SOŠ agropotravinárska a technická,
Kušnierska brána 349/2, Kežmarok

PROGRAMOVÉ VYBAVENIE POČÍTAČOV

Ochrana informácií v počítačových sieťach, kódovanie

3. ročník

Zabezpečenie bezdrôtových sietí, zraniteľnosť bezdrôtových sietí

(Učebný text)

Ing. Peter Barančo

2023

NÁRODNÝ PROJEKT
„Zlepšenie stredného odborného školstva v Prešovskom samosprávnom kraji“

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE

PREŠOVSKÝ SAMOSPRÁVNY KRAJ

„Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci operačného programu Ľudské zdroje“

OBSAH

1 ZABEZPEČENIE BEZDRÔTOVÝCH SIETÍ

Bezpečnosťou siete sa rozumie minimalizácia zraniteľných miest sieťových prostriedkov. Ochranu v sieti si vyžadujú:

- informácie a dáta (vrátane dát spojených s bezpečnostnými opatreniami, napr. heslá),
- služby prenosu a spracovania dát,
- zariadenia,
- užívatelia z hľadiska svojho majetku a identity.

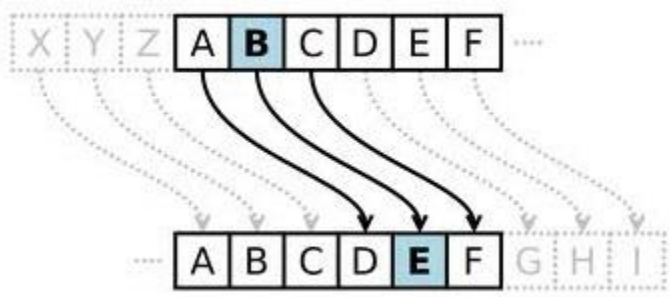
ZAPAMÄTAJTE SI!

Bezpečnosť bezdrôtových sietí môžeme rozdeliť do dvoch hlavných skupín:

- **Šifrovanie** – zabezpečenie prenášaných dát pred odpočúvaním
- **Autorizácia** – riadenie prístupu oprávnených užívateľov

1.1 Šifrovanie

Šifrovanie je postup, ktorý transformuje čistý text (plaintext) do šifrovaného textu (ciphertext) (obr. 1.1). V súčasnosti sa v šifrovaní používajú prevažne symetrické alebo asymetrické algoritmy.



Obr. 1.1 Jednoduché šifrovanie posunutím o určený počet znakov

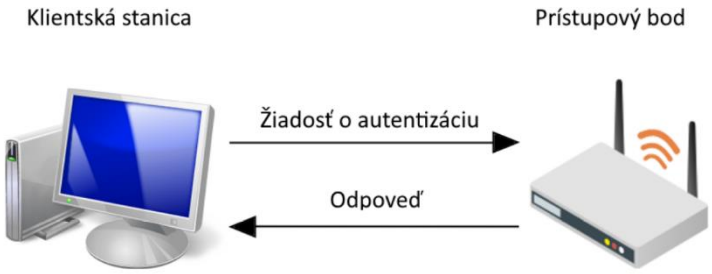
1.2 Autentizácia - AAA (Authenticaton, Authorization, Accounting)

AAA symbolizuje základnú skupinu funkcií, ktoré poskytujú protokoly pre správu prístupu v počítačových sieťach:

- **autentizácia (authenticaton)** – verifikácia používateľovej identity a jeho poverení (napr. heslo, token, digitálny certifikát)(obr. 1.2),
- **autorizácia (authorization)** – poskytovanie prístupu k sieťovým zdrojom a službám; autorizácii predchádza úspešná autentizácia,
- **účtovanie (accounting)** – sledovanie využitia sieťových zdrojov používateľmi; slúži na zisťovanie kto, kedy, ako a načo použil sieťový zdroj.

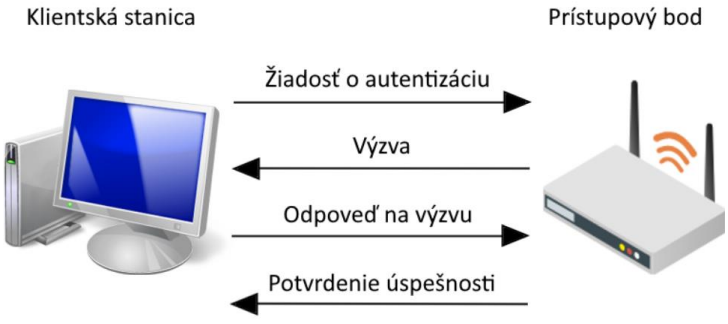
Obr. 1.2 Metódy autentifikácie

1. Autentizácia Open – system:
   - predvolený autentizačný protokol pre bezdrôtové siete,
   - klientská stanica sa môže spojiť s prístupovým bodom aj bez poskytnutia správneho kľúča (obr. 1.3).



Obr. 1.3 Open – system autentizácia

2. Autentizácia Shared-key:
   - stanica, ktorá sa chce pripojiť k sieti, sa musí autentizovať pomocou zdieľaného tajného kľúča (obr. 1.4),
   - správca siete definuje zdieľaný kľúč, a každej stanici, ktorá nemá pridelený kľúč, bude prístup zamietnutý,
   - zdieľaný kľúč používaný na šifrovanie a dešifrovanie dát sa tiež používa na autentizáciu stanice.



Obr. 1.4 Shared – key autentizácia

3. IEEE 802.1x

Autentizačný protokol 802.1x poskytuje mechanizmy pre distribúciu kľúčov, autentizáciu a autorizáciu. Pozostáva z troch entít:

- Supplicant – aplikačný softvér, ktorý je nainštalovaný na zariadení koncového používateľa.
- Autentizátor – zariadenie, ktoré blokuje alebo povoľuje premávku prostredníctvom svojho portu.
- Autentizačný server –verifikuje poverenia supplicanta a upozorňuje autentizátora, či bol, alebo nebol autorizovaný.

4. Filtrovanie MAC adries

Väčšina prístupových bodov ponúka funkciu, ktorá umožňuje správcovi bezdrôtovej siete vytvoriť zoznam MAC adries, určujúci, ktorým zariadeniam bude prístup do siete povolený, respektíve zamietnutý. Bohužiaľ, filtrovanie MAC adries je časovo náročné, pretože všetky adresy sa musia zadať do každého prístupového bodu ručne. Z tohto dôvodu je táto metóda vhodná skôr pre siete s menším počtom klientov a pre staršie zariadenia, ktoré nepodporujú silnejšie nástroje na ochranu.

5. SSID

SSID (Service Set Identifier) je jedinečný identifikátor bezdrôtovej siete. Štandardne vysielajú prístupové body svoje SSID v beacon správe každých pár sekúnd. Môžu byť však nakonfigurované tak, aby nevysielali beacon správy, a tým utajili svoje SSID. Existujú však softvérové nástroje, ktoré umožňujú SSID zistiť, aj keď je vysielanie vypnuté.

Existuje aj ESSID identifikátor WiFi siete (Extended Service Set Identification), ktorý je priamo naprogramovaný do access pointu pre identifikáciu siete, v ktorej sa nachádza. ESSID sa nevysiela, takže pridruženie do Wi-Fi siete je povolené iba autorizovaným staniciam, ktoré hodnotu ESSID siete poznajú. Preto sa siete používajúce ESSID označujú za uzavreté.

2 ZRANITEĽNOSŤ BEZDRÔTOVÝCH SIETÍ

Bezdrôtová sieť neposkytuje žiadnu fyzickú ochranu. Bezdrôtové siete, na rozdiel od káblových, môžu byť napadnuté aj mimo priestorov, v ktorých sa fyzicky nachádzajú. Vlny Wi-Fi sietí sa šíria všetkými smermi a môže ich zachytávať ktokoľvek, kto sa nachádza v ich dosahu. Pri nezabezpečenom prenose dát, silnej autentizácii užívateľa a zabezpečenom prístupe do podnikovej siete sa môžu útočníci dostať k citlivým podnikovým dátam.

2.1 Man-in-the-Middle

Útok Man-in-the-Middle („človek uprostred“) (obr. 2.1) môže byť spustený za účelom odpočúvania bezdrôtovej komunikácie alebo modifikácie prenášaných dát. Tento druh útoku sa vykonáva v sieťach s nezabezpečeným prenosom dát, ako sú napr. verejné Wi-Fi siete.

Obr. 2.1 Man-in-the-Middle

2.2 Podvrhnutie MAC adresy (MAC Spoofing)

Všetky bezdrôtové sieťové karty majú fyzickú adresu známu ako MAC adresa. V nastaveniach prístupových bodov je možné vymedziť, ktorým MAC adresám bude prístup do siete povolený, prípadne zamietnutý. Útočník môže odpočúvaním zachytiť MAC adresu oprávneného zariadenia (prenáša sa nešifrovane) a následne upraviť svoju MAC adresu jednoduchou konfiguráciou v systéme Windows. AP potom útočníkovi umožní prístup do siete.

2.3 Session Hijacking

Prostredníctvom útoku Session Hijacking je útočník schopný ukradnúť legitímnemu používateľovi jeho autorizovanú a autentizovanú reláciu (session). Na jeho spustenie útočník musí byť schopný „tváriť sa“ ako legitímny používateľ bezdrôtovej siete. Skutočný používateľ nemusí ani vedieť, že relácia bola ukradnutá a narušenie v relácii pripisuje nejakej poruche v sieti. Keď útočník získa kontrolu nad reláciou, môže ju použiť na akýkoľvek účel a je schopný udržiavať reláciu dlhšiu dobu.

2.4 DoS - Denial of Service

Útoky DoS (odmietnutie služby) samy o sebe nie sú pokusom o získanie prístupu k údajom. Útok DoS proti bezdrôtovej sieti bráni oprávneným používateľom pristupovať k sieťovým službám alebo

zdrojom. Dôsledkom útoku môže byť, že aplikácie alebo sieťové prostriedky dostupné prostredníctvom bezdrôtovej siete nie sú k dispozícii, nie je možná komunikácia s databázovým serverom alebo pripojenie k internetu.

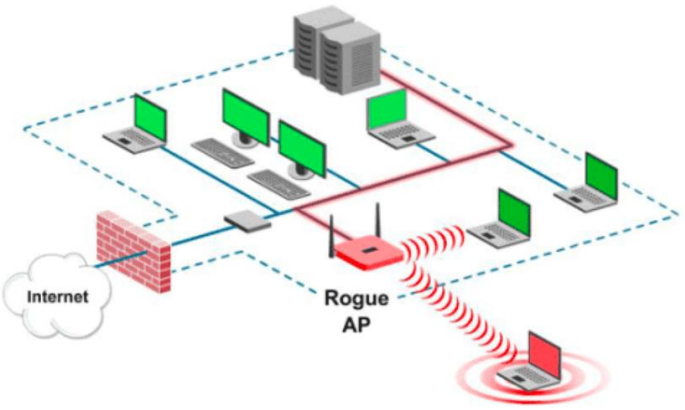
2.5 Wardriving

Odvodený od názvu starej techniky wardialing, ktorá sa používala na automatické vytáčanie telefónnych čísiel s cieľom vyhľadávania modemov pripojených k týmto číslam. Typickým použitím útoku wardriving je vyhľadávanie dostupných 18 bezdrôtových sietí z auta (obr. 2.2).

Obr. 2.2 Wardriving

2.6 Rogue Access Point

Rogue AP je akýkoľvek bezdrôtový prístupový bod, ktorý bol nainštalovaný na káblovej infraštruktúre siete (obr. 2.3) bez súhlasu správcu alebo vlastníka siete, čím poskytuje neoprávnený bezdrôtový prístup ku káblovej infraštruktúre siete. Zamestnanci tieto AP inštalujú na zlepšenie bezdrôtového pokrytia (neuvedomujú si, že robia niečo nebezpečné) alebo poskytnutie bezdrôtového pripojenia na miestach, kde si myslia, že by malo takéto pripojenie existovať.



Obr. 2.3 Rogue Access Point

2.7 Slovníkové útoky

Slovníkový útok využíva fakt, že väčšina hesiel sú slová, ktoré je možné nájsť v slovníkoch. Útočník používa obrovské slovníky alebo databázy, ktoré obsahujú všetky pravdepodobné heslá. Takýto slovník môže obsahovať tisíce mien, prezývok, miest, ulíc, dátumov, poštových smerových čísel a podobne.

OTÁZKY

1. Vymenujte metódy autentifikácie.
2. Vysvetlite rozdiel medzi Open-system a Shared-key autentizáciou.
3. Čo je SSID?
4. Aký druh útoku nám hrozí vo verejných WiFi sieťach?

ZDROJE

Thomas, T. (2005). *Zabezpečení počítačových sítí bez předchozích znalostí.* Brno: CP Books.

Zandl, P. (2003). *Bezdrátové sítě WiFi.* Brno: Computer Press.