

Wireless Ethernet standard, sicurezza e corretta configurazione della rete

Corso di:
Sicurezza su reti
Prof. Alfredo De Santis

A cura dello studente:
Fronza Danilo

Indice

Wireless Ethernet

- Introduzione
- Standard IEEE 802.11
- Tipologie delle WLAN

Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- IEEE 802.1x
- Riservatezza
- WEP
- WPA
- WPA 2

Problemi e soluzioni

- Tipologie di attacchi
- Configurazioni

Wireless Ethernet

- **Introduzione**
- Standard IEEE 802.11
- Tipologie delle WLAN

Wireless Ethernet

Diverse metodologie di trasmissione
dati via etere:

- GPRS
- Bluetooth
- 802.11 o Wireless Ethernet

Proprio di quest' ultima andremo a
trattare

Wireless Ethernet: vantaggi

- Facilità di installazione
- Mobilità
- Buone prestazioni
- Flessibilità
- Costi ridotti

Wireless Ethernet: svantaggi

- Rischi di sicurezza esasperati dalla
tipologia di collegamento
- Onde non confinabili
- Configurazione non ottimale dei sistemi di
sicurezza delle reti

Wireless Ethernet

- Introduzione
- **Standard IEEE 802.11**
- Tipologie delle WLAN

IEEE 802.11

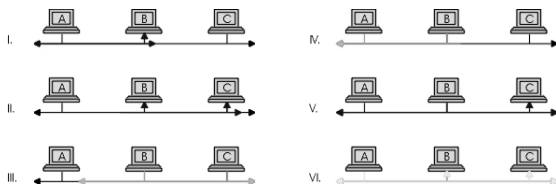
Definisce:

- Strato fisico
- Livello MAC (Medium Access Control)

Fa sì che la wireless LAN venga vista a livello LLC (Logical Link Layer) come una tradizionale rete Ethernet

IEEE 802.11

Utilizza CSMA/CA (Carrier-Sense, Multiple Access, Collision Avoidance) come protocollo trasmissione



IEE 802.11

Quando un nodo deve trasmettere, si assicura che nessun altro nodo stia occupando il canale

Se il canale non è libero, il nodo attende un tempo casuale per ritentare la trasmissione

Bassa probabilità che due nodi scelgano lo stesso tempo

Wireless Ethernet

- Introduzione
- Standard IEEE 802.11
- **Tipologie delle WLAN**

Tipologie WLAN

Due diverse tipologie:

- Rete Strutturata
- Rete Ad-Hoc

Tipologie WLAN

Rete Strutturata

- Suddivisa in celle (BSS) controllate da access point (AP).
- Spesso, l'AP è collegato ad una rete che fornisce servizi: Distribution System (DS)
- Possibilità di creare una rete formata da una singola BSS più un AP
- Il sistema costituito da BSS, AP e DS è visto come un'unica rete 802 e viene denominato Extended Service Set (ESS)
- Può verificarsi roaming del terminale

Tipologie WLAN

Rete Ad-Hoc

- Creata spontaneamente
- Non supporta l'accesso alla rete cablata
- Non necessita di Access Point
- Ogni nodo può comunicare con gli altri

Sicurezza Wi-Fi

■ Introduzione

- Autenticazione
- IEEE 802.1x
- Riservatezza
- WEP
- WPA
- WPA 2

Sicurezza Wi-Fi

Il wireless è per sua natura insicuro, vista l'impossibilità di confinare le onde radio

Occorre:

- Definire preventivamente il livello di sicurezza che si vuole raggiungere
- Ricorrere all'integrazione di diverse tecnologie (anche se si arriva a topologie più complesse e costose)

Sicurezza Wi-Fi

Due aspetti importanti da analizzare:

- Autenticazione
- Riservatezza

Sicurezza Wi-Fi

- Introduzione
- **Autenticazione**
- IEEE 802.1x
- Riservatezza
- WEP
- WPA
- WPA 2

Autenticazione

Autenticazione

- Solo chi ha i permessi adeguati, può spedire e ricevere dati sulla rete
- Rappresenta il primo passo per un dispositivo che si connetta ad una WLAN
- Due tipi di autenticazione:
 - A sistema aperto
 - A chiave condivisa

Autenticazione

Autenticazione a sistema aperto:

- Scambio delle reciproche identità tra le due parti
- Non offre vantaggi in termini di sicurezza

Autenticazione

Autenticazione a sistema aperto:

- Un client invia all'AP un frame di controllo MAC (frame di autenticazione) che indica che questo è un tipo di autenticazione a sistema aperto
- L'AP risponde col proprio frame di autenticazione e la procedura è completa

Autenticazione

Autenticazione a chiave condivisa:

- Assume che ogni stazione abbia ricevuto una chiave segreta condivisa, attraverso un canale sicuro, indipendente dalla rete 802.11

Autenticazione

Autenticazione a chiave condivisa:

- Il client invia all'AP un frame di richiesta di autenticazione con l'identificazione "Shared Key" e col proprio identificativo di stazione
- L'AP risponde con un frame contenente una stringa di testo di prova
- Il client copia la stringa in un frame codificato col WEP e la chiave condivisa e lo invia all'AP
- L'AP riceve il frame, lo decodifica mediante il WEP e la chiave condivisa, lo confronta col frame inviato e invia un messaggio al client con l'esito della procedura

Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- **IEEE 802.1x**
- Riservatezza
- WEP
- WPA
- WPA 2

IEEE 802.1x

- Esempio di autenticazione a chiave condivisa
- Port-based access control mechanism
 - sistema in grado di autenticare un utente collegato ad una determinata porta o AP ed applicare di conseguenza il livello di sicurezza necessario
- Identifica e autorizza un utente su reti wireless ed ethernet
- Permette servizi personalizzati quali il raggruppamento di una classe di utenti in una determinata Virtual LAN
- Si basa su EAPOL che prevede differenti tipologie di autenticazioni, tra cui MD5 e TLS

IEEE 802.1x

Vi sono tre problematiche

- Non definisce un sistema di crittografia, limitandosi ad autenticare l'utente
- Molti degli AP esistenti non dispongono di 802.1x e, se non possono essere aggiornati, vanno sostituiti
- Fino a poco tempo fa, solamente alcuni sistemi operativi supportavano nativamente IEEE 802.1x

IEEE 802.1x

Si serve del protocollo EAP (Extensible Authentication Protocol) per l'autenticazione

EAP supporta differenti schemi e permette di negoziare il protocollo di autenticazione tra i due interlocutori

Attraverso EAP, lo standard IEEE 802.1x permette la distribuzione di chiavi WEP attraverso un frame EAPOL-Key

IEEE 802.1x

Sono stati definiti alcuni schemi EAP, i più famosi dei quali sono:

- EAP-MD5
- EAP-TLS
- EAP-LEAP
- EAP-TTLS
- EAP-PEAP
- EAP-SecurID
- EAP-SIM
- EAP-AKA

IEEE 802.1x

EAP-TLS è lo schema più diffuso per 802.1x/EAP

I componenti che svolgono un ruolo durante l'operazione di autenticazione sono:

- Supplicant (computer dell'utente)
- Authenticator (Access Point)
- Authentication sever (server RADIUS)

IEEE 802.1x

Durante l'autenticazione mediante EAP-TLS, sia il supplicant che l'authentication server devono supportare EAP-TLS, mentre l'AP deve supportare solamente 802.1x/EAP

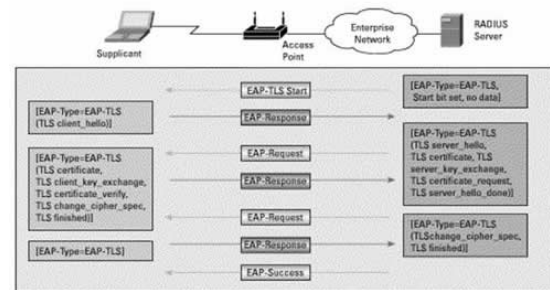
- L'AP non è a conoscenza del tipo di schema di autenticazione EAP

IEEE 802.1x

In dettaglio:

- Il RADIUS server manda il proprio certificato al client e richiede il certificato del client stesso
- Il client valida il certificato ricevuto, risponde con un messaggio EAP contenente il proprio certificato e inizia la negoziazione per la crittografia (algoritmo cifratura e compressione)
- Il RADIUS valida il certificato del client e risponde con le specifiche crittografiche della sessione

IEEE 802.1x



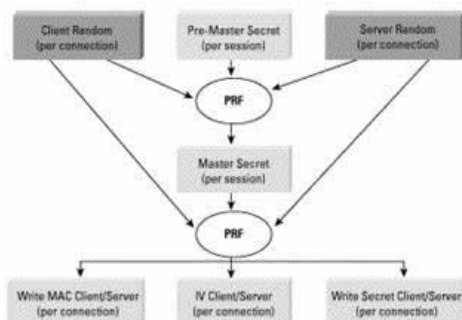
IEEE 802.1x

- Sia il client che il RADIUS server derivano le chiavi di sessione in modo indipendente anche se la lunghezza della chiave di sessione è determinata dall'AP ed è inviata tramite un messaggio EAPOL-Key
- Durante l'handshake TLS, il client genera un pre-master secret, crittografato con la chiave pubblica del server e lo invia al server
- Il pre-master secret, dei valori casuali del client e del server e il master secret vengono usati per generare una chiave per la sessione

IEEE 802.1x

La pseudo-random function (PRF) viene utilizzata per generare la chiave di sessione precedentemente menzionata e viene riutilizzata in seguito insieme al master secret, congiuntamente a dei valori casuali del server e del client ed alla stringa relativa al tipo di crittografia EAP, per generare le chiavi di sessione, le chiavi Message Authentication Code (MAC) e il vettore di inizializzazione (IV)

IEEE 802.1x



Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- IEEE 802.1x
- **Riservatezza**
- WEP
- WPA
- WPA 2

Riservatezza

Qualunque dispositivo 802.11 è capace di ricevere su una qualunque delle frequenze utilizzabili secondo lo standard

- È facile poter essere intercettati.

Per evitare questi inconvenienti, sono stati messi a punto diversi protocolli di cifratura:

- WEP
- WPA
- WPA 2

Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- IEEE 802.1x
- Riservatezza
- **WEP**
- WPA
- WPA 2

WEP

WEP (Wired Equivalent Privacy)

- Cifratura opzionale definita dallo standard 802.11
- È stato inizialmente concepito per dare una protezione all'utente finale simile a quella disponibile attraverso una rete cablata di tipo tradizionale

WEP: Cifratura

- Si aggiunge alla chiave segreta WEP di 40/104 bit, un vettore di inizializzazione (IV) di 24 bit per formare una chiave di 64/128 bit
- L'IV è un numero generato dall'AP o dalla stazione
- La chiave intermedia è l'input dell'algoritmo RC4 che genera una chiave di cifratura di lunghezza fissa

WEP: Cifratura

Parallelamente:

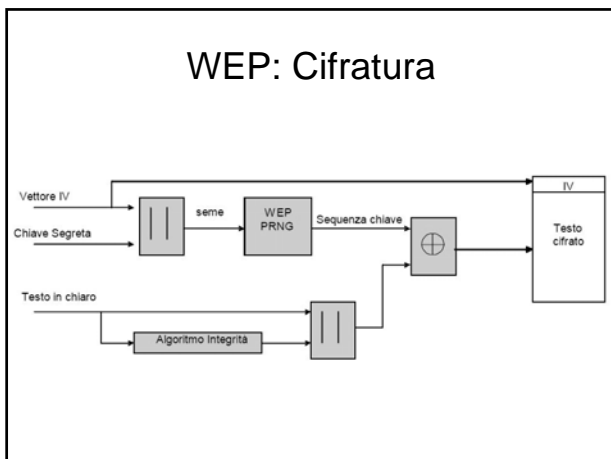
- I dati da cifrare vengono divisi in blocchi di lunghezza fissa e di ogni blocco viene calcolata una checksum CRC a 32 bit che viene aggiunta in coda al blocco
- Il blocco di dati più il checksum forma il Plaintext ed ha la stessa lunghezza della chiave di cifratura

WEP: Cifratura

Infine:

- Si esegue uno XOR del Plaintext con la chiave di cifratura per ottenere il Ciphertext
- Il vettore IV cambia periodicamente a ogni trasmissione
- Ogniquale volta cambia il vettore IV, cambia la sequenza pseudocasuale, complicando le operazioni di intercettazione

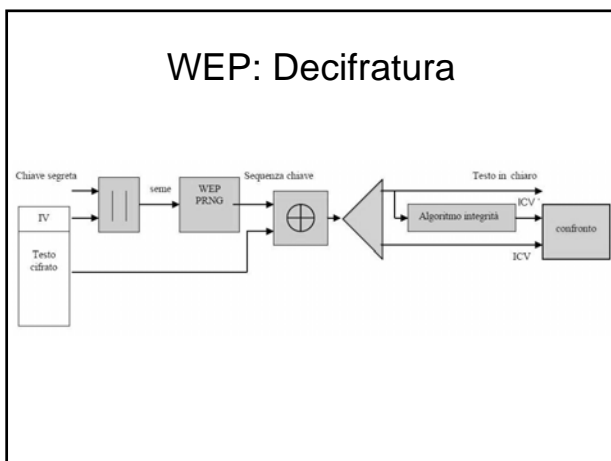
WEP: Cifratura



WEP: Decifratura

- Il ricevitore preleva il vettore IV dal blocco di dati e lo concatena con la chiave segreta condivisa per generare la stessa sequenza utilizzata dal mittente
- Questa sequenza viene unita con uno XOR al blocco in arrivo, in modo da recuperare il testo in chiaro
- Infine, il ricevitore confronta il codice CRC in arrivo con il codice CRC calcolato per verificare l'integrità dei dati

WEP: Decifratura



WEP: Debolezze

L'uso di RC4 ha determinato la maggior debolezza del WEP, dato che esso risulta vulnerabile se vengono utilizzate le chiavi più di una volta

In una rete di medie dimensioni e con un discreto volume di traffico, sono sufficienti pochi minuti affinché vengano riutilizzate le stesse chiavi di cifratura

WEP: Debolezze

Oltre alle debolezze intrinseche del WEP:

- Lo standard IEEE 802.11 non fornisce alcun meccanismo di custodia e configurazioni delle chiavi WEP
- La configurazione delle chiavi WEP è manuale, questo implica una scarsa variazione nel tempo delle chiavi WEP
- Il meccanismo WEP dà una falsa sensazione di sicurezza all'utente finale

Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- IEEE 802.1x
- Riservatezza
- WEP
- **WPA**
- WPA 2

WPA

WPA (Wi-Fi Protected Access)

- È uno sforzo dei produttori nel tentativo di colmare le lacune derivate da WEP
- Cerca di fornire una migliore crittografia dei dati rispetto al WEP e anche un meccanismo per l'autenticazione dell'utente, funzione assente nel WEP

WPA

- Utilizza il Temporary Key Integrity Protocol (TKIP) per crittografare i dati, aumentando la chiave dai 40/104 bit di WEP, fino a 128 bit
- Genera periodicamente e automaticamente una nuova chiave per ogni client
- Implementa un meccanismo di controllo dell'integrità dei dati (MIC) di 8 byte
 - Permette di evitare le alterazioni dei pacchetti trasmessi attraverso la rete wireless
 - Sistema più robusto di quello del WEP con ICV

WPA

- Il MIC viene calcolato separatamente dal client e dall'AP e se risulta differente, il pacchetto viene scartato
- Usa un vettore di inizializzazione IV di 48 bit anziché 24
- WPA implementa i protocolli 802.1x e EAP
 - Insieme formano una forte struttura di autenticazione

WPA

WPA supporta due metodi:

- Personal. È appropriato per case e piccoli uffici che non hanno infrastrutture di autenticazione
 - Una password settata manualmente viene inserita nell'AP e nei client
- Enterprise. Usa un server RADIUS per l'autenticazione
 - Si deve selezionare l'EAP e l'802.1x nelle stazioni wireless

WPA e IEEE 802.1x

- IEEE 802.1x è la metodologia di autenticazione grazie al quale WPA ottiene la migliore resa di autenticazione e cifratura
- WPA necessita che il metodo EAP selezionato dall'amministratore supporti la mutual authentication
 - TLS
 - TTLS
 - LEAP
 - PEAP

WPA e IEEE 802.1x

- Durante il processo di autenticazione un Pairwise Master Key (PMK) viene generato sia sulla stazione che sul RADIUS server
- Il RADIUS manderà il PMK all'AP
- Il PMK non è mai usato direttamente nelle funzioni di cifratura o di hash, ma viene usato per generare chiavi temporanee che verranno usate in queste funzioni
- L'uso di chiavi temporanee è utile al fine di evitare attacchi alla chiave

WPA e IEEE 802.1x

Il WPA ha apportato delle modifiche all'IEEE 802.1x:

- La distribuzione delle chiavi WPA avviene solo dopo che un client si è autenticato correttamente alla rete
- Il processo dello scambio delle chiavi viene chiamato 4-way and Group Key Handshake
 - Il 4-way Handshake determina il PMK usato per il traffico unicast
 - Il Group Key Handshake determina e distribuisce il PMK per il traffico in broadcast
- Questo processo di creazione delle chiavi è stato strutturato per evitare attacchi di tipo man in the middle

WPA e IEEE 802.1x

In dettaglio:

- Gli indirizzi dell'Access Point e del client vengono usati in ogni calcolo del MIC durante il 4-way handshake.
- Vengono usati gli nonces (valori usati una volta sola) durante il calcolo del MIC.
 - Nuovi nonces vengono usati durante ogni 4-way handshake per generare le chiavi temporanee, congiuntamente al PMK.
- Gli nonces assicurano che né il client né l'Access Point siano nella posizione di essere sotto attacchi di tipo replay.

WPA e IEEE 802.1x

Altre modifiche apportate dal WPA all'IEEE 802.1x sono:

1. Aggiunta del parametro PortSecure
 - Quando questo valore è impostato, sia l'authenticator che il supplicant sanno che le chiavi per unicast e broadcast sono valide e pertanto possono essere programmate nel firmware della scheda di rete wireless, in modo da non sovraccaricare il processore principale per la crittografia. Dopo la programmazione della scheda di rete, le successive autenticazioni IEEE 802.1x avvengono in maniera cifrata.

WPA e IEEE 802.1x

2. WPA definisce anche un frame di tipo EAPOL MIC error. Questo pacchetto permette al client di informare l'AP quando è soggetto ad un attacco.
 - Questo pacchetto è inviato all'AP quando il client ha un errore durante la comparazione del MIC nei dati in transito. Quando il client riceve frequentemente pacchetti con errori, allora desume di essere sotto attacco e apposite contromisure vengono prese dall'Access Point, ad esempio attraverso la notifica ad un amministratore.

WPA e IEEE 802.1x

3. Il TKIP usa l'algoritmo RC4, lo stesso usato da WEP, ma ne aggiunge tecniche di protezione per evitare i problemi derivati da WEP
 - Aggiunge una funzione di cambio di chiavi ad ogni pacchetto (evita attacchi su chiavi deboli)
 - Aggiunge un vettore di inizializzazione (IV) più lungo (per ovviare all'osservazione di pacchetti con IV identico)
 - Aggiunge un Message Integrity Code (MIC) (per verificare l'integrità dei dati)

Sicurezza Wi-Fi

- Introduzione
- Autenticazione
- IEEE 802.1x
- Riservatezza
- WEP
- WPA
- **WPA 2**

WPA 2

- Utilizza 802.1x e EAP per l'autenticazione e prevede entrambi i modi Personal e Enterprise
- La differenza sostanziale con WPA è che WPA 2 fornisce un più forte meccanismo di criptaggio attraverso AES
- Con AES la crittografia viene fatta su blocchi di dati invece che bit a bit
- WPA 2 crea delle nuove chiavi ad ogni associazione proprio come WPA.
 - I vantaggi sono che le chiavi di criptaggio usate per ogni utente sulla rete sono uniche e specifiche dell'utente stesso.

Problemi e Soluzioni

- **Tipologie di attacchi**
- Configurazioni

Tipologie di attacchi

Possiamo evidenziare tre macro tipologie di attacchi:

1. All'apparato radio
2. Alla rete aziendale o interna
3. Al client wireless

Tipologie di attacchi

Attacchi all'apparato radio:

- Modifica dei dati in transito
- "Replay" di sessioni eseguite dai client
- Disturbo del segnale radio (Radio Jamming)
- Inserimenti di un finto AP per dirottare la connessione dei dispositivi wireless verso la rete pirata
 - Gli hacker installano un punto di accesso con un segnale più potente nelle loro vicinanze. Gli utenti tenteranno di collegarsi ai falsi server, fornendo nome utente e password e qualsiasi altra informazione riservata

Tipologie di attacchi

Attacchi alla rete aziendale o interna:

- Un aggressore può facilmente entrare nella rete aziendale senza dover preoccuparsi di autenticarsi alla rete
 - Poichè il WEP è l'unico protocollo nello standard IEEE 802.11 per autenticare gli utenti
- Non esiste nessun controllo di accesso verso le risorse della rete interna
 - Un intruso può effettuare qualsiasi operazione sulla rete senza nessuna limitazione

Tipologie di attacchi

Attacchi ai client wireless:

- Molte architetture prevedono che i client wireless vengano visti come risorse interne, anzichè risorse esterne (o untrusted)
 - Eventuali aggressori possono compromettere i client wireless per ottenere preziose informazioni o per usarli come "ponte" per penetrare nella rete aziendale

Problemi e Soluzioni

- Tipologie di attacchi
- **Configurazioni**

Configurazioni

Una corretta configurazione degli apparati è un buon inizio per proteggere la rete wireless.

Grazie ad alcuni accorgimenti, è possibile "sviare" un eventuale intruso nascondendo dettagli preziosi e rendendo più difficile l'identificazione della rete su cui si sta collegando



Configurazioni

- ✓ Cambiare gli SSID di default
- ✓ Utilizzare SSID non descrittivi
- ✓ Disabilitare il Broadcast SSID
- ✓ Cambiare le password
- ✓ Aggiornare il firmware
- ✓ Cambiare spesso le chiavi WEP
- ✓ Abilitare il MAC filtering
- ✓ Spegner l'AP quando non serve
- ✓ Minimizzare l'intensità del segnale
- ✓ Cambiare le community di default di SNMP
- ✓ Limitare il traffico di broadcast
- ✓ Non utilizzare il DHCP
- ✓ Utilizzare una VLAN separata