WiFi
Quanto è sicuro?

Paolo Giardini

Magione, Linuxday 2017

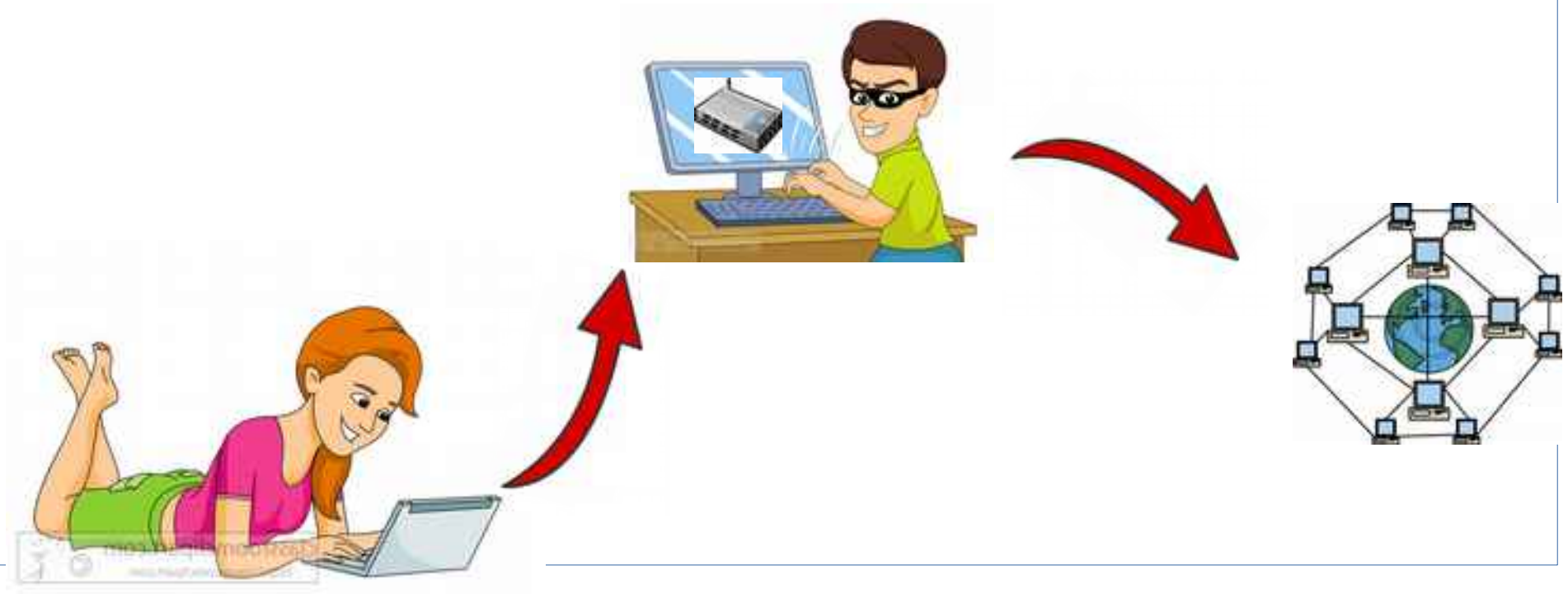
Rischi del WiFi

- E’ possibile trovare Access Point **aperti: pericolo!**
- Protetti con cifratura **WEP** (wireless equivalent privacy): **inutile!**
- Protetti con cifratura **WPA** o **WPA2** (WiFi protected access).
  - Difficile ma non impossibile da bucare, soprattutto se si usano password deboli (attacco dizionario o brute force)
- Problema: tutto il traffico è via radio, quindi **intercettabile!**
- **Client Isolation**: configurazione dell’access point *legittimo* che isola le comunicazioni di ciascun utente impedendo di fatto lo sniffing. **Indispensabile!**

- Rischi:
  - **Fake Access Point**
  - **Man in the Middle**
  - **Sniffing**

Rogue AP attack

1) l’attaccante crea un falso access point
2) la vittima crede di connettersi ad un Access Point legittimo
3) l’attaccante può intercettare tutto il traffico



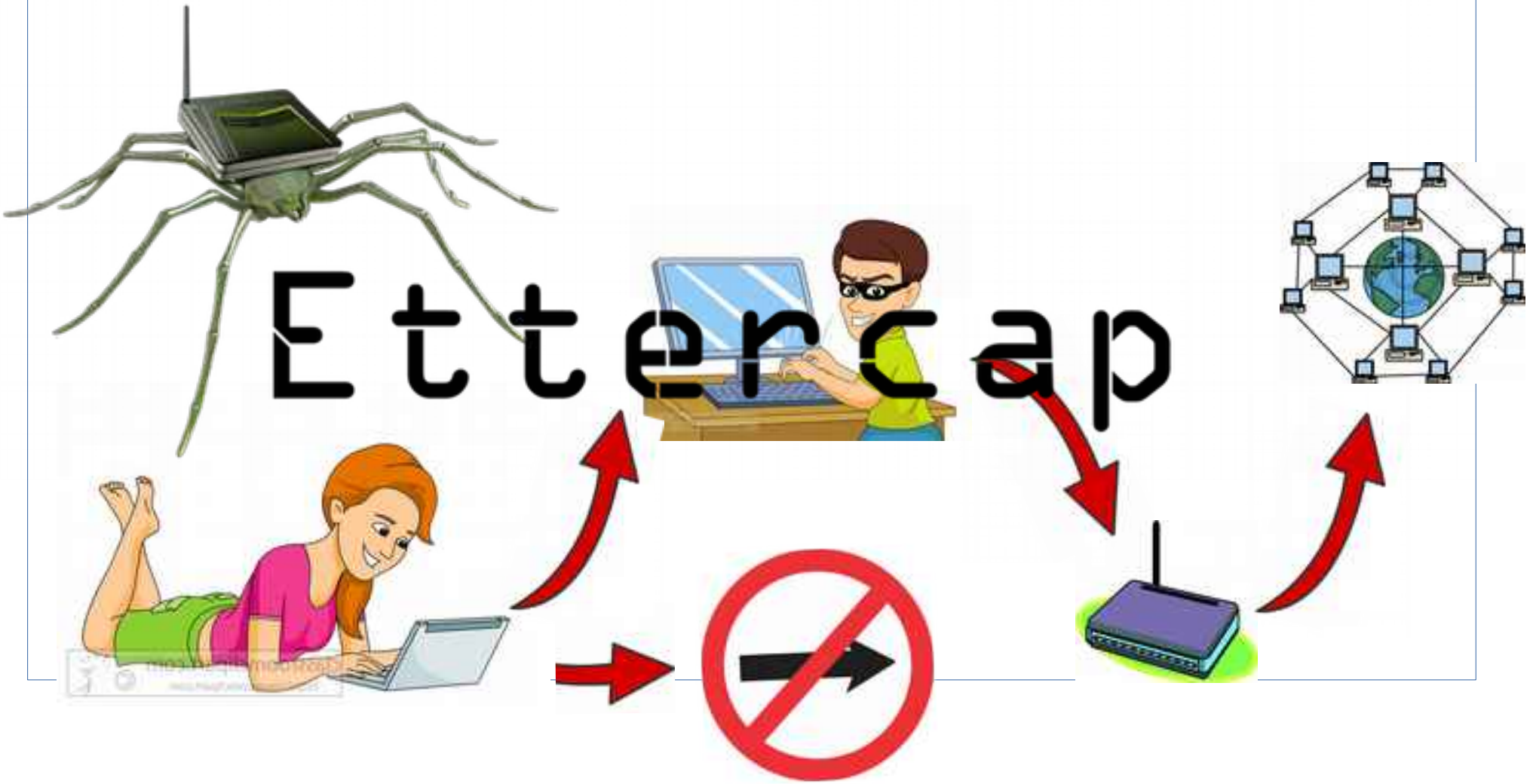
MitM attack

Attacco MITM (Man In The Middle)
Funziona con un Fake Access Point oppure con un access point legittimo ma al quale l'attaccante riesca a connettersi (è aperto o conosce la chiave)

1) l'attaccante individua la vittima ed il gateway
2) sostituisce il suo pc al gateway legittimo (ARP poisoning)
3) la vittima naviga normalmente
4) l'attaccante può intercettare tutto il traffico

MitM attack

Vediamo ora un esempio pratico con ETTERCAP, uno strumento Italiano



Domande?

STUDIO GIARDINI
www.solution.it

paolo.giardini@solution.it

Studio Giardini

SICUREZZA INFORMATICA

Tel.+(39) 337-65.28.76 – 02-006.10.235
Fax +(39) 075 9383 1174
email: studio.giardini@solution.it

creative commons

BY NC ND

http://www.solution.it
http://blog.solution.it