

L'arte dell'intercettazione e dello sniffing

Giuseppe Augiero

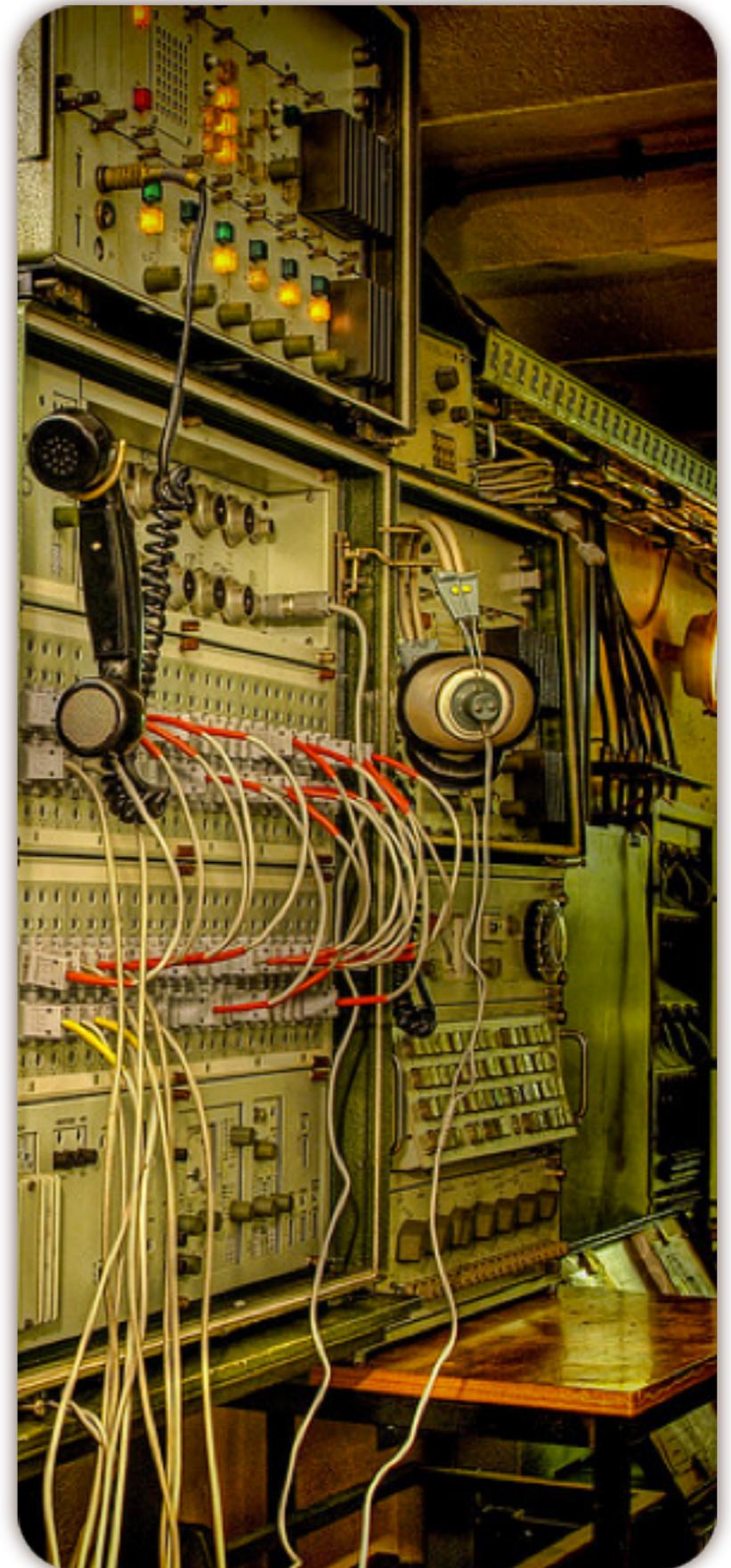
9 dicembre 2010 - Corso "La comunicazione efficace"



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.

2/12



Motivi

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

3/12



Il rame

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

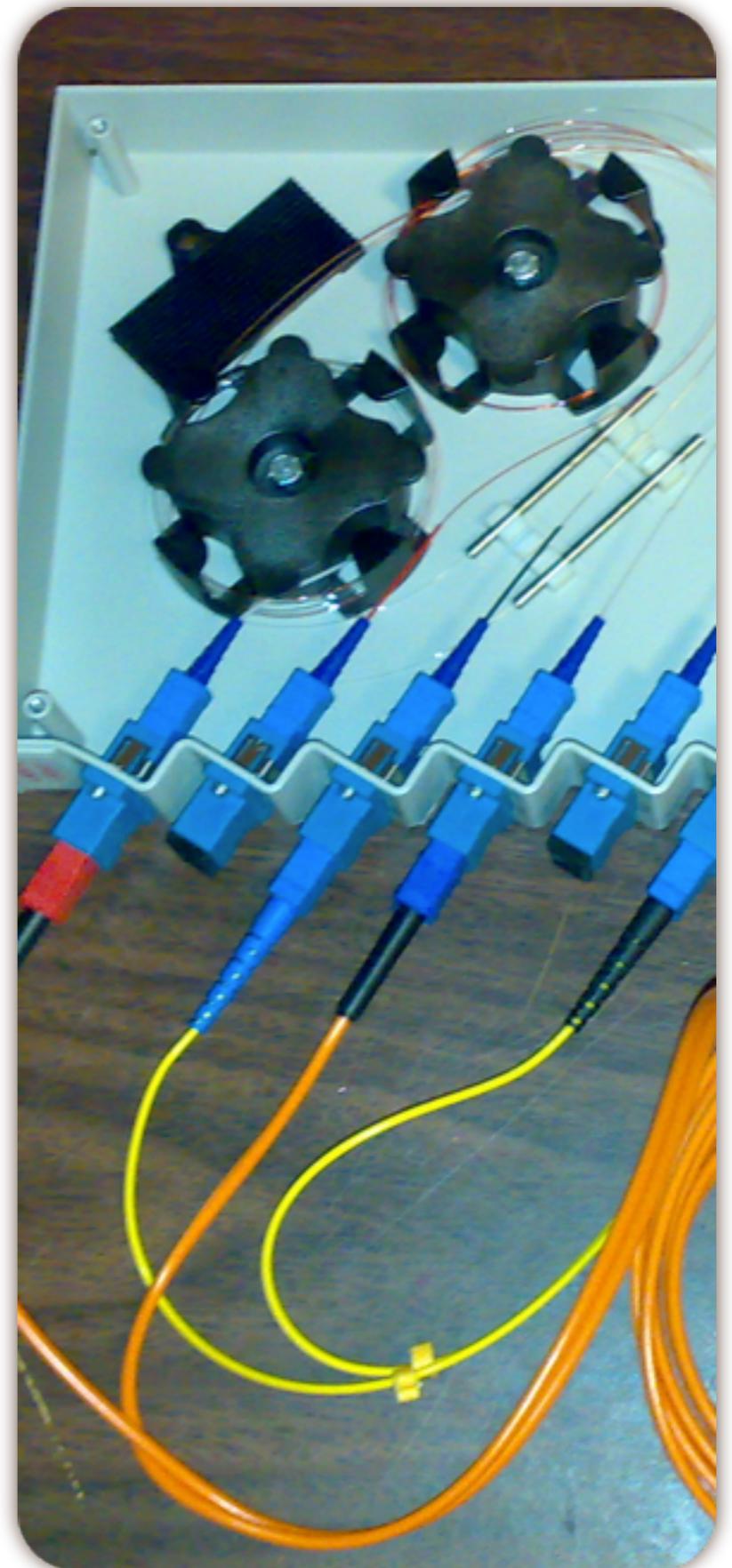
4/12



La fibra ottica

- Nel cavo in fibra ottica il fotone (la luce) trasporta l'informazione.
- Occorrono tecniche più sofisticate del rame per catturare il segnale trasportato da una f.o.

5/12



L'etere

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

6/12



Telefonia fissa

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

7/12



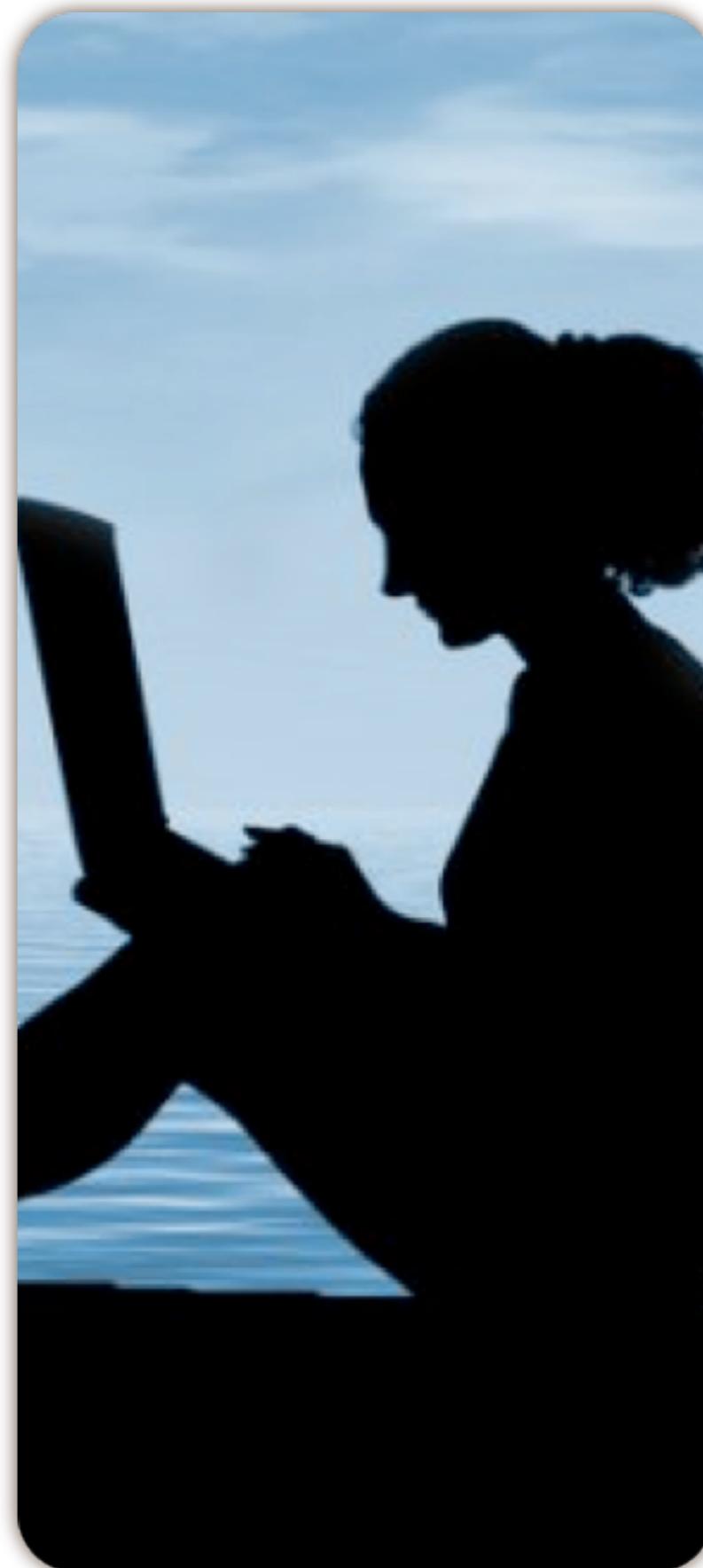
GSM

- Il traffico cellulare (GSM) può essere catturato con hardware dal costo relativamente basso (circa \$ 1.500).
- La comunicazione è cifrata attraverso un protocollo di sicurezza (A5/3) e quindi non immediatamente decifrabile.
- Quest'attività è illegale e quindi non va eseguita.



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.



Privacy

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



Crittografia

- Un buon metodo per proteggere i propri dati può essere quello di utilizzare la crittografia.
- In questo modo non eviteremo l'intercettazione ma almeno non permetteremo la decodifica dei dati.
- La crittografia richiede che il destinatario del messaggio supporti lo stesso algoritmo di cifratura.

11/12

The image shows a collage of mathematical formulas on a dark background. The formulas include:

- $\frac{\partial}{\partial \theta} \int_{\mathbb{R}^n} T(x) f(x, \theta) dx =$
- $f(\xi_1) = \frac{(\xi_1 - a)}{\sigma^2} f_{a, \sigma^2}$
- $f(x, \theta) dx = M \left(T(\xi) \cdot \frac{\partial}{\partial \theta} \right)$
- $\left(L(x, \theta) \right) \cdot f(x, \theta) dx = \int_{\mathbb{R}^n} T(x)$
- $= \frac{\partial}{\partial \theta} \int_{\mathbb{R}^n} T(x) f(x, \theta) dx =$
- $\left[\frac{(\xi_1 - a)^2}{\sigma^2} \right]$



Grazie

Giuseppe Augiero

Email: [giuseppe @ augiero.it](mailto:giuseppe@augiero.it)

Web: www.augiero.it