ONTOLOGY FOR AUTHENTICATION

Autore: Aldo Pedico – Enterprise Cybersecurity & Privacy

Contatto: pedicoaldo@gmail.com

PREMESSA

*Il termine "***ONTOLOGIA***" in uso nelle Scienze dell'Informazione descrive lo scopo del ragionamento induttivo, della classificazione e delle svariate tecniche per la risoluzione di alcuni problemi informatici.*

*Nel caso specifico della "*AUTENTICAZIONE*" s'intende un'indagine del suo fondamento, ovvero è* "lo studio del fondamento di quel che esiste, del come esiste, se è solo pensabile, se è costante, se è universale, se è accertabile."

In questo documento si rappresenta il risultato di uno sforzo per definire l'autenticazione esaminando i meccanismi utilizzati per dimostrare la posizione o l'appartenenza; analizzare metodi, strumenti e tecniche esistenti; e sviluppare una rappresentazione astratta delle funzionalità e dei servizi di autenticazione.

*Questo documento è di complemento agli articoli "***IDENTITÀ DIGITALE***" e "***PERSONAL IDENTITY***" precedentemente pubblicati dal sottoscritto.*

INDICE

Titolo **Pag.**

1 THE AUTHENTICATION ONTOLOGY

Con questo documento ho voluto sintetizzare l'implementazione della componente di autenticazione, composta da un processo di gestione, di autenticazione e di autorizzazione (IDENTITY AUTHORIZATION AND AUTHENTICATION - IAA) *o di attestazione dell'identità.*

*In questo documento raccomando un'*ONTOLOGIA DI AUTENTICAZIONE: *associazioni e relazioni comuni a tutte le metodologie allo scopo di verificare un costrutto precedentemente associato a un'entità o ad un oggetto.*

Il documento inizia con il modo in cui l'autenticazione dell'entità si inserisce nel processo IAA e come si relaziona agli altri componenti di tale processo.

È presentata una tassonomia dell'autenticazione per entrambe le autenticazioni incentrate sull'entità e sugli oggetti.

L'autenticazione dell'entità riceve il termine conferma ed è suddivisa in tre aree di autenticazione:

1) **UOMO-MACCHINA (U-M)**;
2) **MACCHINA-MACCHINA (M-M)**;
3) **UOMO-UOMO (U-U)**.

È quindi presentata l'autenticazione degli oggetti, dato il termine attestazione.

Dopo la discussione sulla tassonomia, sono presentati gli attributi di autenticazione insieme a uno degli aspetti più dibattuti dell'autenticazione: la forza.

Affrontando la necessità di misurare definitivamente la forza dell'autenticazione, sono identificate quattro aree:

1) **SICUREZZA**;
2) **USABILITÀ**;
3) **DISTRIBUIBILITÀ**;
4) **GESTIBILITÀ**.

Per ogni area viene discussa una serie di fattori ambientali adatti alla misurazione.

La figura 1 fornisce una mappa concettuale dell'ontologia.

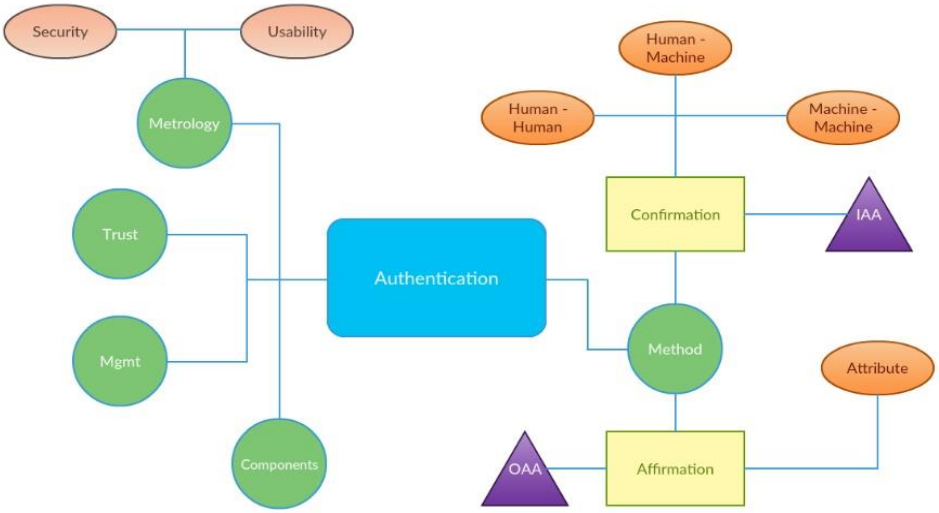

Figure 1 - Concept Map for Authentication Properties

L'autenticazione ha un impatto su diverse aree di un'organizzazione, in particolare la Generazione e il Coordinamento delle politiche e spesso non viene affrontata in standard che si concentrano su un meccanismo specifico.

Un insieme comune di misurazioni che riguardano tutti i meccanismi di autenticazione include:

- ✓ *l'unicità dell'hardware, del software o dei processi che rappresentano l'entità per l'entità che viene autenticata;*
- ✓ *la resistenza della rappresentazione ad essere duplicata o altrimenti compromessa;*
- ✓ *la protezione della rappresentazione durante la consegna al meccanismo di convalida e la protezione del meccanismo contenente il riferimento di autenticazione;*
- ✓ *l'usabilità dell'autenticazione* ***U-M****.*

L'autenticazione è la componente del processo IAA che fornisce un certo grado di garanzia che l'identità assegnata all'entità sia verificata.

La mappa concettuale mostrata nella Figura 1 identifica i fattori chiave osservati dalla valutazione delle metodologie di autenticazione.

Alcuni aspetti dell'ontologia sono di natura gerarchica o strutturale, come la tassonomia dei meccanismi di autenticazione fornita nella Figura 2.

La gestione dell'autenticazione include la relazione tra gestione dell'identità (IDENTITY MANAGEMENT - IM) *e dell'autorizzazione.*

Lo sviluppo, l'implementazione, la manutenzione e il funzionamento di un sito di autenticazione hanno aspetti sia strutturali sia relazionali.

È possibile trovare poche indicazioni per determinare i criteri per la selezione dei meccanismi di autenticazione.

Ad esempio, FIPS 140-2, che viene utilizzato fino al 2025, discute la forza dell'autenticazione semplicemente affermando che:

> "Affinché un tentativo casuale abbia successo, la probabilità deve essere inferiore a una su 1.000.000... (ad esempio, indovinare una password o un PIN, tasso di errore di falsa accettazione di un dispositivo biometrico o una combinazione di metodi di autenticazione)."

E che più tentativi in un periodo di un minuto dovrebbero avere una probabilità di successo inferiore a uno su 100.000.

2 A TAXONOMY OF AUTHENTICATION MECCANISM

2.1 DESCRIZIONE DELLA TASSONOMIA

Una tassonomia dei meccanismi di autenticazione fornisce una struttura per classificare tipi diversi ma correlati di meccanismi di autenticazione.

Questo documento propone una tassonomia composta da due **CLASSI** *principali di* **AUTHENTICATION**:

1) **CONFIRMATION**: *è generalmente utilizzata come verifica di un'entità per gestire le autorizzazioni o l'accesso;*
2) **ATTESTATION**: *è generalmente la verifica di un attributo diretto o indiretto dell'oggetto (non entità) di interesse.*

La **CONFIRMATION** *è composta dai seguenti tre* **DOMINI**:

1) **U-M** *(ad esempio, un utente umano che si autentica su un dispositivo),*
2) **M-M** *(ad esempio, un accesso Internet aziendale automatizzato) e*
1) **U-U** *(ad esempio, recupero della password di persona).*

*L'***ATTESTATION** *ha lo scopo di verificare l'oggetto piuttosto che utilizzare l'oggetto per verificare l'entità che rappresenta, inoltre, è utilizzata su oggetti, dalla filigrana digitale (***WATERMARK***) e fisica alle firme digitali.*

La figura 2 presenta la struttura attuale della tassonomia dell'autenticazione con le classi di **CONFIRMATION** *e* **ATTESTATION**, *nonché i domini* **U-M, M-M, U-U** *e* **ATTRIBUTO**.

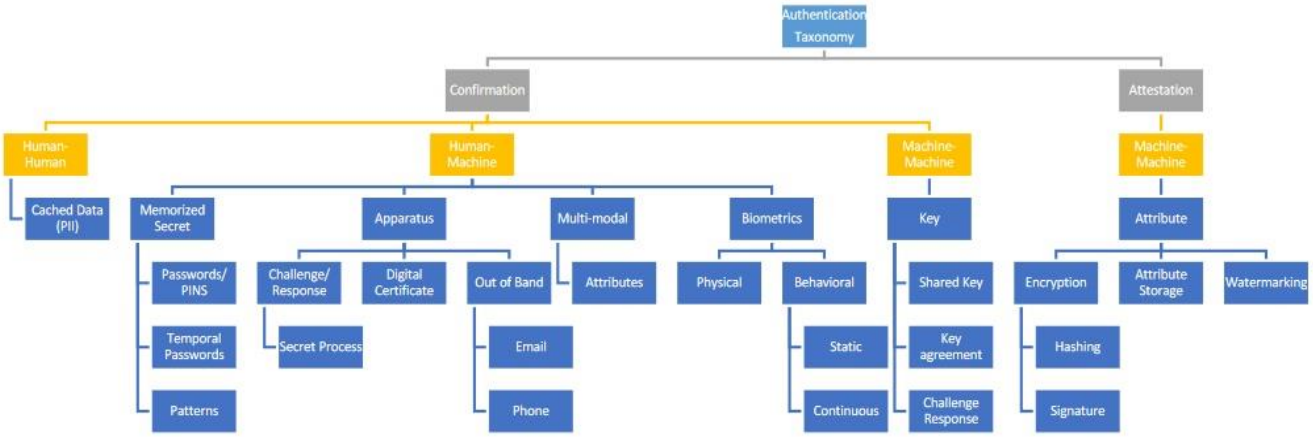

Figure 2 - Authentication taxonomy

2.2 CLASSE: CONFIRMATION

La prima delle due classi attualmente individuate ne è la **CONFIRMATION**.

Il meccanismo di autenticazione conferma che l'hardware, il software o il processo fornito che rappresenta l'entità è valido per l'accesso.

Attualmente ci sono tre domini sotto la conferma di classe: **U-M, M-M** *e* **U-U**.

DOMINI DI CONFIRMATION

La classe di **CONFIRMATION** *autentica un'entità che è tipicamente rappresentata da una o un gruppo di entità.*

L'autenticazione più conosciuta dal pubblico è un essere umano che interagisce con qualche interfaccia o sensore che consente l'accesso da parte di un individuo.

QUESTO DOMINIO È **UOMO-MACCHINA**.

I meccanismi di autenticazione sono spesso necessari per supportare le connessioni attraverso e all'interno di ogni livello del modello OSI (OPEN SYSTEMS INTERCONNECTION).

Anche rimanendo all'interno delle comunicazioni TCP/IP, le autenticazioni sono state ottimizzate per e attraverso i livelli di astrazioni, come quelle presentate nella Figura 3 di seguito.

La figura 3 mostra la gerarchia IP comune dei computer moderni.

La tecnologia di autenticazione **M-M** *spesso cancella l'interfaccia di diversi livelli di comunicazione.*

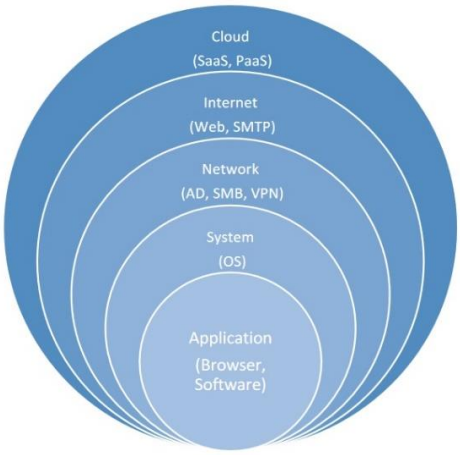

Figure 3 - Authentication Implementation Complexity (not user experience)

Quando si utilizzano servizi web sotto il controllo di un provider, l'utente e le entità aziendali devono accettare le politiche del provider.

QUESTO DOMINIO È **MACCHINA-MACCHINA**.

Un utente in genere considera l'autenticazione a un sito Web da una rete aziendale come un semplice processo di autenticazione. Tuttavia, la Figura 4 mostra le complessità nell'intreccio delle autenticazioni **U-M** *e* **M-M**, *comprese le opzioni per il* **SINGLE SIGN-ON** *per i servizi che possono supportare l'azienda al di fuori della rete.*

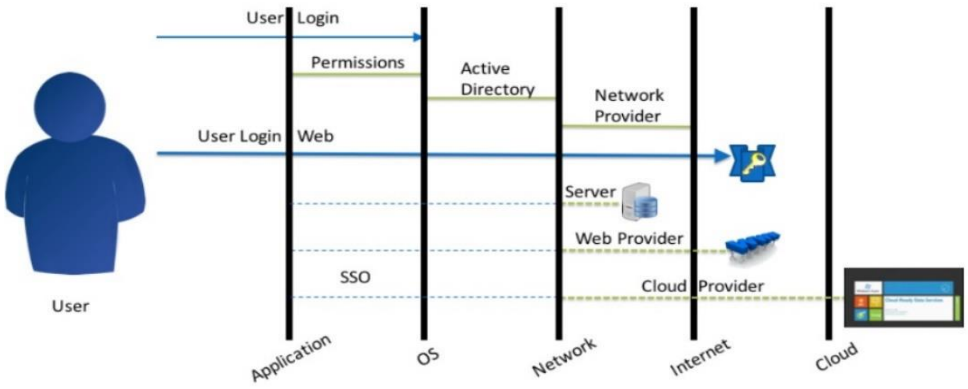

Figure 4 - Human-Machine and Machine-Machine Resources

L'ultimo dominio è solitamente il meno considerato ma il più costoso da gestire.

L'autenticazione **U-U** *è spesso utilizzata come ultima risorsa dopo che l'***U-M** *ha fallito.*

È noto che gli hacker bloccano intenzionalmente un account di autenticazione **U-M** *per tentare di manipolare gli amministratori che supportano l'autenticazione* **U-U** *per fornire all'hacker l'accesso all'account.*

DOMINIO: **UOMO-MACCHINA**

L'autenticazione **U-M** *è una delle interazioni più difficili da affrontare e la difficoltà è spesso attribuita alle differenze nelle capacità tra uomo e macchina.*

Nel dominio **U-M**, *un essere umano ha il controllo dell'hardware, del software o del processo che rappresenta l'entità.*

Per adattarsi alla moltitudine di meccanismi diversi, l'autenticazione **U-M** *è stata ulteriormente suddivisa in tre parti:*

1) **INITIAL**,
2) **MULTI-MODAL** *e*
3) **CONTINUOUS**.

La maggior parte dei meccanismi di autenticazione odierni sono considerati un tipo di meccanismo di autenticazione **INIZIALE**, *che risponde con una singola risposta (cioè SÌ o NO).*

Tre categorie principali di meccanismi di autenticazione **INIZIALE** *attualmente utilizzati oggi sono:*

1) *password*,
2) *dispositivi di autenticazione dedicati e*
3) *biometria*,

con il loro utilizzo principalmente una volta per ogni singola sessione.

L'autenticazione **CONTINUA** *è attualmente rara nell'ambiente di oggi, ma offre molte promesse.*

Essa utilizza un meccanismo che è spesso basato sulla biometria comportamentale *utilizzata in una modalità di campionamento continuo.*

L'autenticazione **U-M**, *multimodale, è qualsiasi combinazione di autenticazione* **INIZIALE** *e/o* **CONTINUA**.

Nei casi in cui all'utente è richiesto di autenticarsi per un insieme di servizi sotto una gestione centralizzata, l'amministrazione utilizza uno schema di memorizzazione nella cache per l'utente.

Una volta che l'utente si è autenticato con successo, il meccanismo di autenticazione può memorizzare nella cache credenziali alternative per alleviare l'onere dell'autenticazione su ciascun sistema quando si prevede che il livello di rischio sia sufficientemente basso.

In questi casi, si tratta di un'autenticazione **M-M** *che rappresenta l'uomo al posto di un'autenticazione* **U-M**.

FAMIGLIA: **MEMORIZED SECRET**

*La definizione più generica di segreto memorizzato è "***QUALCOSA CHE CONOSCI***" che viene condiviso solo con la macchina che conferma l'utente.*

Sebbene esistano diverse forme di segreti memorizzati, tra cui password, numero di identificazione personale (PIN), immagine e suono, vengono tutti utilizzati per dimostrare la conoscenza dell'utente delle informazioni segrete da condividere solo con il server di autenticazione.

Le organizzazioni che utilizzano segreti memorizzati per l'autenticazione spesso seguono le ultime tendenze senza valutarne l'usabilità, rendendo difficile se non onerosa la selezione e l'utilizzo dei segreti memorizzati.

FAMIGLIA: **BIOMETRIC**

*L'autenticazione basata su "***QUALCOSA CHE SEI***" si riferisce spesso all'autenticazione biometrica. Esempi comuni includono impronta digitale, viso, iride e riconoscimento vocale.*

I dati biometrici utilizzati nell'autenticazione iniziale determinano una tantum la certezza che la scansione attiva e i dati biometrici raccolti prima dell'autenticazione provengano dallo stesso utente.

I dati biometrici, che scansionano continuamente e determinano il livello di fiducia che la persona giusta continui a utilizzare il sistema, sono forme di autenticazione **CONTINUOUS**.

Un esempio di raccomandazioni del NIST per l'uso della biometria nei meccanismi di autenticazione è SP 800-76-2.

CATEGORIA: **INITIAL**

Attualmente, l'autenticazione **UOMO-MACCHINA** *più comune è l'autenticazione* **INITIAL**, *questa convalida rapidamente una credenziale (ad esempio, un'impronta digitale) che l'utente ha fornito in precedenza in modo che l'autorizzazione possa consentire all'utente di accedere alle informazioni o funzionalità richieste.*

Una volta completata l'autenticazione iniziale, la connessione rimane finché non viene interrotta dall'utente o da un altro meccanismo di monitoraggio.

CATEGORIA: **CONTINUOUS**

Occasionalmente, gli utenti intenzionalmente o accidentalmente lasciano l'accesso aperto e disponibile ad altri.

Diverse applicazioni basate sulla temporizzazione o altro hardware dedicato tentano di ridurre al minimo questa esposizione.

Quando il fattore raggiunge una soglia predeterminata, l'utente viene autenticato per un certo periodo di tempo, legando più strettamente l'autenticazione all'utente.

Tuttavia, questi meccanismi di autenticazione **CONTINUOUS** *sono spesso limitati nel loro utilizzo a causa della non uniformità degli utenti (ad esempio, limitazioni o cambiamenti mentali o fisici).*

Per risolvere questi problemi, si stanno studiando più meccanismi di autenticazione o meccanismi multimodali per l'uso.

FAMIGLIA: **APPARATUS**

*Un apparato di autenticazione è spesso considerato "***QUALCOSA CHE POSSIEDI***" e può includere PIN o password che cambiano in base all'ora o agli eventi in dispositivi hardware, smartcard o dispositivi basati su RFID.*

Un punto debole comune è relativamente facile perdere il dispositivo.

Questo è in genere contrastato dall'uso di un meccanismo di autenticazione aggiuntivo, come i PIN, raggruppati in una soluzione più forte.

Sono disponibili anche moduli software di questi metodi, sebbene possano essere considerati soluzioni più deboli.

Ad esempio, una smartcard potrebbe supportare un'infrastruttura PKI ed è generalmente considerata una delle forme di autenticazione più efficaci.

Dispositivi come i telefoni cellulari sono talvolta utilizzati come meccanismo di autenticazione secondario.

FAMIGLIA: **MULTI-MODAL**

L'autenticazione **MULTI-MODAL** *è definita come la combinazione di due o più metodi di autenticazione* **U-M**, *sia* **INITIAL** *sia* **CONTINUOUS**, *per aumentare la robustezza di un sistema.*

L'aggiunta di ulteriori forme di autenticazione per aumentare la difficoltà di compromettere un sistema è definita autenticazione a più fattori **(MULTI-FACTOR AUTHENTICATION - MFA)**.

Questo si basa sui tre tipi di autenticazione:

1) **QUALCOSA CHE CONOSCI,**
2) **QUALCOSA CHE HAI,**
3) **QUALCOSA CHE SEI.**

L'autenticazione **MFA** *fa spesso riferimento a un token della smartcard con l'utente che immette una password o un PIN per sbloccare la smartcard.*

I fattori di autenticazione che dovrebbero essere considerati includono compensazioni di vulnerabilità o esposizioni note, nonché impatti sull'usabilità.

L'autenticazione **MULTI-MODAL** *può aggiungere flessibilità a molti dei sistemi di autenticazione attualmente in uso.*

Con le funzionalità aggiuntive dei dispositivi mobili e delle workstation moderne, nonché l'uso di reti distribuite, è possibile valutare più opzioni.

Quando si supportano più tipi di dispositivi, l'autenticazione può essere considerata non solo per la sua forza aggiuntiva, ma anche per l'usabilità.

Attraverso la selezione di un'autenticazione **MULTI-MODAL** *appropriata, può essere possibile affrontare diverse vulnerabilità ambientali mantenendo una postura solida.*

Considerazioni aggiuntive dovrebbero includere il modo in cui vengono integrati, progettati e gestiti.

L'aggiunta di determinati attributi può anche aiutare a rafforzare il processo di autenticazione.

Gli attributi possono essere utilizzati per l'autenticazione e l'autorizzazione o solo l'autorizzazione, a seconda dei meccanismi di ciascuno e di quanto possa essere necessario compartimentare l'accesso.

- ✓ **ATTRIBUTO TIME**

L'autenticazione controllata in determinati giorni della settimana o in alcune ore del giorno è stata supportata in molti sistemi ma viene utilizzata raramente.

Allo stesso modo, le organizzazioni possono scegliere di disabilitare l'autenticazione per determinati utenti durante le vacanze o una malattia prolungata.

I limiti di tempo sono spesso impiegati e accoppiati con monitor di attività per ridurre al minimo l'esposizione dell'accessibilità se sembra che l'utente abbia abbandonato l'accesso.

I limiti di tempo possono essere implementati nell'autenticazione, autorizzazione o in entrambi.

- ✓ **ATTRIBUTO LOCATION**

Ulteriori verifiche possono essere ottenute da attributi relativi alla posizione geografica.

Le posizioni fisiche possono includere GPS, sensori di prossimità e indirizzi IP interni (controllati).

Le posizioni logiche possono includere indirizzo IP identificato o previsto, tempo previsto per la risposta o VPN affidabile.

Anche il numero di accessi simultanei può essere un fattore di limitazione, sebbene ora venga utilizzato meno spesso a causa del numero di dispositivi a cui gli utenti accedono quotidianamente.

DOMINIO: MACCHINA-MACCHINA

Un altro dominio nella classe di **CONFIRMATION** *è l'autenticazione* **M-M**.

Questo dominio è spesso utilizzato per l'autenticazione del sistema organizzativo o di rete, come connessioni di rete per workstation e dispositivi mobili, VPN o comunicazioni business to business.

L'autenticazione basata sui sistemi è spesso basata su uno schema crittografico, come PKI o altro accordo chiave o schema di negoziazione chiave.

Anche gli schemi **Single Sign-On** *che supportano più autenticazioni per un utente dopo l'accesso iniziale dovrebbero essere considerati in questo dominio.*

L'autenticazione **M-M** *viene utilizzata per:*

- ✓ *Autenticazione tramite un collegamento di comunicazione;*
- ✓ *Supportare una rete di dispositivi affidabili;*
- ✓ *Supportare un'autenticazione uomo-macchina automatizzata (cache);*
- ✓ *Fornire altri dati di autenticazione, come la posizione (ad esempio, accesso aziendale ai servizi);*
- ✓ *Fornire servizi affidabili (ad esempio, DNS, NTS, posizione, ecc.).*

Inoltre, l'autenticazione **M-M**:

- ✓ *di solito è di natura crittografica:*
  - ➢ *utilizza spesso i protocolli consigliati dal NIST (ad es. IPSEC, TLS);*
  - ➢ *utilizza una chiave pre-condivisa (simmetrica) o una firma digitale;*
- ✓ *è impostato da un amministratore;*

- ✓ *è spesso trasparente per l'utente;*
- ✓ *può essere un'autenticazione uomo-macchina memorizzata nella cache;*
- ✓ *può collegarsi temporalmente (ricorrente o meno) o può essere autocontrollato (vedere l'attestazione).*

DOMINIO: **UOMO-UOMO**

Il dominio finale nella classe di **CONFIRMATION** *è l'autenticazione* **U-U**.

È spesso utilizzato quando un utente non è in grado di accedere tramite il sistema uomo-macchina.

È considerato l'obiettivo più facile e più suscettibile agli attacchi, principalmente dall'ingegneria sociale.

Se le informazioni utilizzate come autenticatori non sono sufficientemente protette, il "database" dell'autenticatore diventa un'altra fonte di attacco.

Uso principale per l'autenticazione **U-U**: *è stabilita un'identità tramite credenziali provenienti da altre fonti approvate.*

Questa operazione è in genere eseguita tramite la gestione delle identità e non è associata all'autenticazione poiché è utilizzata qui. Un aspetto importante di questa autenticazione è che le credenziali, sebbene fornite dall'utente, sono state autenticate da fonti riconosciute al di fuori dello schema di autenticazione.

Quando i meccanismi di autenticazione primaria sono falliti o bloccati, si usa questa autenticazione **U-U** *come sistema di backup. Quando è utilizzata come sistema di backup, l'autenticazione si basa sui dati memorizzati nella cache, informazioni che in genere sono fornite dall'utente allo scopo di ristabilire la sua identità.*

Quando si considera la forza di un sistema di autenticazione, è necessario considerare anche il sistema di backup.

L'utilizzo degli indirizzi e-mail degli utenti come punto di comunicazione per le informazioni di ripristino può mitigare alcuni problemi di attacco e costi.

Per questi motivi, altre metodologie come la messaggistica di testo attraverso reti esterne sono diventate tecniche di mitigazione automatizzate a livelli popolari per l'autenticazione uomo-uomo.

2.3 CLASSE: ATTESTATION

*Un'altra classe di autenticazione è l'***ATTESTATION** *che autentica un oggetto piuttosto che un'entità.*

Un esempio comune potrebbe essere l'hash di un file per verificare in seguito che non sia cambiato.

Attualmente è stato identificato un solo dominio, l'attributo, ma si prevede che aumenterà.

DOMINIO: **ATTRIBUTE**

Questo dominio conferma un oggetto verificando un attributo dell'oggetto.

*Sebbene un'***ATTESTATION** *possa essere semplice come un controllo CRC, la garanzia spesso si basa su un'operazione crittografica, come un seme o una chiave predeterminata, per rendere più difficile la sostituzione di un nuovo oggetto e determinare un nuovo valore.*

Esempio: un hash con chiave o una firma digitale di un file può accertare se il file rimane invariato, ma non impedisce a un utente di modificare l'associazione del file modificando l'estensione del nome del file.

Possono essere sufficienti indicazioni più semplici di una sospetta modifica del file, come una modifica della data, una modifica della dimensione del file o una misurazione dinamica (ad esempio, monitorare un file di registro per assicurarsi che aumenti solo di dimensioni).

Il monitoraggio di più attributi tende ad aumentare la fiducia raggiunta in presenza di requisiti di garanzia complessi.

Sebbene gli attributi definiti crittograficamente forniscano una quantità significativa di forza rispetto ad altri metodi, potrebbero non essere in grado di caratterizzare l'oggetto come necessario.

L'oggetto più spesso utilizzato come blocco di base per l'attestazione è un file.

L'hardware ha spesso una raccolta di uno o più file software o firmware che vengono verificati all'avvio come parte dell'inizializzazione.

L'autenticazione identificativa, come una firma digitale, è memorizzata come una parte separata del file o esternamente in un'area protetta.

*Tre famiglie di attributi dell'***ATTESTATION** *sono* **ENCRYPTION**, **STORAGE** *e* **WATERMARKING**.

La famiglia dipende dal focus dell'attributo piuttosto che dal meccanismo utilizzato.

FAMIGLIA: **ENCRYPTION**

CATEGORIA**: HASHING**

L'hashing è spesso utilizzato per identificare i dati che non sono stati modificati da quando è stato acquisito l'hash.

L'hashing è generalmente scelto quando l'uso del file è consentito ma le modifiche al file non lo sono.

*Una volta che un hash è stato generato dal file, le informazioni risultanti non possono essere invertite e la dimensione "**dell'impronta digitale**" è ridotta a una lunghezza dipendente dall'algoritmo di hash.*

La protezione dell'hash è importante per evitare che il file venga modificato o che venga generato un nuovo hash per sostituire il vecchio.

La protezione dell'hash può includere l'archiviazione sicura o l'hashing dei dati combinato con una chiave segreta.

- ✓ **DIGITAL SIGNATURE**

Le firme digitali forniscono la verifica che un file non sia stato modificato.

In genere, questo tipo di **ATTESTATION** *esegue l'hashing del file di interesse prima di crittografare l'hash con una firma digitale che può essere ricondotta all'utente e all'autorità di certificazione.*

Due forme principali di firme digitali sono DSA e PKI.

Tuttavia, gli schemi di firme Merkle vengono spesso utilizzati per la protezione blockchain contro il cambiamento.

- ✓ **SYMMETRIC ENCRYPTION**

Se non è necessario avere accesso illimitato al file di interesse, è possibile utilizzare anche la crittografia di un file per assicurarsi che non sia stato inconsapevolmente modificato.

Qualsiasi modifica al file crittografato comporterà l'interruzione e il ripristino della crittografia a meno che la modifica non è identificata e annullata.

Ciò è particolarmente utile per il trasferimento dei dati, che può includere la crittografia prima del trasferimento o uno schema di trasporto come TLS o SSH.

FAMIGLIA: **STORAGE**

Questo è uno dei pochi metodi di attributo di attestazione che non si basa necessariamente sulla crittografia per la protezione ma piuttosto sulla separazione dall'oggetto.

Un attributo può essere memorizzato separatamente dall'oggetto, di solito in uno schema di protezione **IAA (IDENTITY MANAGEMENT AUTHENTICATION AND AUTHORIZATION)** *o in un formato che non può essere facilmente modificato, come l'utilizzo di un hash con chiave o un meccanismo simile.*

Alcuni prodotti di garanzia dipendono dall'archiviazione degli attributi come mezzo per la gestione degli utenti o dei sistemi di rete.

FAMIGLIA: **WATERMARKING**

Il watermarking differisce dalle altre attestazioni in quanto tipicamente si concentra sulla rappresentazione incorporata dai dati piuttosto che sui dati stessi.

Ad esempio, una fotografia a colori digitalizzata spesso non viene riconosciuta guardando i dati.

Tuttavia, quando viene fornita la struttura corretta per i dati, l'immagine può essere visualizzata.

Allo stesso modo, la filigrana crea tipicamente un oggetto incorporato sulla rappresentazione dei dati, come un'immagine.

Esistono molti usi per la filigrana, inclusa l'identificazione del lavoro protetto in modo ovvio o nascosto, il mantenimento del contrassegno quando viene copiato o regolato o diventa evidente quando l'immagine viene copiata.

Sebbene la filigrana non sia necessariamente crittografica, la crittografia viene spesso utilizzata per impedire la manipolazione della filigrana.

2.4 TABELLA RIASSUNTIVA

<table>
<tr><th>CLASSI</th><th>DOMINI</th><th>CATEGORIE</th><th>FAMIGLIE</th><th>ATTRIBUTI</th><th>IM
ID. MANAGEMENT</th><th>AUTHENT.</th><th>AUTHOR.</th></tr>
<tr><td rowspan="5">CONFIRMATION</td><td rowspan="4">U-M</td><td>➢ INITIAL</td><td>➢ MEMORIZED SECRET
“qualcosa che sai”</td><td></td><td rowspan="5">➢ Validate entity docs
➢ Manage entities</td><td rowspan="5">Affirm virtual identity</td><td rowspan="5">Manage virtual identity rights to objects</td></tr>
<tr><td>➢ CONTINUOUS</td><td>➢ BIOMETRIC
“qualcosa che sei”</td><td></td></tr>
<tr><td></td><td>➢ APPARATUS
“qualcosa che hai”</td><td></td></tr>
<tr><td>➢ INITIAL
➢ CONTINUOUS</td><td>➢ MULTI-MODAL
“qualcosa che sai”
“qualcosa che sei”
“qualcosa che hai”</td><td>➢ TIME
➢ LOCATION</td></tr>
<tr><td>M-M</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>U-U</td></tr>
<tr><td>ATTESTATION</td><td>ATTRIBUTE</td><td>➢ HASHING: Digital Signature; Symmetric Encryption</td><td>➢ ENCRYPTION
➢ STORAGE
➢ WATERMARKING</td><td></td><td>➢ Manage Objects
➢ Manage IM and Object Credentials</td><td>Verify Object Goodness</td><td>Authentication might gate object execution</td></tr>
</table>

3 PROPERTIES

Diverse proprietà sono state osservate nella creazione della tassonomia.

La **CONFIRMATION** *e* **L'ATTESTATION** *utilizzano molti degli stessi meccanismi di autenticazione.*

Tuttavia, sono utilizzati in modo molto diverso tra il processo di gestione dell'identità, autenticazione e autorizzazione (IAA) e il processo di gestione degli oggetti, autenticazione e (a volte) autorizzazione (OAA - **OBJECT AUTHENTICATION AND AUTHORIZATION***).*

I meccanismi di autenticazione tra uomo e macchina hanno evidenziato la necessità di comprendere meglio le relazioni di fiducia.

3.1 PANORAMICA DEL PROCESSO IAA PER LA CONFIRMATION

L'autenticazione è un componente del processo IAA, come mostrato nella Figura 5.

Il processo IAA è costituito da tre attività uniche:

1) IDENTIFY;
2) AUTHENTICATE;
3) AUTHORIZE.

Figure 5 - IAA process

Storicamente, un processo IAA era tipicamente implementato come un'unica soluzione monolitica.

Ogni componente del processo IAA dovrebbe essere definito con una serie comune di requisiti applicabili a tutti i prodotti.

Questi requisiti includono la garanzia nella distribuzione e nella gestione dei sistemi.

In questo modo, i fornitori possono fornire prodotti che diano soluzioni mirate compatibili con gli altri componenti.

GESTIONE DELLE IDENTITÀ (IM -IDENTITY MANAGEMENT)

I sistemi di autorizzazione delle entità e i sistemi di autenticazione degli oggetti sono generalmente separati.

Tuttavia, entrambi supportano requisiti simili.

Lo scopo della **DIGITAL IDENTITY** *è il rilascio o l'adozione di un'identità digitale che è logicamente legata a un'entità fisica.*

L'entità fisica si basa sulla ricezione di credenziali di identificazione da parti attendibili, come un passaporto, una licenza o una registrazione aziendale.

L'identità digitale è un artefatto prodotto per stabilire una presenza i sistemi di interesse.

È questa entità digitale che effettua l'autenticazione e il componente di autorizzazione consente o limita una volta autenticato.

La garanzia di fiducia per l'entità fisica è solitamente correlata alla quantità e alla qualità della documentazione di terze parti, mentre la garanzia di fiducia per l'autenticazione dell'entità digitale è relativa alla forza dell'autenticazione utilizzata e al livello di protezione delle risorse a cui accedere.

La garanzia di fiducia per entrambi dovrebbe essere presa in considerazione quando si progetta e si mantiene un sistema.

Oltre ai problemi di identità, **IM** *deve comunicare con entrambi i componenti di autenticazione e autorizzazione per applicare i diritti dell'entità digitale.*

Gli esempi possono includere un amministratore del sito Web, un reparto o un responsabile delle risorse umane o un'organizzazione ombrello congiunta e multiforme.

Una volta che **l'IM** *sarà soddisfatto di avere informazioni sufficienti, creerà un'entità digitale e registrerà l'entità virtuale come un certo livello di operatore, dirigendo gli accessi del sistema su dove e in che modo fornire accesso o supporto.*

Se fatto direttamente, l'IM può emettere all'utente un token, come una carta **PIV**, *che consente l'accesso a qualsiasi sistema che riconosce l'IM come autorità.*

AUTHORIZATION

L'ultimo passaggio del processo **IAA** *è l'applicazione delle autorizzazioni.*

Dopo aver ricevuto un rapporto di successo dal componente d'autenticazione IAA, l'autorizzazione consente all'entità digitale di accedere per eseguire programmi o manipolare informazioni.

Spesso, le autorizzazioni offrono una certa granularità, come la sola lettura, il permesso di eseguire o consentono all'entità di modificare le informazioni.

I controlli e i vincoli dell'autorizzazione sono risolti tramite implementazioni del controllo degli accessi basato sui ruoli **(RBAC - ROLE-BASED ACCESS CONTROL)** e del controllo degli accessi basato sugli attributi **(ABAC - ATTRIBUTE-BASED ACCESS CONTROL)**.

*Il controllo di accesso obbligatorio (***MAC - MANDATORY ACCESS CONTROL***) e il controllo di accesso discrezionale (***DAC - DISCRETIONARY ACCESS CONTROL***) erano le prime implementazioni del controllo di accesso che negava tutto a meno che non fosse consentito (ad esempio, MAC) o consentiva tutto a meno che non fosse negato (ad esempio, DAC).*

Va notato che i controlli di cui sopra sono sotto la componente di autorizzazione IAA.

AUTHENTICATION

Scopo dell'autenticazione è confermare un'identità digitale attraverso la manipolazione di un hardware, software o processo che rappresenta l'entità.

L'identità rappresentata è definita dalla gestione delle identità e comunicata insieme alle informazioni necessarie, spesso solo un'autorizzazione, all'organizzazione responsabile del componente di autenticazione.

In caso di manipolazione riuscita dell'hardware, del software o del processo che rappresenta l'entità, il componente di autenticazione comunica al componente di autorizzazione una conferma o un rifiuto per consentire l'accesso.

L'autenticazione di un'identità digitale è abilitata dalla gestione delle identità.

IM lo fa fornendo al componente di autenticazione o richiedendo che il componente di autenticazione fornisca l'hardware, il software o il processo.

Tuttavia, le autorizzazioni finali per o il rifiuto dell'autenticazione (come la revoca) per ciascuna identità digitale sono fornite dall'IM.

Gli attuali punti di forza dell'autenticazione dipendono dal tipo di meccanismo utilizzato: la biometria dipende da un basso numero di falsi positivi; le password dipendono da tentativi non riusciti; le implementazioni PKI dipendono da forti chiavi pubbliche e private.

L'hardware, il software, la fonte biometrica o la conoscenza sotto il controllo dell'utente sono spesso indicati come token o autenticatore.

Può assumere molte forme diverse a seconda del processo di autenticazione e dei meccanismi utilizzati; nell'autenticazione **uomo-macchina**, *ci sono tre forme di base che vengono spesso discusse:*

1) **qualcosa che conosci**,

2) **qualcosa che hai** *e*

3) **qualcosa che sei**.

Sebbene questi non siano direttamente associati al livello di autenticazione, la combinazione di queste diverse forme di autenticazione è stata storicamente utilizzata per aumentare la fiducia nel processo di autenticazione.

La tabella 1 fornisce un confronto di alto livello dei due processi.

Table 1 - IAA Confirmation vs. OA Attestation

	Identity Management	Authentication	Authorization
Confirmation	Validate entity docs Manage entities	Affirm virtual identity	Manage virtual identity rights to objects
Attestation	Manage Objects Manage IM and Object Credentials	Verify Object Goodness	*Authentication might gate object execution*

3.2 PROCESSO OA (OBJECT AUTHENTICATION) PER L'ATTESTATION

Il processo OA fornisce la garanzia che un oggetto è come previsto utilizzando gli attributi di tale oggetto.

*Il processo è costituito da due componenti: gestione degli oggetti (***OM – OBJECT MANAGEMENT***) e autenticazione.*

Ogni componente ha una serie comune di requisiti, che includono la garanzia nella distribuzione e nella gestione dei sistemi.

Gli esempi di processi OA includono la replica dei dati per sistemi multiistanza, come operazioni bancarie o trasferimento di dati per il magazzinaggio e tipicamente esistono all'interno di un sistema che implementa un processo IAA.

La quantità di fiducia per l'oggetto dipende dalla selezione di uno o più attributi dell'oggetto e dall'ambiente, mentre la garanzia di fiducia è relativa alla forza dell'autenticazione usata per verificare gli elementi dell'oggetto. I requisiti per la garanzia di fiducia per ciascuno dovrebbero essere considerati durante la progettazione o la manutenzione del sistema OA.

OM e autenticazione possono essere combinati o separati a seconda del design OA.

Tuttavia, devono comunicare tra loro, anche se separati, per gestire i diritti.

3.3 AUTENTICAZIONE AFFIDABILE UNIDIREZIONALE (ONE-WAY TRUST AUTHENTICATION)

L'autenticazione unidirezionale è utilizzata quando solo una parte deve stabilire le credenziali, ad esempio quando un utente o un amministratore accede a una workstation autonoma.

Quando un utente dispone di un account su una stazione di lavoro, deve presentare una serie di credenziali che corrispondano a uno degli account impostati nel sistema.

L'utente non ha la certezza digitale che la macchina sia la macchina corretta, tuttavia, la macchina conferma la credenziale dell'utente.

In alcune circostanze, il sistema può essere configurato per consentire a più operatori di accedere a dispositivi con le stesse credenziali.

È indicata come autenticazione basata sui ruoli.

In genere, l'autenticazione è la stessa per l'autenticazione basata sull'identità.

Tuttavia, l'IM ha consentito a diversi operatori di condividere le stesse credenziali (ad esempio, gli amministratori di un set di router di rete).

Sebbene l'autenticazione basata sui ruoli stia perdendo popolarità, esiste ancora e non deve essere confusa con il controllo degli accessi basato sui ruoli (RBAC)*, che si riferisce al controllo delle autorizzazioni di accesso di un operatore autenticato piuttosto che a chi può utilizzare il processo di autenticazione.*

Nei sistemi basati sul web, è comune che il modello di fiducia per la workstation discusso in precedenza venga invertito. Ciò è particolarmente importante perché quando si utilizza Internet, l'utente non ha la certezza di aver raggiunto la macchina corretta. In questo caso, l'utente non effettua il login, ma il server può essere convalidato utilizzando una soluzione PKI basata su TLS o simile.

Nella Figura 6, un'autenticazione unidirezionale è rappresentata visitando un sito Web protetto che utilizza un certificato (l'autenticazione riuscita è in genere indicata da un'icona sul browser) per verificare il server e quindi negoziare la funzionalità di sicurezza. È importante notare che il server ha poca conoscenza dell'utente poiché all'utente non è richiesto di accedere per mantenere la connessione.

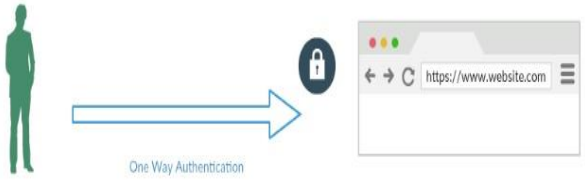

Figure 6 - One-way Authentication

3.4 AUTENTICAZIONE DI FIDUCIA RECIPROCA (MUTUAL TRUST AUTHENTICATION)

L'autenticazione reciproca è in genere utilizzata per convalidare entrambe le entità in una conversazione.

Ad esempio, se un acquirente desidera acquistare qualcosa da un negozio, si autentica nel negozio tramite un account e/o un pagamento, creando livelli di fiducia in ciascuna direzione.

In questo esempio, in genere sono disponibili due diversi metodi di autenticazione.

Tuttavia, è comune un unico meccanismo che supporta l'autenticazione reciproca.

Spesso le aziende desiderano un'autenticazione più forte quando i dipendenti accedono ai servizi dall'esterno della rete aziendale. In tal caso, potrebbero utilizzare una sessione TLS reciproca, che spesso si ritiene abbia una maggiore garanzia in quanto l'utente ottiene un certificato emesso dalla stessa autorità di certificazione o da quella riconosciuta.

L'autenticazione reciproca è illustrata nella Figura 7.

Figure 7 - Mutual Authentication

Sia l'utente che il server dispongono di certificati validi in modo che possano autenticarsi a vicenda tramite qualcosa come il protocollo TLS.

3.5 AUTENTICAZIONE ATTENDIBILE MULTILIVELLO (MULTI-LEVEL TRUST)

Le autenticazioni multilivello sono ottenute mediante una combinazione di relazioni unidirezionali e di fiducia reciproca.

Utilizzando un esempio precedente, è tipico per un server fornire protezione SSL utilizzando il certificato del server al momento dell'acquisto.

Il browser supporta la protezione dell'utente verificando una credenziale valida dalla vetrina online. Tuttavia, il venditore del negozio non sa chi sta navigando a meno che non acceda con alcune credenziali, come un nome utente e una password.

Un acquisto online con carta di credito presenta un insieme di relazioni molto complesso.

La Figura 8 illustra tre relazioni di trust con tre diversi tipi di autenticazione.

L'autenticazione tramite certificati PKI è indicata in ogni entità tranne che per l'utente.

Per effettuare un acquisto su un sito Web, l'utente può accedere con un nome utente e una password o un meccanismo simile per l'archiviazione delle informazioni dell'utente, migliorando la comodità dell'utente e fornendo ulteriori garanzie al negoziante.

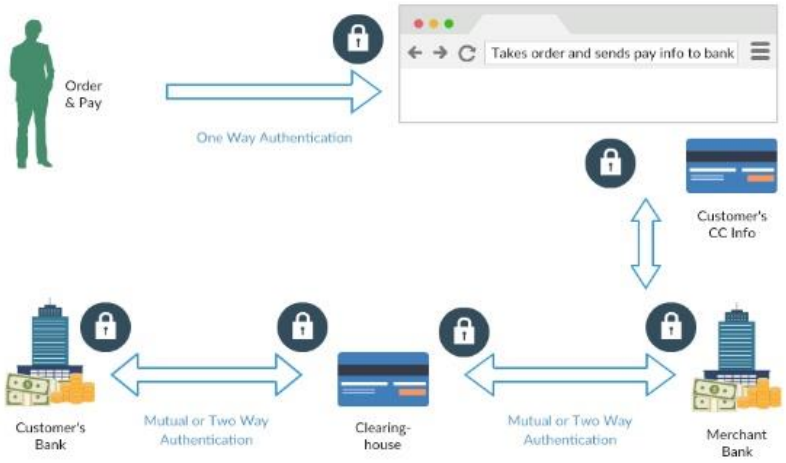

Figure 8 - Multi-path authentication

Sia come parte di tali informazioni che separatamente, le informazioni sulla carta di credito dell'acquirente vengono utilizzate come meccanismo di autenticazione per trasferire denaro dal conto dell'utente al conto del commerciante.

3.6 RELAZIONI DI TRUST NELL'AUTENTICAZIONE DELL'ATTESTAZIONE

L'attestazione si basa in genere su una sola relazione di trust; l'oggetto è lo stesso che ci si aspettava.

*La selezione dell'attributo utilizzato per "***cosa ci si aspettava***" è importante in quanto fornisce l'unicità dell'attributo e può limitare i metodi di protezione ragionevoli per l'artefatto di confronto.*

Ad esempio, un nome file e una data possono essere perfettamente adeguati per specificare un file, ma danno poche garanzie in quanto non sarebbe difficile modificare il contenuto del file.

Tuttavia, l'hashing di un file potrebbe essere un modo intelligente per affermare che il file che rappresenta un oggetto non è cambiato e talvolta vengono utilizzate firme digitali per verificare una parte di un oggetto.

In altri casi, ci si aspetta che alcuni file (ad esempio, file di registro) cambino, ma in genere dovrebbero aumentare di dimensioni solo a meno che il materiale di controllo non sia stato rimosso (cioè manomesso).

L'autenticazione fornisce la quantità di fiducia e dipende da diversi fattori:

1) l'aspetto di un oggetto;

2) l'unicità del manufatto generato;

3) la forza della protezione fornita dal manufatto e possibilmente;

4) la protezione della rete, sebbene sia al di fuori del controllo dell'OA, fornita da l'autorizzazione di un sistema IAA.

OM selezionerebbe l'aspetto dell'oggetto, che avrebbe un impatto sull'unicità del manufatto.

3.7 COMPONENTI DEL MECCANISMO DI BASE

Sebbene la funzione principale dell'autenticazione sia indagare sulle credenziali dell'entità, gli schemi necessari per farlo variano a seconda dei meccanismi di consegna utilizzati per comunicare tra le prove di autenticazione dell'utente e il sistema che esegue la valutazione.

Gli aspetti chiave dell'autenticazione possono avere considerazioni ambientali dipendenti dalla regione.

Ad esempio, un sensore implementato in remoto che deve comunicare su più reti necessiterà anche di un'implementazione più sofisticata di quella di uno connesso direttamente a un dispositivo non in rete contenente memoria interna.

Considerazioni speciali possono essere prese in considerazione per applicazioni, piattaforma locale, rete interna, ambienti web e cloud.

Sebbene la sicurezza fisica sia stata invocata per le implementazioni locali, la protezione attraverso le reti viene comunemente fornita utilizzando tecnologie di crittografia.

In generale, poiché i meccanismi di autenticazione vengono utilizzati su distanze maggiori e piattaforme multiple, sono necessarie implementazioni e interazioni più diversificate per una protezione più forte e versatile.

Cinque componenti di base sono state identificate nei meccanismi:

1) *rappresentazione dell'identità,*
2) *sensori,*
3) *comunicazioni,*
4) *archiviazione,*
5) *elaborazione.*

4 CREAZIONE E MANTENIMENTO DELL'AUTENTICAZIONE

Uno dei maggiori fattori nel decidere quale tipo di meccanismo di autenticazione implementare in un nuovo sistema è **l'adeguatezza** *o* **l'idoneità** *del* **meccanismo**.

Storicamente, il sistema era legato a un mainframe o a workstation in rete e i progettisti di sistema potevano ottimizzare i controlli di autenticazione in un ambiente piuttosto ben definito.

Sebbene sia ancora considerato più facile implementare l'autenticazione in un ambiente ben definito e protetto, la maggior parte degli ambienti odierni è in continua evoluzione e spesso è apertamente accessibile.

L'integrazione dei dispositivi mobili e altre problematiche stanno rendendo l'ambiente estremamente diversificato.

L'implementatore e i responsabili possono risolvere i problemi più comuni considerando **quattro categorie principali**:

1) SECURITY;

2) DEPLOYABILITY;
3) USABILITY;
4) MANAGEABILITY.

1) *La* SECURITY *si concentra sugli aspetti ambientali comuni che un utente malintenzionato può utilizzare per compromettere le credenziali di un utente.*

   Affronta sia la vicinanza a un utente, come sentire un utente che fornisce vocalmente un numero di carta di credito quando contatta la banca sia un utente malintenzionato utilizzando tecniche per ottenere l'accesso in remoto, come indovinare una password o ingannare l'utente tramite false e-mail per compromettere informazioni sensibili.

2) *La* DEPLOYABILITY *si concentra sugli aspetti del processo che sono importanti per i progettisti implementatori. I problemi di implementazione sono spesso correlati ai fattori di costo per alzarsi in piedi o rinnovare una capacità esistente.*

   Affronta la selezione dell'autenticazione dell'utente e il costo di acquisto risultante, i possibili costi di registrazione (separati dalla registrazione per la gestione dell'identità), la consegna, la creazione di criteri, l'istituzione del supporto e la creazione e implementazione della formazione iniziale per utenti e supporto.

3) *L'*USABILITY *si concentra su due aree principali: a) l'esperienza dell'utente finale, b) l'esperienza del supporto o dell'amministratore.*

   È un tentativo di quantificare la quantità di sforzo che un utente valido deve sopportare per raggiungere un obiettivo, come l'autenticazione.

   È stato riferito che quando la barriera alla sicurezza per gli utenti validi è troppo alta, gli utenti si trovano spesso ad essere molto efficaci nel soggiogare la sicurezza.

   Un semplice esempio di ciò potrebbe essere l'utente che pubblica la password sul monitor del computer perché la password era troppo difficile da ricordare.

4) *La* MANAGEABILITY *è l'ultima categoria e affronta l'intero sforzo di supporto necessario per mantenere e garantire il corretto funzionamento del processo di autenticazione.*

   Sebbene la distribuibilità sia addebitata all'implementazione iniziale della registrazione degli utenti, la gestibilità include il provisioning continuo, come l'aggiunta, la rimozione e la manutenzione degli account utente, nonché le politiche e le procedure che li supportano.

   Man mano che i sistemi maturano, le politiche e le procedure devono spesso cambiare a causa di requisiti esterni, inclusa la legislazione, le risorse delle apparecchiature, i miglioramenti tecnologici e il supporto per servizi aggiuntivi.

4.1 ATTRIBUTI DI SICUREZZA

I punti deboli della sicurezza possono essere raggruppati in ingegneria sociale, malware, configurazione errata e vulnerabilità.

SOCIAL ENGINEERING:

- ✓ *OSSERVAZIONE: osservazione dell'utente o dell'ambiente utente utilizzato per ottenere l'accesso.*
- ✓ *FAILOVER: impone a un sistema di utilizzare altri metodi per ottenere l'accesso.*
- ✓ *TIRARE A INDOVINARE (GUESSING): tentativi illimitati di ritentare l'autenticazione.*
- ✓ *RISPETTO (STRICT) RIGOROSO DELLE LINEE GUIDA: le linee guida forniscono un modello, semplificando l'attacco.*
- ✓ *ACQUISIZIONE DATI: utilizzo di lettori collocati con lettori validi per scremare, scansionare o registrare i dati dell'utente senza interrompere la transazione.*
- ✓ *ACQUISIZIONE AUTENTICAZIONE: acquisizione di dispositivi hardware o software di autenticazione; dati biometrici, di posizione o sensibili al tempo; o altre prove di autenticità.*

CONFIGURATION VULNERABILITIES:

- ✓ *REPOSITORY DI PROVE DEL SERVER: mancanza di protezione sufficiente per impedire l'acquisizione e l'attacco offline.*
- ✓ *RISPETTO DELLA COMUNICAZIONE: attacchi MITM, attacchi replay, keylogger.*

INFORMATION LEAKAGE (PERDITA DI INFORMAZIONI, COMPRESE PRIVACY):

- ✓ *PACKAGING: Etichettatura/marchio della carta.*
- ✓ *HELP DESK: informazioni associate all'utente.*
- ✓ *REPORTING: registrazione degli accessi, inclusi posizione, ora, ecc.*
- ✓ *FEEDBACK: visualizzazione delle informazioni sull'ingresso, informazioni udibili, identità, ecc.*

4.2 ATTRIBUTI DI DISTRIBUIBILITÀ (DEPLOYABILITY)

La distribuibilità può essere raggruppata in accessibilità, costo e compatibilità.

ACCESSIBILITY:

- ✓ *CONSIDERAZIONI SULLA DISABILITÀ: l'autenticazione soddisfa i requisiti d'accessibilità dell'utente.*
- ✓ *RESTRIZIONI: l'ambiente supporta i requisiti di sicurezza necessari.*

COST:

- ✓ *COSTO ACCETTABILE PER UTENTE: costo per l'attrezzatura, la registrazione e la gestione di ciascun utente.*
- ✓ *COSTO ACCETTABILE PER IL RISCHIO: il costo è supportato dal costo della perdita o della perdita di accesso.*
- ✓ *COSTI DI IMPLEMENTAZIONE ACCETTABILI: i costi rientrano nel budget di implementazione o rinnovo, inclusi il ripristino e la nuova registrazione.*

COMPATIBILITY:

- ✓ *SISTEMA: funziona con il sistema protetto, inclusi piattaforma, rete e app o plug-in.*

- ✓ *ORGANIZZAZIONE: include la gestione e l'amministrazione dei criteri.*
- ✓ *L'AUTENTICAZIONE PUÒ ESSERE RIDIMENSIONATA: per numero di utenti, numero di server, amministrazione.*

4.3 USABILITY ATTRIBUTES

Gli attributi di usabilità sono associati a efficacia, efficienza e soddisfazione.

EFFECTIVENESS:

- ✓ *Configurazione dell'autenticazione rapida, consegna, assistenza e supporto per i problemi.*
- ✓ *L'inserimento dell'utente non è suscettibile di errori, feedback sufficiente per l'utente.*
- ✓ *Il recupero richiede tempo e impegno minimi.*

EFFICIENCY:

- ✓ *Disponibilità e facilità di comprensione delle politiche e delle procedure di autenticazione.*

SATISFACTION:

- ✓ *Requisiti utente leggeri, nessun requisito di memoria oneroso, nessuna necessità di trasportare token, ecc.*
- ✓ *Contabilità per altri requisiti di autenticazione utente, inclusi siti non associati.*
- ✓ *Integrato con il flusso di lavoro del processo utente.*

4.4 ATTRIBUTI DI GESTIBILITÀ (MANAGEABILITY)

Le considerazioni che affrontano i problemi di gestibilità possono essere raggruppate in costi annuali e disponibilità a lungo termine.

ANNUAL COSTS:

- ✓ *Supporto amministrativo.*
- ✓ *Gettoni.*
- ✓ *Supporto IT per comunicazione, server e archiviazione.*
- ✓ *Supporto e manutenzione del lettore.*

LONG TERM AVAILABILITY:

- ✓ *Gettoni.*
- ✓ *Lettori o altri sensori.*
- ✓ *Hardware e software del server.*

5 METROLOGIA PER L'AUTENTICAZIONE

Storicamente, la forza di un'autenticazione è stata attribuita direttamente alla crittografia utilizzata nel processo decisionale. Ciò non si applica ai meccanismi **U-M** *non basati sulla crittografia, come password o dati biometrici.*

Usare la forza della crittografia come misura è un valore ottimistico.

Ci sono in genere molti problemi di progettazione, implementazione, manutenzione e operativi che riducono drasticamente la forza effettiva del sistema.

Inoltre, averlo basato solo sulla crittografia del processo decisionale ignora qualsiasi:

1) *protezione utilizzata per il trasferimento delle informazioni di autenticazione,*
2) *protezione dei dati segreti durante l'archiviazione;*
3) *difetto di implementazione o configurazione che possa comportare la compromissione.*

Nell'autenticazione con un'interfaccia **U-M** *basata sulla crittografia, sono adottate soluzioni alternative per affrontare i limiti umani.*

Gli utenti sono spesso limitati quando si tratta di ricordare lunghezze di chiavi sufficientemente potenti e il numero di chiavi che dovrebbero conservare per i sistemi a cui accedono.

*Sono state sviluppate alternative che non si basano sul fatto che gli esseri umani ricordino direttamente i componenti di crittografia, ma piuttosto implichino un passaggio aggiuntivo, come "**qualcosa che hai**".*

Per i sistemi che supportano un'interfaccia umana ma non sono basati sulla crittografia, la crittografia può essere utilizzata per aggiungere complessità al sistema e renderlo più difficile per l'attaccante.

Ad esempio, sistemi alternativi possono essere basati su una qualche forma di password o dati biometrici.

Molto lavoro è stato svolto all'interno del dominio uomo-macchina nel tentativo di determinare le metriche di sicurezza per ciascuna famiglia di meccanismi, inclusa l'entropia delle password, i tassi di falsa accettazione della biometria e la forza chiave delle soluzioni PKI. Tuttavia, queste misurazioni non sono facilmente confrontabili tra le diverse famiglie.

A causa della complessità, gli attuali standard per la conferma **U-M** *sembrano affrontare più livelli di sicurezza.*

Tuttavia, sembrano esserci due soluzioni: **1) qualsiasi cosa, 2) autenticazione a "due fattori"**.

5.1 SECURITY

Uno degli aspetti più importanti nella selezione dei meccanismi di autenticazione dovrebbe essere la riduzione al minimo dei compromessi.

REPRESENTATION

Questa è una misura del collegamento tra il token e l'entità da autenticare.

Si prevede che quanto più strettamente il token possa essere legato all'entità, tanto maggiore è la garanzia.

INIMITABLE

Questa è una misura della resistenza del token a essere duplicato o altrimenti compromesso.

Un compromesso è spesso correlato al tipo di autenticazione. Ciò che conta è la resistenza al compromesso, non necessariamente il compromesso specifico applicato.

SECURE DELIVERY

Questa dovrebbe misurare la protezione del token dal punto di ingresso da parte dell'entità al punto di valutazione dell'autenticazione e la decisione della valutazione alla gestione dell'autorizzazione.

La protezione dovrebbe affrontare una combinazione di vulnerabilità dovute a compromissioni, sostituzioni e omissioni non intenzionali dell'utente.

SECURE STORAGE

Questa è una misura della protezione delle informazioni di riferimento che il meccanismo di autenticazione utilizza per verificare l'entità.

La misura di protezione dovrebbe applicarsi sia all'archivio attivo che a qualsiasi archivio di backup.

5.2 USABILITY

L'usabilità si concentra sulle autenticazioni **U-M** *ed è relativamente nuova per i metodi di autenticazione.*

È difficile per la maggior parte degli utenti comprendere il costo della sicurezza, ma scoprono rapidamente come questo influisce sul loro funzionamento.

Maggiore è la pressione del tempo, dell'offuscamento o dell'accuratezza che grava sull'utente durante l'autenticazione, maggiore è la possibilità di errore.

L'usabilità è spesso valutata in base alla misura in cui gli utenti possono raggiungere obiettivi specifici con efficacia, efficienza e soddisfazione in uno specifico contesto di utilizzo.

Ad oggi, la maggior parte del lavoro nella valutazione dell'usabilità dell'autenticazione ha utilizzato uno standard che affronta l'usabilità dei display video, ISO 9241-11. In IOS 9241-11, ci sono tre aree di interesse:

1) *la* **SATISFACTION**, *che è una misurazione soggettiva;*
2) *l'***EFFECTIVENESS** *e*
3) *l'***EFFICIENCY** *che possono essere calcolate.*

ESSERE **EFFICACI** SIGNIFICA FARE LE COSE GIUSTE; ESSERE **EFFICIENTI** SIGNIFICA FARE GIUSTE LE COSE.

EFFICACIA

L'efficacia è una misura dell'accuratezza e della completezza con cui gli utenti raggiungono obiettivi specifici.

Questa misurazione è spesso ottenuta collezionando errori dell'operatore, come errori di battitura, inserimento di carte al contrario o errori biometrici dovuti alle abitudini dell'utente.

Ulteriori misure potrebbero includere la disponibilità di ausili, come procedure e aspettative, utilizzo di casseforti per password o implementazioni **SINGLE SIGN-ON**.

EFFICIENZA

L'efficienza è misurata come le risorse spese in relazione all'accuratezza e completezza con cui gli utenti raggiungono gli obiettivi.

L'archivio delle password, le password scritte e il riutilizzo delle password sono esempi che influiscono sull'efficienza dell'autenticazione.

Il livello di impegno di Bitcoin per elaborare la **BLOCKCHAIN** è un esempio in cui l'efficienza è compromessa per aumentare la sicurezza.

SODDISFAZIONE

La soddisfazione è un obiettivo per raggiungere la libertà dal disagio e atteggiamenti positivi nei confronti dell'uso del prodotto.

La misurazione della soddisfazione è una misurazione qualitativa e, come tale, è più soggettiva.

Può essere meno affidabile dell'efficacia o dell'efficienza nel processo decisionale, ma è una misura importante della volontà dell'utente di supportare l'autenticazione.

6 RIFERIMENTI

1) NIST IR 8344 – Ontology for Authentication