


Segretezza (confidenzialità)


Nota la policy su chi debba conoscere l'informazione, la segretezza è facile da definire. Si dice anche che "la policy è applicata". Grazie alla critto-analisi moduli la robustezza dei critto-sistemi.

 **Domanda d'esame:** Cosa significa rompere un crypto-sistema, ovvero fare crypto-analisi?

Esempio di risposta: dedurre i contenuti di un crypto-testo, pur non conoscendo la chiave per decrittarlo.

Autenticazione

Autenticare significa **riconoscere**. Il riconoscimento presuppone di avere già a disposizione un campione o template, con cui confrontare poi il nuovo input.

 **Domanda d'esame:** a chi fa comodo l'autenticazione?

Esempio di risposta: fa comodo ad entrambi gli attori in gioco, l'utente ed il sistema con cui esso vuole interagire. Chi si autentica tutela il proprio spazio da altri, chi autentica tutela i propri servizi ed è allineato alle normative.

Alcune misure di autenticazione

- **conoscenza** (password, PIN)
- **possesso** (smart card e smart token)
- **biometria** (impronte, iride)
 - La biometria può anche essere intesa come una sottocategoria del possesso.

Nessuna di queste misure è infallibile e spesso sono combinate insieme (e comunque fallibili)

Autenticazione e segretezza sono due concetti sommabili ma distinti. Ci si può autenticare ma mostrare ciò che si sta facendo. Quasi sempre è rilevante che **l'utente possa autenticare il sito**. Il sito, per offrire un certo servizio, autentica a sua volta l'utente.

Integrità

Fare in modo che l'informazione non sia stata alterata in maniera indebita (illecita).

Misure per l'integrità:

- **Checksum**
- **Firma elettronica**

Un flusso di bit sarà sempre alterabile. Spesso gli strumenti fatti per garantire l'integrità nelle reti non bastano nei sistemi moderni, questo perché nel tempo **il modello di rischio è cambiato**. Un controllo come quello del checksum risolve i problemi di alterazione "naturale" dei pacchetti, dati magari da interferenze, ma non è una contromisura efficace in presenza di un vero attaccante. La firma digitale invece è più robusta.

Privatezza

Sicurezza e privatezza sono due concetti differenti, seppur spesso confusi. La privacy è un **diritto alla segretezza**. Possiamo distinguere inoltre tra **hard-privacy** e **soft-privacy**.

Misure di privatezza:

- policy e consenso ad esse

Realisticamente oggi le misure di contenimento ed hardenizzazione sono da applicare all'intera catena di fiducia, e non solo ai mezzi di autenticazione ed accesso.

Elenco di lettura

- [Finger vein recognition biometrics](#)
- [Blind injection](#)