introduction to computer security

definizione

è un **processo**, ovvero una serie di azioni che rendono la rete sicura. La sicurezza deve essere garantita in tutti gli aspetti del sistema, dal livello fisico alla gestione degli utenti. 6 temi per i quali garantire sicurezza:

- data availability
- data authentication
- data integritu
- secrety of data (confidentiality)
- access control
- anonimity

service availability

il servizio deve essere sempre disponibile. Quando la disponibilità è violata, significa che si è vittimi di un attacco **DoS** (Denial of Service). Garantire la disponibilità è difficile, ci sono dei limiti fisici, l'attaccante tenterà di saturarli. L'obiettivo è quindi quello di rendere questo tipo di attacchi più costosi possibile per gli attaccanti.

data confidenciality/secretcy

i dati scambiati devono essere privati e non devono essere letti da nessuno all'interno della comunicazione. Le reti Ethernet permettono lo *sniffing* dei pacchetti degli altri computer. Per poter garantire la confidenzialità dei dati, è necessario adottare tecniche di **Encryption**

data integrity

i dati inviati devono raggiungere la destinazione senza essere modificati. L'integrità dei dati è ottenuta grazie a meccanismi di **hashing**.

authentication

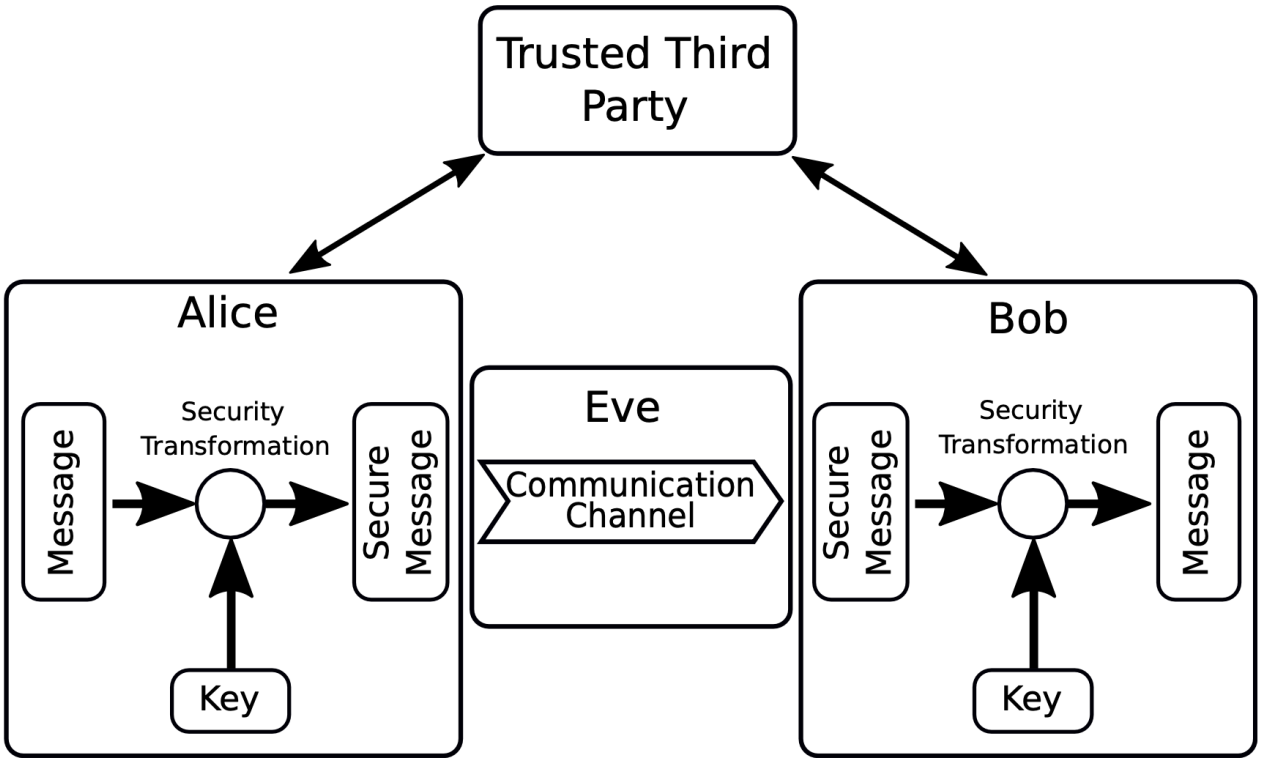
è possibile dividere l'autenticazione in 2 categorie:

- **data origin authentication**: bisogna assicurarsi che le informazioni inviate provengano effettivamente da chi dice di averle indicata.
- **peer entity authentication**: chi riceve l'informazione deve assicurarsi che la sorgente del mittente sia quella che ci si aspetta l'autenticazione è ottenuta grazie a meccanismi di **firme digitali**.

access control

l'accesso al servizio deve essere limitato solo alle persone autorizzate.

system model



questa astrazione è possible usarla per qualsiasi sistema dove hai:

- un mittente e un destinatario
- un nemico che tenta di attaccare il sistema

encryption in transit vs E2E encryption

Fig. 1a: Encryption in transit

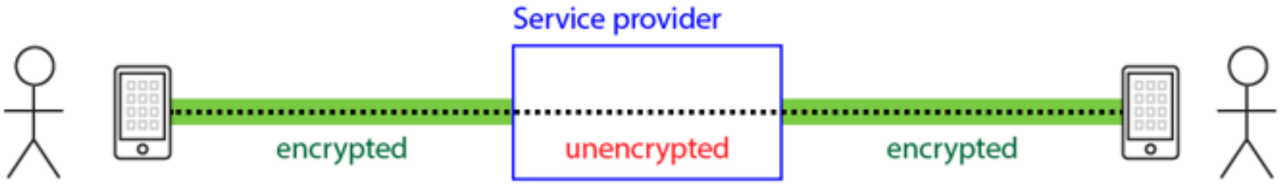


Fig. 1b: End-to-end encryption