La sicurezza nelle reti Wireless
Tecniche di protezione

Giuseppe Paterno'
IT Consultant
Architetture reti e sicurezza

Chi sono

- Lavoro in Sun Microsystems Italia da 4 anni. Sono un consulente presso la practice Solutions & Architectures di Professional Services nell'ambito delle reti e sicurezza.
- Sono un appassionato di informatica, in particolare sulle reti, sulla sicurezza e Linux (uso dalla versione 0.99p di Kernel). Dedico il mio (poco) tempo libero a sperimentare nuove soluzioni ed a partecipare attivamente alle community (Sikurezza, Italian Linux Society, ecc...)
- Maggiori informazioni sul mio sito personale: http://www.gpaterno.com/

Agenda

- Panoramica sulle tecnologie Wireless
- Le Wireless LAN ed il WEP
- I pericoli delle reti Wireless
- Usare al meglio gli Access Point come protezione di base
- L'auditing come verifica della propria rete

Agenda

- Autenticazione delle Wireless LAN
- Usare IPSec come ulteriore barriera
- Le evoluzioni della sicurezza
- Rilevare gli intrusi
- Quali tecniche da utilizzare in quali ambienti
- E se entrano? Gestire un incidente.

Panoramica sul Wireless

Le tecnologie “wireless”

- GSM
  - GPRS
  - EDGE
- UMTS
- IRDA
- BlueTooth
- DVB (Digital Video Broadcasting)
- Wireless LAN

GSM

- GSM: Global System for Mobile Communications
  - Allocazione di frequenza (900Mhz, 1800Mhz, 1900Mhz US)
  - Trasmissione della voce
  - SMS nato come messaggi di controllo, ma utilizzato dai clienti per messaggi (successo inatteso)
  - Dati basati su CSD fini a 9600b/s nello spettro 900Mhz, 14400b/s nella frequenza 1800Mhz

GSM (GPRS ed EDGE)

- GRPS
  - Offre servizi estesi sull'esistente GSM/TDMA
  - Tecnologia Packet switching basata su protocollo X.25
  - Velocità massima teorica di trasmissione di 171.2kb/s, velocità effettiva simile a modem (56kb/s)
- EDGE
  - Sull'esistente GSM
  - Massima velocità di trasmissione sino a 384 Kbps

UMTS

- UMTS: Universal Mobile Telecommunications System (o 3rd Generation GSM)
  - Universalmente disponibile, sia per sistemi mobili che terrestri (conosciuto principalmente per mobili)
  - Identica esperienza per l'utente (es. Numero telefonico, indirizzario ecc.)
  - Differenti tecnologie d'accesso: CDMA (Code Division Multiple Access) vs. TDMA (Time Division Multiple Access)
  - Più larghezza di banda (bandwidth): UMTS usa Wideband-CDMA (W-CDMA) air interface, es. 5MHz vs 1,25MHz di GSM

UMTS

- data rates:
    - 144 kbps per mobile rural outdoor
    - 384 kbps per mobile urban outdoor
    - Fino a 2 Mbps per mobile indoor e short range outdoor
    - Fino a 5 Gb/s (per il landline UMTS)
- Basato su ATM e IP

Bluetooth

- Consente la realizzazione di wireless personal area network (WPAN)
- Connette device in prossimità o a corto raggio radio device (10 Metri)
- Evoluzione dell' IRDA
- Frequenze da 2.45 GHz ISM 'free band'
- Fornisce interconnessione voce e dati a basso costo, bassa potenza, robusto, sicuro, efficiente e ad alta capacità con trasmissione fino a 1 Mb/sec

Digital Video Broadcasting (DVB)

- Usato comunemente per le trasmissioni televisive satellitari (DVB-S)
- Da poco sono iniziate le trasmissioni digitali terrestri (DVB-T)
- Il DVB e' un livello di trasporto, analogamente alla tecnologia IP
- L'interattivita' viene gestita con MHP (Java)
  - Esistono Set-Top Box con canali di ritorno Modem o Ethernet con IP

Le Wireless LAN ed il WEP

Wireless LAN (o Wi-Fi)

- Standard IEEE 802.11 [a|b|g]
- Vista logicamente come ethernet tradizionale
- Diffusione in vertiginoso aumento negli ultimi mesi:
  - Necessita' di mobilita' in aumento
  - Copertura in ambienti aperti
  - Difficolta' di cablaggio (palazzi antichi,ospedali, ...)
  - Facilita' di installazione
  - Costi ridotti

Wireless LAN

- Livello fisico
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
- Banda di frequenza
  - 2.4GHz e 5GHz
- Velocità di trasmissione
  - Fino a 11 Mb/s (802.11b)
  - Fino a 54 Mb/s (802.11a e 802.11g)
- Basato su CSMA/CA (Carrier-Sense, Multiple Access, Collision Avoidance)

Struttura delle Wireless LAN

- IEEE 802.11 permette due tipi di reti
- Rete strutturata
  - Suddivisa in celle o BSS (Basic Service Set) ognuna controllata da un Access Point (AP)
  - L'identificativo di un BSS e' il Service Set Identifier (SSID)
  - Piu' celle vengono chiamate ESS (Extended Service Set)
- Rete Ad-Hoc
  - Composta da solo computer, senza AP

WEP

- Wired Equivalent Privacy (WEP) e' il meccanismo di protezione di IEEE 802.11
- E' una chiave condivisa (shared key) conosciuta dal client e dall'Access Point
  - La chiave WEP e' di 40 o 104 bit
  - Viene concatenato con un vettore IV di 24 bit
- Il meccanismo di crittografia si basa su RC4
- Gli studi di Stubblefield, Ioannidis e Rubin hanno dimostrato la debolezza di WEP
  - Analizzando sufficiente traffico e' possibile ricavare la chiave

WEP e i rischi di sicurezza

- WEP da una falsa sensazione di sicurezza
- I rischi esistono anche nelle reti tradizionali “wired”
  - Le problematiche di insicurezza delle reti vengono esasperate in un ambiente di tipo wireless
- La trasmissione attraverso onde radio non è confinabile ad uno spazio ben definito
  - Come per l'ascolto di una radio, è possibile per un potenziale intruso avvicinarsi all'esterno del palazzo e “captare” le onde radio.

Attacchi alle Wireless LAN

Si possono raggruppare in tre famiglie:

- Attacchi agli apparati radio
- Attacchi alla rete interna/aziendale
- Attacchi ai client Wireless

Attacchi agli apparati radio

- E' possibile ricavare il contenuto dei dati trasmessi (username e password)
- Modifica dei dati in transito
- Denial of Service tramite disturbo radio (Radio Jamming)
- Dirottamento dei client su un finto AP (Man in the middle)

Attacchi alla rete interna

- IEEE 802.1 autonomamente non prevede autenticazione dei client
- Un qualsiasi aggressore, una volta ricavata la chiave WEP, puo' accedere alla rete senza autenticarsi
- Nessun controllo di accesso (chi accede a cosa)

Attacchi ai client Wireless

- I client wireless vengono spesso visti come risorse internet (trusted) invece di risorse esterne (untrusted)
- Gli agressori possono compromettere i client per:
  - Ottenere preziose informazioni
  - Usare il client come “ponte” per accedere alla intranet

Usare al meglio gli Access Point come protezione di base

Il perche' della sicurezza

Perche' mi devo proteggere ? Non ho nessun dato da rubare o nessun segreto. A cosa mi serve la sicurezza ?

E' fondamentale capire che non e' importante proteggerci solo quando i dati o i sistemi sono critici per il nostro business.

Molto spesso ignoriamo che se i nostri sistemi sono stati usati come “ponte” per attaccare qualche altra azienda, la responsabilità legale è solo ed esclusivamente nostra, finche' non dimostriamo il contrario attraverso i log.

Configurazioni di default

La configurazione standard e' uno dei maggiori fattori di rischio per la sicurezza in genere, ancor di piu' in ambiente Wireless.

Questa regola vale anche per i sistemi operativi e gli apparati di rete. Usare le configurazioni e le password di default e' la causa primaria di intrusioni.

Configurarazioni di default

La corretta configurazione di un Access Point e' il primo ed essenziale passo per rendere sicura la nostra rete

Effettuare una corretta configurazione significa anche evitare di essere vittima di wardriver casuali. In alcune piccole aziende e SOHO queste regole sono sufficienti ad avere una adeguata protezione.

Hardening di AP

- Cambiare gli SSID di default
  - L'SSID identifica una rete wireless. Lasciare un SSID di default significa dire all'intruso aver lasciato la configurazione di fabbrica
- Utilizzare SSID non descrittivi
  - Evitare di comunicare ad un intruso preziosi dettagli con un nome troppo descrittivo (es: nome societa' o il luogo). Si consiglia di usare nomi anonimi (es: XM3MI1)

Hardening di AP

- Disabilitare il Broadcast SSID
  - Gli apparati inviano frames contenenti l'SSID della rete wireless per configurare automaticamente il client, ma servono anche agli aggressori per individuarvi. Alcuni apparati (quelli a basso costo) possono non supportare questa opzione
- Cambiare le password
  - E' bene cambiare tutte le password di default degli AP, scegliendone una alfanumerica di almeno 8 caratteri

Hardening di AP

- Aggiornare il firmware
  - Durante una scelta di un AP e' preferibile orientarsi verso un apparato che supporti l'aggiornamento del firmware.
  - Assicurarsi sempre di avere un firmware aggiornato per evitare probabili buchi di sicurezza
- Chiavi WEP
  - Anche se WEP non e' adeguato, rappresenta comunque un ostacolo: ci vogliono dai 100 Mb ad 1 Gb di dati catturati e 5/6 ore per trovare la chiave. L'aggressore deve essere ben motivato
  - E' bene cambiare spesso le chiavi WEP

Hardening di AP

- Abilitare il MAC Filtering
  - Molti AP hanno la possibilita' di inserire i MAC address delle schede Wireless abilitate ad usare la rete wireless.
  - ATTENZIONE! Il MAC address di una scheda puo' essere cambiato facilmente, pertanto non bisogna usarlo come unico metodo di protezione.
- Spegnere l'AP quando non serve
  - Molti intrusi agiscono di notte o nel fine settimana. Quando possibile spegnere gli AP durante gli orari di non utilizzo, ad esempio collegandoli ad un timer.

Hardening di AP

- Minimizzare l'intensita' del segnale
  - Gli intrusi sfruttano la propagazione delle onde radio per collegarsi fuori dal perimetro aziendale (da qui “parking lot attack”)
  - Scegliere un luogo all'interno dell'edificio e limitare la propagazione radio alla sola area che deve essere coperta (usare strumenti di misurazione)
- Cambiare le community SNMP di default
  - Su molti AP esiste un agente SNMP. Se la community e relativa password non e' configurata correttamente, un intruso puo' leggere e scrivere la configurazione dell'AP

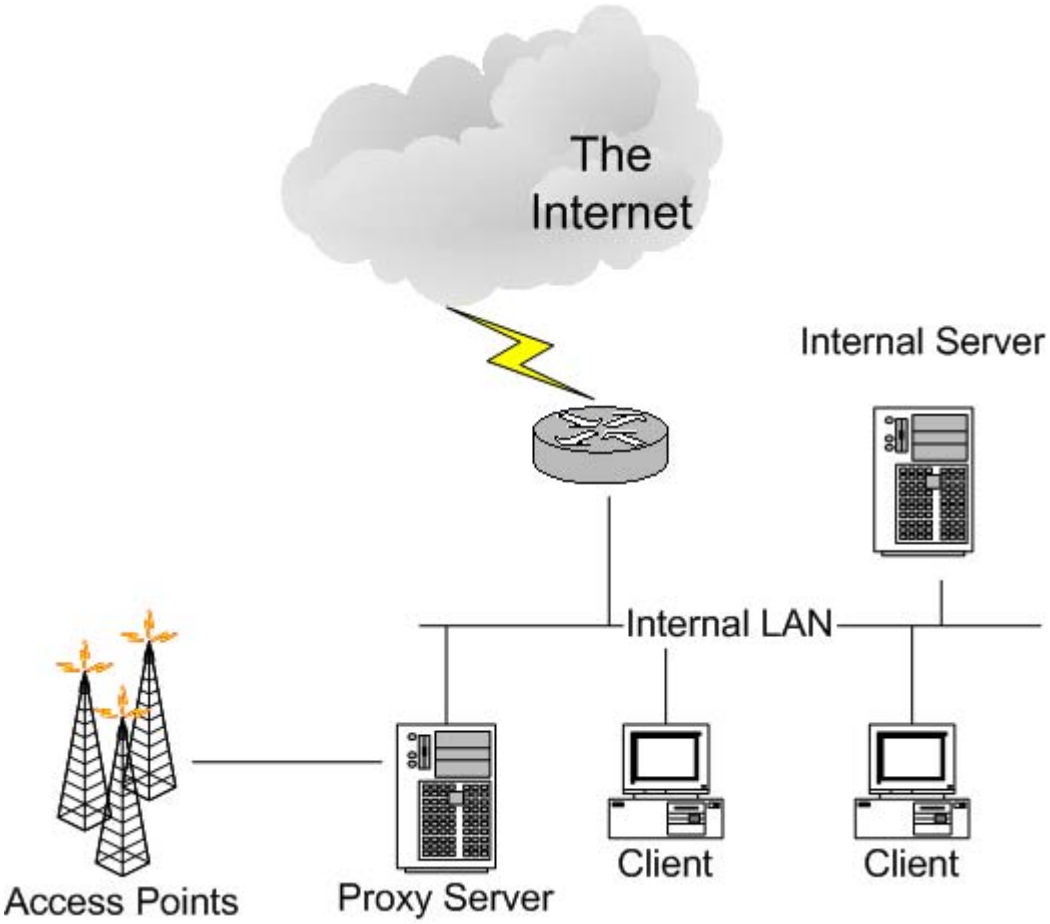
Hardening di AP

- Limitare il traffico di broadcast
  - Alcuni protocolli (es: NetBIOS over TCP/IP) usano i broadcast.
  - I broadcast incrementano velocemente il vettore IV di WEP, pertanto rendendo piu' agevole la decriptazione di WEP.
  - Disabilitare il NetBIOS over TCP/IP quando possibile
- Protezione del client
  - Il client puo' essere usato come ponte per raggiungere la rete interna. Installare sempre un personal firewall per ridurre i rischi di attacco

Hardening di AP

- Non usare il DHCP
  - E' consigliabile usare indirizzamenti statici quando possibile. Questo consente di non rilasciare IP address e informazioni preziose (DNS, WINS, ecc..) a chi riesca ad associarsi ad un eventuale AP
  - Non usare indirizzamenti IP facili da intuire come 192.168.0.0 o 192.168.1.0
- Uso di una LAN/VLAN separata
  - In ambienti piu' complessi del SOHO, e' consigliabile separare il traffico Wireless dalla rete interna
  - Usare un proxy, un router con le ACL o un firewall per unire i due ambienti

Inserimento di Proxy/Router



L'auditing come verifica della propria rete

Auditing

- Meccanismo per controllare lo stato e la sicurezza della nostra rete wireless
- E' un'attivita' che si ripete ciclicamente:
  - Non va fatta solamente all'inizio
  - Serve per verificare la corretta configurazione dei nostri AP e della loro propagazione radio
  - Serve per controllare eventuali AP collegati senza autorizzazione: cosa succede se un utente inserisce “temporaneamente” un AP alla rete interna con i parametri di default ?

Cosa serve ?

- Computer portatili e/o palmari
- Schede wireless potenti (200mw)
- Schede wireless con antenna diversity (due ingressi)
- Antenne direttive e antenne omnidirezionali
- Un software di auditing per le reti wireless, es:
  - Kismet per Linux
  - NetStumbler per Windows
  - MiniStumbler per PocketPC
- Sono le tecniche usate dai wardrivers e dai warwalkers

Cosa fanno i software ?

- Esaminano pacchetti di sincronizzazione (beacon packets) per trovare tutti i punti di accesso.
- Determinano l'SSID e il nome degli AP.
- Esaminano i pacchetti sonda (probe packets) e le risposte a questi.
- Esaminano i pacchetti dei dati.
- Determinano la presenza di meccanismi di cifratura.
- Esaminano i pacchetti di autenticazione ed il relativo metodo.

Cosa fanno i software ?

- Esaminano il numero di client nella rete.
- Determinano la versione di firmware presente sui singoli punti di accesso.
- Determinano la quantità dei dati trasmessi per eventuali attacchi al WEP
- Alcuni di essi ricavano le informazioni relative ai sistemi Cisco attraverso il Cisco Discovery Protocol (CDP)

Autenticazione delle Wireless LAN

Autenticazione degli utenti

- IEEE 802.11 da solo non e' in grado di identificare univocamente un singolo utente
- E' impossibile pertanto applicare specifici permessi ad un determinato utente
- Ci sono due possibilita'
  - PPPoE
  - IEEE 802.1x

PPPoE

- Point-to-Point over Ethernet (PPPoE) e' nato per le tecnologie broadband quali ADSL e Cable modems
- Ideale per gli Internet Service Provider per i propri HotSpot pubblici
  - Permette di integrarsi con le infrastrutture dial-up esistenti
  - Permette servizi personalizzati, quali la portabilita di un IP address per utente
  - Permette di integrare l'offerta wireless in una offerta complessiva wholesale di rivendita della propria rete attraverso le VPDN (cosi' come avviene con i modem e ADSL). Ad esempio, riaffittando la rete ad ISP piu' piccoli o ad aziende private.

PPPoE

- Risolve i problemi di autenticazione per gli AP che non supportano IEEE 802.1x (es: utenza SOHO)
- E' sufficiente disporre di un router Cisco o di un computer con due interfaccie di rete piu' il software
  - RASPPPoE di Robert Schlabbach per Windows (http://www.raspppoe.com/)
  - Roaring Penguin per Linux (http://www.roaringpenguin.com/products/rp-pppoe/index.php)

IEEE 802.1x

- E' lo standard di autenticazione sulle reti ethernet Wired e Wireless
- Permette di:
  - autorizzare un utente all'accesso alla rete
  - Raggruppare classi di utenti in specifiche VLAN (es: consulenti, gruppo IT, ecc..)
- Basato su Extensive Authentication Protocol Over Lan (EAPOL)
  - Permette differenti tipologie di autenticazione

IEEE 802.1x

- Non definisce un sistema di crittografia
  - Si limita ad utenticare l'utente
  - E' pero' in grado di integrarsi con WEP, distribuendone le chiavi
- Alcuni AP non lo supportano
  - Soprattutto quelli a basso costo
  - PPPoE e IPSec (vedremo in seguito) possono sopperire a questa mancanza

IEEE 802.1x

- E' necessario disporre dell'infrastruttura RADIUS
- E' necessario acquistare il software client per i sistemi
  - Solo Windows XP e 2000 hanno il software compreso, ma limitato a TLS e PEAP (proprietario)
  - Il costo della distribuzione potrebbe non e' un problema per un'azienda con un numero limitato di client, potrebbe esserlo per un ISP o un operatore mobile che decidesse di offrire accesso

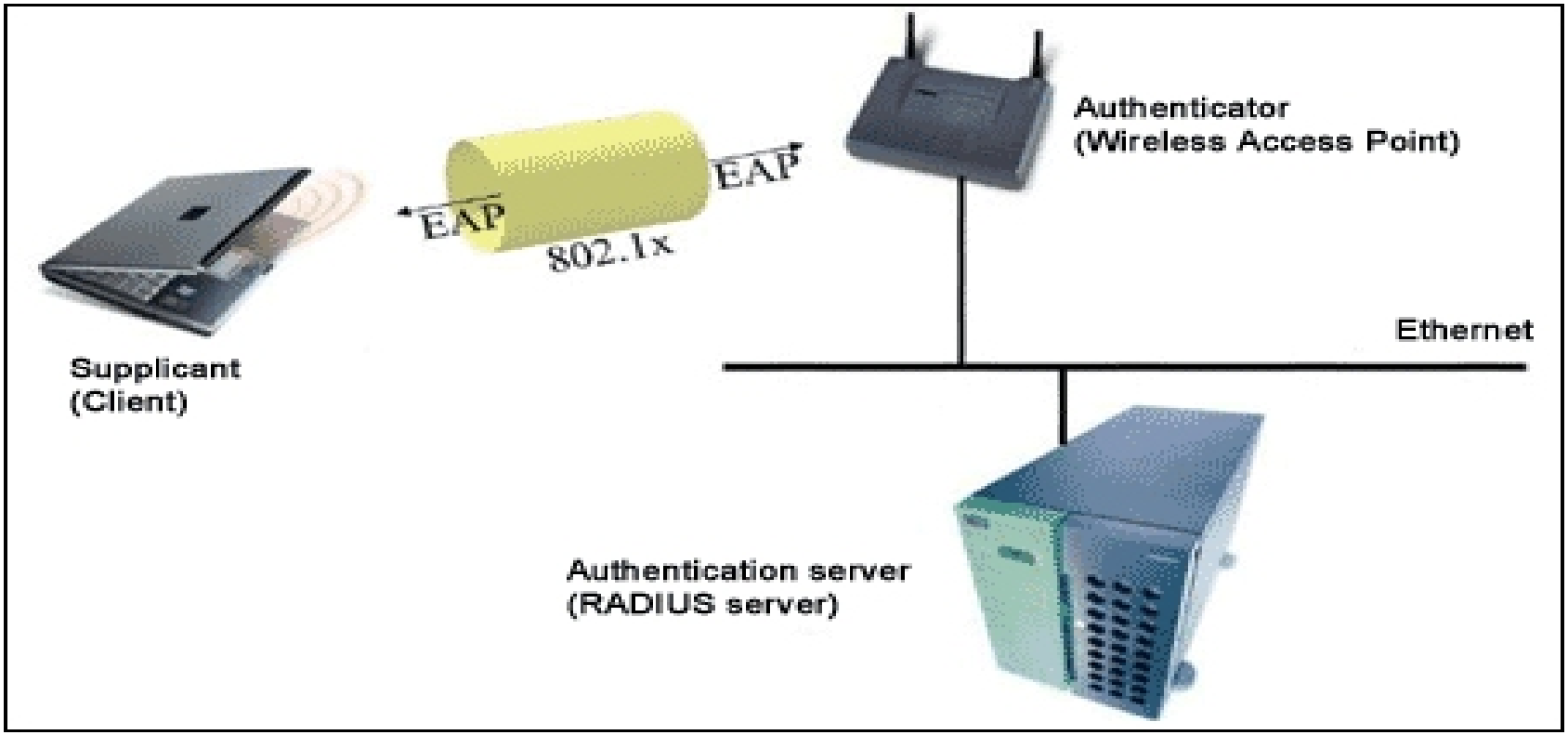
IEEE 802.1x ed EAP

- 802.1x e' un “Port-based access control mechanism”
- Il protocollo Extensible Autentication Potocol (EAP), inizialmente pensato per il PPP, viene incapsulato su Ethernet
  - EAPOL (EAP over LAN) usato per l’autenticazione
  - EAPOW (EAP over WirelessLAN) usato per il delivery della chiave WEP e per l’inizio della sessione
  - EAPOL ha un ethertype dedicato 0x888e

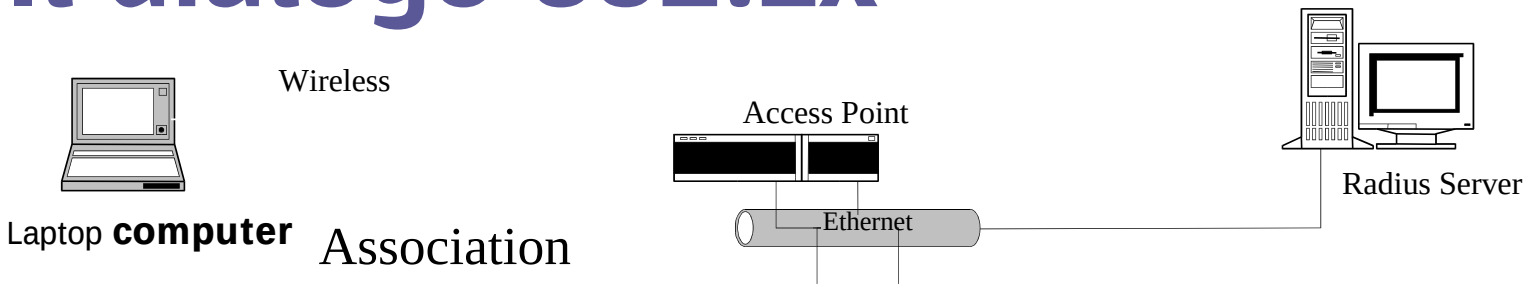
Architettura di IEEE 802.1x

- L'architettura dell'autenticazione coinvolge tre elementi:
  - Il Supplicant (client)
  - Authenticator (l'Access Point)
  - Authentication server (RADIUS)

Architettura di 802.1x



Il dialogo 802.1x



802.11 Associate-Request

802.11

802.11 Associate-Response

RADIUS

EAPOW-Start

EAPOW

EAP-Request/Identity

EAP-Response/Identity

Radius-Access-Request

EAP-Request

Radius-Access-Challenge

EAP-Response (credentials)

Radius-Access-Request

EAP-Success

Radius-Access-Accept

EAPOW-Key (WEP)

EAP e l'autenticazione

- EAP e' un framework di autenticazione (RFC 2284)
  - Definisce solamente un “imbustamento”, al cui interno viaggiano gli schemi di autenticazione
  - Gli schemi di autenticazione, detti METODI, sono molteplici e alcune volte PROPRIETARI
  - Si differenziano in due gruppi fondamentali: tunneled e non-tunneled

Protocolli non-tuneled

- Protocolli semplici definiti all'interno della “busta” EAP
- Differenti metodi di autenticazione, i piu' diffusi:
  - EAP-MD5
  - EAP-LEAP
  - EAP-TLS
  - EAP-SIM
  - EAP-AKA

EAP-MD5

- Mandatory nelle implementazioni EAP
- Viene calcolato un hash MD5 della password e inviata in chiaro
- Non supporta la distribuzione dinamica delle chiavi WEP
- Non e' consigliabile utilizzarlo, perche' e' possibile derivare la password da un hash MD5 con tools come mdcrack

EAP-LEAP

- Light EAP (LEAP) e' un protocollo proprietario Cisco
- Nel mondo Wireless, copre il 46% delle autenticazioni
- E' possibile derivare la password tramite attacchi di forza bruta

EAP-TLS

- Transport Layer Security (TLS) e' definito nel RFC 2716
- Usa certificati digitali X.509 per l'autenticazione utente
- Permette la “mutual authentication”, ovvero vengono verificati sia il certificato client che quello server (evita gli attacchi man-in-the middle)
- Permette la derivazione della chiave WEP e la sua distribuzione
- E' pero' oneroso da mantenere in quanto presuppone la distribuzione dei certificati digitali ai client

EAP-SIM / EAP-AKA

- Destinato al mercato dei “mobile operators”
- Concettualmente simile a EAP-TLS
- Usa come chiave la SIM (GSM) o la USIM (UMTS)
- Entrato a far parte dello standard di 3G
- Supporta il fast reconnect

Protocolli tunneled

- Si basa sul concetto del “doppio imbustamento”
  - All'interno di un metodo EAP viene incapsulato un altro metodo EAP
- Il primo metodo (la busta esterna) viene usato per:
  - creare un canale sicuro su cui trasmettere username e password
  - per generare la chiave WEP
- Il secondo metodo (la busta interna) permette di autenticare effettivamente l'utente
- I piu' famosi sono TTLS e PEAP

EAP-TTLS

- Il Tunneled Transport Layer Security (TTLS) e' il piu' “standard” tra i due protocolli tunneled
- Protocollo a due fasi
  - Nella prima vengono verificate le credenziali del server tramite il suo certificato, quindi creato un canale “sicuro”
  - Nella seconda il client viene riconosciuto attraverso un altro metodo di autenticazione EAP, es: EAP-MD5, EAP-PAP, ecc...
- Permette la derivazione e la distribuzione della chiave WEP

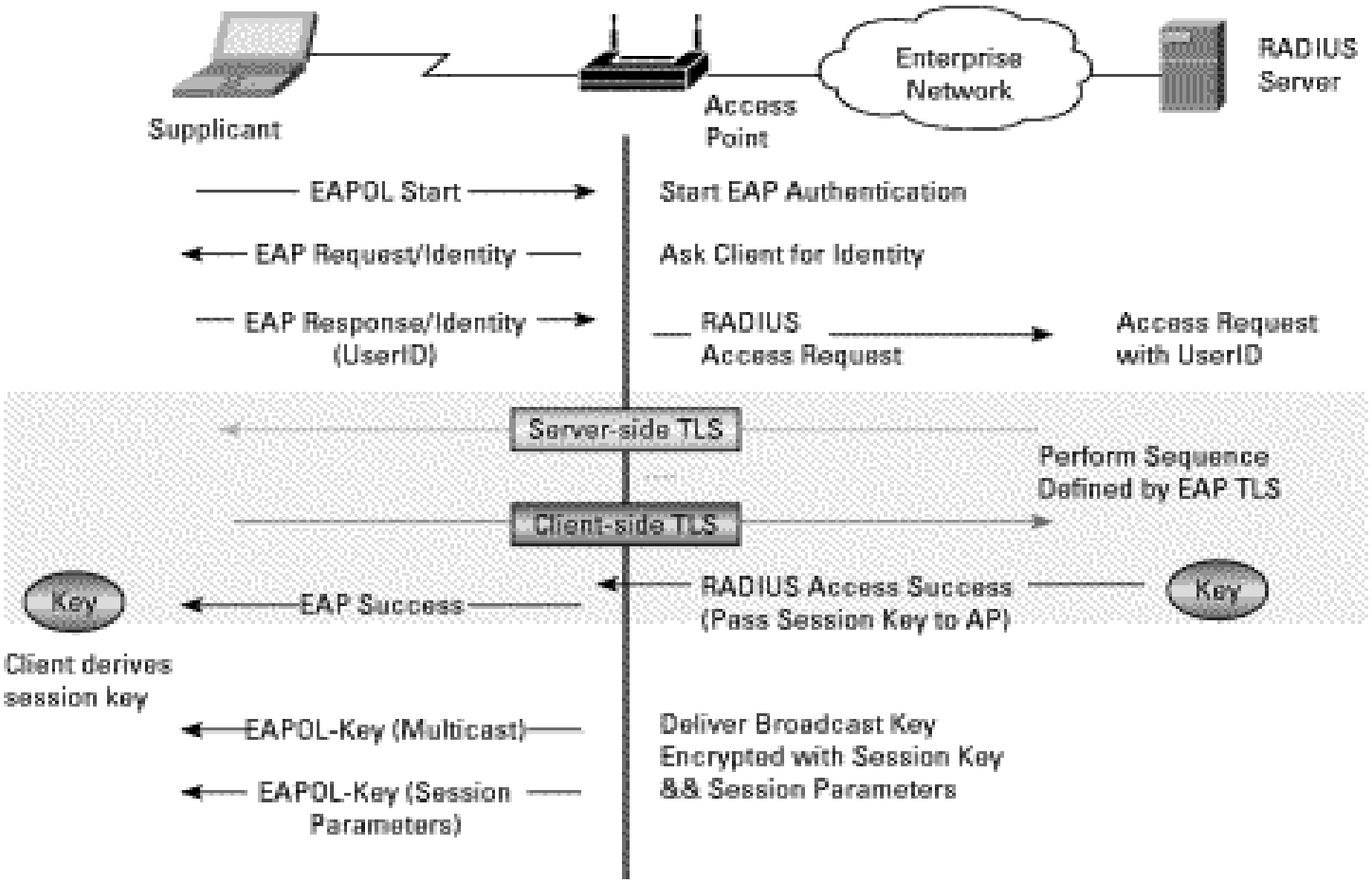
EAP-PEAP

- Protected EAP (PEAP) e' un protocollo piu' “proprietario”
- E' stato comunque pubblicato come Internet Draft da Cisco, Microsoft e RSA
- Molto simile concettualmente a TTLS
- Al contrario di TTLS, PEAP non supporta i metodi “legacy” quali EAP-PAP, EAP-CHAP, EAP-MD5, ecc...
- Di fatto, l'unico protocollo “incapsulato” e' EAP-MSCHAPv2

EAP e WEP

- EAP nelle reti Wireless e' in grado di derivare la chiave WEP, se il protocollo interno lo supporta (es: EAP-TLS e EAP-TTLS)
- Viene distribuito attraverso la frame EAPOL-Key
- Il vantaggio e' che ogni client ha una chiave WEP diversa e per un periodo limitato di tempo (configurabile sull'AP)
- Attenua notevolmente le problematiche relative alla sicurezza di WEP
- Come funziona ?

EAP e WEP


Supplicant
Access Point
Enterprise Network
RADIUS Server
EAPOL Start
Start EAP Authentication
EAP Request/Identity
Ask Client for Identity
EAP Response/Identity (UserID)
RADIUS Access Request
Access Request with UserID
Server-side TLS
Perform Sequence Defined by EAP TLS
Client-side TLS
Key
EAP Success
RADIUS Access Success (Pass Session Key to AP)
Key
Client derives session key
EAPOL-Key (Multicast)
Deliver Broadcast Key Encrypted with Session Key && Session Parameters
EAPOL-Key (Session Parameters)

Autenticazione wireless

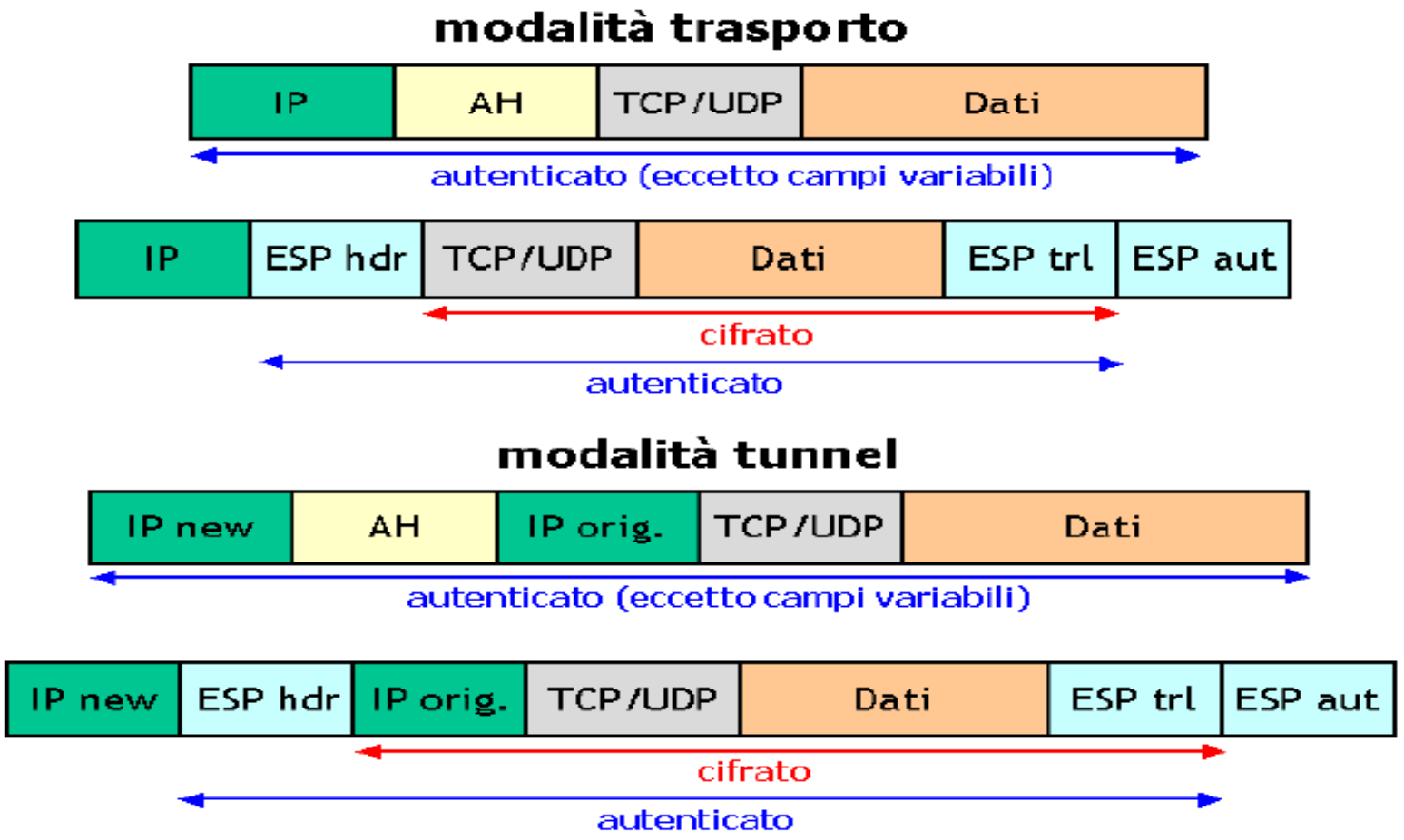
- Abilitate sempre l'autenticazione dei client quando possibile.
- Qualora in azienda:
  - I vostri Access Points supportino IEEE 802.1x
  - Abbiate un radius disponibile o facilmente installabile/integrabile in azienda (es: dominio Windows 2000 o accesso remoto)
- Se siete un ISP o WISP
  - Valutate l'impatto di IEEE 802.1x
  - Alternativamente il PPPoE

Usare IPSec come ulteriore barriera

Cos'e' IPSec

- L'IP Security Protocol (IPSec) e' la tecnologia piu' diffusa per il dialogo sicuro tra computers
- Fornisce al TCP/IP funzionalita' di autenticazione, integrita' e confidenzialita'
- Largamente diffuso come protocollo per le VPN
- Puo' essere usato in due modi
  - Tunnel mode: incapsula un datagramma IP al suo interno (es: IP privati all'interno degli IP pubblici), utilizzo per le VPN
  - Transport mode: rende sicura la comunicazione tra due computer, es: tra un application server e un db server

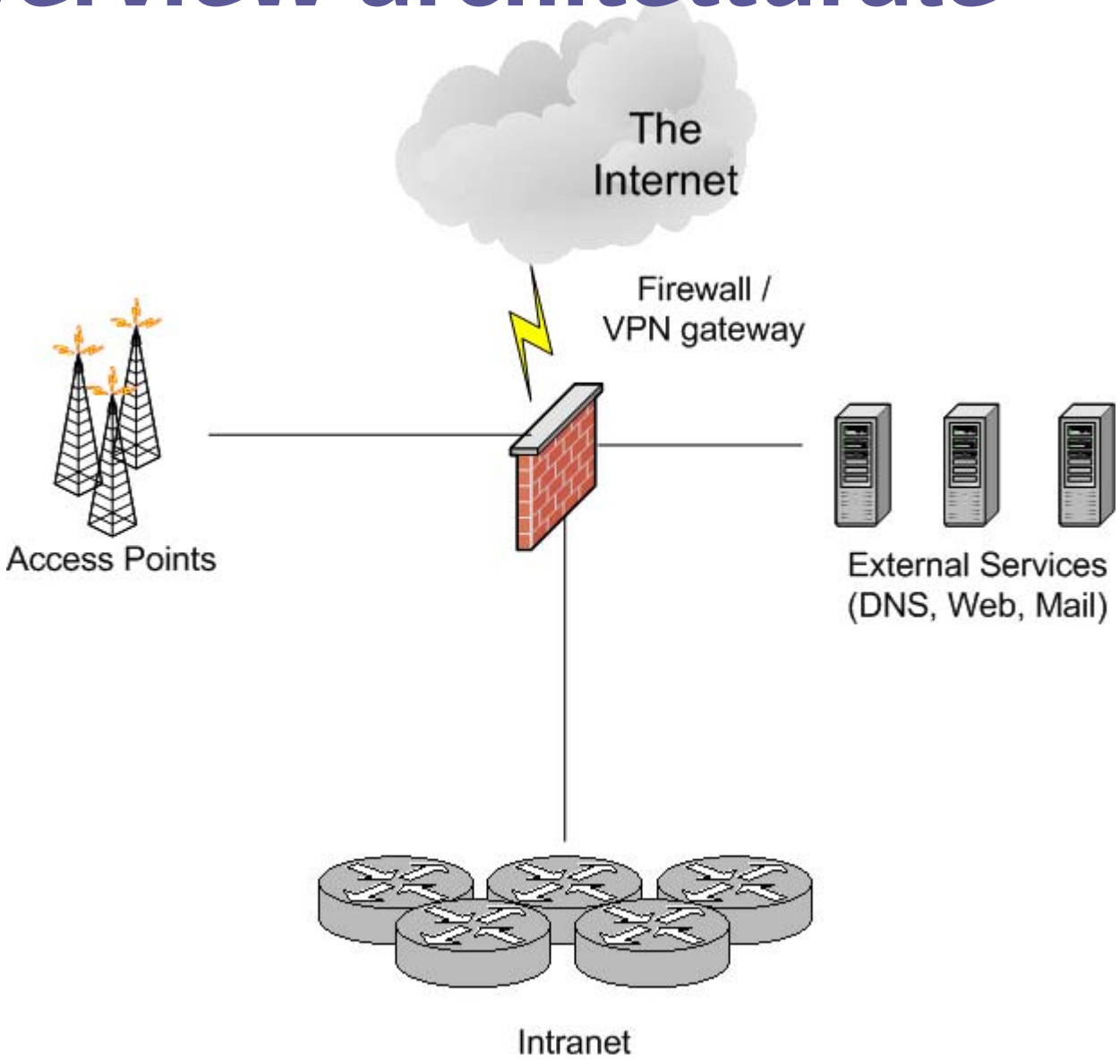
Transport vs. Tunnel mode



IPSec e il wireless

- A cosa mi serve IPSec in ambiente Wireless ??
  - Quando gli Access Point non hanno la funzionalita' IEEE 802.1x (tunnel mode)
  - Quando l'ambiente e' estremamente critico da un punto di vista del business e si necessita una confidenzialita' maggiore (transport/tunnel mode)
- Si integra perfettamente in un ambiente complesso dove esiste gia' un Firewall con divese DMZ
- Solitamente gli Access Points vengono attestati in una DMZ separata, alla stessa stregua di un Remote Access Server

Overview architetturale



IPSec e il riuso dei tools

- Molti sistemi operativi e firewall includono IPSec
- Perche' non usare i tool che abbiamo a disposizione per difenderci meglio ?
- Ricordarsi di proteggere i client oltre che la propria infrastruttura:
  - Equipaggiate i client con un personal firewall ed un antivirus
  - Aggiornate il sistema con le ultime patch

Le evoluzioni della sicurezza

WPA

- Il Wireless Protected Access (WPA) e' nato per colmare le lacune di WEP
- Creato per essere compatibile con l'hardware in commercio (802.11b e 802.1g) e solitamente fornito come “firmware upgrade”
- WPA prevede l'autenticazione del client
  - Tramite Pre-Shared Key (PSK) per utenti SOHO
  - Tramite IEEE 802.1x per ambienti corporate

WPA

- WPA e' un framework che si appoggia su WEP, TKIP e AES (mandatory solo su 802.11i/WPA2)
- WEP supportato, ma di default usa Temporary Key Integrity Protocol (TKIP)

WPA in dettaglio

Le caratteristiche di WPA si possono riassumere in cinque categorie:

- Network Capability Determination
- Authentication
- Key Management
- Data Privacy
- Data Integrity

Network Capability Determination

- Agisce a livello 802.11
- Comunica informazioni su WPA nei Beacon Packets, Probe Response e (Re) Association Requests.
- Le informazioni includono il metodo di autenticazione (IEEE 802.1x o Pre-Shared Key) e il tipo di cifratura (WEP, TKIP o AES).

Authentication

- Due tipologie di autenticazione:
  - 802.1x/EAP
  - Pre-Shared Key (PSK), nel caso non si disponga di un RADIUS server (tipico ambiente SOHO).
- La prima metodologia é quella preferita da WPA in quanto é in grado di distribuire chiavi differenti per sessione attraverso i messaggi EAPOL-Key.

Key Management

- WPA ha un robusto sistema di generazione/manutenzione di chiavi che integra funzioni di autenticazione e privacy.
- Le chiavi sono generate dopo che il client si é autenticato alla rete e dopo un *4-way handshake* tra il client e l'Access Point.

Data Privacy/Data Integrity

- Data privacy come crittografia
- WPA usa il Temporary Key Integrity Protocol (TKIP) per incapsulare WEP.
- Attraverso sofisticate tecniche di crittografia é possibile evitare i problemi di WEP.
- TKIP include un Message Integrity Code (MIC) alla fine di ogni messaggio non criptato per evitare che i pacchetti vengano modificati da un potenziale aggressore.

TKIP

- Usa 124-bit contrariamente a 104-bit di WEP
- Le chiavi vengono generate dinamicamente e distribuite tramite EAPOL-Key
- Include un Message Integrity Check (MIC) permette di evitare l'alterazione dei pacchetti
  - Il MIC viene calcolato autonomamente dal client e dal server.
  - Il pacchetto viene scartato se il MIC non coincide

WEP vs. WPA

Protocollo	WEP	WPA
Crittografia	• Crittografia debole • Chiave a 40-bit o 104-bit • Chiavi statiche: tutti i client sulla rete hanno la stessa chiave • Distribuzione manuale della chiave	• Rimuove i problemi di WEP • Chiave a 128-bit • Chiavi dinamiche: ogni utente, ogni sessione e ogni pacchetto ha chiave differfente • Distribuzione automatica delle chiavi
Autenticazione	Debole: la chiave WEP viene usata come autenticazione	Attraverso IEEE 802.1x e EAP

WPA2

- Standard del Wi-Fi alliance
- WPA 2 e' conosciuto come IEEE 802.11i
- E' una evoluzione di WPA, con l'inclusione di Advanced Encryption Standard (AES)
- AES sara' il default, ma TKIP rimarra' per compatibilita' verso i vecchi apparati
- Sara' necessario un hardware differente per supportare AES

Rilevare gli intrusi

Fidarsi e' bene, non fidarsi...

- L'attacco alle reti Wireless e' ben piu' grave di un attacco Internet
- Solitamente la rete Wireless viene vista come “trusted” rispetto ad Internet
  - In questo modo attaccarla e' piu' semplice perche' si riesce ad eludere alcuni livelli di firewall comodamente seduti in macchina parcheggiati fuori dall'edificio
  - E' bene non fidarsi mai, vedendola come se fosse una rete DMZ

Quando e come rilevarli ?

- Rilevare gli intrusi Wireless e' quindi equivalente a rilevare intrusi Internet
  - E' necessario dotarsi di IDS da inserire nella DMZ o VLAN su cui vengono attestati gli Access Points
- Rilevare gli intrusi (Internet o Wireless) attraverso un IDS significa avere una struttura 24hx24h
  - E' inutile inserire un IDS se non abbiamo qualcuno che in tempo reale monitorizza la situazione, soprattutto in ambito Wireless.
  - E' necessario pertanto prenderli “sul fatto”, perche' altrimenti non possiamo bloccarli: sapere a posteriori cosa e' successo non serve!

Quando e come rilevarli ?

- Si integra perfettamente se abbiamo altre sonde IDS sparse sulla nostra rete
- Un IDS in ambito Wireless e' fondamentale quando la nostra sede e' ben conosciuta ed il target e' molto appetibile

HoneyNet

- Una HoneyNet è una rete che funge da esca a potenziali aggressori.
  - È una rete fittizia, deliberatamente aperta, che contiene pochi sistemi e il cui solo scopo è disorientare l'intruso e far perdere all’attaccante tempo prezioso.
  - Tanto più è credibile la HoneyNet, tanto l'intruso non si accorgerà che si tratta di una rete fittizia e che è sotto osservazione.
- Una volta che l'intruso è intrappolato nella HoneyNet, è possibile studiarne il comportamento e le tipologie di attacco che è solito utilizzare. Inoltre è possibile identificarlo ed eventualmente coinvolgere le autorità competenti durante l'attacco.

HoneyNet

L'uso di HoneyNet è utile quando la wireless è installata presso sedi importanti dove è fondamentale la confidenzialità delle informazioni, ma allo stesso tempo è palese al pubblico la conoscienza di tale sede.

Ad esempio le sedi principali degli istituti di credito, in quanto le informazioni sulla loro locazione sono di pubblico dominio.

Quali tecniche da utilizzare in quali ambienti

Le problematiche

Non esiste una “soluzione” al Wireless (e alla sicurezza in genere), ma varie tecniche e componenti da “incastrare”.

Maggiore e' il contenuto da proteggere, maggiori le contromisure da adottare

L'uso improprio o “ponte”

- Uno degli aspetti sottovalutati e' anche l'uso improprio della propria rete
- Molto spesso i “cracker” usano una rete che non ha nessun contenuto interessante come “ponte” per attaccare la rete di qualcun altro
  - Vediamo un esempio:

L'uso improprio o “ponte”

- L'intruso entra nella rete Wireless di un'agenzia viaggi per penetrare nei sistemi di prenotazione delle Ferrovie
- La responsabilita' penale potrebbe ricadere sull'amministratore dell'agenzia viaggi in quanto responsabile della macchina sorgente dell'attacco
- Fino a che le autorità giudiziarie non avranno dimostrato che l'attacco è stato provocato da un intruso attraverso opportune indagini, l'amministratore di sistema sarà responsabile di tale attacco.

Cosa va bene per me?

Distinguiamo quattro ambienti:

- SOHO
- Piccola e Media Impresa (PMI)
- Aziende medio/grandi (Corporate)
- ISP e Operatori Mobili

SOHO

- Nella maggior parte dei casi e' sufficiente configurare opportunamente l'Access Point
- Cambiare periodicamente le chiavi WEP

PMI

- Affiancare all'opportuna configurazione degli Access Point un sistema di autenticazione, se si valuta che il contenuto da proteggere sia importante
  - IEEE 802.1x qualora si disponesse di un server RADIUS e degli AP che lo supportino. Usare un metodo EAP in grado di generare le chiavi WEP
  - Qualora non si disponga di 802.1x, usare PPPoE cambiando spesso le chiavi WEP o abilitando l'encryption a livello PPP (Microsoft Point-to-Point Protocol Encryption o MPPE)

Corporate

- La configurazione corretta degli Access Point e l'adozione dell'autenticazione 802.1x sono alla base
- Utilizzare IPSec quando necessario (ad esempio se il contenuto da accedere e' il database principale)
- Dotarsi di IDS anche sulla VLAN dedicata al Wireless, qualora abbiamo gia' IDS nella nostra rete (quindi siamo attrezzati per rispondere agli attacchi)
- Usare una HoneyNet se siamo un “obiettivo sensibile”

ISP/Operatore Mobile

- Il caso dell'ISP o degli operatori mobili e' molto particolare, in quanto:
  - non c'e' niente da proteggere
  - Il SSID deve essere ben visibile dall'utente e comunque e' pubblico (l'hotspot deve essere ben visibile!)
  - La potenza trasmissiva non deve essere limitata e il segnale deve essere ben distribuito
  - L'autenticazione serve solo ai fini di billing
- Le regole di base non si applicano in questo caso

ISP/Operatore Mobile

- L'unica “regola” e' quindi l'autenticazione per questioni di billing
- IEEE 802.1x si integra perfettamente con una infrastruttura RADIUS, ma bisogna verificare che il RADIUS supporti EAP
  - Se siete un operatore mobile, usate EAP-SIM
  - Valutate l'impatto di 802.1x: alcuni OS non hanno il client 802.1x
- Se uno dei propri obiettivi e' “rinvendere” la propria infrastruttura, e' consigliabile usare PPPoE analogamente all'ADSL

E se entrano ?
Gestire un incidente

L'importanza della gestione

- E' importante proteggere la propria rete
- E' ancora piu' importante capire cosa fare in caso di intrusione o di sospetta violazione di qualche sistema.
- Non si può rendere totalmente sicuro un sistema e bisogna tener presente che un aggressore piuttosto motivato potrebbe comunque violare il sistema (es: Social Engineering)

I sospetti

Alcuni sintomi che potrebbero evidenziare una intrusione

- Segnalazioni di attività sospette provenienti dalla sua macchina;
- La macchina si comporta in modo strano. Es: risulta molto lenta, ma il programma *top* non segnala nulla di particolare; uno o più filesystems sono pieni, ma non si riesce a scoprirne le cause;
- Il traffico in rete è molto elevato;
- Connessioni da locazioni insolite;
- I file di log sono incompleti o addirittura scomparsi;
- Alcune utility di sistema/file di configurazione sono state modificate

I sospetti

- Cercare un rootkit sulla macchina tramite un rilevatore (es: chkrootkit)
  - L'intruso potrebbe aver creato il suo rootkit per evitare di essere rilevato
- Consultarsi con gli amministratori di sistema, rete e sicurezza per correlare gli eventi sospetti

Cosa fare

- Razionalizzare in una policy scritta un processo di Gestione degli Incidenti
- Staccare la macchina dalla rete
- Raccogliere a macchina accesa le prove, es: log (file di messages,xferlogs,wtmp) se ancora integri
- Fare un backup completo della macchina ai fini legali
- Staccare il disco per un'analisi a posteriori (Forensic Analysis)
- Se si ha il sospetto che l'intruso abbia attaccato qualcun altro, avvertire tempestivamente la Polizia Postale presentando quanto raccolto (logs, backup, ...)

Ripristinare il servizio

- Non fidatevi dei backup periodici: non si sa con certezza quando l'intruso potrebbe essere entrato
- Formattare la macchina, reinstallare il sistema operativo e applicare le ultime patch
- Reinstallare gli applicativi dal CD originale e le ultime patch
- Ripristinare dai backup solamente i dati e le configurazioni degli applicativi
- Rianalizzate le configurazioni per verificare che non siano state alterate

La sicurezza nelle reti Wireless
Tecniche di protezione

gpaterno@gpaterno.com