L’arte dell’intercettazione e dello sniffing

Giuseppe Augiero

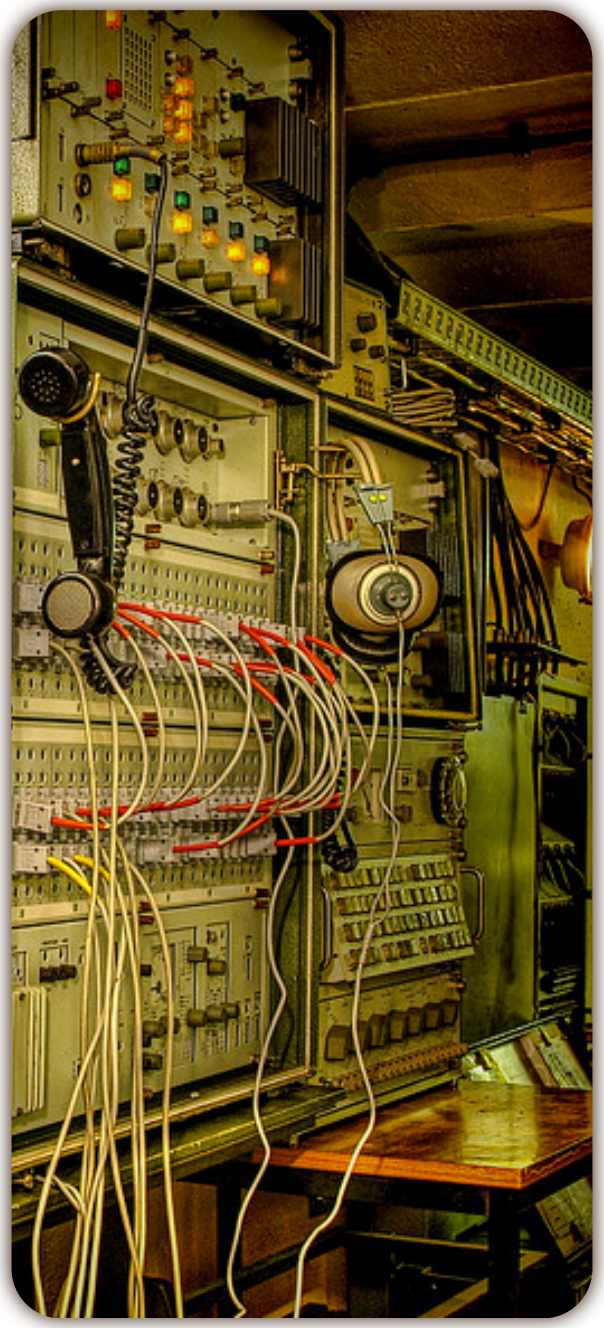
23 ottobre 2010 - Linux Day 2010 - Dipartimento di Informatica dell’Università degli Studi di Pisa - Gulp Gruppo Utenti Linux Pisa

Disclaimer

- Il seguente materiale ha scopo unicamente didattico.
- L'intercettazione è un reato punibile penalmente.
- Lo scopo di questo seminario è far conoscere quali siano le tecniche da adottare per aumentare il proprio grado di sicurezza e proteggere la propria privacy.
- Qualsiasi altro utilizzo è vietato. L'autore non si assume alcuna responsabilità per usi impropri.

Intercettazione

- Nel gergo telematico per intercettazione si intende l'operazione di cattura di un segnale analogico o digitale che trasporta una comunicazione tra un sorgente e un destinatario.
- Intercettare non significa decodificare.



L’informazione

- “ Riuscire ad accedere alle comunicazioni, oggi, significa accedere alle vita delle persone...”

Motivi

- Le motivazioni di una intercettazione possono essere diverse.
  - intercettazioni per motivi legislativi.
  - intercettazioni criminali.
  - intelligence.
  - attività di management.
  - attività di studio/ricerca.

Tecniche

- Le tecniche che andremo ad analizzare si basano tutte sul concetto di “Man in the middle”.

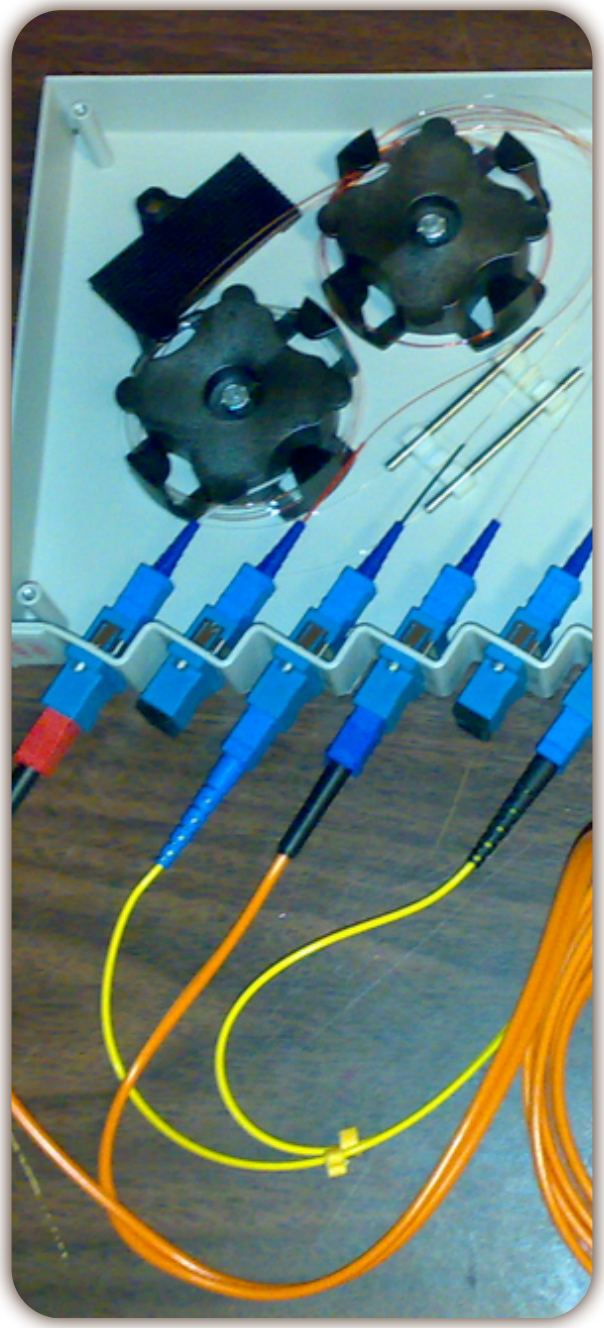
Il mezzo fisico

Il rame

- La comunicazione avviene attraverso la propagazione di un segnale elettrico.
- La cattura del segnale è alquanto semplice e non richiede particolare strumentazione.

La fibra ottica

- Nel cavo in fibra ottica il fotone trasporta l'informazione.
- Occorrono tecniche più sofisticate del rame per catturare il segnale.



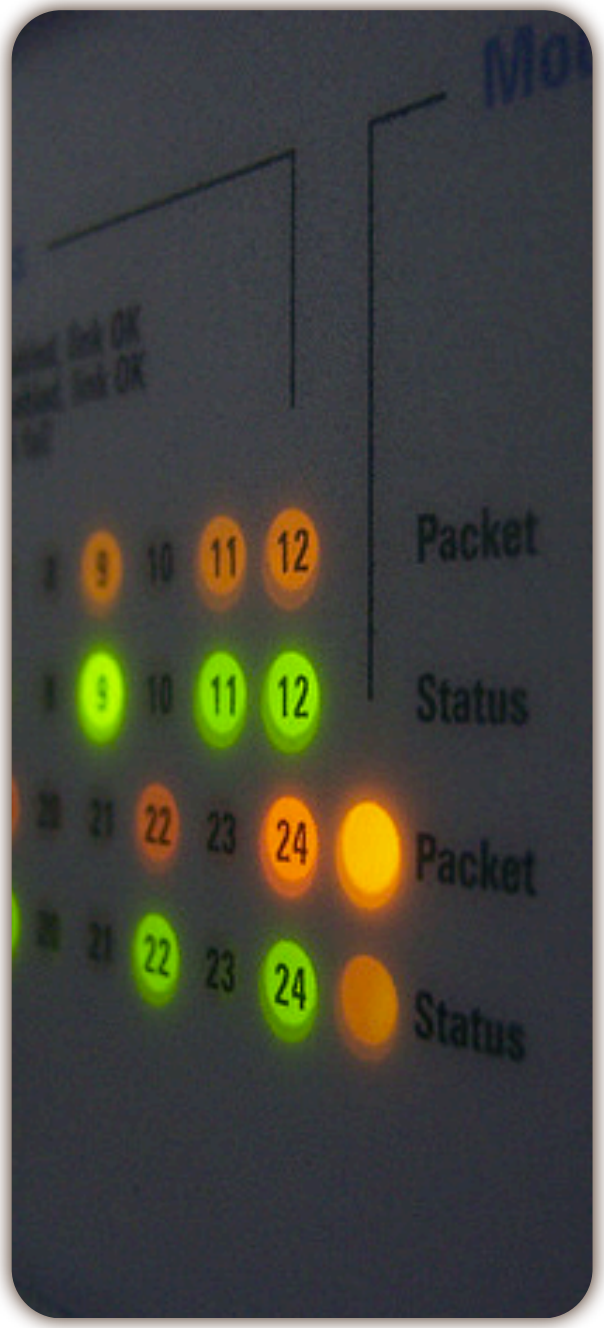
L’etere

- I sistemi wireless utilizzano onde radio a bassa potenza.
- La comunicazione può essere intercettata catturando le onde trasmesse.
- Attenzione al rumore.

I protocolli e il datalink

Ethernet

- Ingredienti per lo sniffing:
  - Tap o porta switch in SPAN.
  - Personal computer con porta ethernet.
  - Software di analisi.
  - Sistema in bridge (opzionale).

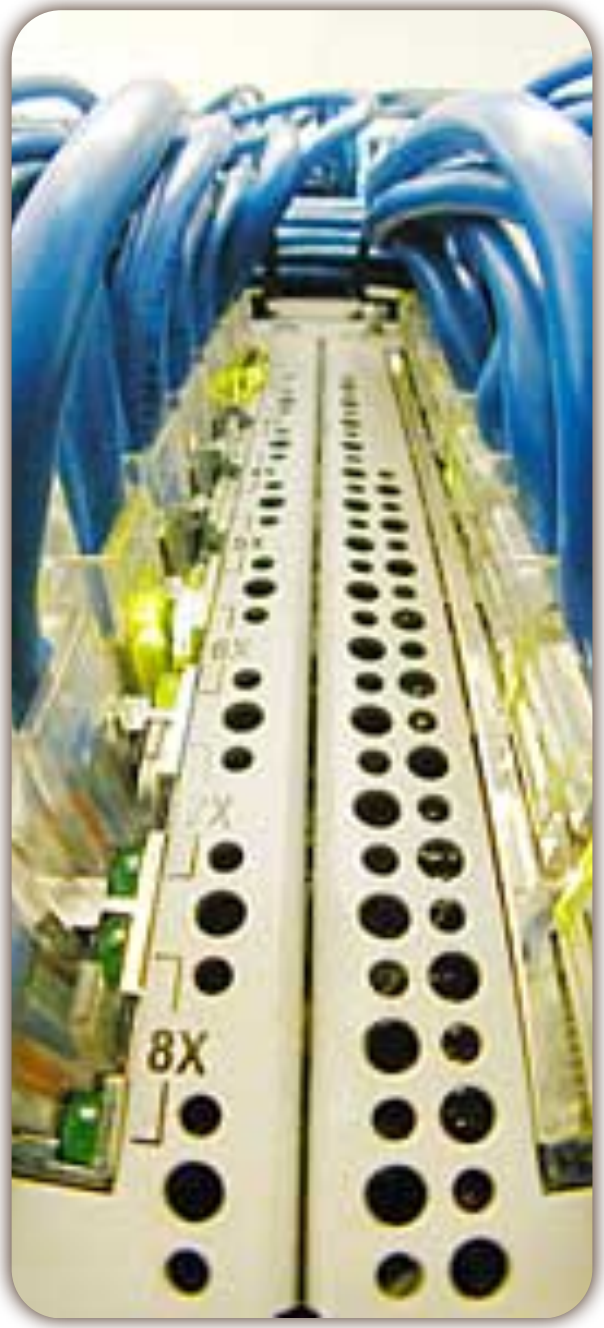


Telefonia fissa

- Bastano due coccodrilli e un telefono per poter “ascoltare” una telefonata.
- La situazione si complica se la linea utilizza il protocollo ISDN, ma con gli strumenti giusti si riesce a sniffare la comunicazione.

Dsl

- Il segnale dsl che transisa su doppino telefonico può essere catturato attraverso un “Tactical Adsl Probe”.
- Due modalità operative: Bridge o Trasparent mode.



Bluetooth

- Un penna bluetooth, un pc e un po' di software open source bastano per catturare il traffico.
- Requisito fondamentale: essere molto vicini alla sorgente di trasmissione.

GSM (I)

- Con hardware dal costo relativamente basso (circa $ 1.500) è possibile catturare il traffico di un telefonino gsm.
- Il traffico è cifrato attraverso il protocollo A5/3 e quindi non immediatamente decifrabile.
- Quest'attività è illegale e quindi non va eseguita.

GSM (II)

- Tipicamente gli uplink delle bts trasmettono in chiaro.
- La situazione cambia completamento con lo standard 3G o LTE.

Onde convogliate

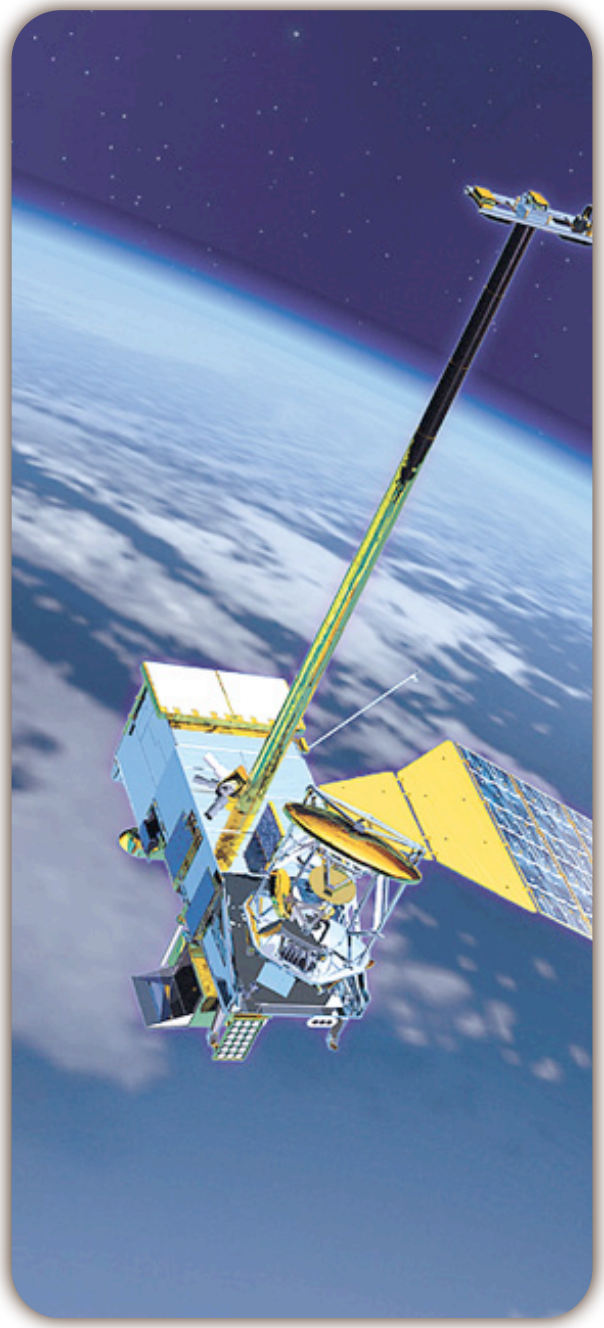
- Un qualsiasi apparato powerline configurato ad hoc posizionato sullo stesso impianto elettrico dei dispositivi che si vogliono analizzare permette di catturare il traffico dati.
- Molti dispositivi ad onde convogliate non supportano la crittografia o la crittografia è debole (56 bit).
- I contatori Enel dovrebbero funzionare da filtro per le comunicazioni powerline.

Wifi

- La cattura del traffico wifi (e non la decodifica) è ormai diventato un gioco da ragazzi.
- Occorre possedere un personal computer dotato di scheda wireless configurata in “Monitor mode” e del software ad hoc.
- Fake access point e Ap Rouge.

Il satellite

- Comunicazione di tipo broadcast.
- La decodifica può non essere possibile.
- Canali uplink e di servizio trasmettono in chiaro.



Applicazioni

Spyware

- Se non è possibile attaccare la comunicazione, soprattutto per quanto riguarda la sua decodifica, è magari molto più semplice attaccare uno dei due interlocutori.

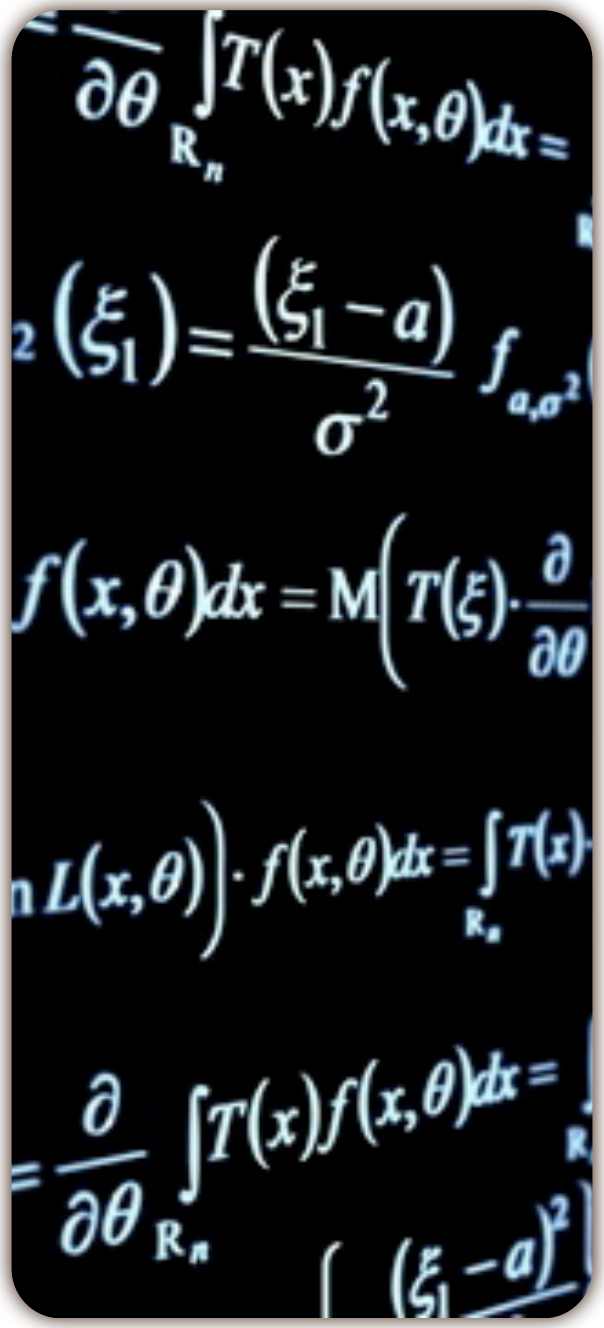
Evitare lo sniffing

Privacy

- E’ fondamentale tutelare la propria privacy.
- Proteggere i propri dati non è sinonimo di voler nascondere qualcosa di illegale.
- Non sappia in che mani possono finire le nostre informazioni.

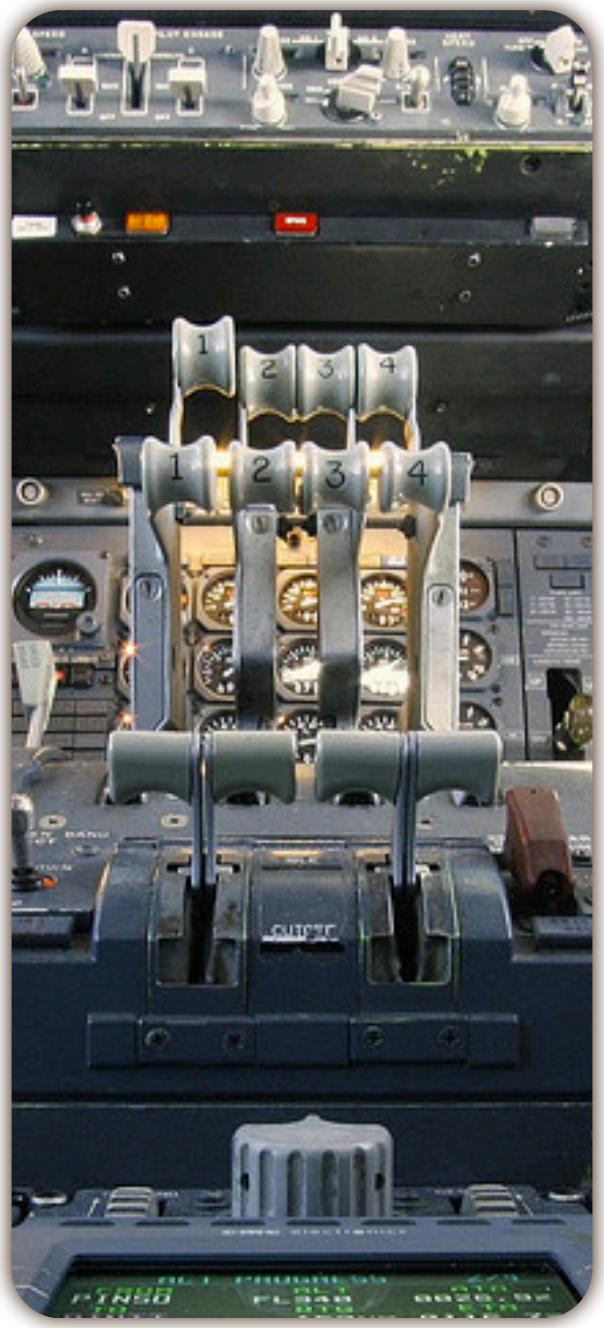
Crittografia

- Un buon metodo per proteggere i propri dati può quello di utilizzare la crittografia.
- In questo modo non evitiamo lo sniffing ma almeno non permettiamo la decodifica dei dati.
- La crittografia richiede che anche il destinatario del messaggio supporti lo stesso algoritmo crittografico.



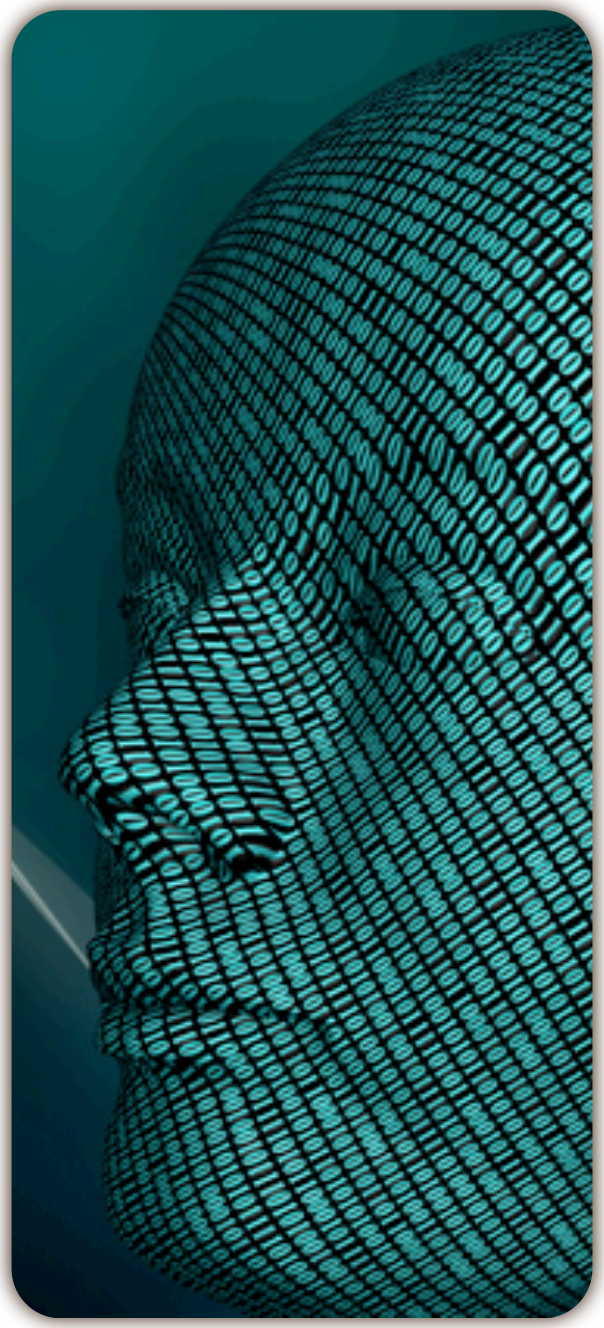
Analogico e Digitale

- Scrambling o Encryption?
- Connessione analogica o connessione digitale?
- Segnalazione inbound o outbound?



Security Model

- End to End security.
- End to Site security.
- Mixed setup.



Open vs Closed

- Attenzione agli algoritmi di cifratura utilizzati.
- Gli algoritmi più robusti sono quelli pubblici.
- Diffidate della bontà di algoritmi proprietari.

Domande? -> Risposte!

Giuseppe Augiero

Email: giuseppe at augiero.it

Web: www.augiero.it

Grazie

www.augiero.it