

Telecom & Capital Express

Managed Security Provider

Fabrizio Croce

Viale Gandhi, 23

10051 Avigliana (TO)

Tel. 011- 97.69.511

Fax. 011-97.69.500

fabrizio.croce@tc-express.it



La sicurezza delle Wireless LAN: Analisi delle contromisure

Wireless LAN e Security

Debolezze

I problemi principali di sicurezza introdotti da una Wireless LAN sono dovuti al protocollo 801.11b (Wi-Fi) riguardo:

- **Autenticazione**
- **Criptazione**

Wireless LAN e Security

Criptazione

Wire Equivalent Privacy (WEP), algoritmo di criptazione dei dati trasmessi con il segnale radio con chiave a 40 o 128 bit

WEP è debole: E' noto come il WEP abbia una grossa vulnerabilità dovuta alla staticità delle chiavi di criptazione ed al riuso del key stream che permette ad un intrusore di decodificare i dati dopo aver catturato un certo ammontare di traffico.

WEP spesso disabilitato: Moltissime Wlan, sovente in ambienti pubblici, hanno il WEP non abilitato, talvolta per permettere interoperabilità con client diversi. La sua abilitazione è importante per poter bloccare gli sniffing occasionali e complicare la connessione all'access point dal momento che oltre l' SSID devono coincidere anche le chiavi di criptazione. Però anche con il WEP abilitato i pacchetti di controllo rimangono in chiaro

Wireless LAN e Security

Autenticazione

Per potersi collegare ad un Access Point, un client manda in broadcast su tutti i canali disponibili il suo Mac ed il suo SSID. Il primo access point che li riceve gli risponde con il suo SSID, canale da utilizzare e Mac Address. A questo punto il client ha identificato l'access point con il quale iniziare il processo di autenticazione che può avvenire con due metodi: Il primo è l'open key oppure se il WEP e' abilitato, il shared key



Wireless LAN e Security

Autenticazione

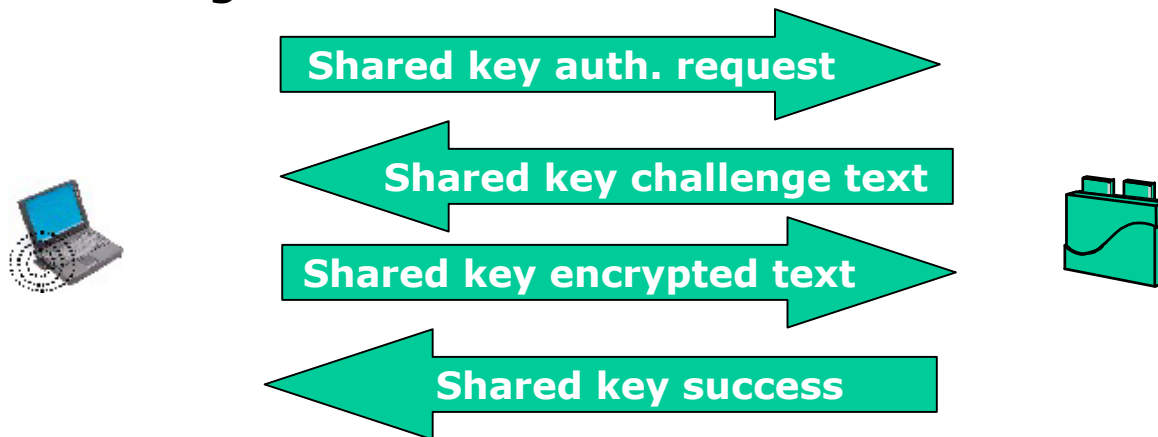
Open key: l'autenticazione è in chiaro e qualunque client può autenticarsi con l'access point. Se abilitata la crittazione, viene accettato traffico solo con chiave di crittazione WEP coincidente a quella dell'access point



Wireless LAN e Security

Autenticazione

Shared key: Utilizzato solo con WEP attivo, prevede che il client richieda l'autenticazione all'access point il quale trasmette in risposta un pacchetto di challenge. Il client risponde criptando il pacchetto con la propria chiave WEP. L'access point decrypta la risposta e la confronta con il pacchetto di challenge che aveva inviato. Se sono uguali, il client ottiene l'accesso alla rete. Il pacchetto di challenge è trasmesso dall'access point in chiaro ed un eventuale intrusore potrebbe ricavare la chiave WEP usata per la codifica andando a confrontare la risposta criptata con il pacchetto di challenge.



Wireless LAN e Security

Autenticazione IEEE 802.1x

IEE sta rilasciando il protocollo **802.1x** che sarà uno standard per il controllo degli accessi, *port-based*. Il controllo di accesso fornisce un meccanismo attraverso cui autenticare e autorizzare i dispositivi connessi ad una porta LAN e bloccare l'accesso a quella porta, nel caso in cui il processo di autenticazione e di autorizzazione fallisca. Parte del protocollo è basato sull'EAP (Extensible Authentication Protocol) che permette ai client di autenticarsi ad un server RADIUS

Nonostante sia stato ideato per reti Ethernet cablate, lo standard è stato adattato per l'utilizzo su reti LAN wireless IEEE 802.11 in quanto è in grado di coprire la maggior parte delle vulnerabilità dovute alla autenticazione ed alla staticità delle chiavi di criptazione

Windows XP include il supporto dell'autenticazione IEEE 802.1X per tutte le schede di rete basate su LAN, incluse reti Ethernet e wireless

Wireless LAN e Security

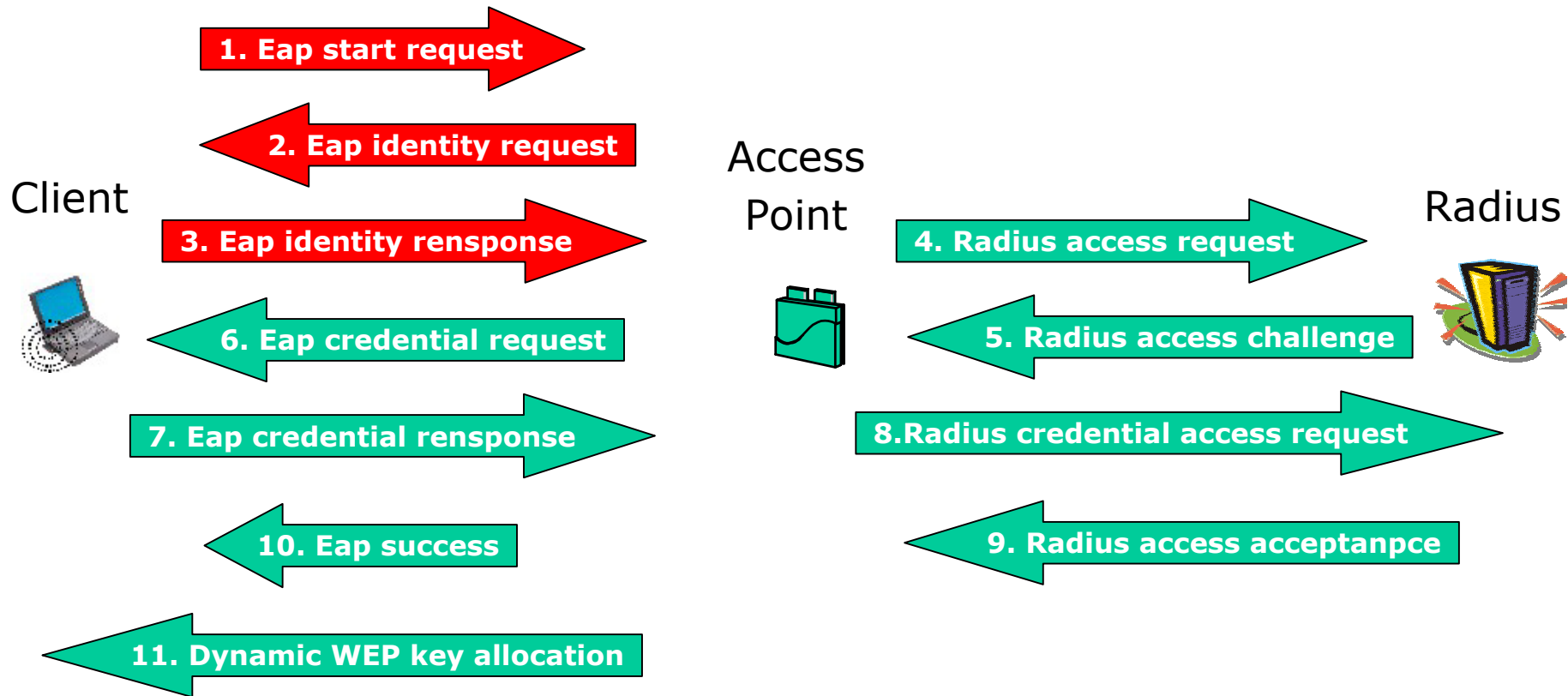
IEEE 802.1x nel Wireless

Con l' IEEE 802.1X, il client associato all' Access Point non ottiene la connessione fisica alla rete durante la fase di autenticazione. L'access point inizia il dialogo EAP con il client e gestisce la comunicazione con il server EAP-Radius. Quando le credenziali del client sono accettate dal Radius, questi rilascia all'access point le policy di accesso e questi permette la connessione alla rete wired con le opportune restrizioni.

Tramite l' EAP l'access point assegna al client una chiave WEP a 128 bit dinamica per ogni sessione prevenendo attacchi tipo sniffing, man in the middle, WepCrack ed altri. La trasmissione delle chiavi WEP è criptata utilizzando chiavi separate generate dal server radius e passate all'access point.

Wireless LAN e Security

IEEE 802.1x nel Wireless



Wireless LAN e Security

IEEE 802.1x nel Wireless

Attualmente l' IEEE 802.1X è adottata ancora da pochi produttori con delle versioni per-standard. Tra l'altro sono stati rilevati due potenziali vulnerabilità del protocollo, molti vendor attendono quindi il rilascio dello standard corretto:

Dal momento che non vi è una autenticazione reciproca client-access point è potenzialmente possibile un attacco man-in-the-middle durante l'autenticazione.

In seguito al fatto che pacchetti 802.11 di controllo non sono autenticati vi è la potenziale possibilità di eseguire una hijacking della sessione sniffando il MAC dell'access point durante l'autenticazione. Spoofando questo MAC si può sconnettere il client associato alla porta autenticata e sostituircisi.

Wireless LAN e Security Attacchi

A seguito di quanto descritto, gli attacchi possibili su una wireless lan possono essere riassunti in:

Attacchi di inserzione

Intercettazione e monitoraggio del traffico Wireless

Errate configurazioni degli access point o dei client

Attacchi diretti da Client a Client

War Driving

Wireless LAN e Security

Attacchi di inserzione

Inserzione di dispositivi non autorizzati su una Wlan:

Inserimento di client non autorizzati: Un attaccante si connette ad un access point e superando i meccanismi di autenticazione si introduce nella rete.

Inserimento di access point non autorizzati: Un attaccante connette alla rete un access point permettendo la connessione alla rete di client non autorizzati anche non interni alla azienda anche a distanze notevoli.

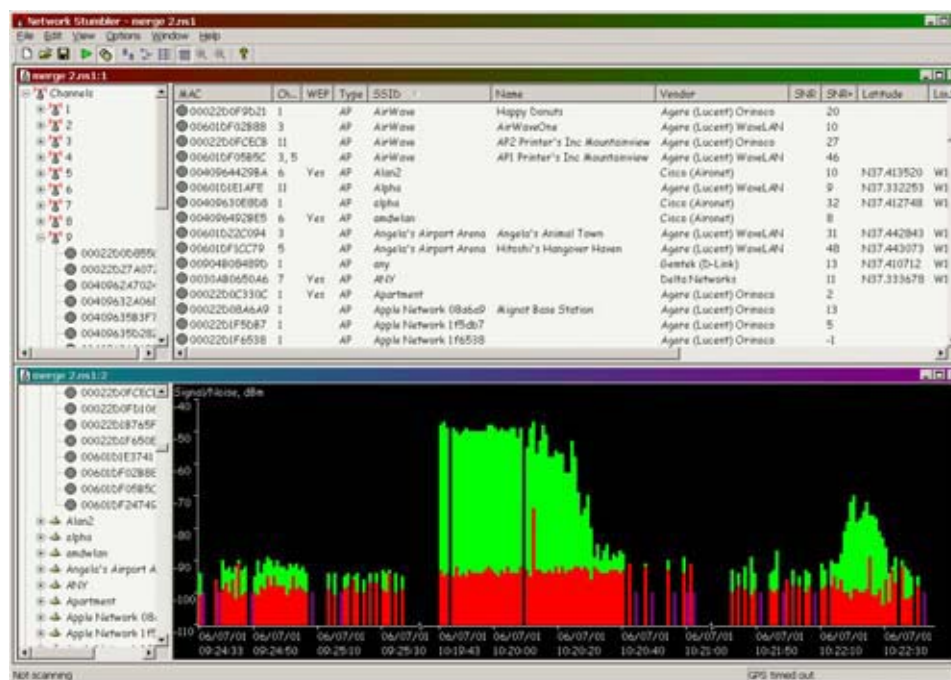
Access point "clone" (Evil Twin): Viene inserito un accesso point illegittimo con segnale molto forte, clone di un access point legittimo. Molti client si collegheranno a questo access point e l'attaccante potrebbe sniffare dati sensibili.

Wireless LAN e Security

Intercettazione e Monitoraggio

Intercettazione del traffico di rete su una Wlan:

Wireless sniffer: Un attaccante utilizza un tool di sniffing wireless (NetStumbler, AirSnort) con il quale intercetta il traffico radio, anche da parecchie centinaia di metri di distanza, cercando soprattutto le informazioni di sessione (username e password).

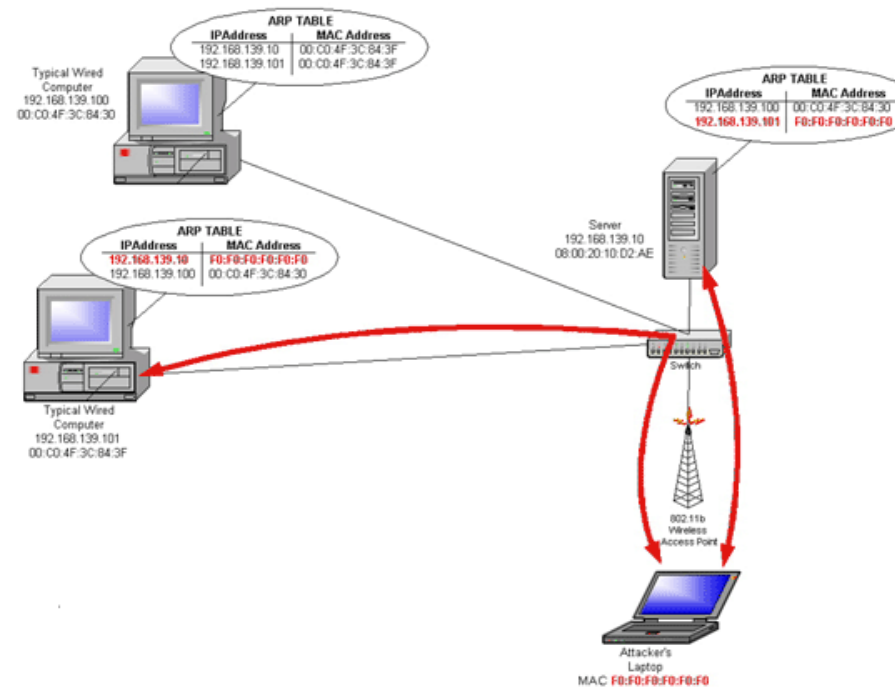


Wireless LAN e Security

Intercettazione e Monitoraggio

Intercettazione del traffico di rete su una Wlan:

Spoofing Arp: Un attaccante utilizza un tool come Dsniff tramite il quale, corrompendo la tabella ARP dell'access point, può trasparentemente far transitare tramite di se il traffico destinato da un client ad un'altra macchina (server, gateway..) sniffandolo.



Wireless LAN e Security

Intercettazione e Monitoraggio

Intercettazione del traffico di rete su una Wlan:

Hijacking SSL e SSH: utilizzando la tecnica dello spoofing Arp tramite Dsniff, un attaccante può dirottare sessioni TCP comprese SSL e SSH. Il Client riceve solo un warning che le credenziali dell'host e del certificato sono cambiate chiedendo conferma dell'accettazione di quelle nuove.

Wireless LAN e Security

Errate Configurazioni

et Server ID (SSID), un identificatore in chiaro, configurabile, che ermette ai client di comunicare con un Access Point che abbia lo stesso SSID, è equivalente ad una Shared Password tra il client e access point.

Default SSID: Molti non cambiano l' SSID di default degli Access Point. Cisco usa "tsunami", 3Com "101", Intel "intel" e così via.

Secure Access Mode: Solo se questa funzione degli access point Lucent è abilitata c'è il controllo dell' SSID. In caso contrario l'SSID può essere vuoto o impostato ad 'any'.

Brute force SSID: Dal momento che spesso gli SSID sono nomi comuni, un attaccante può scoprirlo con un semplice attacco di forza bruta.

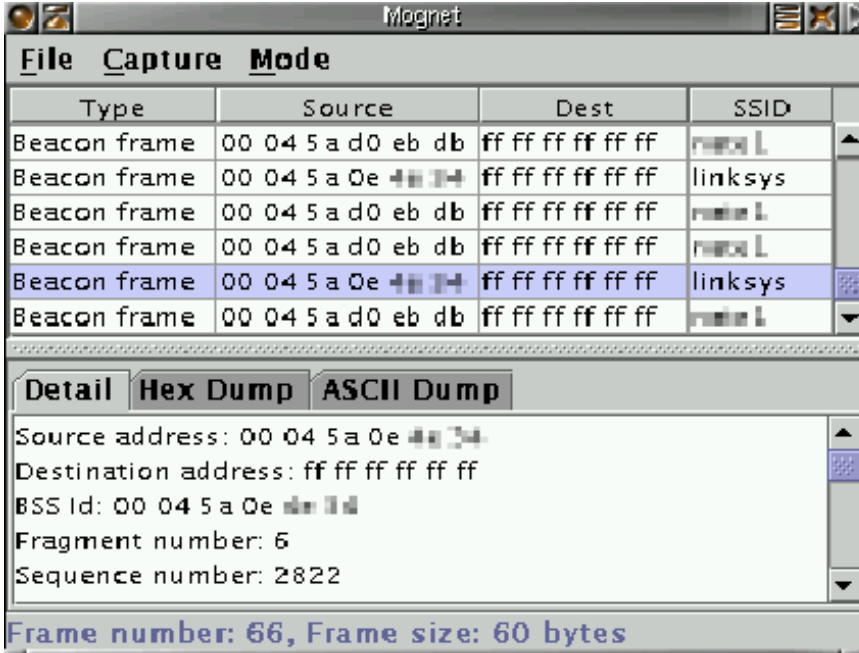
Wireless LAN e Security

Errate Configurazioni

egue su Set Server ID (SSID):

SSID in chiaro: Anche se è abilitata la criptazione WEP, SSID continua ad essere trasmesso in chiaro

Broadcast SSID: Molti AP trasmettono il proprio SSID in chiaro tramite dei pacchetti di broadcast (beacon). Anche se il broadcast viene escluso, dal momento che l' SSID è in chiaro, basta sniffare la connessione di un client.



The screenshot shows the Wireshark interface in 'Magnet' mode. The main pane displays a list of captured packets, all of which are Beacon frames. The columns shown are Type, Source, Dest, and SSID. The Source column contains MAC addresses: 00 04 5a d0 eb db and 00 04 5a 0e 4b 34. The Dest column contains the broadcast address ff ff ff ff ff ff. The SSID column shows 'raspberrypi' and 'linksys'. The 'linksys' entry is highlighted in blue. Below the list, the 'Detail' pane is expanded to show the structure of the selected beacon frame, including Source address, Destination address, BSS Id, Fragment number, and Sequence number.

Type	Source	Dest	SSID
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	raspberrypi
Beacon frame	00 04 5a 0e 4b 34	ff ff ff ff ff ff	linksys
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	raspberrypi
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	raspberrypi
Beacon frame	00 04 5a 0e 4b 34	ff ff ff ff ff ff	linksys
Beacon frame	00 04 5a d0 eb db	ff ff ff ff ff ff	raspberrypi

Detail Hex Dump ASCII Dump

Source address: 00 04 5a 0e 4b 34
Destination address: ff ff ff ff ff ff
BSS Id: 00 04 5a 0e 4b 34
Fragment number: 6
Sequence number: 2822

Frame number: 66, Frame size: 60 bytes

Wireless LAN e Security

Errate Configurazioni

Ioliti Access Point permettono il proprio monitoraggio e configurazione tramite SNMP (Simple Network Management Protocol)

Password community di default: Sovente l' SNMP viene abilitato con le sue password di default (public, private)

Vulnerabilità di SNMP : Molte implementazioni dell' SNMP sono state scoperte vulnerabili. Il progetto PROTOS realizzato alla Università finlandese di Oulu mette in risalto i problemi di sicurezza dell' SNMP <http://www.ee.oulu.fi/research/ouspg/protos>
L'unica possibilità è quella di controllare con il vendor la presenza di queste vulnerabilità e richiedere eventualmente le patch al firmware.

Wireless LAN e Security

Errate Configurazioni

Access Point con configurazioni di default

Installazione plug&play: molti vendor, per rendere semplice l'installazione degli access point, mettono di default molti parametri ed abilitando il DHCP in modo che l'access point funzioni immediatamente e velocemente. L'installatore si trova con apparati 'plug&play' che funzionano al volo ma senza una parametrizzazione avanzata possono rivelarsi molto vulnerabili. In più, spesso, il monitoraggio e la configurazione è con interfacce grafiche in http non protette di default neanche con password.

Wireless LAN e Security

Attacchi Client - Client

Due client wireless possono comunicare tra loro senza bisogno di un access point, per questo motivo un client può essere vulnerabile ad un attacco diretto.

Attacco a risorsa: Se il client ha delle risorse condivise o programmi di file sharing, un attaccante potrebbe averne accesso sfruttando errate configurazioni (mancanza password, etc..)

Denial of service: Il client Wireless può essere vulnerabile ad attacchi DOS come synflood, teardrop etc da altri client wireless.

Wireless LAN e Security War Driving

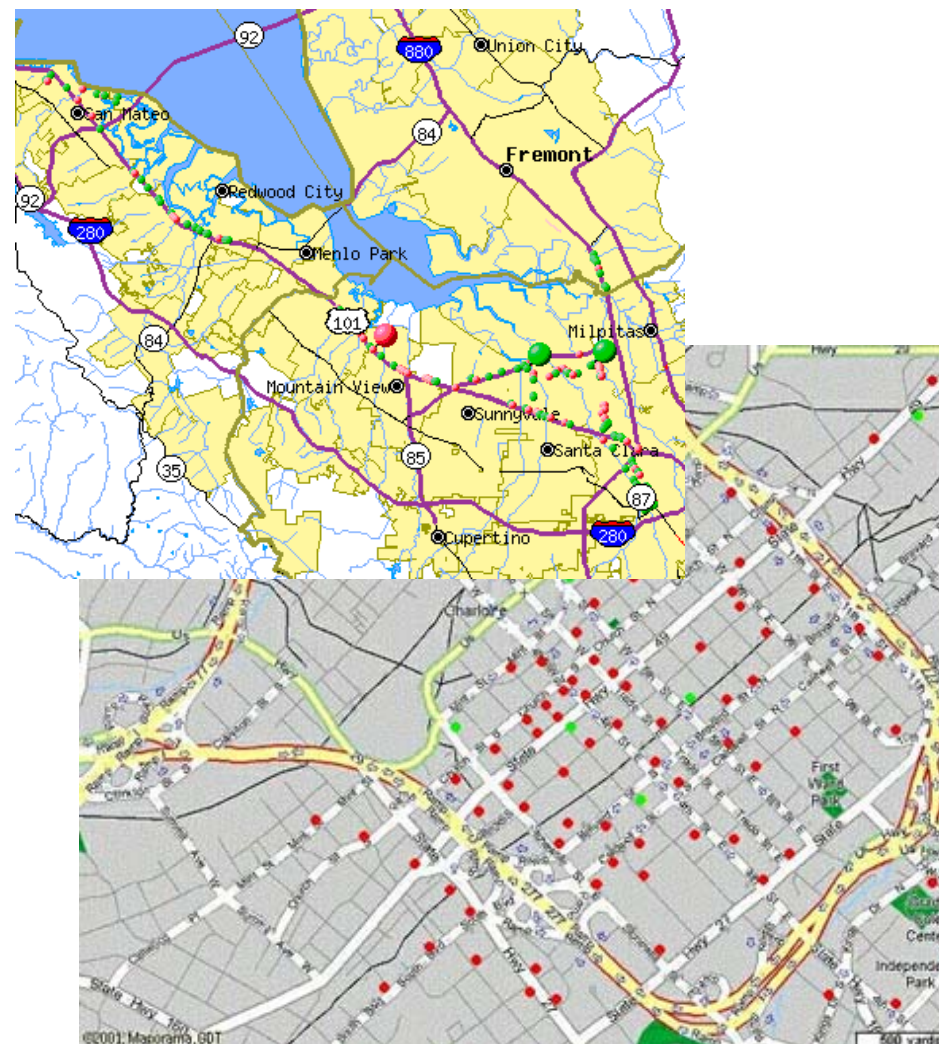
Attività di hacking delle reti wireless dove una stazione mobile wireless (Pc, scheda wireless, GPS ed antenna direzionale) dotata di sniffer radio, è posta in un veicolo e coprendo una certa area si va alla ricerca degli access point



Wireless LAN e Security War Driving

tramite l'attività di War Driving, vengono create delle mappe del territorio con la localizzazione degli access point scoperti e le loro eventuali vulnerabilità, (senza WEP ad esempio)

Da momento che spesso queste mappe sono pubbliche e inserite su internet, questo potrebbe consentire a terzi male intenzionati di sfruttare queste vulnerabilità per introdursi nella rete o sniffarne il traffico.



La sicurezza delle Wireless LAN: Analisi delle contromisure

Standard vulnerabile: Prodotti proprietari?

- Considerando che lo standard Wi-Fi ha delle vulnerabilità, si potrebbe pensare di adottare una infrastruttura con apparati NON a standard 802.11b, ad esempio apparati che usino la modulazione analogica FHSS anziché la digitale DSSS.
- Questo ci tutelerà maggiormente dai tentativi da intrusione ma avremmo un limite di banda che è di 2Mbit/sec per il FHSS anziché gli 11Mbit/sec del DSSS.
- Come tutte le soluzioni basate su apparati non standard si avranno dei problemi di scalarità in quanto si dovranno adottare apparati dello stesso produttore limitando la scelta di questa soluzione a Wlan 'chiuse' in un particolare ambiente particolarmente sensibile dove non sia importante la velocità e la interoperabilità

Standard vulnerabile: Prodotti proprietari?

- Dal momento che la criptazione WEP dello standard Wi-Fi è dimostrato essere debole, si potrebbe adottare una criptazione più forte NON a standard 802.11b come l' RC4 a chiave 128 Bit che qualche produttore propone.
- Anche in questo caso introdurremo dei problemi di scalarità ed interoperabilità in quanto, ad esempio, se avessimo l'access point di un produttore e le schede di un altro produttore, per permettere a questi ultimi client di accedere alla rete sarà necessario disabilitare la criptazione, riaprendo la falla di sicurezza

Le linee guida della Sicurezza Wireless Wi-Fi

- Progettazione della architettura della Wireless Lan e corretta installazione degli apparati
- Trattare la rete Wireless come una rete 'insicura', definire delle politiche di sicurezza che portino, ad esempio, ad introdurre meccanismi di strong authentication che implicino l'identificazione dell'utente
- Utilizzare meccanismi di criptazione che utilizzino una generazione dinamica delle chiavi di criptazione, al limite in ogni sessione.
- Security assessment ed auditing della infrastruttura wireless, dei firewall e degli eventuali sistemi IDS

Progettazione della Architettura

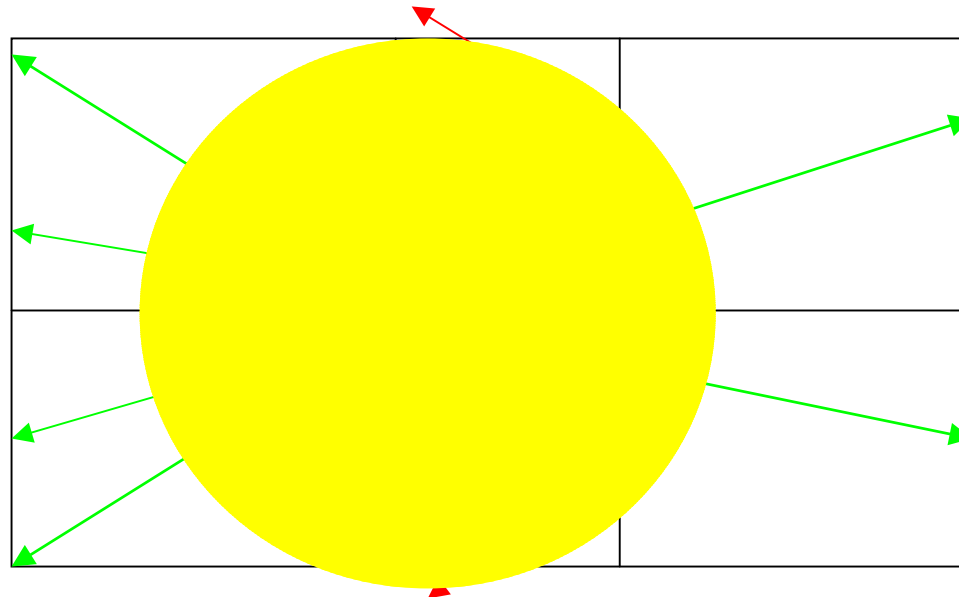
Effettuare un network assessment della **attuale** rete cablata al fine di identificarne la corretta topologia e gli eventuali punti di debolezza **a prescindere** dalla futura implementazione della Wlan.

Definire le politiche di chi utilizzerà il wireless, identificarli, raggrupparli, decidere a quali risorse potranno accedere ed in che tempi

Installare una Wlan pilota **NON in produzione** al fine di verificare che l'integrazione alla attuale rete fisica non generi problemi. Verificare in quella sede che le politiche di sicurezza siano applicabili, le prestazioni accettabili, valutare le eventuali modifiche da compiere sugli applicativi al fine di migliorare le prestazioni e la sicurezza degli stessi.

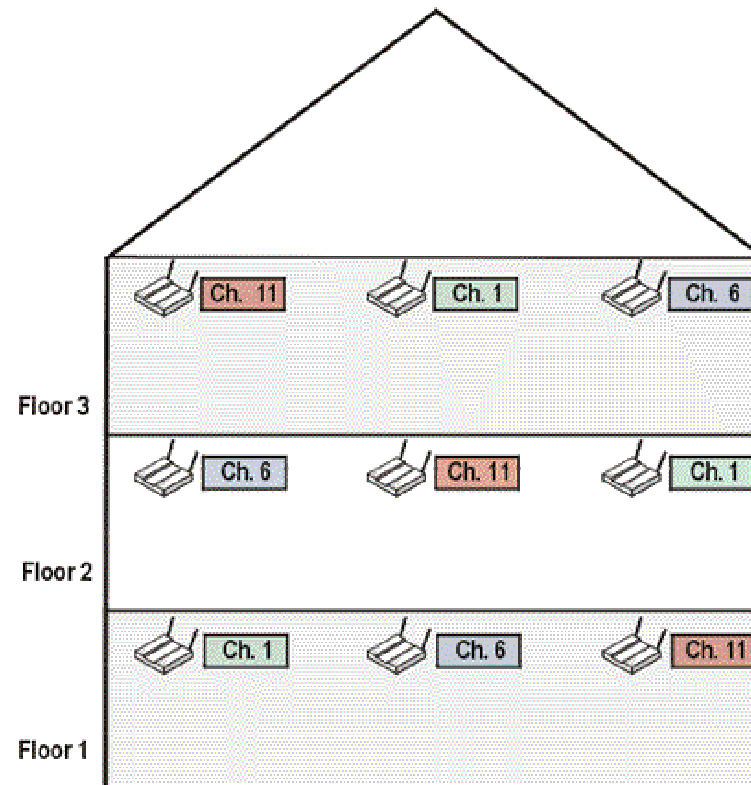
Progettazione della Architettura

Studio della planimetria del sito al fine di individuare il numero di Access Point necessari e la loro posizione rispetto la propagazione con la scelta della migliore antenna e suo corretto posizionamento tenendo conto dei lobi di propagazione e delle riflessioni.



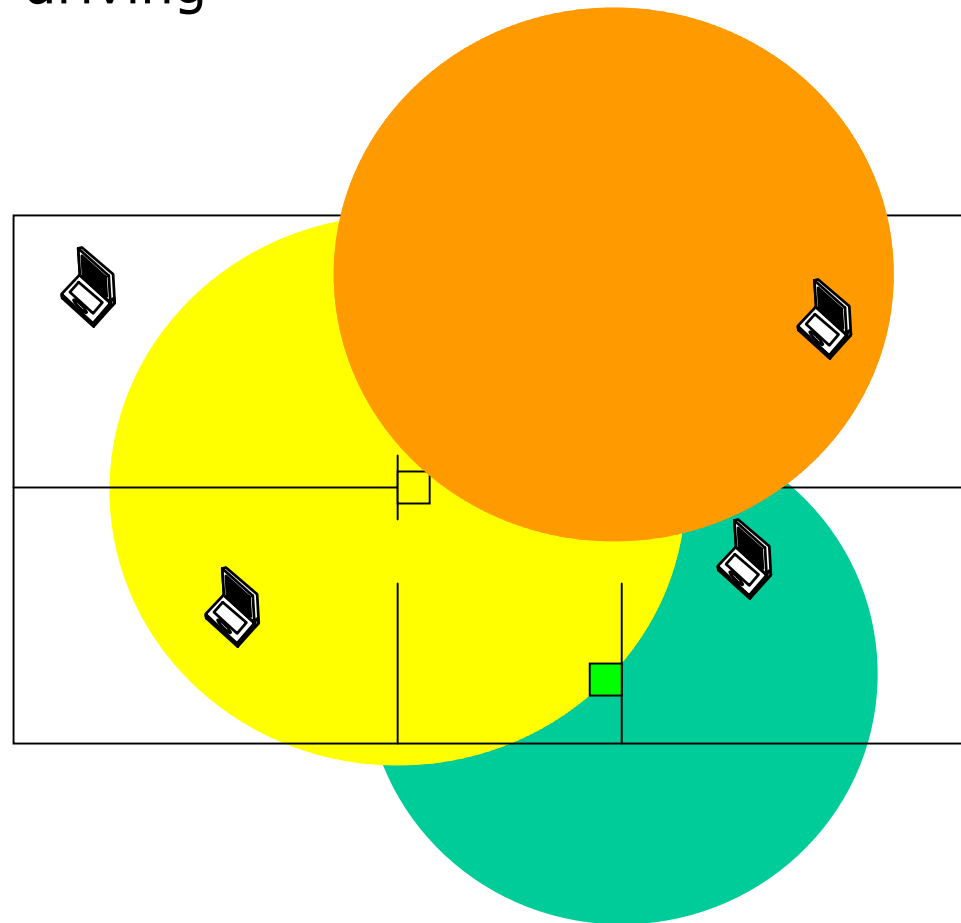
Progettazione della Architettura

Nel caso di access point adiacenti, utilizzare canali diversi per minimizzare problemi di crosstalk che potrebbero diminuire le prestazioni. Tenere sempre in considerazione che la propagazione e' una sfera a 3 dimensioni



Progettazione della Architettura

Verifica strumentale del sito per verificare la posizione corretta degli AP, per garantire la massima copertura radio interna con la minima fuoriuscita del segnale radio dal sito per non favorire attività di war driving



Progettazione della Architettura

La verifica è sperimentale con test di 'building walkthrough' al fine sia della verifica della copertura che delle prestazioni della Wlan in accordo alle specifiche richieste.

The screenshot shows the Linktest software interface. At the top, the title bar reads "Linktest". Below it, the "IP Address of Access Point" is set to "192.168.0.7". The "Number of Packets" is set to "50" and the "Packet Size" is set to "460". There are two sliders: the first for "Number of Packets" ranges from 1 to 1000, and the second for "Packet Size" ranges from 64 to 2048. A checkbox for "Continuous Linktest (Ignore Number of Packets)" is unchecked. Below these are "Receive Statistics" and "Transmit Statistics" sections. The "Receive Statistics" section shows "Packets Received OK = 52" and "Percent Packets Received OK = 100%". The "Transmit Statistics" section shows "Packets Transmitted OK = 52" and "Percent Packets Transmitted OK = 100%". Other statistics include "Status = Associated", "Current Link Speed = 11 Mbps", "Associated Access Point Name = office AP", and "Associated Access Point MAC = 00:40:96:49:5C:45". At the bottom, there are three progress bars: "Current Signal Strength" at 40%, "Current Signal Quality" at 95%, and "Overall Link Quality" labeled as "Fair". At the very bottom, there are buttons for "Start", "Defaults", "Help", "OK", and "Cancel".

Receive Statistics	Current	Cumulative Total
Packets Received OK	= 52	= 52
Percent Packets Received OK	= 100%	

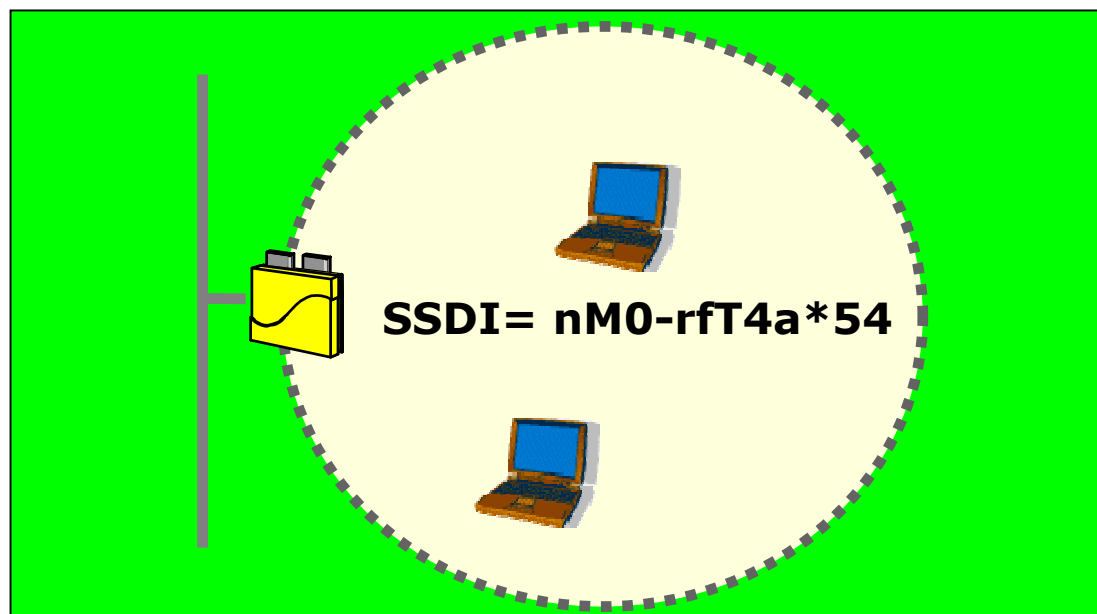
Transmit Statistics	Current	Cumulative Total
Packets Transmitted OK	= 52	= 52
Percent Packets Transmitted OK	= 100%	

Current Signal Strength: 40%
Current Signal Quality: 95%
Overall Link Quality: Fair

Installazione

Identificare la Wlan

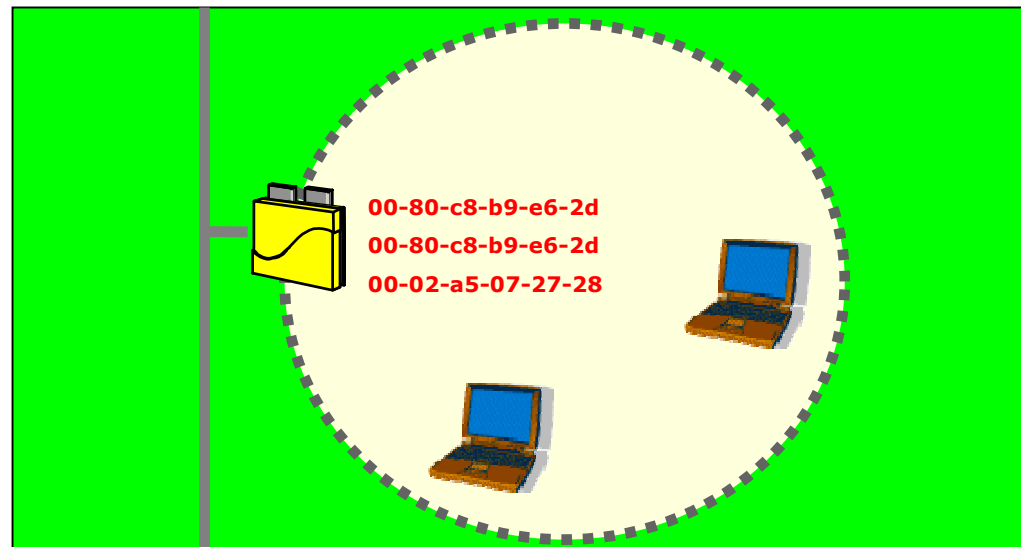
- Negli access point configurare un SSID a livello di password sicura (15 caratteri, simboli, cifre, lettere) e non utilizzare l'SSID di default.
- Disabilitare, se possibile, il Broadcast dell'SSID



Installazione

Access list: MAC Filtering

- Inserire direttamente o tramite un RADIUS l'elenco dei MAC address delle NIC autorizzate a collegarsi ad un dato access point
- Mantenere l'anagrafe interna delle NIC radio per evitare furti o sparizioni
- Per prevenire l'ARP spoofing, usare tabelle di ARP statiche negli access point per accedere a servizi ben determinati



Installazione Abilitare il WEP

Nonostante siano riconosciute le debolezze dell'algoritmo di criptazione adottato dall' 802.11, il WEP consente di proteggerci dai tentativi di intrusione più semplici e rende comunque non leggibili i nostri dati alla maggioranza dei malintenzionati. La sua mancata adozione consente letteralmente a chiunque di introdursi sul nostro network.

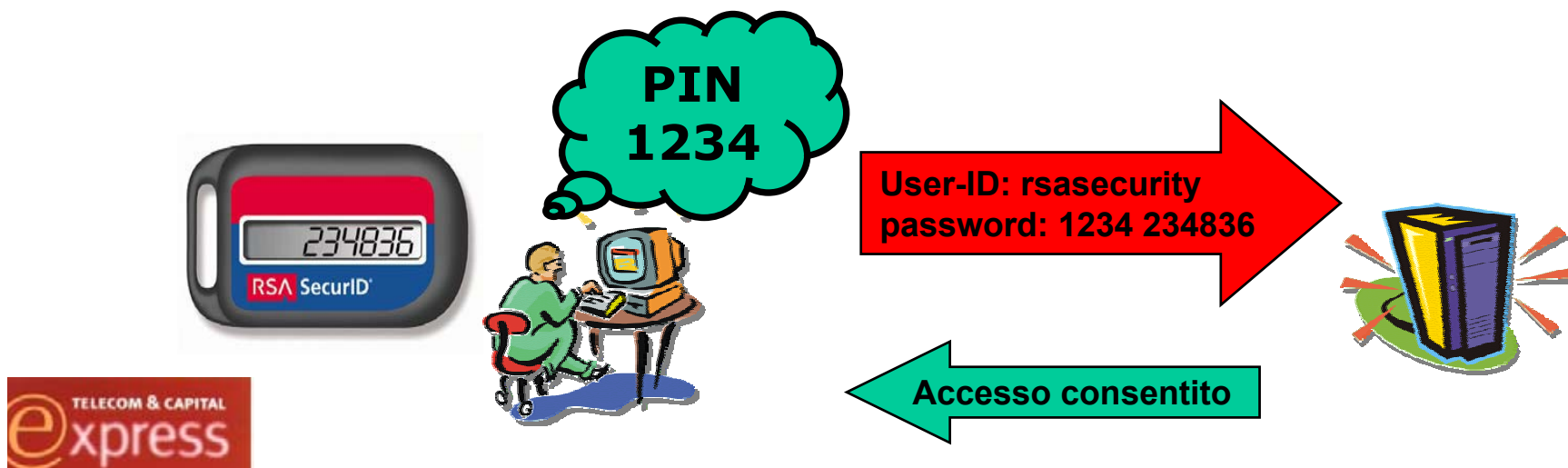
L'eventuale tempo e costo per un intrusore per decriptare i nostri dati è direttamente proporzionale alla loro sensibilità. Nel caso comunque di presenza di wireless in un sito sensibile, si adotteranno contromisure aggiuntive come le VPN.

Installazione: Autenticare ed identificare

Implementare una autenticazione più forte sia a livello fisico che di utente.

A livello fisico può essere adottata, se supportata, l' 802.1x anche se è ancora un draft.

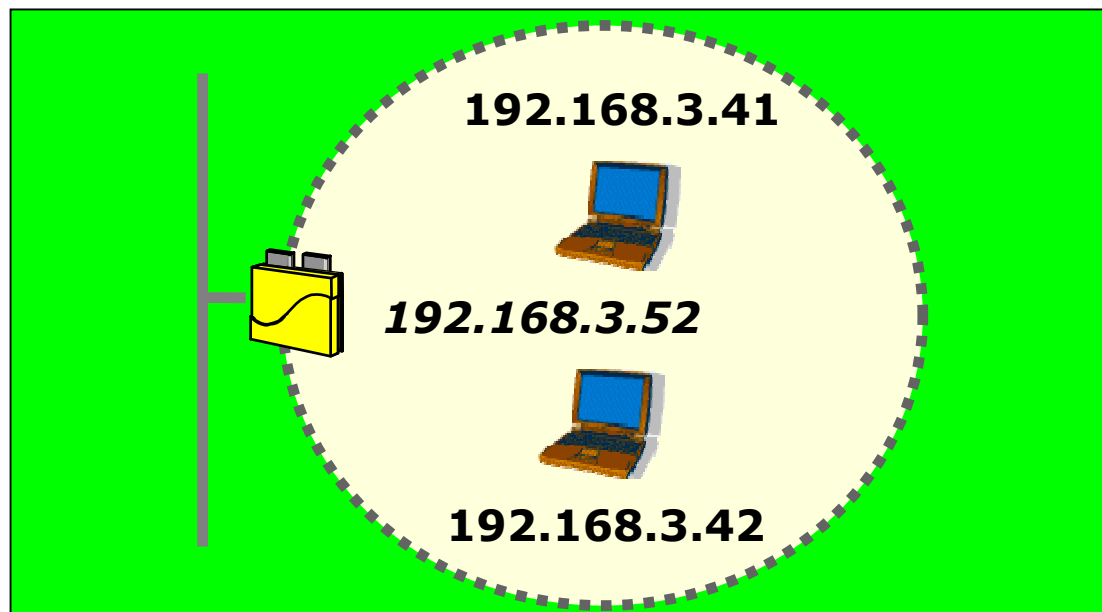
A livello utente utilizzare un server Radius oppure introdurre la strong authentication a due fattori tramite i token o tramite i certificati digitali



Installazione

Non utilizzare il DHCP nelle Wlan

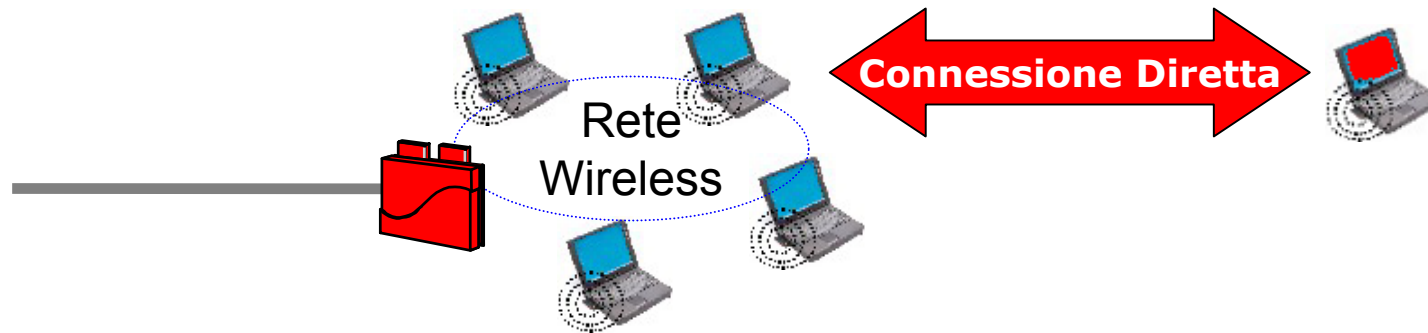
- L'utilizzo del DHCP è estremamente rischioso in una Wlan in quanto la eventuale intromissione su un Access Point darebbe all'intrusore un notevole vantaggio mettendogli a disposizione un IP valido
- Assegnare staticamente gli IP ai client della Wlan



Wlan insicura

Proteggere i singoli client

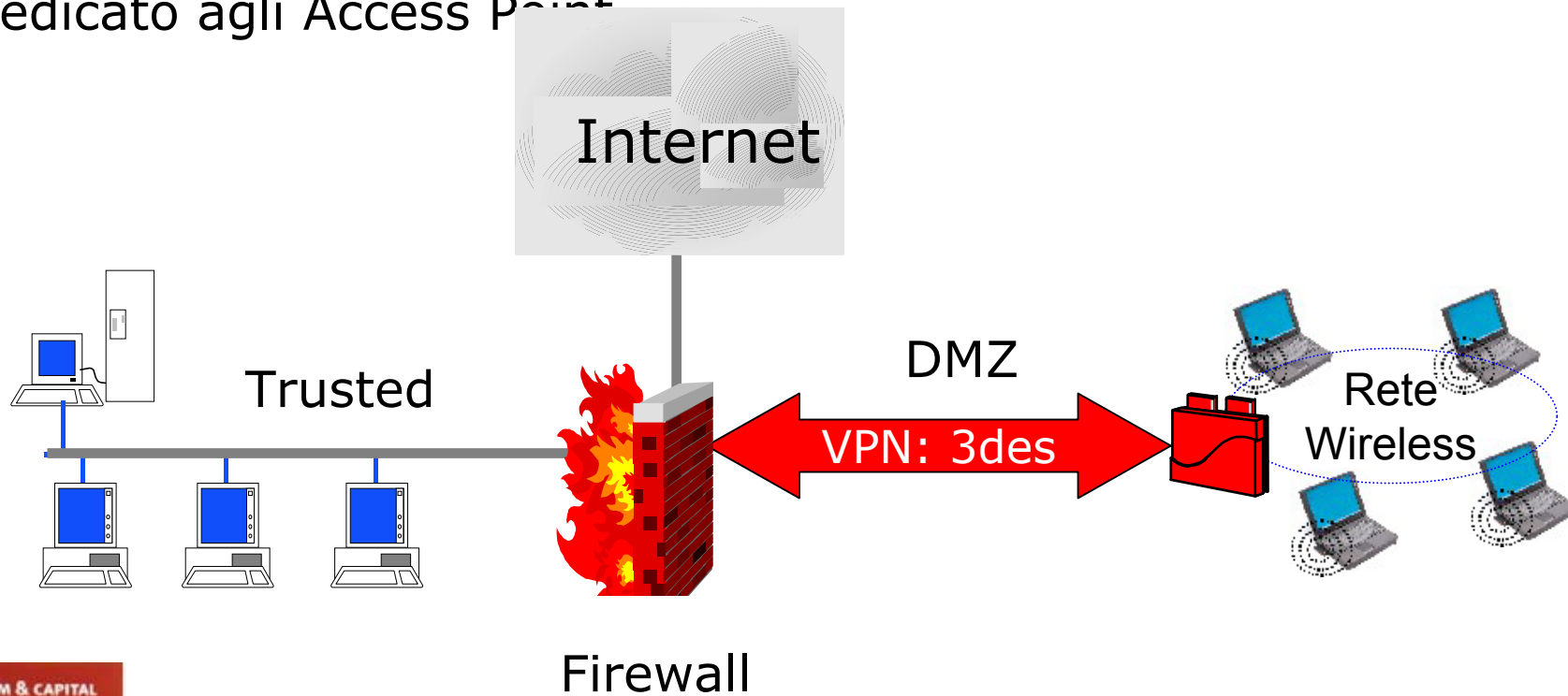
I client dalla Wlan possono essere vulnerabili ad attacchi diretti via radio al momento che il protocollo Wi-Fi consente una connessione peer to peer anche in assenza di access point. I client devono essere quindi protetti con dei personal firewall e dotati di password sulle eventuali condivisioni.



Wlan insicura

Utilizzare VPN su Wireless

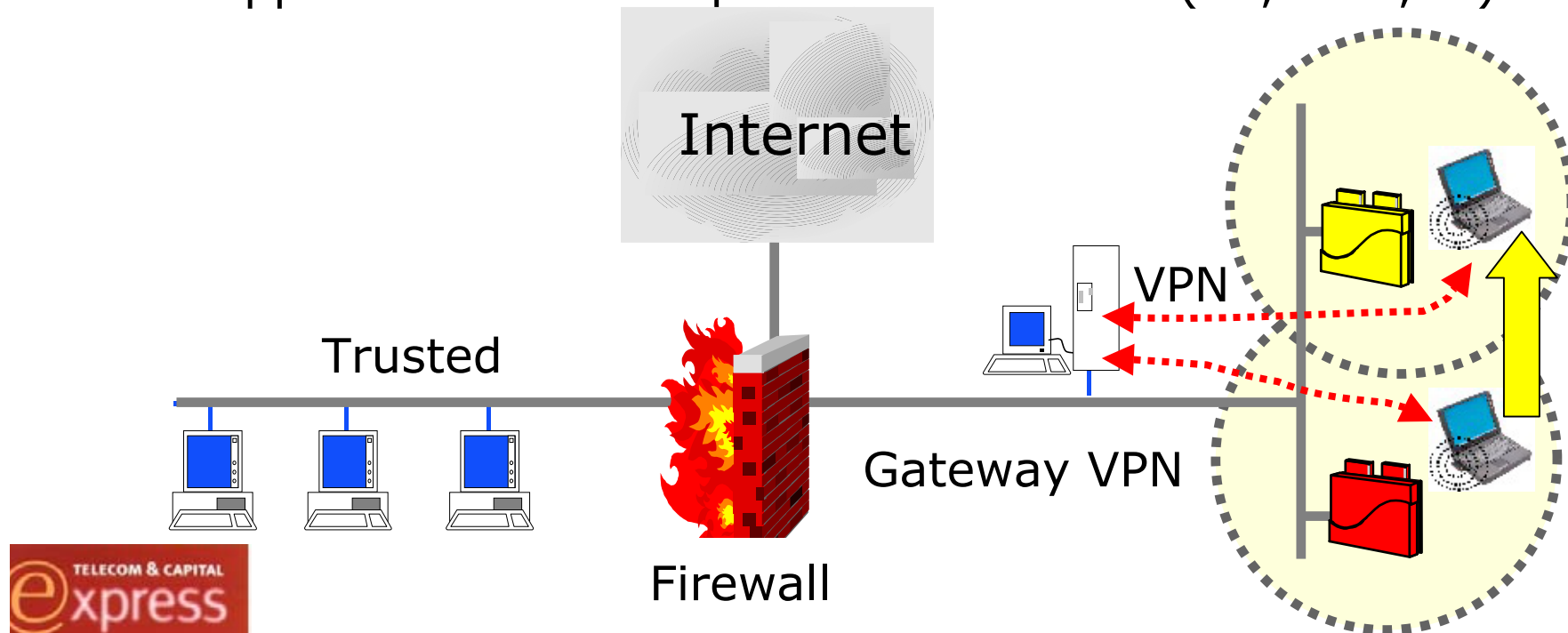
- I client dalla Wlan possono utilizzare il PPTP o meglio l'IPsec con i meccanismi di criptazione come DES o 3DES e gestione delle chiavi in modo dinamico con IKE. Si può installare un gateway VPN a monte degli AP, magari tramite un firewall dedicato agli Access Point



Wlan insicura

Utilizzare VPN su Wireless

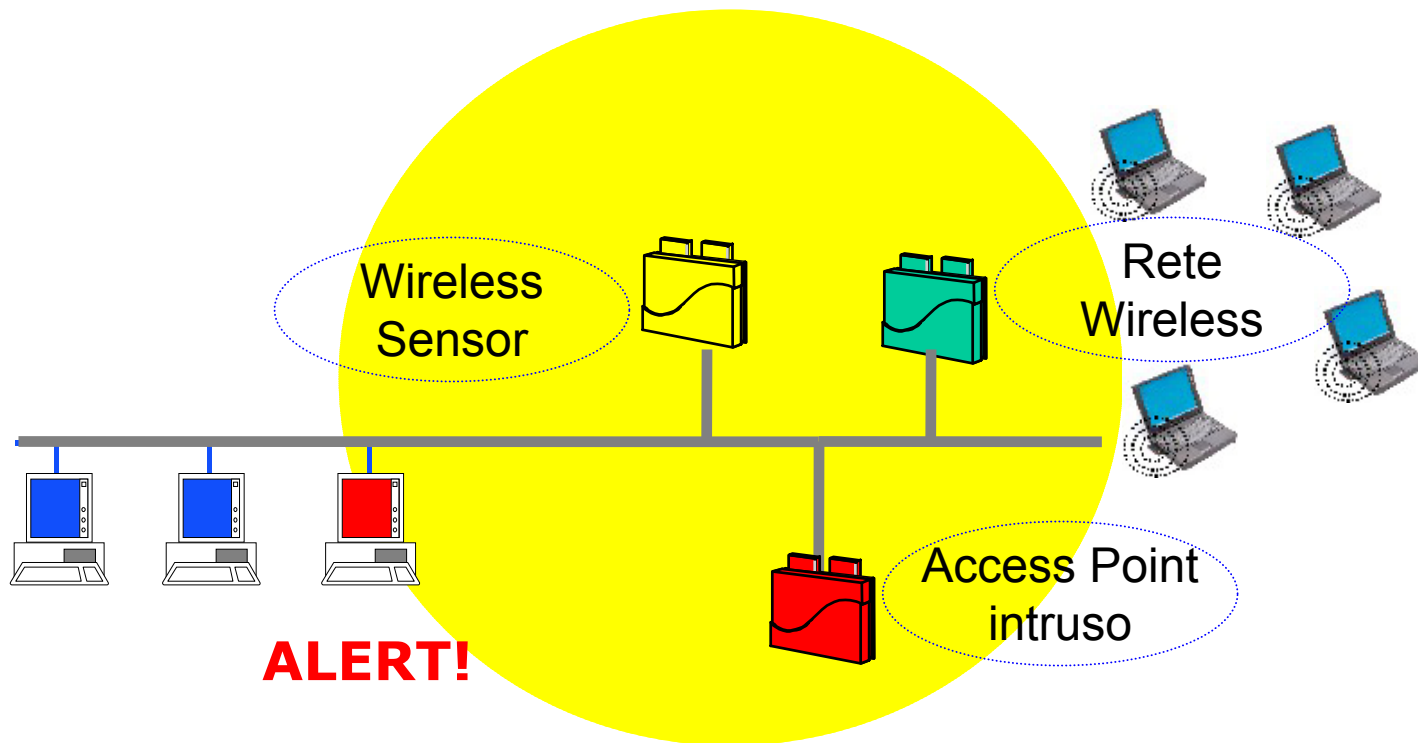
- La limitazione delle VPN su Wireless VPN è lo standard IPsec che non permette il roaming tra gli access point non consentendo così la mobilità. Esistono Gateway VPN proprietari i quali sono in grado di mantenere il tunnel anche se l'endpoint è una infrastruttura di roaming. Il limite attuale è il supporto unicamente per client Windows (98,2000,XP)



Security Assessment & Auditing

Rilevamento dei 'rogue AP'

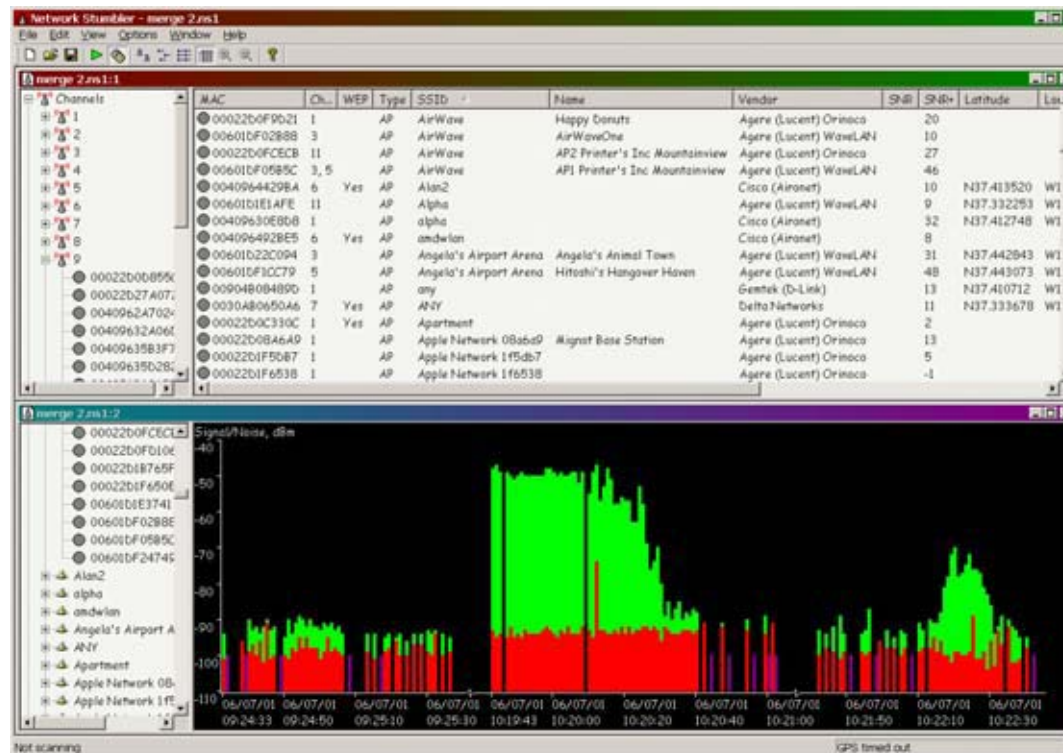
Inserzione di sensori wireless sulla rete al fine di captare pacchetti radio provenienti da dispositivi non autorizzati come Access Point o client con notifica immediata presso un sistema di IDS



Security Assessment & Auditing

Rilevamento dei 'rogue AP'

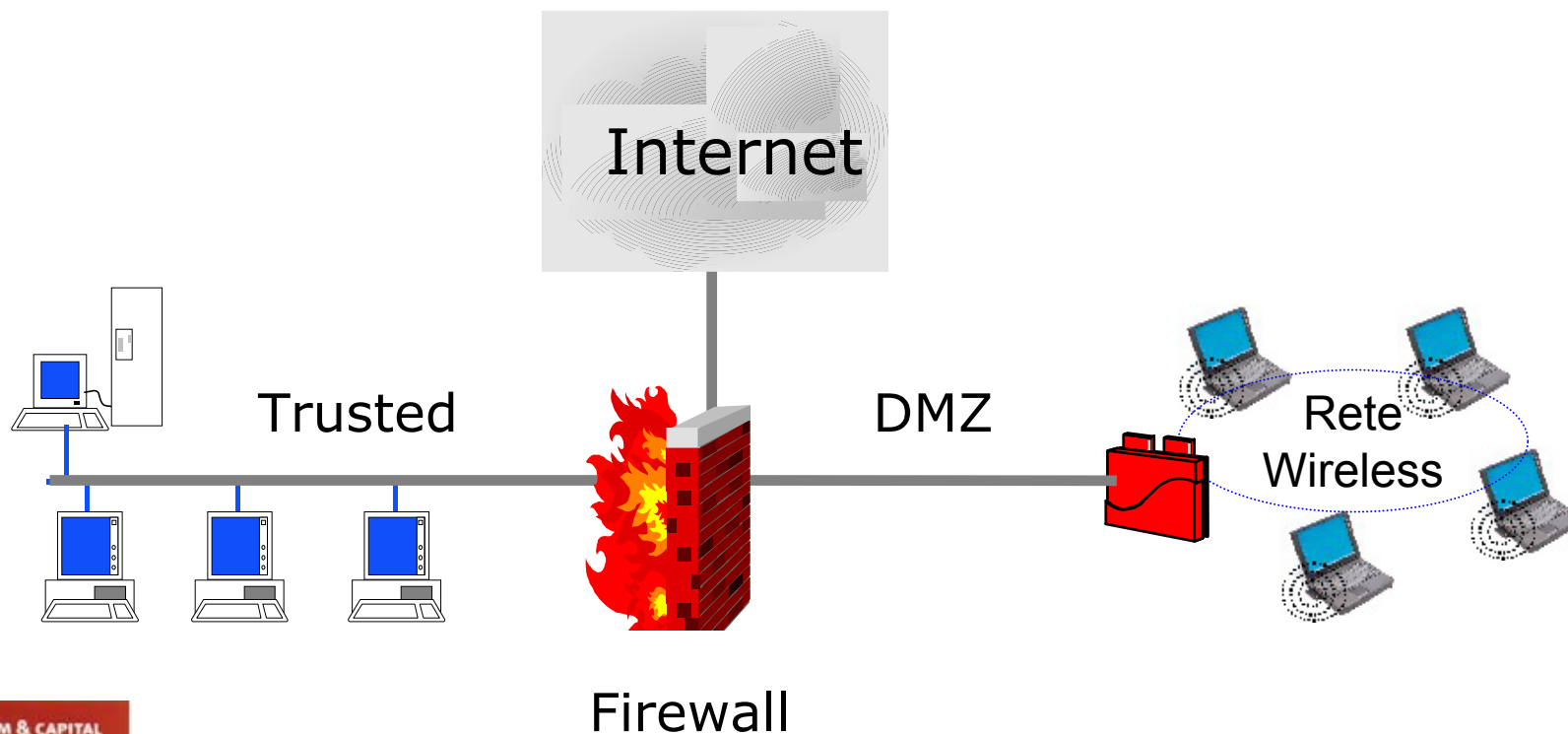
La mancanza di uno strumento IDS wireless porta alla necessità di uno scan periodico manuale dello spazio aziendale con software di Wireless sniffing il quale è in grado di rilevare gli Access Point ed in congiunzione con un GPS dare la loro esatta posizione



Security Assessment & Auditing

Monitoraggio del firewall e dell' IDS

Continuo monitoraggio 24x7 del firewall, e dei suoi file di log per la verifica del rispetto delle policy e la eventuale identificazione di attività sospette nel network



Sicurezza nelle Wireless Lan

Conclusioni

Le Wireless LAN vanno trattate come una rete insicura

Gli indiscussi benefici di mobilità, scalarità ed economicità delle installazioni devono essere subordinati alle esigenze di sicurezza

Utilizzare sicuramente le Wireless LAN a fronte di una corretta installazione e pianificazione della stessa