# Appunti di Cybersecurity - Lezione 1

## Introduzione generale alla Cybersecurity

La cybersecurity rappresenta una delle aree più complesse, dinamiche e strategiche del panorama tecnologico e sociale contemporaneo. La sua importanza cresce parallelamente alla digitalizzazione delle infrastrutture, dei servizi e dei processi produttivi. Tuttavia, la disciplina è ancora frammentata e difficile da sistematizzare, a causa di motivi storici e della natura interdisciplinare del campo.

### Origini storiche

- Anni '60-'70: sicurezza informatica nasce in ambito militare e scientifico per proteggere mainframe e controllare privilegi utenti.
- Anni '80: diffusione PC e reti locali, focus su protezione sistemi operativi e dati distribuiti.
- Anni '90-inizio 2000: con Internet e TCP/IP si diffondono firewall, antivirus e sistemi IDS.
- Anni 2000: emergono esigenze di protezione delle transazioni, crittografia avanzata e tutela dei dati personali.
- Anni 2010: pervasività di dispositivi mobili, cloud computing e IoT estende la superficie d'attacco a livello globale.

### Frammentazione ed eterogeneità

Il settore è caratterizzato da un ecosistema di soluzioni software, protocolli, standard e normative spesso non interoperabili. Ciò genera vulnerabilità e ostacola modelli di sicurezza condivisi.

### Natura interdisciplinare

La cybersecurity si colloca all'incrocio di:

- Informatica e ingegneria (strumenti tecnici)
- Matematica e crittografia (fondamenti logici)
- Diritto e governance (responsabilità e privacy)
- Scienze sociali e cognitive (comportamenti umani e ingegneria sociale)
- Economia e gestione del rischio (impatti finanziari e strategici)

# L'identità digitale come nucleo centrale della sicurezza

L'identità digitale è il fulcro di ogni meccanismo di autenticazione, autorizzazione e responsabilità nei sistemi. Essa definisce chi può accedere a un sistema, quali azioni può compiere e a chi sono attribuibili le operazioni.

## Concetti chiave

- **Identificatore**: valore univoco per distinguere un'entità digitale (es. nome utente, email, DID blockchain).
- **Attributo**: informazioni associate all'identità, descrivendo ruoli, autorizzazioni o contesto operativo.

## Modelli di architettura

### Architetture decentralizzate

**Centralizzato** Unica autorità gestisce identificatori e attributi (es. Active Directory). Vantaggi: semplicità di gestione. Svantaggi: punto unico di fallimento.

**Federato** Condivisione di identità e attributi tra domini di fiducia tramite standard (SAML, OAuth2, OpenID Connect). Esempi: SPID, eduGAIN.

**Decentralizzato** L'identità è autogestita dall'utente con DID e Verifiable Credentials senza autorità centrale, permettendo selective disclosure.

## Casi d'uso complessi

- Identità multi-ruolo (es. medico-ricercatore con accessi differenziati)
- Deleghe temporanee gestite da policy automatizzate (es. smart contract)
- Identità dispositivi IoT con analisi comportamentale per individuare anomalie
- Pseudonimizzazione e privacy differenziale per anonimizzare dati operativi
- Identità blockchain con attestazioni verificabili crittograficamente

# Classi di sistemi distribuiti e problematiche identitarie

**Client-Server centralizzato** *Esempio tipico:* Portale SPID, database aziendale.
*Caratteristiche:* Controllo unico e autenticazione centralizzata, semplice ma punto unico di fallimento.

**Multi-tier / Microservizi** *Esempio tipico:* Applicazioni cloud-native.
*Caratteristiche:* Servizi indipendenti, richiedono identità tra servizi e token di sessione.

**Peer-to-Peer (P2P)** *Esempio tipico:* Torrent, blockchain.
*Caratteristiche:* Nodi equivalenti, identità distribuita difficile da revocare.

**Federato** *Esempio tipico:* SPID, eduGAIN.
*Caratteristiche:* Domini con fiducia reciproca, coordinamento di policy e attributi.

**Decentralizzato** *Esempio tipico:* SSI, Wallet eIDAS 2.
*Caratteristiche:* Identità autogestita, sovranità personale, complessità tecnica.

# Soluzioni di gestione dell'identità

## Identità Centralizzata

- Basata su un unico Identity Provider (es. Active Directory, LDAP)
- Vantaggi: gestione semplice e auditing centralizzato
- Svantaggi: punto singolo di compromissione, scalabilità limitata
- Caso reale: attacco ransomware blocca accesso a tutti i servizi

## Identità Federata

- Basata sulla fiducia tra domini tramite SAML, OAuth2, OpenID Connect
- Vantaggi: interoperabilità, riduzione password, Single Sign-On
- Svantaggi: configurazioni e sincronizzazioni complesse
- Esempio: federazione universitaria EduGAIN

## Identità Decentralizzata (SSI)

- Basata su DID e Verifiable Credentials verificati su blockchain
- Vantaggi: controllo utente, verificabilità indipendente, interoperabilità globale
- Svantaggi: complessità tecnologica, assenza di quadri giuridici chiari, difficoltà recupero chiavi
- Esempio: diploma digitale universitario in portafoglio digitale

## Identità di dispositivo nei sistemi IoT

- Ogni dispositivo possiede un'identità verificabile
- Tecniche: certificati digitali X.509, autenticazione mutual TLS, TPM/HSM
- Sfide: limitazioni energetiche, aggiornamento chiavi, interoperabilità multi-vendor
- Soluzioni emergenti: identità leggere con token simmetrici o blockchain edge
- Esempio: rete agricola intelligente con autenticazione distribuita

# Analisi comparativa modelli di identità

**Centralizzato** **Vantaggi:** Facilità controllo, auditing centralizzato.
**Limiti:** Punto singolo di fallimento.
**Esempi:** LDAP, Active Directory.

**Federato** **Vantaggi:** Interoperabilità, delega di fiducia.
**Limiti:** Complessità, manutenzione.
**Esempi:** SPID, eduGAIN.

**Decentralizzato (SSI)** **Vantaggi:** Sovranità utente.
**Limiti:** Recupero credenziali complesso.
**Esempi:** eIDAS 2, Wallet.

**IoT-based** **Vantaggi:** Scalabilità, automazione.
**Limiti:** Risorse limitate, revoca difficile.
**Esempi:** Smart Agriculture.