CYBER SECURITY

La Crittografia

CIFRARE ?

IPsec supporta due modalità di funzionamento:

- *Transport mode*
  - connessione **host-to-host**;
  - usato dagli end-point, non dai gateway;
  - in caso di cifratura, viene cifrato solo il payload dei datagrammi IP, non l'header;
  - computazionalmente leggero;
  - ogni host che vuole comunicare deve avere tutto il software necessario ad implementare IPsec;
  - si aggiunge solo l'header IPsec; gli indirizzi mittente e destinatario degli end-point sono rilevabili.
- *Tunnel mode*
  - connessione **gateway-to-gateway**;
  - in caso di cifratura, viene cifrato tutto il pacchetto IP originale;
  - utilizzato per realizzare le **VPN**;
  - computazionalmente oneroso;
  - solo i gateway devono avere il software IPsec;
  - si hanno punti di centralizzazione, quindi single point of failure;
  - utilizza un doppio incapsulamento

La DIFESA... Dati: Crittografia

- Molte aziende che gestiscono i dati degli utenti sono solite cifrarli. Le banche, ad esempio, spesso cifrano i propri siti con certificati SSL e TLS. ➔ **HTTPS**
- Ricordate però, i metodi crittografici proteggono **solo le vostre comunicazioni**. Una volta che i vostri dati si trovano sul server di un'azienda, potrebbero essere vulnerabili agli attacchi sulla rete aziendale.

La DIFESA... Dati: Crittografia

- È utile inoltre sapere che le chiamate su Skype sono cifrate al 100%, purché siano fatte al 100% su Skype. Ma se si chiama da Skype un normale numero telefonico, il collegamento a PSTN (rete telefonica ordinaria) non sarà cifrato. Questo potrebbe permettere a qualcuno di intercettarvi. È possibile sfruttare la crittografia anche per i messaggi su Facebook, selezionando "Conversazioni segrete" da smartphone iPhone o Android, ma non da PC o laptop.

- Uno dei motivi per cui WhatsApp è diventato così famoso è la sua crittografia end-to-end dei messaggi. Anche altre app offrono la crittografia dei messaggi, ma non la attivano in modo predefinito. In tal caso, cercate l'impostazione per attivarla. Perché mai non dovreste farlo?

La DIFESA... Dati: Crittografia

- Skype : comunicazioni cifrate al 100%, purché siano fatte al 100% su Skype. Ma se si chiama da Skype un normale numero telefonico, il collegamento a PSTN (rete telefonica ordinaria) non sarà cifrato.

- Uno dei motivi per cui WhatsApp è diventato così famoso è la sua crittografia end-to-end dei messaggi.
- Anche altre app offrono la crittografia dei messaggi, ma **non la attivano in modo predefinito**. In tal caso, cercate l'impostazione per attivarla. Perché mai non dovreste farlo?

La DIFESA... Dati: Crittografia

- Considerate anche l'utilizzo di **Tor**, un browser anonimo e cifrato, che impedirà alla vostra cronologia di ricerca di venire tracciata.
- I giornalisti investigativi lo usano spesso, così come le ONG che lavorano in ambienti ostili.
- Tuttavia, Tor **non è completamente sicuro**: è noto che vi si possano prendere dei malware ed è comunque **vulnerabile** agli attacchi **"man in the middle"**.