

# Gestione sicura di una rete wireless

**Alessandro Berta**

Technical Manager

[a.bertha@elmat.com](mailto:a.bertha@elmat.com)





## Tecnologie wireless di successo

- Ad oggi, per la realizzazione di una rete di comunicazioni digitali wireless possiamo pensare di basarci su tecnologie di successo più o meno mature:

1. sistemi aperti WiFi (IEEE 802.11,b,g,a)



2. sistemi proprietari basati su ETSI HiperLAN



3. sistemi aperti WiMAX (IEEE 802.16)



- Ogni tecnologia offre vantaggi e svantaggi in termini di prestazioni, sicurezza ed economicità.
- Andremo ad analizzare gli aspetti della sicurezza.



# Reti Private e ad Accesso Pubblico

- Le reti di telecomunicazioni wireless possono inoltre essere divise in due categorie:

- Reti ad Uso Privato
- Reti ad Accesso Pubblico

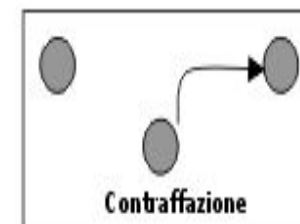
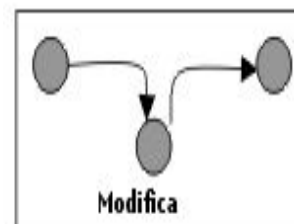
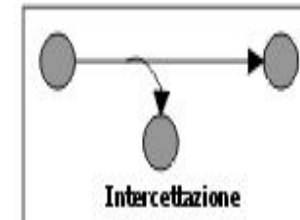
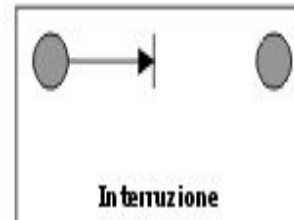
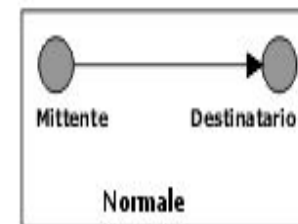


- Gli utilizzatori delle reti sono diversi.
- Le problematiche di sicurezza sono differenti.
- E' consigliabile l'utilizzo di tecnologie e prodotti differenti.

# Sicurezza di una trasmissione

Quali sono i principali problemi di sicurezza in una trasmissione?

- ❶ **Interruzione:** jamming, DoS
- ❷ **Intercettazione**
- ❸ **Alterazione:** integrità, Man in the middle
- ❹ **Contraffazione:** autenticazione mittente



Analisi di un attacco



## Requisiti sicurezza Rete Privata

- La Rete Privata è topologicamente ben definita e scarsamente variabile nel tempo.
- Non e' richiesto che nuovi elementi si possano inserire acquistando autonomamente i propri terminali
- Ci sono minori complessità per l'autenticazione in quanto i nodi sono noti a priori.
- Sono molto importanti gli aspetti legati alla non intercettabilità (cifatura forte) ed alla impenetrabilità.





## Requisiti sicurezza Rete Pubblica

- In una rete wireless destinata all'accesso del maggior numero possibile di utenti il sistema deve essere più "aperto".
- Si pretende facilità di connessione, nessuna barriera legata all'HW, standardizzazione.
- L'attenzione si deve quindi concentrare sull'autenticazione dell'utente.





## Rete Privata realizzata con WiFi

- Ci sono indubbiamente vantaggi in economicità.
- Il meccanismo di sicurezza attualmente disponibile è il WiFi Protected Access (WPA)
- Il WPA aggiunge al WEP un miglioramento della cifratura (TKIP) ed un'autenticazione più forte nelle sue due versioni:
  1. Pre-shared key
  2. infrastruttura 802.1x (server autenticazione esterno)
- Gli svantaggi sono legati alla larghissima diffusione di apparati WiFi ed alla scoperta di una **vulnerabilità nel WPA.**





## Vulnerabilità del WPA

- In un articolo di Seth Fogie apparso a Marzo su [ciscopress.com](http://ciscopress.com) si dimostra una debolezza del WPA con Pre-Shared Key
- Si tratta della possibilità di effettuare un attacco dizionario brute-force con un tool di crack chiamato **CoWPAtty**
- Se la Pre-Shared Key è una password comune, con poca entropia, i tempi di successo sono ragionevoli, **simili a quelli del WEP**.
- La vulnerabilità è assente nel WPA con server di autenticazione esterno 802.1x (canale criptato di scambio chiavi)





## Reti private ed 802.1x

- L'infrastruttura 802.1x prevede un server di autenticazione esterno all'apparato wireless, tipicamente RADIUS.
- Nelle reti private wireless la presenza di un server RADIUS è poco comune, a causa dei costi e della gestione non banale.
- Soprattutto per link semplici (es. collegamento Punto-Punto) appare soluzione eccessivamente complessa e dispendiosa.





## WiFi non è soluzione ideale

- **Riassumendo, per realizzare una rete privata wireless, che risulti il più possibile inaccessibile, la tecnologia WiFi non è la soluzione ideale:**
  - 1. Hardware è abbondantemente disponibile**
  - 2. Interoperabilità tra brand diversi**
  - 3. WPA-PSK non sicuro se password "debole"**
  - 4. WPA-802.1x sicuro ma ha costi maggiori e gestione complessa per reti medio-piccole.**





## I sistemi wireless HiperLAN

- Nel mercato sono disponibili sistemi wireless basati su **ETSI HiperLAN**
- Sono gli unici autorizzati per uso privato in outdoor nella banda 5.4 GHz.
- Il leader del mercato italiano è Alvarion con i prodotti:
  - ✘ BreezeNET B: Punto-Punto
  - ✘ BreezeACCESS VL: Punto-Multi-Punto
- Altri 4-5 vendor sono presenti con apparati più o meno similari.





## Reti private con HiperLAN?

- Sono sistemi dotati di meccanismi di sicurezza forti e senza interoperabilità.
- Per poter accedere ad una rete HiperLAN è necessario avere apparato della stessa marca e modello.
- Gli apparati sono più costosi e molto meno diffusi di quelli WiFi: 1° grado di sicurezza intrinseca.
- Nei sistemi HiperLAN autenticazione e non intercettabilità sono basati sull'algoritmo di cifratura a blocchi **AES** con Pre-Shared key.
- AES è molto più potente dell'RC4 con TKIP usato nel WPA.
- La vulnerabilità del WPA-PSK non è sfruttabile.





## Reti private ed HiperLAN

- Non è quindi necessario prevedere un server esterno per autenticazione forte.
- Inoltre le prestazioni funzionali di HiperLAN sono decisamente superiori ai sistemi WiFi:
  - ✗ maggiore copertura e distanze (1 Watt e.i.r.p.)
  - ✗ maggiore capacità (n° canali 5.4 GHz)
  - ✗ link in condizioni Non-Line-Of-Sight
- Questo unito all'elevato grado di sicurezza fanno preferire HiperLAN al WiFi per realizzare una rete wireless ad uso privato.





## WiMAX e le Reti private

- WiMAX promette di essere la prossima rivoluzione nel wireless digitale
- La tecnologia IEEE 802.16/ETSI HiperMAN è superiore in prestazioni a WiFi ed HiperLAN.
- La parte security è garantita da architettura basata su **certificati X.509** assegnati alle Unità Client (CPE).
- Con il certificato si criptano in 3DES alcune Traffic Key, diverse per ogni singola CPE.
- Dalle Traffic Key si generano delle chiavi temporanee a 128 bit per la cifratura RC4 dei dati.
- Il sistema sembra essere ad oggi esente da vulnerabilità.





## WiMAX e le Reti private

### Ma i sistemi WiMAX sono adatti per le Reti private?

- WiMAX inizialmente sarà solo su banda licenziata 3.5 GHz.
- WiMAX è architettura classe operatore, con Stazioni Radio Base molto costose.
- L'interoperabilità tra vendor è uno svantaggio e non un elemento positivo dal lato della sicurezza della Rete Privata.
- La differenza di prestazioni radio (copertura radio, throughput, NLOS) tra HiperLAN e WiMAX non è abissale.





## Confronto prestazioni HiperLAN vs. WiMAX

- Confrontiamo i prodotti Alvarion, già presente sul mercato con sistemi sia WiMAX che HiperLAN:
  - ✘ BreezeACCESS VL      HiperLAN 5.4 GHz
  - ✘ BreezeMAX 3500      IEEE 802.16 3.5 GHz
- Il confronto viene fatto con calcolo teorico del Link Budget sotto le seguenti ipotesi comuni:
  1. Clear Line Of Sight tra le antenne
  2. Tx Power = 30 dBm (1 Watt) EIRP
  3. Fade Margin 10 dB
- Si evidenzia un raddoppio di prestazioni, ma non un miglioramento di uno o più ordini di grandezza





Cabling & networking distribution. **People always on.**



## Rete Privata sicura ed efficiente

Dalle considerazioni fatte finora, si evince che tra le 3 tecnologie trattate, **HiperLAN** ad oggi offre il miglior "trade off" tra:

1. Sicurezza
2. Prestazioni
3. Costi
4. Semplicità gestione

per realizzare Reti wireless ad Uso Privato.





## Reti per Accesso Pubblico

- In Italia si possono realizzare solo Hot Spot in aree confinate a “frequentazione pubblica” e reti di Accesso radio dietro conseguimento di una licenza di sperimentazione.
- Le reti dedicate all’accesso da parte di grandi bacini di utenza devono tendenzialmente sfruttare tecnologie di larga diffusione:
  - ✗ standardizzazione
  - ✗ economicità
- WiFi risponde bene a questi requisiti.






## Quale tecnologia per reti aperte?

- Infatti fino ad oggi ci si è basati su WiFi (802.11b,g) nelle sue varie versioni per realizzare gli Hot Spot.
- All'estero (USA, UK, Francia, Spagna,...) si sono realizzate anche reti Broadband Wireless Access sempre con tecnologie WiFi-based.
- I sistemi HiperLAN, pur avendo prestazioni migliori, hanno il limite della mancanza di interoperabilità tra vendor.
- HiperLAN non appare una soluzione percorribile per una rete aperta.





## WiMAX per reti ad Accesso Pubblico

- IEEE 802.16 è il nuovo paradigma del Broadband Wireless Access:
  1. Alta capacità di trasmissione
  2. Copertura: buone prestazioni NLOS
  3. Interoperabilità: certificazione WiMAX Forum 
  4. Larga diffusione futura dei client: chipset by INTEL in milioni di pezzi.
- Si tratta di un'architettura Carrier-class, non alla portata di tutti.
- In Italia **WiMAX è bloccato** in attesa di evoluzioni della normativa o degli apparati (nuove frequenze di funzionamento).





## Gestione sicura del WiFi

- WiFi unica tecnologia in Italia per Hot Spot ed Accesso aperto.
- Necessaria autenticazione forte degli utenti.
- WPA-PSK non garantisce livello adeguato sicurezza: serve una struttura addizionale
- Nella prossima presentazione verrà proposta **un'alternativa alla classica soluzione RADIUS-based.**
- La Gestione sicura della rete wireless WiFi può venire operata da un:

**CLAVISTER Security Gateway**





# Gestione sicura del WiFi

**Grazie per l'attenzione!**

**Passo la parola a...**

**Nicola Sotira**

**CLAVISTER**

