 10^{14}$
5	Malá a velká písmena, číslice, speciální znaky	92	$5,13 \cdot 10^{15}$

Útok hrubou silou byl proveden pouze matematicky. Pro výpočet byly použity hodnoty průměrných rychlostí, které byly získány v předchozím slovníkovém útoku za použití jednotlivých hardwarových konfigurací, a počet variant obsažených v každé nadefinované kategorii. Výsledné hodnoty jsou součástí tabulky 7, kdy jsou odhadnuty maximální časy pro nalezení hesla.

Jak je vidět, v případě numerického hesla je prolomení možné za dvě hodiny s použitím šestnácti jader procesoru a tří dnů pouze s využitím jednoho procesoru. Od třetí kategorie, která obsahuje pouze malá písmena anglické abecedy a číslice, je nalezení hesla na této hardwarové konfiguraci takřka nemožné, jelikož maximální doba lámání je v desítkách až tisících let.

Tabulka 7: Výsledky útoku hrubou silou

Počet jader	**Kategorie**				
	1	**2**	**3**	**4**	**5**
1×1,8 GHz	3 dny	15 let	209 let	16 205 let	380 901 let
2×1,8 GHz	2 dny	8 let	120 let	9 257 let	217 578 let
4×1,8 GHz	1 den	6 let	83 let	6 481 let	152 339 let
4×2,5 GHz	13 hodin	3 roky	45 let	3 480 let	81 794 let
4×3,2 GHz	9 hodin	2 roky	29 let	2 250 let	52 877 let
8×2,8 GHz	4 hodiny	352 dní	13 let	1 009 let	23 706 let
16×2,8 GHz	2 hodiny	227 dní	8 let	652 let	15 318 let

7.7 Útok na WPS

V této části je ukázána realizace útoku na síť, která podporuje připojování pomocí funkce WPS. Před samotným útokem ovšem muselo dojít ke konfiguraci přístupového bodu a spuštění služby WPS, jejíž povolení bylo provedeno v záložce QSS.

```
QSS Status: Enabled
Current PIN: 03872710
```

V první fázi útoku došlo k oskenování bezdrátových sítí a ověření dostupnosti WPS. Na základě výběru nástrojů v kapitole 4.2 byl pro skenování využit nástroj Wash, který byl spuštěn příkazem:

```
root@testPC:~# wash --interface wlan1mon
BSSID             Channel RSSI WPS Version WPS Locked  ESSID
00:02:72:XX:XX:XX   4      00    1.0            No      NET_NED
50:46:5D:XX:XX:XX   6      00    1.0            No      Palenikovi
1C:BD:B9:XX:XX:XX   8      00    1.0            No      Lada M
A0:F3:C1:XX:XX:XX  11      00    1.0            No      testWIFI
```

Výpis zachycuje čtyři bezdrátové sítě, mezi nimi i testovací síť `testWIFI`, které měly funkci WPS povolenou a z hlediska bezpečnosti se tak vystavovaly možnému riziku. Nicméně test byl proveden na zmiňovanou síť `testWIFI`, kdy byl aplikován útok hrubou silou zaměřený na prolomení PIN kódu pomocí nástroje Reaver. Test probíhal automaticky, kdy byly generovány náhodné PIN řetězce a zasílány přístupovému bodu pro ověření. K zahájení testu posloužil příkaz:

```
root@testPC:~# reaver --interface wlan1mon --bssid A0:F3:C1:XX:XX:XX --delay 10 -vv
```

V příkazu jsou obsaženy parametry, které specifikují cílovou síť a vlastnosti útoku. Parametr `--interface` určuje rozhraní pro odchyt paketů, `--bssid` směruje útok pouze na konkrétní přístupový bod podle uvedené MAC adresy a `--delay` nastavuje prodlevu mezi zasíláním jednotlivých variant PIN kódu. Poslední parametr `-vv` (zkratka very verbose neboli v překladu velmi upovídaný) zobrazuje detailní výpis zpráv, které při útoku slouží jako zpětná vazba.

Po spuštění nástroje Reaver se vyčkává na příchozí Beacon rámec, jenž je pravidelně odesílán z přístupového bodu, kterým jsou klienti informováni o jeho přítomnosti. Po přijetí tohoto rámce následuje asociace útočníkova stroje s definovaným přístupovým bodem na konkrétním vysílajícím pásmu. Teprve po těchto krocích nástroj přistoupí k zahájení útoku, kdy jsou postupně generovány náhodné PIN kódy, které jsou po částech zasílány přístupovému bodu k ověření.

```
[+] Waiting for beacon from A0:F3:C1:XX:XX:XX
[+] Switching wlan1mon to channel 11
[+] Associated with A0:F3:C1:XX:XX:XX (ESSID: testWIFI)
[+] Starting Cracking Session. Pin count: 1, Max pin attempts: 11000
[+] Trying pin 33335674.
[+] Sending EAPOL START request
[+] Received identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
```

Maximální množství PIN kombinací je stanoveno pouze na jedenáct tisíc, což je dáno implementační chybou blíže popsanou v kapitole 3.4.2. Při útoku si útočníkův stroj s přístupovým bodem vymění sedm zpráv, které jsou označeny M1–M7. První zprávu M1 vysílá přístupový bod, v níž jsou obsaženy identifikační informace, jako je model, výrobce a hodnota veřejného klíče označeného PKE (Enrollee public key).

Poté klient odpovídá zprávou M2, ve které zasílá své identifikační údaje, klíč PKR (Registrar public key) a autentizační klíč AuthKey, na niž přístupový bod odpovídá zprávou M3. Až ve zprávě M4 je zaslána první čtyřmístná část PIN kódu.

Jak je vidět ve výpisu výše, v průběhu útoku byla čtvrtá zpráva odeslána, ovšem odpovědí jí byla zpráva WSC NACK, jež informovala o přijetí nesprávné kombinace

a ukončení dočasné komunikace. Po neúspěšném pokusu bylo navázáno opětovné spojení s nově vygenerovaným PIN kódem.

Po otestování pěti PIN kódů v řadě došlo k náhlému ukončení komunikace a vypsání varovného upozornění, že přístupový bod útok rozpoznal a brání se tak proti dalším útočným pokusům. Po použití nástroje Wash bylo zjištěno, že přístupový bod funkci WPS uzamknul, což se projevilo ve sloupci `WPS Locked`. Mohlo se jednat o dočasné znepřístupnění služby nebo zablokování služby pro konkrétní fyzickou MAC adresu, což se ovšem liší v závislosti na výrobci a implementaci přístupového bodu.

```
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

Pro ověření, zda bylo WPS zablokováno vůči MAC adrese, byl použit nástroj Macchanger, s jehož pomocí byla vygenerována nová, náhodná fyzická adresa. Před nastavením muselo dojít k vypnutí rozhraní, nastavení nové adresy a poté k opětovnému zapnutí rozhraní.

```
root@testPC:~# ifconfig wlan1mon down
root@testPC:~# macchanger -r wlan1mon
Current MAC:   98:DE:D0:XX:XX:XX
Permanent MAC: 98:DE:D0:XX:XX:XX
New MAC:       BA:B7:A6:XX:XX:XX
root@testPC:~# ifconfig wlan1mon up
```

Ani po přenastavení MAC adresy nedošlo ke zpřístupnění funkce WPS, což znamená, že v případě tohoto přístupového bodu nemá fyzická adresa na uzamčení služby vliv. Při delším skenování bylo zjištěno, že uzamknutí služby není pouze dočasné, nýbrž trvalé, a jeho zrušení je možné provést pouze restartováním přístupového bodu.

Využitý přístupový bod má tedy implementován kvalitní ochranný systém, díky němuž je téměř nemožné útok zrealizovat, což je ovšem příhodné z hlediska bezpečnosti. Při tomto provedeném testu se bohužel nepodařilo zabezpečení prolomit a získat bezpečnostní PIN kód.

V případě, že by přístupový bod neměl implementovanou ochranu, by bylo heslo s největší pravděpodobností nalezeno a proběhly by i zbylé komunikační zprávy mezi útočníkem a přístupovým bodem. To znamená, že by došlo k výměně výše zmíněných zpráv pouze s tím rozdílem, že by byla první část PIN kódu (zpráva M4) úspěšně potvrzena zprávou M5 jdoucí od přístupového bodu.

Poté by došlo k vyslání i druhé PIN části v klíčové zprávě označené M6, na kterou by přístupový bod naposledy odpověděl zprávou M7. Nalezený PIN kód by byl vypsán útočníkovi i s následně odchyceným WPA-PSK klíčem. Následující výpis je pouze ukázkový, poněvadž ho reálně nebylo docíleno.

```
[+] Pin cracked in XX seconds
[+] WPS PIN: ‘03872710‘
[+] WPA PSK: ‘hardwarovou‘
[+] AP SSID: ‘testWIFI‘
```

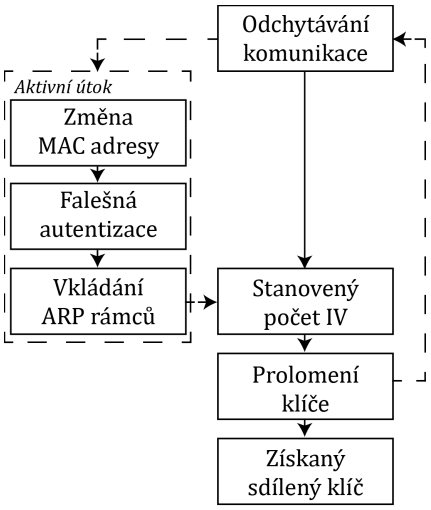
8 Diskuze

8.1 Testování WEP

Měření protokolu WEP bylo provedeno za pomoci pasivního útoku PTW, při kterém byla pouze zachytávána probíhající komunikace. Kvůli snížení časové náročnosti a vytvoření stejných podmínek pro všechna testovaná hesla, bylo na klientském stroji záměrně zahájeno stahování většího množství dat. Díky tomu bylo umožněno vykonat testování rychleji, neboť v síti probíhal přenos dat, který mohl být zachycen.

V případě, že by byl alespoň jeden klient k testované bezdrátové síti připojen, ale probíhala by minimální nebo žádná datová komunikace, musel by být aplikován aktivní způsob útoku. Pro získání bezpečnostního klíče by bylo využito metody vkládání ARP paketů do sítě, čímž by byl útočníkův stroj nucen se aktivně zapojit do útoku. Při aplikaci aktivního útoku je značně snížena časová složitost potřebná k odcizení klíče.

Jak je uvedeno v dokumentaci nástroje Aircrack-ng (2009-2017), před vykonáním aktivního útoku musí nejdříve dojít ke změně fyzické adresy útočníkova stroje za adresu již připojeného klienta, pokud se v síti nějaký nachází. Poté je útočníkem provedena falešná autentizace k bezdrátové síti a uměle udržována asociace. Po odchycení jednoho ARP paketu dochází k úpravě sekvenčního čísla obsaženého v hlavičce a zaslání zpět přístupovému bodu. Takovýmto způsobem je v síti vygenerován provoz, díky čemuž jsou navýšena probíhající data, která je možno odchytit. Na obrázku 19 je vidět upravený postup s využitím aktivního útoku.



Obrázek 19: Průběh pasivního a aktivního útoku na zabezpečení WEP

Při testu bylo bráno v úvahu doporučení potřebného množství inicializačních vektorů, kdy bylo rozlišeno, zda se jedná o 64 či 128bitovou variantu. Ovšem při výpisu dostupných sítí není útočník žádným způsobem informován o typu použí-

vaného klíče. Z pohledu reálného útočníka by tedy nedošlo k rozlišení těchto dvou typů, a proto by bylo využito doporučené množství na prolomení 128bitového klíče.

Jak již bylo uvedeno, nástroj Aircrack-ng navrhuje odchycení 40 000 inicializačních vektorů pro druhou variantu klíče. Podle autorů útoku PTW je ovšem tato hodnota účinná maximálně v padesáti procentech měření. Pro 95% úspěšnost prolomení autoři stanovují množství 85 000 inicializačních vektorů (Pyshkin, 2007).

Pokud by tato hodnota byla použita při provedeném testu, veškerá hesla by byla odchycena při prvním pokusu měření. V případě 64bitového klíče by došlo ke značnému prodloužení času i nadbytečnému množství inicializačních vektorů. Ovšem při testování 128bitového klíče by byly výsledky o poznání příznivější. Potřebný čas by se odhadem pohyboval okolo tří minut a k selhání by došlo jen zřídka.

V konečném důsledku nemá neefektivně zvolená hodnota inicializačních vektorů vliv na prolomení WEP klíče. I přes komplikace a prodloužení času nakonec došlo k nalezení všech stanovených hesel ve všech kategoriích, což dokazuje velké riziko z hlediska bezpečnosti, kvůli kterému byla podpora standardu WEP ukončena.

8.2 Testování WPA2

Testování standardu WPA2 typu Personal proběhlo na šesti hardwarových sestavách s tím, že bylo využito i virtuálních počítačů. Standard byl ověřen pomocí hesel, k čemuž byl vytvořen scénář definující sedm kategorií, které se vzájemně lišily složitostí a obsahem znaků.

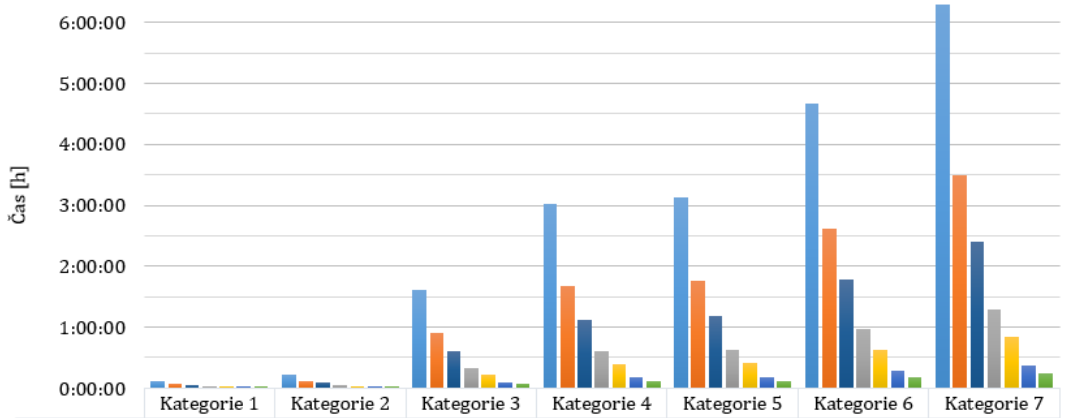
Před měřením muselo dojít k odchytu čtyřcestné výměny, která posloužila k otestování a odhalení předsdíleného hesla mimo dostupnou bezdrátovou síť. Klientovi byl zaslán deautentizační rámec, po jehož opětovném připojení byla získána a uložena výměna, která posloužila k nalezení hesla a otestování zabezpečení na více hardwarových sestavách.

Při testování byl zaznamenáván čas a průměrná rychlost prolomení jednotlivých hesel na všech hardwarových konfiguracích. Byl získán přehled prezentující časovou náročnost jednotlivých kategorií nezávisle na sobě.

Z pohledu útočníka, který by heslo chtěl prolomit, je ovšem časová náročnost odlišná. Při reálném útoku záleží na celkovém čase lámání, neboť útočník nemá žádné informace o hesle a musí využít systematický postup útoku, při kterém by mohlo být heslo nalezeno.

Pokud by při měření byla použita tato myšlenka, nebyl by na heslo konkrétní kategorie použit pouze vymezený slovník, ale veškeré nadefinované slovníky. Testování by tedy probíhalo vždy se stejným průběhem, kdy by na každé heslo byly postupně použity veškeré slovníky vytvořené na základě scénáře. Při neúspěchu nalezení hesla v přiřazeném slovníku by byl použit slovník následující.

Při aplikaci tohoto postupu by se naměřené hodnoty velmi lišily. Na základě této úvahy byly výsledné hodnoty upraveny a celkové časy potřebné na prolomení hesel specifických kategorií jsou vidět na obrázku 20.



	Kategorie 1	Kategorie 2	Kategorie 3	Kategorie 4	Kategorie 5	Kategorie 6	Kategorie 7
1×1,8 GHz	0:06:28	0:12:51	1:36:04	3:00:52	3:08:20	4:39:43	6:17:11
2×1,8 GHz	0:03:46	0:07:26	0:54:11	1:40:55	1:45:33	2:36:30	3:29:28
4×1,8 GHz	0:02:37	0:05:13	0:36:38	1:07:38	1:11:12	1:47:10	2:23:34
4×2,5 GHz	0:01:24	0:02:47	0:19:32	0:36:17	0:38:12	0:57:38	1:17:17
4×3,2 GHz	0:00:57	0:01:49	0:12:40	0:23:29	0:24:41	0:37:16	0:50:04
8×2,8 GHz	0:00:24	0:00:48	0:05:40	0:10:30	0:11:04	0:16:47	0:22:29
16×2,8 GHz	0:00:16	0:00:31	0:03:44	0:06:50	0:07:12	0:10:49	0:14:26

Obrázek 20: Časová náročnost postupného slovníkového útoku

Z těchto výsledků je zřejmé, že i použití nenáročných hybridních slovníků má vcelku vysokou časovou náročnost. Při šestnácti jádrech byla maximální potřebná doba prolomení hesla ze sestavených kategorií čtrnáct minut a dvacet šest sekund. Ovšem při použití pouze jednoho jádra procesoru prolomení trvalo šest hodin a sedmnáct minut.

Ke slovníkovému útoku lze využít i jiné, volně dostupné slovníky v různých jazycích. Nevýhodou však je, že většina slovníků je vytvořena pro anglicky mluvící země a v případě lámání hesel českých domácích bezdrátových sítí jejich použití není příliš efektivní. Nicméně i v operačním systému Kali Linux je dostupný slovník obsahující obrovské množství používaných hesel, která byla prolomena a zaznamenána v průběhu let.

Jak uvádí Julian Dunning (2017), slovníkový útok je základní a mnohdy dostačující metoda pro odhalení hesla. Při neúspěchu se zavádí hybridní slovník, který byl použit i při testu zabezpečení, jenž základní slovník rozšiřuje číslicemi a speciálními znaky. Pokud není heslo nalezeno ani po aplikaci hybridního slovníku, přistupuje se k principu maskování, kdy se napadá struktura hesla. Poslední variantou útoku je hrubá síla, která postupně zkouší veškeré varianty ze zadaných znaků a číslic.

Útok hrubou silou se mnohdy nedoporučuje kvůli své velké časové náročnosti, jak bylo vidět na straně 55. Pro tyto účely je možné do lámání zapojit i výkon grafické karty nebo využít počítačový cluster, který spojuje více výkonných počítačů v jeden, což mnohonásobně urychluje průběh zjišťování hesla.

Standard WPA první generace nebyl testován, jelikož se jedná o předchůdce standardu WPA2 a byl vytvořen pouze jako dočasný bezpečnostní mechanismus.

Standardy aplikují stejnou autentizační politiku pouze s rozdílným šifrovacím algoritmem, a tak by i standard WPA byl otestován za pomoci slovníkového útoku. WPA využívá protokol TKIP, jenž aplikuje šifru RC4, čímž by mohlo dojít k o něco rychlejšímu nalezení bezpečnostního klíče.

8.3 Testování WPS

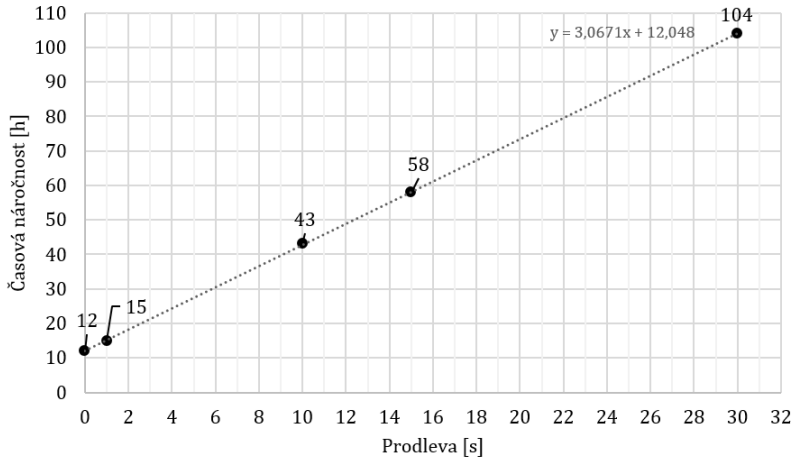
Při testování funkce WPS nedošlo k úspěšnému prolomení PIN kódu a útočníkovi tak nebyl povolen přístup do sítě. Přístupový bod po získaní pěti nesouhlasných PIN kódů vedený útok rozpoznal a službu trvale zablokoval. Společnost TP-LINK své přístupové body ošetřuje proti útokům vedeným proti službě WPS, což je z hlediska bezpečnosti výhodné.

Ovšem u jiných výrobců či starších přístupových bodů může dojít k prolomení PIN kódu i následnému odhalení hesla zabezpečujícího komunikaci uvnitř bezdrátové sítě. Z tohoto důvodu je vhodnější tuto službu, která je ve výchozím stavu zapnutá, raději deaktivovat a zamezit tak možnému riziku.

Při testování byla nastavena časová prodleva, která zajišťuje prodlení mezi odesíláním jednotlivých PIN kombinací útočníkem. Využívají se z důvodu snížení detekce útoku ze strany přístupového bodu, který má možnost funkci WPS dočasně deaktivovat a prodloužit útočníkovi dobu útoku.

Odezva testovaného přístupového bodu a výměna zpráv M1–M4 mezi bodem a útočníkem trvala čtyři sekundy. Poté útočníkův stroj vyčkal deset sekund, po jejichž uplynutí navázal novou komunikaci a odeslal nově vygenerovaný PIN kód.

Při nastavení různé časové prodlevy mezi odesíláním jednotlivých PIN kombinací dochází k nárůstu celkového času, což je zachyceno na obrázku 21. Na první pohled je zřejmé, že i minimální navýšení prodlevy má značný vliv na časovou náročnost prolomení funkce WPS. Ovšem jedná se pouze o matematické vyjádření, které se v reálném případě může měnit.



Obrázek 21: Časová náročnost při změně prodlevy

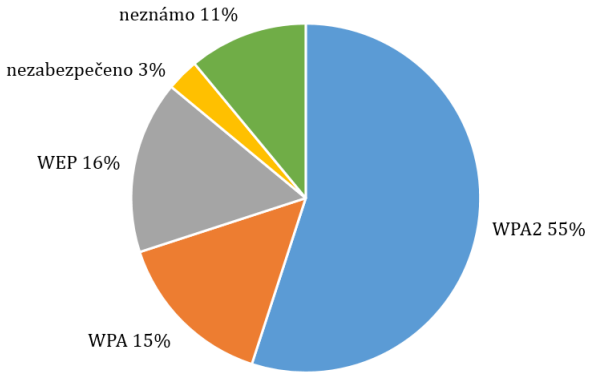
Autoři nástroje Reaver (Offensive Security, 2017a) stanovují maximální dobu na prolomení PIN kódu od čtyř do deseti hodin v závislosti na konkrétním přístupovém bodě.

8.4 Doporučení zabezpečení

V práci byly představeny hrozby a nedostatky zabezpečení WEP, které je v dnešní době již označeno za nedostatečné. Z výsledků je patrné, že při lámání hesla nezáleží na jeho složitosti, jelikož s dostatečným počtem inicializačních vektorů dojde k jeho odhalení, a to při použití obou délek klíčů.

Standard WEP by neměl být používán v domácích bezdrátových sítích, jelikož může dojít k neoprávněnému přístupu a využívání sítě. Pokud je WEP využit pro zabezpečení veřejných bezdrátových sítí, měla by být implementována autentizace pomocí otevřeného systému, u které nedochází k předání sdíleného klíče při čtyřcestné výměně. Komunikace může být šifrována, ovšem útočník nemá šanci klíč odchytnout při ověřování klienta.

Jak vyplývá z rozboru českého projektu Wifileaks (2017), který se zabývá skenováním českých bezdrátových sítí, je WEP stále využíván a to v celých šestnácti procentech (obrázek 22), což představuje 392 472 bezdrátových sítí. Tyto sítě jsou zranitelné proti nezákonnému vniknutí a využití útočníkem.



Obrázek 22: Využití typů zabezpečení, zdroj: (Wifileaks, 2017)

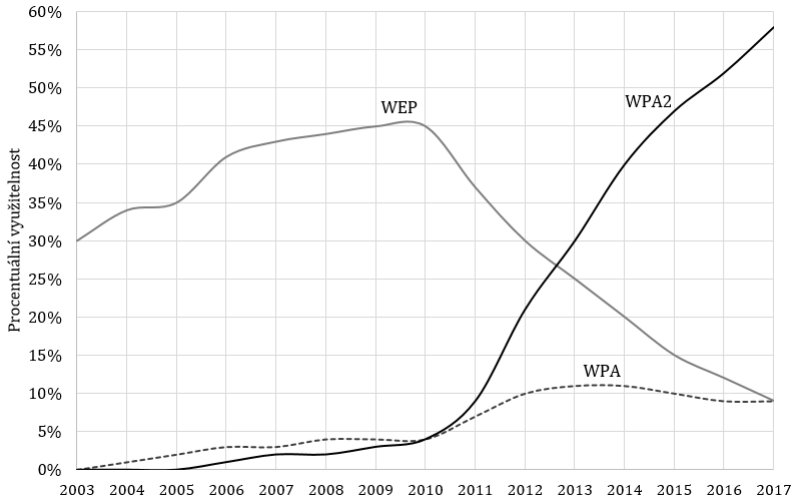
Nejlepší variantou pro zabezpečení domácích bezdrátových sítí je standard WPA2 typu Personal, který je již aplikován v 55 % českých bezdrátových sítí. Jak bylo zjištěno při měření, pro vysoký stupeň zabezpečení a minimalizaci proniknutí do bezdrátové sítě je nutné použít kvalitní heslo s velkou procentuální složitostí, která je ovlivněna délkou řetězce a použitými znaky.

Při použití jednoduchých slovníkových hesel, případně s doplněním o čísla či speciální znaky na konec nebo na začátek, dojde k prolomení v krátkém časovém intervalu, což je ovšem dáno útočníkovou hardwarovou konfigurací. Z těchto důvodů je vhodné vytvářet hesla jako náhodné řetězce s velkým obsahem různých znaků.

Pro zvýšení složitosti by heslo mělo obsahovat malá i velká písmena, číslice a několik speciálních znaků, které by měly být vhodně poskládány.

K tvorbě hesel lze využít náhodných generátorů, které jsou k dispozici prostřednictvím webových stránek. Příkladem je generátor hesel společnosti Symantec, vyvíjející antivirové programy Norton, který generuje hesla podle zadané délky a vybraných kritérií jako je obsažení číslic, speciálních znaků či diakritiky (Norton Identity Safe, 1995–2017).

Zajímavý je časový průběh využití jednotlivých typů zabezpečení, který je publikován mezinárodním portálem WiGLE (2001–2017), jenž ze získaných dat vytváří mapu zobrazující naskenované bezdrátové sítě i s jejich vlastnostmi.



Obrázek 23: Časový průběh využití zabezpečení, zdroj: (WiGLE, 2001–2017)

Zabezpečení WEP bylo prolomeno v roce 2001 a nahrazeno za standard WPA již v roce 2003. Jak je vidět z obrázku 23, propad zabezpečení WEP nastal až po roce 2010. Od tohoto roku vzrůstalo využití zabezpečení WPA2, což bylo dáno rozšiřujícími se domácími bezdrátovými sítěmi, které se staly velmi oblíbenými s příchodem chytrých telefonů.

Ovšem jak uvádí společnost Wi-Fi Alliance (Diamond, 2006), standard WPA2 musí být povinně implementován do bezdrátových prvků již od roku 2006, aby mohly být označeny bezpečnostní známkou nazývající se Wi-Fi CERTIFIED. Tímto předpisem byly výrobci nuceni implementovat tento standard do svých produktů a podpořit tak využití nejnovější metody pro zabezpečení bezdrátových sítí.

9 Závěr práce

Cílem této bakalářské práce bylo otestování typů zabezpečení spadajících do standardu IEEE 802.11, jež jsou určené pro domácí bezdrátové sítě. K testu byl použit scénář, který definoval několik kategorií specifikujících hesla s rozdílnou procentuální složitostí. Měření odolnosti zabezpečení probíhalo na operačním systému Kali Linux, který byl na jednom útočníkově stroji nainstalován jako výchozí systém. Další vybrané hardwarové konfigurace, jimiž byly stroj klienta a počítače Mendelovy univerzity v Brně, využívaly tento systém skrze virtuální stroj.

V první části práce byly představeny jednotlivé bezpečnostní standardy, mezi které se řadí WEP a WPA/WPA2 typu Personal, a ověřovací funkce WPS. Dále byly prezentovány jejich autentizační procesy, šifrovací mechanismy a existující útoky, které mohou být proti těmto zabezpečením použity. V další kapitole byla popsána základní myšlenka penetračního testování a byly vybrány nástroje, jež prakticky posloužily při testování standardů.

Ve druhé části práce byla vybrána hardwarová konfigurace a vytvořen scénář pro provedení systematického testu. Nejdříve bylo otestováno zabezpečení WEP, u kterého byla testována 64 i 128bitová varianta, k čemuž byl využit útok PTW. Výsledkem testu bylo zjištění, že útok není složitostí použitého klíče nijak limitován. Po získání dostatečného množství potřebných inicializačních vektorů došlo k odhalení hesla ve všech nadefinovaných kategoriích. Tento typ zabezpečení by se v domácích bezdrátových sítích používat neměl, jelikož nezajišťuje dostatečnou bezpečnost při autentizaci klienta do sítě ani při šifrování probíhající komunikace.

Dále bylo otestováno zabezpečení WPA2 využívající předsdílený klíč, což bylo provedeno pomocí slovníkového útoku a následně i matematicky pomocí útoku hrubou silou. Ke slovníkovému testu posloužilo třicet pět hesel, která se lišila složitostí i celkovou délkou řetězců. Po získání všech čtyřcestných výměn určitých hesel bylo přistoupeno k offline testování, kdy mohla být hesla odhalována mimo dostupnou bezdrátovou síť. K tomu bylo postupně využito šest strojů, z nichž každý obsahoval jiné množství jader procesoru.

Z výsledků slovníkového útoku bylo zřejmé, že při použití triviálního bezpečnostního hesla je i zabezpečení WPA2-PSK prolomitelné. Počet jader procesoru o různé frekvenci měl vliv na průměrnou rychlost lámání, která je určena počtem otestovaných hesel za sekundu, a tím i na celkový čas potřebný ke zjištění bezpečnostního hesla.

K získání předsdíleného klíče byl využit i útok pomocí hrubé síly, který byl v práci simulován pouze matematicky na nadefinovaných kategoriích. Bylo dokázáno, že aplikace tohoto útoku na použité hardwarové konfiguraci by bylo značně neefektivní kvůli své vysoké časové náročnosti, kdy by byla hesla ze stanovených kategorií nalezena až po tisících letech. Z toho vyplývá, že zabezpečení WPA2 Personal musí využívat složitého hesla, aby byla zajištěna maximální ochrana a minimalizováno riziko na odcizení hesla útočníkem.

Posledním testovaným typem byl standard WPS, jehož PIN kód se při útoku nepodařilo prolomit. Využívaný přístupový bod prováděný útok odhalil a funkci zablokoval, aby nemohlo dojít k prozrazení kódu. Nicméně jiné přístupové body nemusí mít tuto ochranu implementovanou, a proto je vhodné tuto funkci raději deaktivovat.

Práce by mohla posloužit méně zkušeným uživatelům, kteří ve svých domácnostech bezdrátovou síť využívají, ale nemají základní informace o možných hrozbách těchto sítí. Při tvorbě sítě je doporučováno aplikovat nejnovější zabezpečení WPA2, ovšem bezpečnostní heslo je ponecháno na volbě vlastníka. Neznalí uživatelé pro bezpečnostní klíče většinou volí jednoduchá a snadno zapamatovatelná slovníková hesla, čímž ovšem dochází k nedostatečnému zajištění bezpečnosti sítě.

Pro zaručení maximální ochrany domácí bezdrátové sítě je vhodné využít předpokladů standardu WPA2 Personal, což znamená aplikovat silné bezpečnostní heslo, a pro eliminaci rizik vypnout funkci WPS.

10 Reference

AIRCRACK-NG. *Aircrack-ng* [online]. Colorado, USA: Aircrack-ng, © 2009–2017 [cit. 2017-01-30]. Dostupné z: https://www.aircrack-ng.org/doku.php.

ALAMANNI, MARCO. *Kali Linux Wireless Penetration Testing Essentials* [online]. Birmingham, UK: Packt, © 2015 [cit. 2017-04-07]. ISBN 978-1-78528-085-6. Dostupné z: https://goo.gl/uQIs0o.

BALOCH, RAFAY. *Ethical Hacking and Penetration Testing Guide* [online]. Boca Raton, USA: CRC Press, © 2015 [cit. 2017-01-29]. ISBN 978-1-4822-3162-5. Dostupné z: https://goo.gl/TNV8UF.

BROAD, JAMES A ANDREW BINDNER. *Hacking with Kali: Practical penetration testing techniques.* Waltham, USA: Syngress, © 2014. ISBN 978-0-12-407749-2.

CARROLL, BRANDON. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce.* Brno: Computer Press, © 2011. ISBN 978-80-251-2884-8.

COLEMAN, DAVID, DAVID WESTCOTT, BRYAN HARKINS A SHAWN JACKMAN. *CWSP Certified Wireless Security Professional Official: Study Guide: Exam PW0-204* [online]. Indianapolis, USA: Wiley, © 2010 [cit. 2017-04-07]. ISBN 978-0-470-43891-6. Dostupné z: https://goo.gl/Sz3hE0.

DIAMOND, MICHAEL. WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products. In: *Wi-Fi Alliance* [online]. Austin, USA: Wi-Fi Alliance, 2006 [cit. 2017-05-11]. Dostupné z: http://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products.

DUNNING, JULIAN. Statistics Will Crack Your Password. In: *Praetorian* [online]. Austin, USA: Praetorian, © 2017 [cit. 2017-03-04]. Dostupné z: https://www.praetorian.com/blog/statistics-will-crack-your-password-mask-structure.

EDICE CZ.NIC. *CZ.NIC: Správce domény CZ* [online]. Praha: CZ.NIC, © 2017 [cit. 2017-03-03]. Dostupné z: https://knihy.nic.cz/.

EDNEY, JON A WILLIAM A. ARBAUGH. *Real 802.11 security: Wi-Fi protected access and 802.11i* [online]. Boston, USA: Addison-Wesley, © 2004 [cit. 2017-04-01]. ISBN 0-321-13620-9. Dostupné z: https://goo.gl/gscteY.

ENGEBRETSON, PATRICK. *The Basics of Hacking and Penetration Testing: Ethical hacking and penetration testing made easy.* Second Edition. Waltham, USA: Syngress, © 2013. ISBN 978-012-4116-443. Dostupné z: https://goo.gl/rSxbFl.

EXTRA DICTIONARIES - CZECH. *Zip Password Recovery* [online]. Zip Password Recovery, © 2016 [cit. 2017-03-04]. Dostupné z: http://www.zip-password-cracker.com/files/czech.zip.

Fern Pro. *Fern Pro* [online]. Fern Pro, 2017 [cit. 2017-01-30]. Dostupné z: http://www.fern-pro.com/.

Gast, Matthew S. *802.11 Wireless Networks: The Definitive Guide* [online]. Second edition. Sebastopol, USA: O'Reilly, © 2005 [cit. 2017-04-01]. ISBN 978-0-596-10052-0. Dostupné z: https://goo.gl/cBGnSi.

Glevický, David. *Zabezpečení bezdrátových sítí proti pokročilým útokům* [online]. Hradec Králové, 2016 [cit. 2017-03-11]. Dostupné z: http://theses.cz/id/88pa5u/STAG85843.pdf. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Ondřej Hornig.

Hucaby, Dave. *CCNA Wireless 640-722 Official Cert Guide.* Indianapolis, USA: Cisco Press, © 2014. ISBN 978-1-58720-562-0.

Hunt, Troy. *The science of password selection* [online]. Sydney, AUS: Troy Hunt, 2011 [cit. 2017-03-04]. Dostupné z: https://www.troyhunt.com/science-of-password-selection/.

ISECOM. *OSSTMM: Open Source Security Testing Methodology Manual* [online]. Spain: ISECOM, © 2017 [cit. 2017-01-28]. Dostupné z: http://www.isecom.org/research/osstmm.html.

Kizza, Joseph Migga. *Guide to computer network security.* Third edition. New York, USA: Springer Berlin Heidelberg, © 2015. ISBN 978-144-7166-535.

Kolouch, Jan. *CyberCrime* [online]. Praha: CZ.NIC, © 2016 [cit. 2017-03-03]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf.

Kurose, James a Keith Ross. *Počítačové sítě.* Brno: Computer Press, © 2014. ISBN 978-80-251-3825-0.

Lammle, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802.* Brno: Computer Press, © 2010. ISBN 978-80-251-2359-1.

Lieskovan, Tomáš. *Moderní trendy v zabezpečení Wi-Fi sítí standardu IEEE 802.11* [online]. Brno, 2015 [cit. 2017-03-11]. Dostupné z: https://www.vutbr.cz/studium/zaverecne-prace?zp_id=85256. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Pavel Endrle.

Miessler, Daniel. 10 million password list. In: *GitHub* [online]. San Francisco, USA: GitHub, 2016 [cit. 2017-03-04]. Dostupné z: https://goo.gl/rFiSYE.

NIST. *NIST: Technical Guide to Information Security Testing and Assessment* [online]. Gaithersburg, USA: NIST Pubs, 2017 [cit. 2017-01-28]. Dostupné z: https://www.nist.gov/node/589581.

Norton Identity Safe. *Generátor hesel* [online]. Mountain View, USA: Symantec Corporation, © 1995–2017 [cit. 2017-04-23]. Dostupné z: https://identitysafe.norton.com/password-generator.

Odom, Wendell, Rus Healy a Naren Mehta. *Směrování a přepínání sítí: autorizovaný výukový průvodce.* Brno: Computer Press, © 2009. ISBN 978-80-251-2520-5.

Offensive Security. *Kali Linux Tools Listing* [online]. USA: Offensive Security, © 2017 [cit. 2017-01-30]. Dostupné z: http://tools.kali.org/tools-listing.

Offensive Security. *Kali Linux: Official Documentation* [online]. Offensive Security, © 2017 [cit. 2017-03-03]. Dostupné z: http://docs.kali.org/introduction.

Offensive Security. *Kali Linux Downloads* [online]. USA: Offensive Security, © 2017 [cit. 2017-03-03]. Dostupné z: https://www.kali.org/downloads/.

Pecha, František. *Nástroje a metody pro prolamování bezdrátových sítí norem IEEE 802.11 s použitím virtualizace* [online]. České Budějovice, 2015 [cit. 2017-03-11]. Dostupné z: http://theses.cz/id/gpjbw1/Bakalarka.pdf. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Přírodovědecká fakulta. Vedoucí práce Jan Fesl.

Policie České republiky. *Kyberkriminalita* [online]. Česká republika: Policie ČR, © 2017 [cit. 2017-01-30]. Dostupné z: http://www.policie.cz/clanek/kyberkriminalita.aspx.

PTES. *PTES Technical Guidelines* [online]. USA: GNU Free Documentation License 1.2, 2014 [cit. 2017-01-29]. Dostupné z: http://www.pentest-standard.org/.

Pyshkin, Andrei, Erik Tews a Ralf-Philipp Weinmann. Breaking 104 bit WEP in less than 60 seconds. In: *Cryptology ePrint Archive* [online]. Darmstadt, Germany: Cryptology ePrint Archive, 2007 [cit. 2017-04-22]. Dostupné z: http://eprint.iacr.org/2007/120.pdf.

Ramachandran, Vivek a Cameron Buchanan. *Kali Linux Wireless Penetration Testing: Beginner's Guide* [online]. Second edition. Birmingham, USA: Packt, © 2015 [cit. 2017-04-14]. ISBN 978-1-78328-041-4. Dostupné z: https://goo.gl/KO1o7X.

Rydlo, Jan. *Využití penetračního testování v bezdrátových sítích* [online]. Hradec Králové, 2016 [cit. 2017-03-11]. Dostupné z: http://theses.cz/id/wdo1dq/STAG85818.pdf. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Josef Horálek.

Sajvera, Miroslav. *Bezdrátové sítě a jejich zabezpečení* [online]. Hradec Králové, 2015 [cit. 2017-03-11]. Dostupné z: http://theses.cz/id/322io7/STAG64132.pdf.

Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Vladimír Soběslav.

Skovajsa, Tomáš. *Bezpečnost WiFi sítí* [online]. Brno, 2012 [cit. 2017-03-11]. Dostupné z: http://is.muni.cz/th/208041/fi_m/tomas_skovajsa.pdf. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Zdeněk Říha.

Sosinsky, Barrie. *Mistrovství - počítačové sítě.* Brno: Computer Press, © 2011. ISBN 978-80-251-3363-7.

Šenovský, Jakub. *Nástroj pro analýzu zabezpečení bezdrátových sítí* [online]. Brno, 2014 [cit. 2017-04-07]. Dostupné z: https://www.vutbr.cz/studium/zaverecne-prace?action=detail&zp_id=79906. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Lukáš Aron.

Štefanec, Filip. *Předcházení útokům na standard 802.11* [online]. Brno, 2015 [cit. 2017-03-11]. Dostupné z: https://www.vutbr.cz/studium/zaverecne-prace?zp_id=85213. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Bohumil Novotný.

Vaudenay, Serge a Amr M. Youssef. *Selected areas in cryptography 8th Annual International Workshop* [online]. 8th Annual International Workshop. Toronto, Canada: Springer, © 2001 [cit. 2017-04-07]. ISBN 978-354-0455-370. Dostupné z: https://link.springer.com/chapter/10.1007/3-540-45537-X_1.

Wifileaks. *Wifileaks* [online]. Wifileaks, © 2017 [cit. 2017-04-13]. Dostupné z: http://www.wifileaks.cz/.

WiGLE. *WiGLE* [online]. WiGLE, 2001–2017 [cit. 2017-04-13]. Dostupné z: https://wigle.net/.

Zákon č. 40/2009 Sb.: trestní zákoník. In: *Sbírka zákonů.* Praha: Ministerstvo vnitra, 2009, ročník 2009, částka 11, číslo 40. ISSN 1211-1244. Dostupné z: www.mvcr.cz/soubor/sb011-09-pdf.aspx.

Přílohy

A Skripty pro sestavení slovníků

Bezpečnostní klíč standardu WPA2 musí být delší než osm znaků, tudíž muselo dojít k filtraci slov ještě před sestavením modifikovaných slovníků. V první a druhé kategorii byla pro hesla použita pouze písmena anglické abecedy, a proto byla ze slovníku odfiltrována všechna slova obsahující méně než osm znaků.

Třetí a čtvrtá kategorie byla rozšířena o číslice umístěné před nebo za slovo, kdy bylo možné ve slovníku ponechat i slova o délce sedm znaků. U kategorií obsahujících zdvojená slova byla vybrána slova minimálně obsahující čtyři znaky.

K provedení filtrace slov a uložení do nového souboru byl využit příkaz `cat [slovnik] | pw-inspector -m [minimální délka slova] -M [maximální délka slova] > [nový slovník]`.

Přidání čísla před a za slovo

```
#!/bin/bash
vstup="$1"
vystup1="$2"
vystup2="$3"
while I= read radek
do
    for i in {0..9}
do
    echo $radek$i >> $vystup1
    echo $i$radek >> $vystup2
done
done < "$vstup"
```

Po uložení skriptu muselo dojít ke změně práv, aby byl skript spustitelný (vlastnost execute). Změna byla provedena příkazem `chmod 744 skript1.sh`. Poté mohlo dojít ke spuštění skriptu pomocí `./skript1.sh vstup.txt vystup1.txt vystup2.txt`.

Zdvojení slov

```
#!/bin/bash
vstup="$1"
vystup="$2"
while I= read radek
do
    echo $radek$radek >> $vystup
done < "$vstup"
```

Pro spuštění byl volán příkaz `./skript2.sh vstup.txt vystup.txt`.

B Vybraná hesla pro otestování zabezpečení

Tabulka 8: Hesla určená pro 64bitový WEP

Kategorie 1	**Kategorie 2**	**Kategorie 3**	**Kategorie 4**	**Kategorie 5**
12345	heslo	abc12	Hesl0	H*sl0
11111	laska	123qw	Qwe12	12#Qw
00000	lovec	test1	HroM3	Hr$M3
54321	asdfg	drak3	Cat28	Abc1*
36987	kocka	0pice	Kare1	St1n?

Tabulka 9: Hesla určená pro 128bitový WEP

Kategorie 1	**Kategorie 2**	**Kategorie 3**	**Kategorie 4**	**Kategorie 5**
1234567890123	nejdelsiheslo	hvezdnevalky1	ManSuperMan12	MeHe$$lo12345
6969696969696	pustmedovnitr	slunecnisvit3	MatrixMatrix0	PrinceZZna94?
0101010101010	kouzelneheslo	hesloheslo123	MilujiTe12345	Gandalf_Sedy5
6543210123456	heslonawifinu	vstupzakazan9	MojeHeslo0987	Kapitan?netu3
0159875321059	parekvrohliku	internet12345	Adidassadida7	Pen*zePen*ze8

Tabulka 10: Hesla určená pro WPA2

	Pořadí	Vybrané slovo
Kategorie 1	22 660	hardwarovou
	56 333	nejpropracovanejsimu
	83 338	odmerenou
	116 372	radkovacem
	154 689	vyvoznimu
Kategorie 2	10 731	Dedicich
	42 641	Monarchy
	79 608	Obetovala
	134 183	Strepiny
	162 363	Zaznivalo
Kategorie 3	236 862	extrapolace1
	514 055	mohutnem4
	702 464	nemoderniho3
	1 292 735	promluva4
	1 796 437	vysvobozeni6
Kategorie 4	78 796	5bubnovity
	573 257	6nasobenec
	841 769	8neuveritelny
	1 072 414	3pobloudilcovi
	1 330 025	4pujcime
Kategorie 5	745	agenturouagenturou
	13 567	ciferneciferne
	61 768	mickemmickem
	91 037	neprerusneprerus
	170 780	slovanovaslovanova
Kategorie 6	33 051	aritmetickologickearitmetickologicke0
	448 010	katerinakaterina9
	604 238	meandrmeandr7
	1 381 372	prednostiprednosti1
	1 700 281	slavickyslavicky0
Kategorie 7	176 309	8depresedeprese
	353 596	5honzahonza
	502 691	0korunkakorunka
	1 460 805	4privandrovalciprivandrovalci
	2 210 475	4zateczatec

C Přiložené CD

Přiložené CD obsahuje:

- zhotovené skripty pro tvorbu modifikovaných slovníků
- slovníky použité při slovníkovém útoku na standard WPA2
- zachycené čtyřcestné výměny pro otestování zabezpečení WPA2
- naměřené výsledky standardu WEP a WPA2