# WEP

První bezpečnostní protokol byl nazván Wired Equivalent Privacy nebo WEP. Tento protokol zůstal bezpečnostním standardem od roku 1999 do roku 2004. Ačkoli tato verze protokolu byla vytvořena pro ochranu, přesto měla poměrně průměrnou úroveň zabezpečení a byla obtížně nastavitelná. V té době byl dovoz kryptografických technologií omezen, což znamenalo, že mnoho výrobců mohlo používat pouze 64bitové šifrování. Jedná se o velmi nízké bitové šifrování ve srovnání s 128bitovými nebo 256bitovými možnostmi, které jsou dnes k dispozici. Nakonec protokol WEP nezačal dále rozvíjet.

# WPA

Pro zlepšení funkcí WEP byl v roce 2003 vytvořen protokol Wi-Fi Protected Access (chráněný přístup Wi-Fi). Tento vylepšený protokol měl stále relativně nízkou bezpečnost, ale bylo snadnější jej nastavit.

Technologie WPA se skládá z následujících komponent:

* Protokol 802.1 x — univerzální protokol pro ověřování, autorizaci a účetnictví.
* Протокол EAP — расширяемый протокол аутентификации (Extensible Authentication Protocol).
* Protokol TKIP protokol dočasné integrity klíčů, jinou možnost překladu — protokol integrity klíčů v čase (Temporal Key Integrity Protocol).
* Mic — kryptografická kontrola integrity paketů (message Integrity Code).

# WPA2

Technologie WPA byla dočasným opatřením před uvedením standardu 802.11 i do provozu. Dalším vývojem tohoto protokolu je WPA2. WPA2 je definován standardem IEEE 802.11 i přijatým v červnu 2004. V něm jsou implementovány CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) a šifrování AES (Advanced Encryption Standard), díky které WPA2 stal bezpečněji než jeho předchůdce. CCMP je šifrovací protokol 802.11 i vytvořený jako náhrada za TKIP, povinný šifrovací protokol WPA a WEP jako spolehlivější možnost. Jako šifrovací algoritmus se tam používá pokročilý šifrovací standard AES. A pro správu a distribuci klíčů se stále používá protokol 802.1x.

# Co je WPA3?

V roce 2018 představila Wi-Fi Alliance WPA3. WPA3 nabízí pokročilé možnosti šifrování vysoce citlivých dat, bezpečnost přenosu zajišťuje za pomoci nejnovějších bezpečnostních metod a zároveň neumožňuje používání zastaralých protokolů. Ke svému fungování naopak vyžaduje používání chráněných rámců správy (Protected Management Frames - PMF). Je dokonce možné je nahrát na starší zařízení, pokud na ně výrobce myslí při sestavování bezpečnostních záplat. Musí jej však podporovat i zařízení účastníka sítě, což by ale neměl být tak zásadní problém. WPA3 bez problémů spolupracuje se zařízeními, kompatibilními s protokolem WPA2. V současné chvíli je zavedení tohoto protokolu u zařízení volitelné, postupem času se stane povinným.

# WPA-PSK vs. WPA-Enterprise

# Slovníky

Zpočátku není známo ani kolik znaků tvoří zvolené heslo oběti. Právě z tohoto důvodu útočníci velmi zřídka používají veřejné slovníky. Zde je již třeba využít dovednosti sociálního inženýrství. Přesněji řečeno, stačí k často používaným možnostem přidat informace o oběti: jméno, příjmení, datum narození atd. to pomůže mnohokrát zvýšit šanci na úspěšný útok. Níže budou uvedeny příkazy pro implementaci této metody.

# Možnosti prolomení

## Brute-force

## Útok pomocí metody KRACK

Útok se nazývá KRACK, což je zkratka pro Key Reinstallation Attacks. Manipuluje s úvodním čtyřcestným handshakem, který je použit pro výměnu šifrovacího klíče používaného během další komunikace. KRACK zneužívá chyby ve třetím kroku, kdy je možné klíč poslat několikrát. Pokud je to uděláno správným způsobem, může být úvodní nonce použit tak, že to kompletně boří bezpečnost šifrování. Vice můžete přečíst [zde](https://www.krackattacks.com/).

## Útok pomocí nastavení stejného SSID na falešném AP

Nejprve hacker skryje signál skutečného přístupového bodu. Pak se vydává za skutečný AP s identickým SSID. Uživatel připojený k falešnému přístupovému bodu nebude mít podezření na nic a útočník bude sledovat veškerý provoz, který prochází touto sítí. Tento druh útoku se nazývá Man-in-the-Middle (Člověk uprostřed).

Například hackeři kolem 11:30 prolomili bezplatné Wi-Fi sítě moskevského metra. Výsledkem je, že tisíce cestujících viděly porno na obrazovkách svých telefonů a tabletů namísto obvyklé úvodní stránky a výzvy k přihlášení do sítě.

## Krádež hesla pomoci sociálního inženýrství

Definovat jednoznačně termín sociálním inženýrství je poměrně složité. Obecně se dá říct, že jde o způsob získávání užitečných informací od různých lidí, kdy tito lidé netuší, že se stávají cílem útoku. Jsou pak ochotni vyzradit například své osobní údaje, přístupová hesla čí jiné informace, které mohou útočníkovi pomoci získat neautorizovaný přístup do zabezpečeného systému, případně využít tyto informace k podvodu či odcizení něčí identity.

Hlavní myšlenka sociálního inženýrství je tedy následující: proč se obtěžovat s používáním technických prostředků a různých nástrojů k prolamování hesel, když je nejjednodušší někoho přimět k tomu, aby toto heslo řekl sám? Ne nadarmo se říká, že nejslabším článkem každého bezpečnostního systému je člověk. A právě sociální inženýrství této skutečnosti využívá, či lépe řečeno zneužívá.

# Certifikát

Certifikát slouží k ověření identity. Dá se používat i pro identifikaci osob, ale my se s ním budeme setkávat zejména jako s prostředkem pro ověření autenticity serveru, ke kterému se připojujeme. V SSL certifikát je vždy podepsán. Buď může být podepsán sám sebou (tzv. Self-signed Certificate), nebo je podepsán jiným certifikátem, tzv. certifikační autoritou (Certificate Authority, CA).   
Filozofie je taková, že do uživatelského SW jsou (pokud možno nějakým bezpečným způsobem) nahrány certifikáty těch autorit, kterým uživatel věří.

# Bezpečnostní zásady

Chcete-li chránit firemní bezdrátovou síť je nutné:

* Skrýt a změnit SSID používanou ve výchozím nastavení na jakoukoli nejasnou hodnotu.
* Omezit sílu signálu bezdrátových zařízení.
* Nepoužívat WEP a nasadit šifrování WPA pomocí 802.1x.
* Zabraňte klientským pracovním stanicím připojit se k dostupným bezdrátovým sítím.
* Změnit standardní heslo na směrovači.
* Nepoužívat veřejné otevřené sítě.

# Závěr

Zabezpečení bezdrátové sítě se v průběhu času měnilo, aby se stalo spolehlivějším, ale současně i více jednoduché z hlediska jeho nastavení. Ale bez ohledu na to, jak zlepšit protokoly nejdůležitější zranitelnost bude vždy zůstat člověkem. Nikdo není imunní vůči hackování phishingem nebo sociálním inženýrstvím, ale pokud budete dodržovat výše uvedené zásady bezpečnosti, pak to pomůže chránit vaši síť před hacking.