LEZIONE 1 – INTRODUZIONE GENERALE ALLA CYBERSECURITY

Premessa

La **cybersecurity** costituisce oggi una delle aree più complesse, dinamiche e strategiche dell'intero panorama tecnologico e sociale. La sua importanza cresce proporzionalmente alla digitalizzazione delle infrastrutture, dei servizi e dei processi produttivi, ma la disciplina resta frammentata e difficile da sistematizzare. Ciò deriva tanto da **motivi storici** quanto da **cause contingenti**, legate all'evoluzione disomogenea delle tecnologie e alla natura **intrinsecamente interdisciplinare** della materia.

Origini storiche e sviluppo disomogeneo

Le prime forme di sicurezza informatica nacquero negli anni '60 e '70 in ambito **militare e scientifico**, con l'obiettivo di proteggere l'accesso ai mainframe e controllare i privilegi degli utenti. Negli anni '80, con la diffusione dei personal computer e delle reti locali, l'attenzione si spostò verso la protezione dei sistemi operativi e dei dati memorizzati in ambienti distribuiti.

Con l'avvento di **Internet** e del **protocollo TCP/IP**, la sicurezza assunse una dimensione globale: nacquero i firewall, gli antivirus e i primi sistemi di rilevamento delle intrusioni (IDS). Negli anni 2000, la crescita dei servizi online e del commercio elettronico impose nuove esigenze: protezione delle transazioni, crittografia avanzata, gestione delle identità e tutela dei dati personali.

Nel decennio successivo, la pervasività dei dispositivi mobili, del cloud computing e dell'Internet of Things ha esteso la superficie d'attacco a scala planetaria, rendendo la cybersecurity un problema **sistemico** che coinvolge infrastrutture critiche, economia e geopolitica.

Frammentazione e eterogeneità delle soluzioni

La cybersecurity non si è sviluppata come una scienza unitaria, ma come un insieme di risposte specifiche a problemi emergenti. Ne è derivato un

ecosistema di soluzioni eterogenee — software, protocolli, standard, normative — spesso non interoperabili tra loro.

Esempi significativi di questa frammentazione sono:

- la molteplicità di **standard tecnici** (ISO/IEC 27001, NIST 800, CIS Controls, ENISA Guidelines);
- la coesistenza di **framework nazionali e internazionali** con approcci differenti;
- la presenza di **soluzioni tecnologiche proprietarie** non sempre compatibili o verificabili.

Questa eterogeneità, unita alla rapida obsolescenza delle tecnologie, genera **vulnerabilità strutturali** e ostacola la costruzione di modelli condivisi di sicurezza.

Un'area intrinsecamente interdisciplinare

La cybersecurity si colloca all'intersezione tra molteplici saperi.

- **Informatica e ingegneria** forniscono gli strumenti tecnici per la protezione dei sistemi e delle reti.
- **Matematica e crittografia** definiscono i fondamenti della sicurezza logica e computazionale.
- **Diritto e governance** regolano la responsabilità, la privacy e la conformità normativa (GDPR, NIS2, Cyber Resilience Act).
- **Scienze sociali e cognitive** analizzano il comportamento umano, principale vettore di rischio attraverso l'ingegneria sociale.
- **Economia e gestione del rischio** valutano l'impatto finanziario e strategico delle minacce.

Questa natura multidisciplinare, se da un lato rappresenta una ricchezza, dall'altro rende difficile definire un linguaggio comune e un corpus teorico unificato. L'assenza di una epistemologia condivisa della sicurezza costituisce tuttora una delle principali criticità del settore.

Dalle fragilità storiche alle sfide contemporanee

Le vulnerabilità della cybersecurity moderna derivano in larga parte da **scelte architetturali storiche** — protocolli nati senza requisiti di sicurezza

intrinseci, modelli di fiducia implicita, soluzioni locali poi globalizzate. A ciò si aggiungono:

- la **complessità crescente delle infrastrutture digitali**;
- la **dipendenza da terze parti** e da supply chain globali;
- la **scarsità di competenze interdisciplinari** e di modelli di governance integrata.

Il risultato è un sistema complessivo fragile, in cui la sicurezza è spesso trattata come elemento accessorio e non come proprietà strutturale dei sistemi informativi.

L'identità digitale come nucleo centrale della sicurezza

In questo corso prenderemo come punto di partenza uno dei temi più centrali e trasversali della cybersecurity contemporanea: **l'identità digitale**.

L'identità digitale è il fondamento di ogni meccanismo di **autenticazione**, **autorizzazione** e **responsabilità**. Essa definisce chi può accedere a un sistema, quali azioni può compiere e a chi è attribuibile una determinata operazione. Ma non è solo un concetto tecnico: è il punto di incontro tra dimensione tecnologica, giuridica e sociale.

Analizzare la sicurezza a partire dall'identità significa affrontare i nodi più profondi della fiducia digitale, della protezione dei dati e della responsabilità nei sistemi distribuiti. È proprio attorno al modo in cui costruiamo, gestiamo e proteggiamo le identità che si giocano oggi le principali sfide della cybersecurity.

Identificatori e attributi dell'identità digitale: architetture e casi d'uso reali

Ogni sistema informatico che implementa un modello di sicurezza fondato sull'identità deve distinguere tra identificatore, credenziale e attributo. Questi tre elementi non sono equivalenti, ma cooperano nel definire in modo preciso chi o cosa accede, con quali permessi e in quali condizioni.

Gli attributi possono essere statici (es. nome, codice fiscale) o dinamici (es. ruolo temporaneo, contesto di accesso, geolocalizzazione).
Nei sistemi moderni, la gestione di attributi dinamici consente politiche di sicurezza adattive e contestuali.

Identificatore e attributo: concetti chiave

1. L'identificatore è un valore univoco che consente di distinguere un'entità digitale da tutte le altre. Può essere un nome utente, un indirizzo e-mail, un identificativo numerico o un Decentralized Identifier (DID) in architetture blockchain.
2. L'attributo, invece, è un'informazione associata all'identità, come il ruolo, l'affiliazione o il livello di autorizzazione, che ne descrive le proprietà e i diritti operativi.

L'implementazione pratica del concetto di identità digitale varia secondo il tipo di architettura. I modelli principali sono centralizzato, federato e decentralizzato.

• Architetture centralizzate – In questi sistemi (es. Active Directory o LDAP) l'identificatore è gestito da un'unica autorità. Gli attributi sono memorizzati in un database locale e utilizzati per controllare l'accesso alle risorse. Questo approccio è efficiente ma presenta un punto unico di fallimento e scarsa scalabilità in ambienti multi-organizzazione.

• Architetture federate – Basate su standard come SAML, OAuth2 e OpenID Connect, consentono a più domini di fiducia di condividere identità e attributi. Esempi concreti sono SPID per i servizi pubblici e eduGAIN nel mondo universitario. Un utente può autenticarsi presso il proprio Identity Provider (IdP) e accedere a un Service Provider (SP) esterno, che riceve attributi firmati digitalmente per autorizzare l'accesso.

• Architetture decentralizzate – Con la Self-Sovereign Identity (SSI) e i Decentralized Identifiers (DID), l'identità non è più controllata da un'autorità centrale. Gli attributi sono gestiti in portafogli digitali e verificati

tramite credenziali crittografiche (Verifiable Credentials). Questo approccio consente all'utente di condividere solo gli attributi necessari (selective disclosure) e di dimostrare la propria identità in modo verificabile ma senza cedere il controllo dei dati personali.

CASI D'USO COMPLESSI DEL CONCETTO DI ATTRIBUTO E IDENTIFICATORE

Le architetture moderne richiedono che l'identità digitale sia flessibile e adattabile a contesti dinamici. Ecco alcuni scenari non banali che mostrano l'importanza della corretta gestione di identificatori e attributi.

Caso 1 – Identità multiruolo in ambiente sanitario

Un medico che lavora anche come ricercatore accede con la stessa identità digitale ma con attributi diversi: nel contesto clinico, ha accesso ai dati dei pazienti; nel contesto di ricerca, solo a dati anonimizzati. Il sistema IAM (Identity and Access Management) assegna attributi dinamici in base al contesto operativo.

Caso 2 – Deleghe temporanee e ruoli dinamici

In una pubblica amministrazione, un dirigente può delegare temporaneamente i propri diritti di firma a un collega. L'attributo 'delegato' ha validità limitata nel tempo e viene gestito da un sistema di policy basato su smart contract. Al termine del periodo, l'attributo decade automaticamente senza intervento manuale.

Caso 3 – Identità di dispositivi IoT e attributi comportamentali

In una smart factory, ogni sensore possiede un identificatore univoco e una serie di attributi che descrivono il tipo di dati inviati e la frequenza di trasmissione. Se un sensore comincia a inviare dati fuori frequenza, un sistema UEBA (User and Entity Behavior Analytics) può rilevare la deviazione e segnalare un potenziale attacco o guasto.

Caso 4 – Pseudonimizzazione e privacy differenziale

Nei servizi digitali di sanità o istruzione, l'uso di pseudonimi come identificatori temporanei consente di separare l'identità reale dai dati operativi. Un sistema di privacy differenziale può generare identificatori diversi per ogni sessione, preservando l'anonimato pur mantenendo la tracciabilità interna delle attività.

Caso 5 – Identità blockchain e attestazioni verificabili

In ecosistemi di filiera agroalimentare o energetica, i nodi blockchain rappresentano organizzazioni o sensori. L'identificatore è un DID, mentre gli attributi includono certificazioni (es. biologico, provenienza, orari di consegna). Le attestazioni vengono verificate crittograficamente, consentendo fiducia distribuita senza autorità centrale.

Sintesi e schema concettuale

L'evoluzione dell'identità digitale mostra che la sicurezza non risiede solo nelle credenziali, ma nel modo in cui gli identificatori e gli attributi vengono gestiti, condivisi e verificati. L'adozione di modelli dinamici e distribuiti richiede equilibrio tra interoperabilità, privacy e controllo.

In sintesi:
• L'identificatore stabilisce l'unicità.
• Gli attributi definiscono il contesto e i diritti.
• Le architetture determinano la fiducia e la scalabilità.

Il valore dell'identità nei sistemi distribuiti

3.1 Introduzione

Nei sistemi distribuiti moderni — che includono architetture cloud, reti IoT, infrastrutture federate e blockchain — il tema dell'identità digitale assume un valore economico, tecnico e strategico.
La corretta gestione dell'identità non è solo una questione di autenticazione, ma di **fiducia distribuita**: ogni nodo del sistema deve poter essere riconosciuto e autorizzato a comunicare con altri in modo sicuro.

L'identità digitale diventa così un **bene primario**: la sua compromissione può generare perdita di riservatezza, manipolazione dei dati o interruzione dei servizi.
Nel contesto dei sistemi distribuiti, il modello CIA (Confidentiality – Integrity – Availability) è lo strumento di riferimento per comprendere le implicazioni di tali violazioni.

3.2 Classi di sistemi distribuiti e problematiche identitarie

I sistemi distribuiti possono essere classificati in varie categorie, ciascuna con proprie esigenze e limiti di identificazione.

Classe di sistema	Esempio tipico	Caratteristiche	Implicazioni sull'identità
Client–Server centralizzato	Portale SPID, database aziendale	Controllo unico, autenticazione centralizzata	Gestione semplice ma rischio di punto unico di fallimento
Multi-tier / Microservizi	Applicazioni cloud-native	Servizi indipendenti,	Richiede identità service-to-service e token di sessione

Classe di sistema	Esempio tipico	Caratteristiche	Implicazioni sull'identità
		comunicanti via API	
Peer-to-Peer (P2P)	Torrent, reti blockchain	Nodi equivalenti, senza centro di controllo	Identità distribuita, difficile da revocare
Federato	SPID, eduGAIN	Domini autonomi ma con fiducia reciproca	Coordinamento di policy, ruoli e attributi
Decentralizzato (SSI)	Wallet eIDAS 2	Identità autogestita dall'utente	Sovranità personale, ma complessità tecnica

🟦 **Esempio 1 – SPID come identità federata**
In SPID, diversi provider autenticano utenti secondo regole comuni stabilite da AgID. L'identità è valida in tutti i servizi aderenti, ma ogni provider conserva la propria base dati.

🟦 **Esempio 2 – Identità IoT in una smart factory**
Un sensore di temperatura invia dati firmati digitalmente; se l'identità del sensore non è verificata, un dispositivo malevolo può sostituirlo generando dati falsi, compromettendo l'integrità del processo industriale.

3.3 Soluzioni di gestione dell'identità nei sistemi distribuiti

3.3.1 Identità centralizzata

Basata su un unico **Identity Provider (IdP)** che controlla tutte le autenticazioni.
Esempi: Active Directory, Kerberos, LDAP.

Vantaggi: semplicità di gestione, auditing centralizzato.
Difetti: punto singolo di compromissione, scalabilità limitata.

🟦 **Caso reale – Directory aziendale unica**
Un attacco ransomware sul dominio blocca l'intero sistema di login, rendendo inaccessibili tutti i servizi.

3.3.2 Identità federata

Modello basato sulla fiducia tra domini: **SAML**, **OAuth 2.0**, **OpenID Connect**.
Ogni organizzazione mantiene il controllo dei propri utenti, ma accetta credenziali emesse da domini fidati.

Vantaggi: interoperabilità, riduzione del numero di password, Single Sign-On (SSO).
Difetti: configurazioni complesse, sincronizzazione policy tra domini.

🟦 **Esempio – Federazione universitaria europea**
EduGAIN consente agli studenti di accedere a servizi di altre università mantenendo le proprie credenziali locali.

3.3.3 Identità decentralizzata (Self-Sovereign Identity – SSI)

Basata su ***Decentralized Identifiers (DID)*** e ***Verifiable Credentials (VC)***.
Nessun server centrale: le attestazioni di identità vengono verificate su blockchain pubbliche o permissioned.

Vantaggi: controllo dell'utente, verificabilità indipendente, interoperabilità internazionale.
Difetti: complessità tecnologica, mancanza di quadri giuridici uniformi, difficoltà di recupero in caso di perdita delle chiavi.

🟦 **Esempio – Diploma digitale universitario SSI**
Lo studente riceve un attestato firmato digitalmente e lo conserva nel

proprio wallet. L'azienda verifica la firma tramite blockchain, senza accedere ad alcun database centrale.

3.3.4 Identità di dispositivo nei sistemi IoT

Ogni dispositivo deve possedere un'identità verificabile. Tecniche principali:

- Certificati digitali X.509.
- Autenticazione ***mutual TLS***.
- Moduli di sicurezza hardware (TPM, HSM).

Sfide: limitazioni energetiche, aggiornamento chiavi, interoperabilità multi-vendor.
Soluzioni emergenti: identità leggere basate su token simmetrici o blockchain edge.

🟦 **Esempio – Rete agricola intelligente**
Sensori distribuiti autenticano i dati tramite certificati generati dal cloud; la revoca è gestita via ledger distribuito per garantire tracciabilità.

3.4 Analisi comparativa dei modelli di identità

Modello	Vantaggi	Limiti	Esempi
Centralizzato	Facilità di controllo, auditing	Punto singolo di fallimento	LDAP, AD
Federato	Interoperabilità, delega di fiducia	Complessità e manutenzione	SPID, eduGAIN

Modello	Vantaggi	Limiti	Esempi
Decentralizzato (SSI)	Sovranità dell'utente	Recupero credenziali complesso	eIDAS Wallet
IoT-based	Scalabilità, automazione	Risorse limitate, revoca difficile	Smart Agriculture
Ibrido	Bilancia controllo e autonomia	Architetture complesse	Multi-cloud federato