COMPUTERWORLD

WLAN sikkerhedsbegreber -- beskrivelse

Indeholder en kort beskrivelse over de forskellige sikkerhedsværltøjer og standarder der findes for WLAN idag!

Skrevet den **03. Feb 2009** af **irma_n1** I kategorien **Netværk / Generelt** | ★★★☆☆

Kryptering

Når man krypterer data koder man meddelelsen så den fremstår som ulæselig. En vigtig forudsætning for kryptering er nøgler. Nøgler er den information computerne bruger til at kryptere og dekryptere meddelelser.

Der findes to typer af krypterings algoritmer, og disse er symmetriske eller asymmetriske.

Symmetrisk kryptering er når både afsender og modtager har en fælles nøgle som de bruger at kryptere og dekryptere data med. Symmetrisk kryptering foregår hurtigt og dens styrke afhænger af nøglens størrelse og ens evne til at holde nøglen hemmeligt. Dens ulempe er at den er delt, hvilket betyder at når nøglen bliver sendt over et åbent netværk kan den stjæles og bruges til at dekryptere data.

Assymetrisk kryptering er lidt mere avanceret. Her indgår der to forskellige nøgler: en offentlig nøgle som er tilgængelig til alle, og en privat nøgle som brugerne holder hemmeligt. Disse to nøgler danner et par, så data der krypteres med den ene nøgle kan kun dekrypteres med den anden nøgle. Dette betyder at for at du kan kryptere en tekst til en anden person, skal du have den persons offentlige nøgle med hvilke du krypterer dataet med. Selvom alle kender den offentlige nøgle kan man ikke bryde krypteringen, da kun den private nøgle kan dekryptere data, hvilket betyder at når udvekslingen af den offentlige nøgle over et åbent net, komprimerer ikke krypteringen ligesom den gør med symmetrisk kryptering.

Både AES og RC4, der er krypterings algoritmer der bruges i 802.11, er symmetriske, mens assymetriske krypteringer bruges i bl.a. digital signatur.

WEP Kryptering

WEP står for Wired Equilvalent Privacy og er den mest basale krypterings algoritme i 802.11 standarderne. Den bruges til at kryptere kommunikationen mellem en acces point og klienten. Når man bruger WEP skal både klienten og acces pointet blive enige om at bruge den samme nøgle, hvilket betyder at dens krypterings algoritme RC4 er symmetrisk. WEP krypterings nøgler kan have en størrelse mellem 40-128bits, mens der er producenter som f.eks. D-Link der tilbyder ekstensions der kan køre helt op til 256bit. Forskellen mellem disse størrelser er længden af krypteringsnøglen. Hvis man f.eks. bruger 64bit nøglen så er krypterings teksten 10 hex decimaler lang, mens den med 128bit har 26 hex tegn. Jo større bit nøglen har jo bedre, men man skal dog også tænke på at den dermed optager mere båndbredde og at det tager klienten eller acces pointet længere tid at dekryptere den.
Der er problemer med WEP, da dens krypterings algoritme, RC4, ikke er så svær og er dermed let at bryde. Samtidig understøtter WEP ikke automatisk udveksling af nøgler mellem en acces point og klienten. Dette betyder at man manuelt skal konfigurere alle klienter med de nødvendige nøgler, og samtidig også selv sørge for at skifte nøglerne. Men WEP er bedre end ingenting. WEP krypterer data framen, så det bliver svært for programmer der analyserer pakker til at læse det egentlige data. Der findes værktøjer og metoder som hackere kan bruge til at decrypte WEP, så folk med de rigtige færdigheder og motivationer kan let bryde WEP. IEEE har dog lavet alternative til WEP der løser dens problemer. Disse er WPA og 802.1x standarden.

Autentikation

Med autentikation identificerer man en bestemt bruger eller en bestemt maskine efter forudbestemte kriterier som f.eks. brugernavn eller mac adresse.

MAC Adresse validering
Næsten alle producenter har dette værktøj installeret i deres acces point. Måden hvorpå dette virker, er at man indtaster alle klienternes MAC adresse i en tabel i acces pointet. Hver gang en klient prøver at associere sig med acces pointet, checker denne klients MAC adresse og sammenligner den med de adresser som findes i tabellen. Ligesom med WEP og SSID, så findes der også værktøjer, med hvilke man kan spoofe MAC adresser, så en hacker skal "bare" sniffe sig til en legitim klients adresse.
Selvom WEP kan blive brudt og MAC lister er usikre, er det bedre at implementere et lille niveau af sikkerhed end ingenting. Fra sikkerhedens synspunkt, er alt der hæver sikkerheden er en fordel, da dette gør det sværere for en hacker at bryde ind.

SSID

SSID står for Server Set Identifier, og er et acces point identifikation, der muliggør at en klient kan kommunikere med en bestemt acces point. Hver acces point kommer med en default SSID, som er kendt til omverden, hvilket gør det let for hackere at trænge ind i de netværk der kører med default konfigurationer. Cisco's default SSID er tsunami, mens 3Com har 101. Samtidig kommer alle acces points med default adgangskode og brugernavn, så som det første er det vigtigt at man husker at ændre SSID, brugernavn og password.
Derudover er det en god ide at slukke for SSID broadcast. Acces pointet sender, hver femte sekund, et beacon frame hvori SSID navnet er vedhæftet. Navnet sendes som almindelig tekst. Ved at man slukker for SSID broadcast resulterer det i at operative systemer, som f.eks. Windows XP, ikke kan opdage SSID og automatisk konfigurere netkortet til at køre på det netværk. Når man slukker for broadcast kan man ikke "se" netværket, men man skal vide at det er der. Dette resulterer i at en hacker skal bruge mere svære midler til at finde ud af hvilket SSID netværket kører med. Disse midler er programmer som f.eks. AirMagnet eller AiroPeek, som er programmer der analyserer data pakker. Dette betyder, at når en legitim bruger prøver at associere sig med acces pointet, sniffer hackeren disse pakker og bruger programmerne til at finde ud af hvilken SSID netværket har, hvorefter han kan konfigurere sit netkort til at køre med denne. Man skal dog bruge masser af data og tid på at sniffe disse, hvilket får de fleste "almindelige" hackere til at gå et andet sted.
De tre værktøjer, MAC, WEP og SSID, identificerer alle maskinen, mens der ingen brugervalidering er, hvilket klart er et ulempe her.

VPN

Inden 802.1x og WPA kom på markedet var der mange virksomheder, som brugte VPN forbindelser for både at kryptere og autentisere brugerne på WLAN. For WEP krypteringen var svag, og der var ingen autentikations metoder, undtagen SSID der var en slags adgangskode til netværket, som man skulle kende til at logge på acces pointet, hvis altså SSID broadcast var slukket.

VPN bliver normalt brugt til at lave en sikker og privat forbindelse over et åbent netværk som Internettet. Når en remote user ønsker at logge på hans lokale netværk, laver man ved hjælp af VPN software og hardware, et slags point-to-point forbindelse mellem brugeren og serveren. På den måde ser det ud som om man sender data på et privat link, selvom det faktisk er over Internettet, hermed navnet Virtual Private Network. Måden hvorpå VPN fungerer, er, at den ved hjælp af f.eks. protokollen IPSec autentisere brugeren inden dataene bliver sendt. Der laves en tunnel som er krypteret, og brugere som ikke bruger den rigtige kryptering og som ikke er autentiseret kan ikke komme ind i tunnelen og læse data. For at kryptere forbindelsen kan VPN bruge AES krypteringsmetoden, som er meget stærkere end wep.

Måden hvorpå VPN kan bruges på et WLAN netværk er, at man f.eks. kobler acces pointet til en VPN gateway. Dette betyder, at man behandler alle trådløse klienter som remote users og at kommunikationen

mellem acces pointet og klienten er krypteret, så fremmede ikke kan lytte til denne.

Men med de nye sikkerheds metoder og værktøjer for trådløse netværk, er VPN ikke så attraktiv, når det skal bruges i forbindelse med WLAN. Ulemperne ved VPN er, at man for det første er nødt til at investere i software og udstyr, så som switche, routere og servere, der understøtter VPN. Desuden er installationen og vedligeholdelse af VPN forbindelser noget der kræver masser af tid. Man skal sørge for at alle klienter bruger den rigtige VPN forbindelse og at alle klienter har VPN software installeret. Samtidig hvis virksomheden f.eks. får besøgende, skal disse også have installeret eller konfigureret VPN, selvom de måske kun skal bruge forbindelsen i kort tid.
Desuden er man, hver gang en klient roamer eller computeren går i standby, nødt til at logge på igen. Alt dette er et unødvendigt pris og overhead for som sagt er der alternativer til VPN, og dette er standarden 802.11i og dens komponenter.

802.11i
Da IEEE indså at wep, med dens kryptering og manglende autentikations funktioner, havde svagheder, begyndte de at udarbejde en sikkerheds standard, der kunne implementeres med 802.11 a/b/g standarderne. Dette resulterede i 802.11i standarden, som blev certificeret i juni 2004, og de første produkter som understøtter denne blev udgivet i september 2004, efter at de blev wi-fi certificeret. Man skal dog bemærke, at 802.11i nu kaldes for WPA2, som implementerer alle de påbudte komponenter fra 802.11i. Jeg vil fra nu af kalde denne standard for WPA2.

Da det tager lang tid at udarbejde og certificere en standard, udgav IEEE i samarbejde med Wi-Fi, dele af WPA2 standarden for at imødekomme brugernes sikkerhedsbehov. Disse er 802.1x og WPA.

WPA

WPA star for Wi-Fi protected access og blev udgivet I 2003, og dens formål er at erstatte WEP I fremtiden, da der findes værktøjer på Internettet der kan bryde WEP.
For at forbedre data krypteringen, bruger WPA Temporal Key Integrity Protocol (TKIP), og samtidig introducerer den 802.1x som bruges til autentikation af klienter.

WEPs svaghed er, at den bruger et statisk RC4 kryptering, hvilket betyder at nøglerne ikke bliver ændret og dermed giver det hackerne mulighed til at sniffe nok data til at bryde krypteringen. WPA løser dette ved at bruge TKIP protokollen, som periodisk ændrer nøglerne, hvilket betyder at hackerne ikke får nok tid til at bryde nøglen, og selvom de bryder den er det for sent da nøglen allerede er blevet ændret.

Med standarden WPA2 (802.11i) har IEEE udgivet en ny version af WPA, som sjovt nok også hedder WPA2! Forskellen mellem WPA og WPA2 er, at version 2 i stedet for RC4 bruger Advanced Encryption Standard (AES) som dens krypterings algoritme.

AES kører med nøgler helt op til 256bit og er samtidig den bedste krypteringsmetode der findes på markedet i dag. For at opgradere ældre WLAN udstyr fra WEP til WPA er det nok med bare en firmware upgrade. Men for at opgradere til WPA2 er det nødvendigt, for de ældre modeller, at installere chips der understøtter AES.

For at udføre autentikation bruger WPA/WPA2 standarden 802.1x.

802.1x

802.1x håndterer autentikation og nøgle styring. Når man implementerer 802.1x skal man også bruge en autentikations server som f.eks. en RADIUS server. Denne slags implementering kaldes for "entreprise WPA mode", hvor RADIUS serveren står for godkendelse af brugerne.

Måden hvorpå 802.1x virker er følgende: En trådløs klient ønsker at associere sig med en acces point. Acces pointet sender derefter et anmodning til RADIUS serveren, ved hjælp af en autentikations protokol

som f.eks. LEAP (Light Extensible Authentication Protocol). Serveren checker login informationerne, og hvis brugeren bliver godkendt, giver serveren en krypterings nøgle til acces pointet. Acces pointet bruger denne nøgle til at kryptere kommunikationen til klienten og transmitterer derefter en nøgle til klienten. Hermed har klienten adgang til netværket og kommunikationen mellem acces point og klienten er krypteret. Derefter kan klienten logge på de nødvendige netværks domæner. Under hele sessionen bliver nye krypterings nøgler genereret af serveren (dynamisk nøgle udveksling) og sendt til klienten.

Som nævnt før bruger 802.1x en autentikationsprotokol når acces pointet og serveren snakker sammen for at validere klienten. 802.1x specificerer ikke hvilken protokol man skal bruge. I stedet for specificerer den at EAP (Extensible Authentication Protocol) skal bruges. EAP er en encapsulation protokol, der tillader at man kan vælge forskellige slags autentikations metoder som f.eks. chips eller certifikater. Protokoller der kan bruges med 802.1x:

- LEAP (Lightweight Authentication Extension Protocol) som er lavet af Cisco og kan kun bruges med Cisco udstyr. Den er svagere end de to andre protokoller. Måden hvorpå den virker er at den forlanger at både klienten og serveren skal autentisere hinanden ved hjælp af adgangskoder. Desuden udleverer den krypterings nøgler. Ulempen er at hackerne stadigvæk har mulighed til at sniffe sig til f.eks. adgangskoder.
- EAP-TLS (EAP-with Transport Layer Security) er den eneste protokol der er standardiseret af IETF. Den kræver at både klienten og serveren skal bevise deres identitet ved hjælp af nøgler som f.eks. certifikater eller smart Card. Denne udveksling er krypteret af en TLS tunnel, hvilket gør protokollen meget modstandsdygtigt mod hacker angreb.
- EAP-TTLS (EAP - with Tunneled TLS) og PEAP (Protected EAP) er udkast til protokoller hvis opgave er at gøre 802.1x anvendelse lettere. Protokollerne gør det lettere for virksomheder der ikke kører med certifikater, at bruge 802.1x. I stedet for at man bruger certifikater til at identificere klienter, kan man bruge windows login og adgangskoder. De servere der understøtter disse to checker så disse hos Windows Domain Controler eller andre brugere databaser som f.eks. Active Directory.

802.1x understøttes af Windows XP, 2000 og 2003. Udover autentikations fordele så er det også en fordel at en RADIUS server kun stoler på en acces point som den er konfigureret til at kende, og hermed forebygges "man in the middle" risikoen, som vil blive beskrevet senere.

Mange mennesker tror at 802.11i/WPA2 standarden er endnu en standard til WLAN som f.eks. 802.11 a/b/g. Men dette er ikke rigtigt. 802.11i er en ekstension til disse tre standarder, hvis henblik er at erstatte den svage WEP og gøre WLANs mere sikre

Udover 802.1x og WPA/WPA2 adresserer standarden ad-hoc kommunikation og gøre den mere sikker. Desuden adresserer den VoIP (voice over IP) så telefoner der bruger disse kan have en hurtigt og sikker roaming.

Kommentar af nogetfx d. 21. Feb 2005 | 1

Glimrende artikel, 5 min på layout ville dog ikke være spildt...

Kommentar af kenp d. 15. Feb 2005 | 2

OK artikel må straks få lavet link til den fra min :)

Kommentar af jpvj d. 17. Feb 2005 | 3

En masse information. Jeg synes ikke at der forklares noget som helst, blot er der en masse opremsninger af forskellige udtryk.

Som begynder læsning er den uforståelig. For folke med kendskab til kryptografi er det blot let læste

oplysninger eller trivialiterer...

Kommentar af xz619 d. 19. Feb 2005 | 4

udemærket artikel, dog er "access" med 2 s'er - og ikke som du skriver det acces ;D.

Kommentar af 123freddy d. 16. Feb 2005 | 5

Kommentar af alister_crowley d. 14. Feb 2005 | 6

Her er ihvertfald masser af tekst, dog ligner det noget rip-off eller en artiklen skrevet til andetsteds i først omgang.
Men jeg forstår stadigvæk intet af det :)