Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
CRISTINA ALCARAZ
UNIVERSITÀ DI MALAGA, SPAGNA

Ringraziamenti

- *Cofinanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili per essi.*
- *Accordo di progetto n. 101083594*

Argomento 6: Sicurezza Selezione e implementazione dei controlli per ambienti energetici

Panoramica

- Selezionare e implementare controlli di sicurezza adeguati in base alle esigenze specifiche dei sistemi energetici
- Implementare politiche di password complesse e autenticazione a più fattori (MFA) per proteggere gli account degli utenti
- Crittografare i dati sensibili inattivi e in transito per impedire accessi non autorizzati e violazioni dei dati
- Applicare regolarmente aggiornamenti di sicurezza e patch ai sistemi software per risolvere le vulnerabilità

Cristina Alcaraz, Università di Malaga, Spagna

Argomento 6: Sicurezza Selezione e implementazione dei controlli per ambienti energetici

Panoramica

- Selezionare e implementare controlli di sicurezza adeguati in base alle esigenze specifiche dei sistemi energetici
- **Implementare politiche di password complesse e autenticazione a più fattori (MFA) per proteggere gli account utente**
- Crittografare i dati sensibili inattivi e in transito per impedire accessi non autorizzati e violazioni dei dati
- Applicare regolarmente aggiornamenti di sicurezza e patch ai sistemi software per risolvere le vulnerabilità

Cristina Alcaraz, Università di Malaga, Spagna

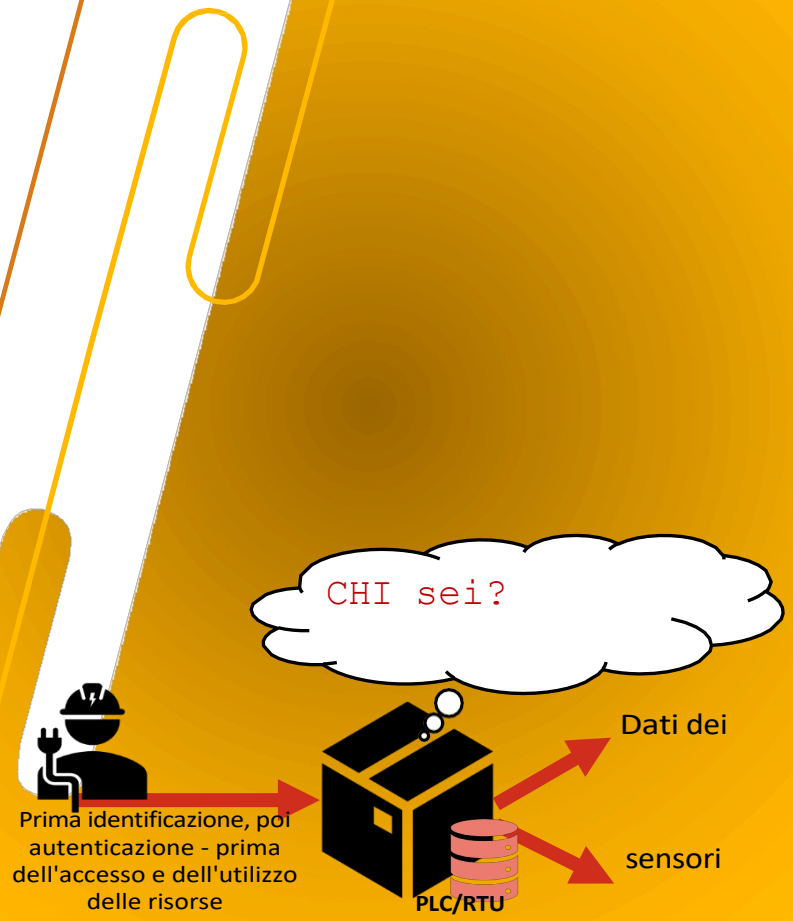
Autenticazione e identificazione

- Come discusso in precedenza, il National Institute of Standards and Technology (NIST) ha definito **l'autenticazione** come il modo per
  - "*verificare l'identità di un utente, un processo o un dispositivo, spesso come prerequisito per consentire l'accesso alle risorse di un sistema*"
  - Ciò significa anche che il processo di autenticazione include anche un processo **di identificazione** implicito per identificare utenti, processi o dispositivi

Fonte: CSRC, "Glossario", NIST, 2024.
URL: https://csrc.nist.gov/glossary

Autenticazione e identificazione

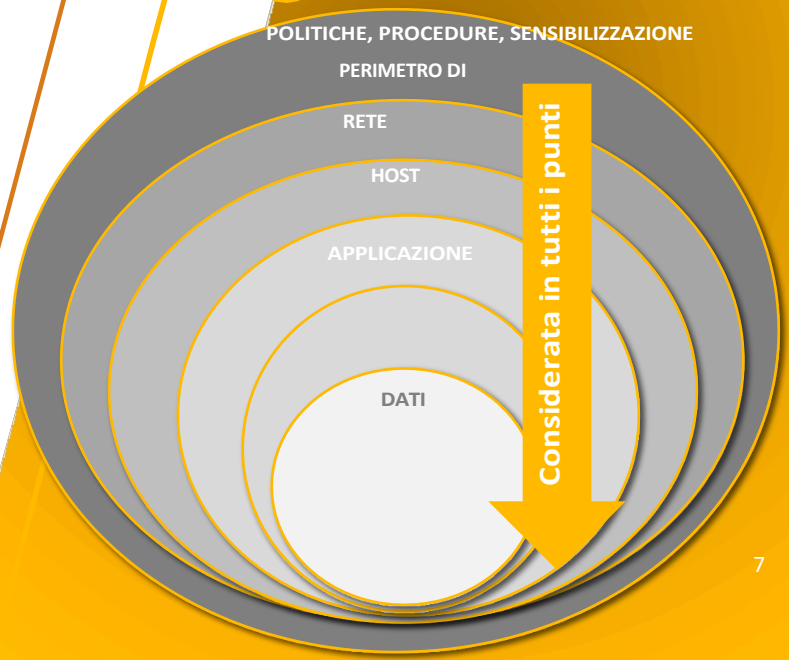
- Come discusso in precedenza, il National Institute of Standards and Technology (NIST) ha definito **l'autenticazione** come il modo per
  - "*Verificare l'identità di un utente, un processo o un dispositivo, spesso come prerequisito per consentire l'accesso alle risorse di un sistema*".
  - Ciò significa anche che il processo di autenticazione include anche un processo **di identificazione** implicito per identificare utenti, processi o dispositivi
- Nei sistemi di alimentazione, queste risorse possono essere:
  - Il perimetro di rete e le sue risorse (router, switch, proxy...)
  - Il server SCADA
  - Dispositivi PLC/RTU
  - Sensori, attuatori
  - Sistemi operativi
  - File, database e archivi
  - Applicazioni software
  - Ecc. – *qualsiasi sistema o dispositivo a cui gli utenti possono avere accesso*



Fonte: CSRC, "Glossario", NIST, 2024.
URL: https://csrc.nist.gov/glossary

Autenticazione nei sistemi di alimentazione

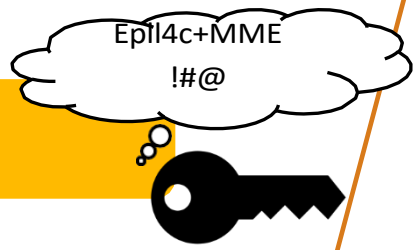
- L'autenticazione è infatti un requisito fondamentale nelle infrastrutture basate su IT/OT e corrisponde **alla prima linea di difesa**
- Questa caratteristica è presa in considerazione anche dall'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) per le reti intelligenti
  - Nella sua relazione sulle "*Misure di sicurezza adeguate per le reti intelligenti*", aggiunge l'autenticazione come parte integrante di:
    - Controllo logico degli accessi (SM 9.3): *«Il fornitore dovrebbe garantire l'accesso logico alle entità autorizzate ai sistemi informativi delle reti intelligenti e* ai perimetri *di sicurezza*».
    - Accesso remoto sicuro (SM 9.4): *«Il fornitore dovrebbe istituire e mantenere un accesso remoto sicuro, ove applicabile, ai* sistemi *informativi delle reti intelligenti*».
  - Per entrambe le condizioni, è essenziale gestire i metodi di autenticazione e le misure di identificazione.
- Pertanto, l'autenticazione DEVE anche essere parte integrante della **difesa in profondità** e deve essere contemplata dal punto di vista normativo e tecnico.



Fonte: ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'attuazione delle misure di sicurezza", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

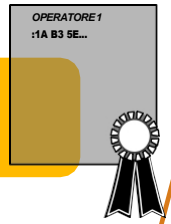
Autenticazione nei sistemi di alimentazione

- Esistono tre modi per autenticarsi:



Cosa so?

- Autenticazione basata su informazioni note solo all'entità corrispondente



Cosa ho?

- Autenticazione basata su qualcosa che l'entità possiede

Chi sono?

- Autenticazione basata su una caratteristica biometrica

Autenticazione nei sistemi di alimentazione

- Esistono tre modi per autenticarsi:

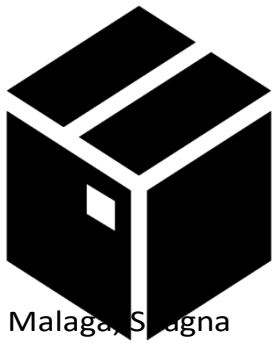
Cosa so?

Cosa possiedo?

Chi sono?

NOME UTENTE /

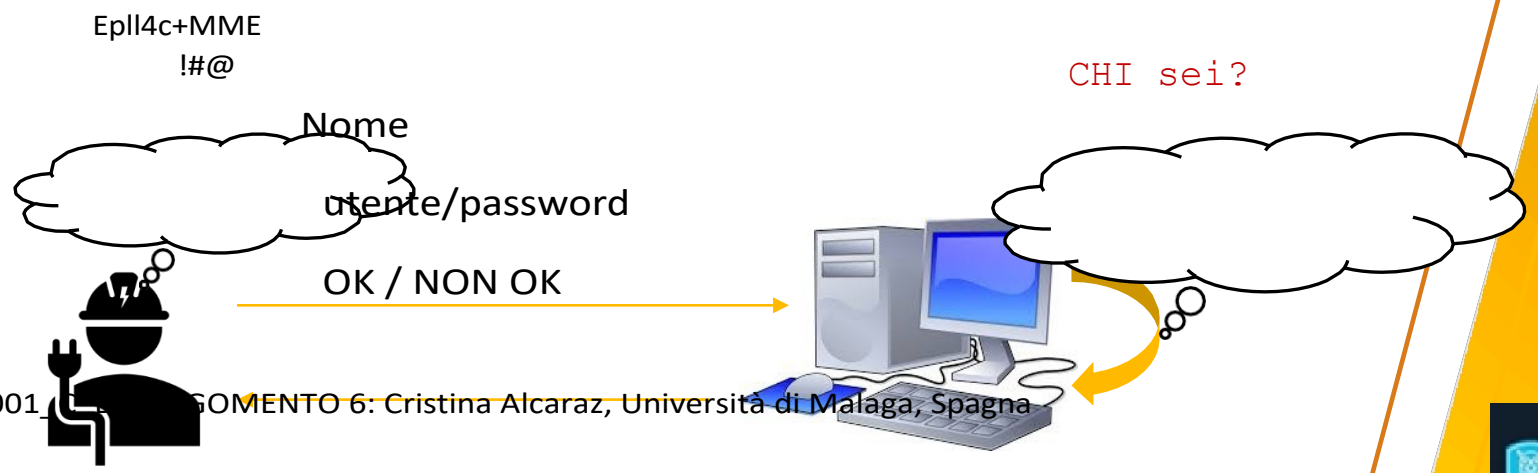
P A S S W O R D



PLC/RTU
Server SCADA HMI

Autenticazione basata su nome utente/password

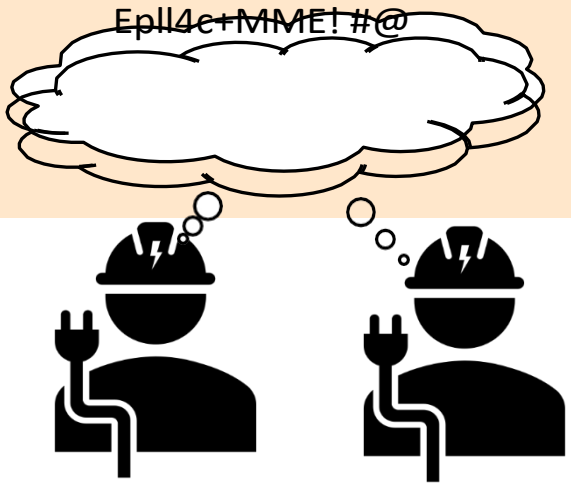
- Nei **sistemi basati su password**, gli utenti, i dispositivi e i processi DEVONO essere registrati con un identificatore univoco insieme a un segreto per consentire l'accesso
- La procedura è semplice:
  1. L'entità fornisce innanzitutto al nodo di destinazione o al server di autenticazione le informazioni necessarie per la sua verifica
  2. Il nodo di destinazione o il server di autenticazione verifica l'identità e il segreto associato
  3. Se tutte queste informazioni sono valide, l'accesso viene concesso



Autenticazione basata su nome utente/password

- Nei sistemi di autenticazione basati su password, si presume che gli utenti conoscano determinate informazioni che nessun altro dovrebbe conoscere: le "password".
- Tuttavia:

Caratteristiche	Inconvenienti (a seconda del token)	Raccomandazioni per le politiche
• La password può essere trasmessa da un utente a un altro, ad esempio in situazioni di emergenza • Può essere utilizzata da più utenti contemporaneamente, ad esempio in situazioni di emergenza	• È assolutamente necessario utilizzare password complesse e non ripeterle • Difficile ricordare tutte le password utilizzate • Per entrambi i motivi, spesso si ricorre a un gestore di password	• Utilizzare frasi lunghe come password o parole complesse con valori alfanumerici • Promuovere la reimpostazione regolare delle password • Evitare di reimpostare password semplici e correlate • Impostare blocchi in base al numero di tentativi • Utilizza server di database di autenticazione robusti, con SALT



Autenticazione basata su nome utente/password supportata da hash

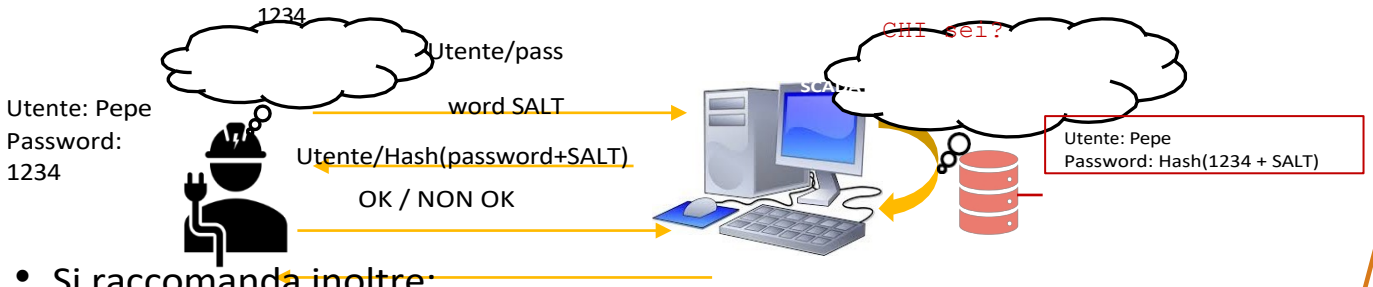
- Le password NON devono essere memorizzate in chiaro
  - Gli account utente memorizzati su un sistema sono normalmente protetti con un valore "hash" associato alla password

Utente: Pepe
Password: 1234

- Quando gli operatori/utenti umani desiderano accedere a una risorsa, viene richiesta la password, che viene sottoposta a hash e confrontata con la password sottoposta a hash memorizzata

Autenticazione basata su nome utente/password supportata da SALT

- Tuttavia, gli aggressori potrebbero essere in grado di lanciare attacchi con dizionario / attacchi Rainbow Table
  - Consiste nel preparare un file con tutte le possibili combinazioni HASH per ottenere la password iniziale
- Per evitare attacchi di tipo "dizionario", è necessario utilizzare un valore "**SALT**"
  - **HASH (PASS + SALT)** in modo tale che SALT sia un numero casuale elevato (minimo 10 valori)



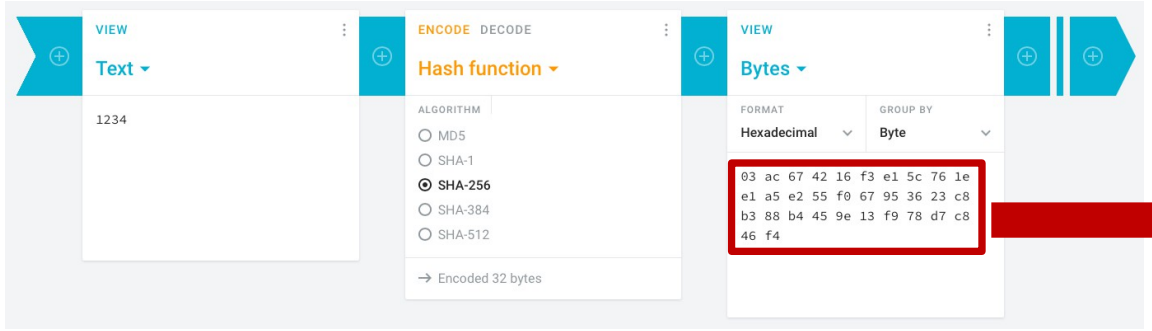
- Si raccomanda inoltre:
  - Non riutilizzare gli stessi valori salt nelle successive ricodifiche
  - Utilizzare funzioni hash robuste (e lente), come PBKDF2*, bcrypt o Argon2id

Attacco dizionario

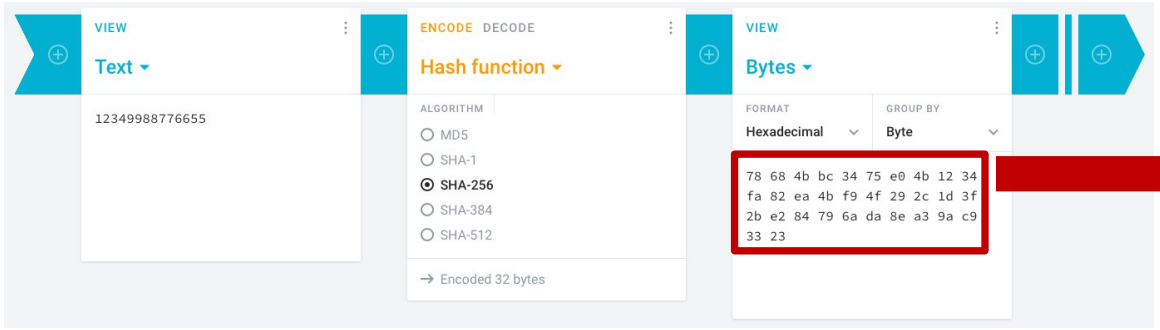
H(1234)→ fallito H(1234Mom)→ fallito H(1234Mylove)→ fallito H(1234Daughter)→ riuscito!

Autenticazione basata su nome utente/password con supporto SALT

- Un modo rapido per mettere in pratica questa lezione è utilizzare lo strumento online **cryptii** (https://cryptii.com):
  - Creare una password con hash (1234)



  - Creare una password con hash + SALT (9988776655)



I due output (o hash) sono completamente diversi per valori di input diversi: uno è più robusto dell'altro

ALIMENTAZIONE

Fonte: Wierk, Cryptii, 2024.
URL: https://cryptii.com

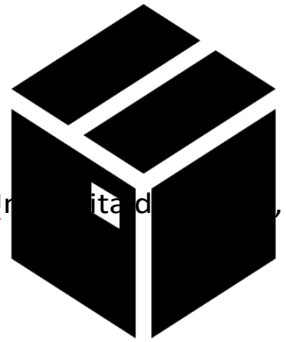
Autenticazione nei sistemi di alimentazione

- Esistono tre modi per eseguire il processo di autenticazione:

Cosa possiedo?

Chi sono?

T O K E N

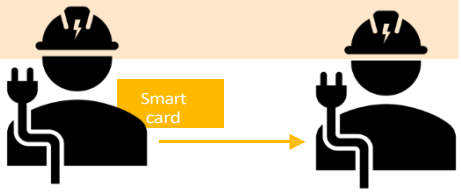


PLC/RTU
Server SCADA HMI

Autenticazione basata su token

- Nei **sistemi di autenticazione basati su token**, gli operatori/utenti possiedono un oggetto fisico che in qualche modo prova la loro identità, come ad esempio:
  - Smartcard, chiavette USB, certificati digitali (contenenti la chiave pubblica degli operatori umani), ecc.
- Tuttavia:

Caratteristiche	Inconvenienti (a seconda del token)
• Il token può essere trasferito da un utente all'altro, ad eccezione dei certificati • Solo un utente alla volta può utilizzarlo	• Non provano effettivamente l'identità degli utenti • Chiunque sia in possesso del token può essere autenticato • In caso di smarrimento o danneggiamento, l'utente legittimo non ha più la possibilità di essere autenticato • Il token può talvolta essere contraffatto

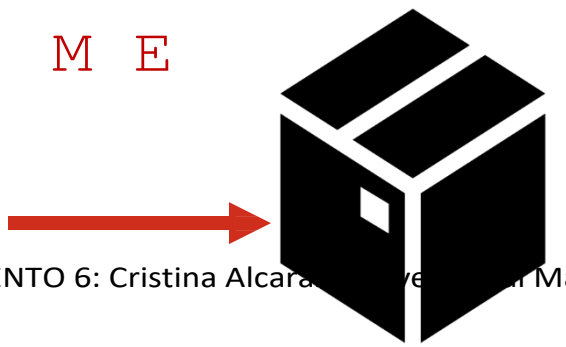


Autenticazione nei sistemi di alimentazione

- Esistono tre modi per eseguire il processo di autenticazione:

Cosa possiedo?

Chi sono?



PLC/RTU

Server SCADA

HMI

Autenticazione basata su dati biometrici

- Nei **sistemi di autenticazione basati sulla biometria**, alcune informazioni vengono estratte dalle caratteristiche biologiche dell'utente (impronte digitali, iride, voce, ecc.).
- Tuttavia:

Caratteristiche	Svantaggi
• I dati biometrici non possono essere trasferiti da un utente all'altro • Solo l'utente può utilizzare i propri fattori biometrici	• Il profilo utente deve essere memorizzato sul computer prima che possa avvenire l'autenticazione • Questi sistemi richiedono misure di protezione speciali • Memorizzazione dei dati biometrici in elementi sicuri per impedire la fuga di dati sensibili • Questi sistemi sono più costosi rispetto ai sistemi precedenti • Se un fattore biometrico viene perso, è perso per sempre, ad esempio un'impronta digitale a causa di un'ustione. • Non tutti i fattori biometrici sono adatti agli ecosistemi industriali, come la voce, a causa del rumore industriale

Autenticazione utente - 2FA, altri

- Finora abbiamo visto i fattori di autenticazione più comuni, ma questi possono essere combinati con altri
- Ad esempio:
  - Con qualcosa che indica la mia POSIZIONE
    - **Autenticazione basata sulla posizione** al momento dell'esecuzione dell'operazione
    - **Autenticazione basata sull'IP** - scopo simile
  - Con qualcosa che IO faccio
    - **Autenticazione basata sul comportamento dell'utente**, come premere un tasto, azionare uno schermo, ecc.
  - Con qualcosa che indica lo STATO CONTESTUALE
    - **Autenticazione basata sul contesto**, come rumore industriale elevato, temperatura elevata dell'area, radiazioni elevate o intossicazione per gli operatori, ecc.

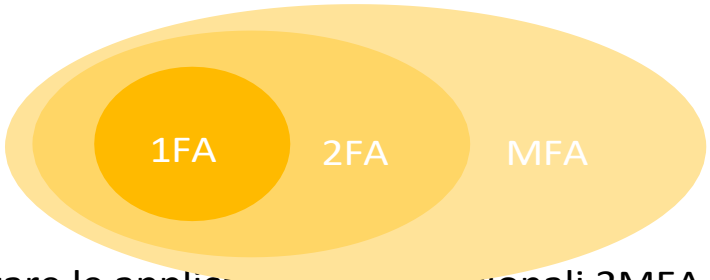
Autenticazione utente - 2FA, altri

- Finora abbiamo visto i fattori di autenticazione più comuni, ma questi possono essere combinati con altri
- Ad esempio:
  - Con qualcosa che indica la mia POSIZIONE
  - Con qualcosa che FACCIO
  - Con qualcosa che indica lo STATO CONTESTUALE

- La combinazione di fattori di autenticazione dà luogo **all'autenticazione a più fattori**
  - 1FA (fattore singolo): quando viene applicato uno dei meccanismi sopra indicati
  - 2FA (due fattori): quando vengono combinati due dei meccanismi sopra indicati (ad esempio, password + token)
  - MFA (multifattoriale): si applicano più di 2 combinazioni (ad es. password + token + dati biometrici)

Autenticazione utente - 2FA, altro

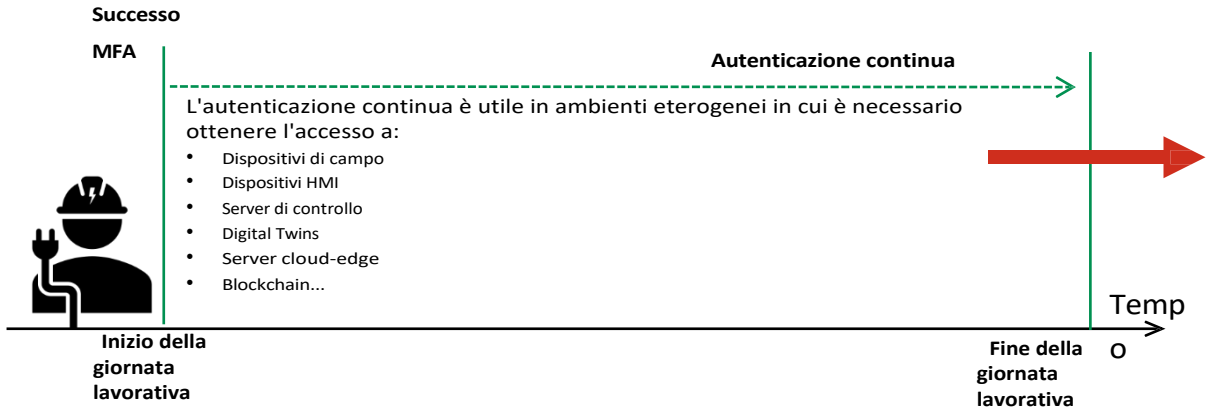
- Maggiore è la combinazione, più robusto sarà il processo di verifica, con conseguente **autenticazione forte**
  - Ciò evita, ad esempio, potenziali rischi di furto d'identità creando livelli di autenticazione che verificano più volte l'identità di un'entità



- Potremmo adattare le applicazioni convenzionali 2MFA nei sistemi di controllo energetico, quali:
  - Google Authenticator o Microsoft Authenticator
    - Entrambe utilizzano codici casuali per consentire l'accesso sicuro ai servizi online, come gli account utente
    - Cioè, fornisce un doppio controllo, almeno sugli account utente considerati "ad alto rischio"

Autenticazione utente - 2FA, altro

- L'uso della MFA è supportato anche da direttive esistenti come la direttiva europea **NIS2 (Network and Information Security)** - DIRETTIVA (UE) 2022/2555
  - Che copre settori critici come quello "energetico", compresi elettricità, riscaldamento e raffreddamento, petrolio, gas e idrogeno
  - La direttiva sottolinea l'importanza dell'uso **dell'autenticazione a più fattori e** delle soluzioni **di autenticazione continua**



I vantaggi rilevanti **dell'autenticazione continua** sono:

- Maggiore produttività grazie alla riduzione del processo di autenticazione ad ogni accesso
- Trasparenza per amministratori IT/OT, ingegneri, manager...
  - anche se questo dipende dall'approccio
- Elevate garanzie di sicurezza

Fonte: Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, 2022
URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27

Osservazioni finali

- Nel corso di questo argomento abbiamo esaminato i fattori di autenticazione più rilevanti presenti in letteratura
  - Esplorandone il significato e la capacità di combinazione
- In particolare, abbiamo esplorato:
  - 1FA, basato su ciò che so, ciò che ho, ciò che sono, ciò che faccio, …
  - 2FA, basata sulla combinazione di due fattori
  - MFA, basato sulla combinazione di più fattori
- Ma abbiamo anche constatato la necessità di prendere in considerazione i quadri normativi che supportano la tecnica
  - Soprattutto quelli incentrati sul settore energetico, come la direttiva NIS2
- Nella NIS2 viene menzionato il concetto di "autenticazione continua"
  - Questo approccio può aggiungere un valore significativo alla catena di produzione e può favorire l'emergere di situazioni in cui le tecniche di autenticazione vengono applicate correttamente
  - Tuttavia, non tutti gli approcci sono efficaci: l'uso di fattori biometrici può essere appropriato, ma in alcuni ambienti industriali può essere difficile da applicare

Riferimenti e fonti

1. CSRC, "Glossario", NIST, 2024.
   URL: https://csrc.nist.gov/glossary
2. Wierk, Cryptii, 2024. URL:
   https://cryptii.com
3. ENISA, "Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'attuazione delle misure di sicurezza", 2012.
   URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids
4. Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27
5. DeepL Translator per la revisione:
   https://www.deepl.com/translator

Connettiti con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Per qualsiasi domanda, non esitate a contattare:

- Cristina Alcaraz
  Professore associato
  Università di Malaga
  alcaraz@uma.es