Elementi essenziali e gestione della sicurezza informatica per il settore energetico

CSP001_C_E

PRESENTAZIONE DI:
ANTONIO MUÑOZ
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 5: Sicurezza Progettazione e implementazione sicura per i sistemi energetici

Panoramica

- Progettazione e implementazione di architetture di rete sicure per i sistemi energetici
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzo della segmentazione di rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- Impiego di VPN per un accesso remoto sicuro ai sistemi energetici e ai dati sensibili

Antonio Muñoz, Università di Malaga, Spagna

Argomento 5: Sicurezza Progettazione architettonica e implementazione per sistemi energetici

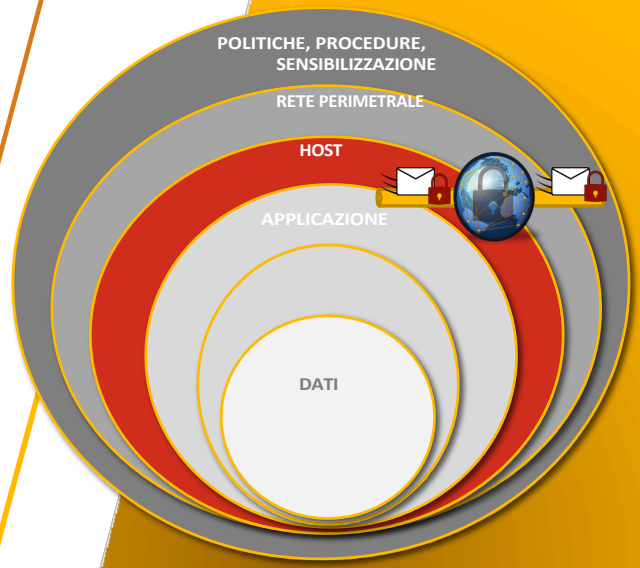
Panoramica

- Progettazione e implementazione di architetture di rete sicure per sistemi energetici
- Architettura di rete sicura nel settore energetico, compresi i sistemi SCADA, le reti intelligenti e altre risorse energetiche critiche
- Utilizzo della segmentazione di rete per isolare i sistemi critici e ridurre l'impatto degli attacchi informatici
- Configurazione di firewall e sistemi di controllo degli accessi per proteggere le reti energetiche e limitare gli accessi non autorizzati
- Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e proteggere le reti
- **Utilizzare VPN per un accesso remoto sicuro ai sistemi energetici e ai dati sensibili**

Accesso remoto sicuro ai sistemi energetici

- In linea con i principi della difesa in profondità, l'accesso remoto fa parte della protezione a livello di rete

- L'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) nel documento "*Misure di sicurezza adeguate per le reti intelligenti*" identifica anche l'accesso remoto come una priorità:
  - "*Il fornitore dovrebbe stabilire e mantenere un accesso remoto sicuro, ove applicabile, ai sistemi informativi delle reti intelligenti*" – SM 9.4
- **Le reti private virtuali** (VPN) sono i meccanismi più comuni per l'accesso remoto
  - Una VPN è definita dal National Institute of Standards and Technology (NIST) come "*una rete virtuale costruita su reti esistenti in grado di fornire un meccanismo di comunicazione sicuro per i dati e le informazioni IP trasmesse tra* reti".



ID	SM 9.4
Measure	Secure remote access.
Definition	The provider should establish and maintain secure remote access where applicable to smart grid information systems.
Example	[From NISTIR 7628 - SG.AC-2 Remote Access Policy and Procedures - Requirement 1] The organisation documents allowed methods of remote access to the smart grid information system. [From IEC 62443 - 4.3.3.6.6 Develop a policy for remote login and connections] The organisation shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity.

La virtualizzazione della rete è spesso collegata al concetto di "tunneling".

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

Elementi principali di una VPN e fasi di esecuzione

- Una VPN comprende una serie di **elementi essenziali**:
  - Server VPN o gateway VPN
  - Il client VPN corrisponde a un'applicazione specifica (ad esempio Tunnelblick o OpenVPN) in grado di comprendere una serie di condizioni di configurazione e interfacce
  - Configurazioni relative alle interfacce e ai componenti virtuali, nonché al tipo di crittografia, autenticazione, meccanismi di scambio delle chiavi, ecc.
  - Protocolli di comunicazione VPN

Elementi principali di una VPN e fasi di esecuzione

- Una VPN comprende una serie di **elementi essenziali**:
  - Server VPN o gateway VPN
  - Il client VPN corrisponde a un'applicazione specifica (ad esempio Tunnelblick o OpenVPN) in grado di comprendere una serie di condizioni di configurazione e interfacce.
  - Configurazioni relative alle interfacce e ai componenti virtuali, nonché al tipo di crittografia, autenticazione, meccanismi di scambio delle chiavi, ecc.
  - Protocolli di comunicazione VPN

- La sicurezza garantita da una VPN segue una serie di **fasi di esecuzione**:
  - Autenticazione reciproca
  - Negoziazione dei parametri di sicurezza
  - Creazione del canale di comunicazione punto-punto sicuro

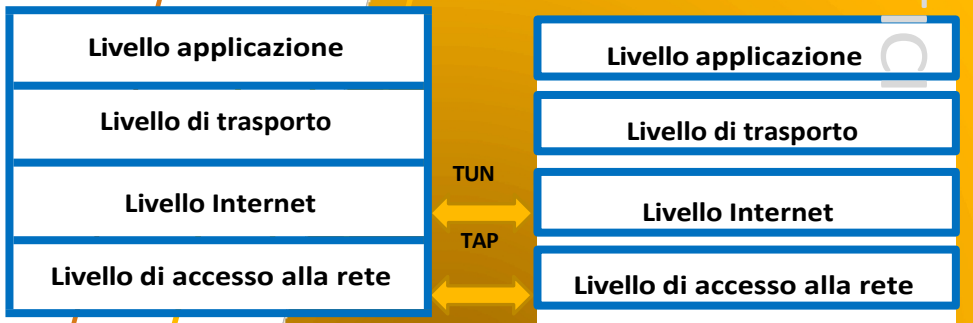
Quattro tipi di VPN

- **VPN con accesso remoto**: un tipo di VPN che consente agli utenti (ad esempio amministratori IT/OT, ingegneri, dirigenti, ecc.) di connettersi alle risorse di un'organizzazione da remoto
- **VPN host-to-host**: simili alle VPN con accesso remoto, ma la connessione avviene tra due computer, ad esempio due server, anziché tra un client e un server
- **VPN site-to-site**: una variante della VPN nota come "site-to-site" applicata per collegare due o più LAN (LAN-to-LAN), come ad esempio due o più reti aziendali appartenenti a infrastrutture diverse (ad es. SCADA-SCADA).
  - La connessione viene stabilita tra i gateway/router delle LAN

- **webVPN**: questo tipo di VPN consente l'accesso remoto tramite un server web, evitando la necessità di installare software client

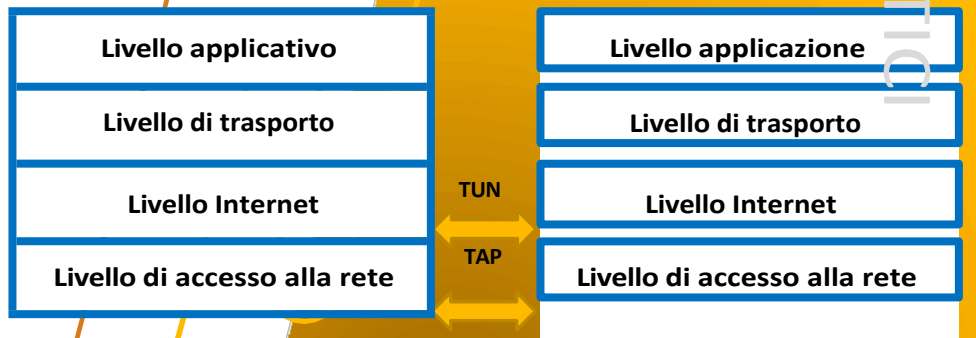
Tipi di interfacce e protocolli VPN

- Per connessioni veloci, è possibile configurare la VPN utilizzando interfacce virtuali che consentono di emulare le istanze di connessione di una rete fisica dal kernel del sistema operativo
- Esistono due tipi di **interfacce virtuali**:
  - **TUN**: funziona a livello di rete e incapsula i frame a livello di rete, facilitando la gestione dei pacchetti IPv4 e IPv6 e il loro instradamento
  - **TAP**: funziona solo sul livello di collegamento, quindi incapsula i frame a livello di collegamento
- Ciò significa anche che le interfacce TUN/TAP consentono l'invio di pacchetti dallo stack TCP/IP corrispondente e dal sistema operativo, emulando anche la ricezione di pacchetti dalla destinazione
  - Sfortunatamente, non tutti i protocolli VPN supportano entrambe le interfacce, TUN/TAP



Tipi di interfacce e protocolli VPN

- Per connessioni veloci, è possibile configurare la VPN utilizzando interfacce virtuali che consentono di emulare le istanze di connessione di una rete fisica dal kernel del sistema operativo
- Esistono due tipi di **interfacce virtuali**:
  - **TUN**: funziona a livello di rete e incapsula i frame a livello di rete, facilitando la gestione dei pacchetti IPv4 e IPv6 e il loro instradamento
  - **TAP**: funziona solo sul livello di collegamento, quindi incapsula i frame a livello di collegamento
- Ciò significa anche che le interfacce TUN/TAP consentono l'invio di pacchetti dallo stack TCP/IP corrispondente e dal sistema operativo, emulando anche la ricezione di pacchetti dalla destinazione
  - Sfortunatamente, non tutti i protocolli VPN supportano entrambe le interfacce, TUN/TAP
- Attualmente esistono molti tipi di **protocolli VPN** che funzionano sui diversi livelli dello stack TCP/IP
  - Livello applicativo: **SSH**
  - Livello di trasporto: **TLS, QUIC, OpenVPN, Wireguard**
  - Livello Internet: **IPSec**
  - Livello di accesso alla rete: **L2TP/IPSec, MACSec**



Si noti che in questo corso verranno esaminati solo alcuni di questi protocolli, non tutti

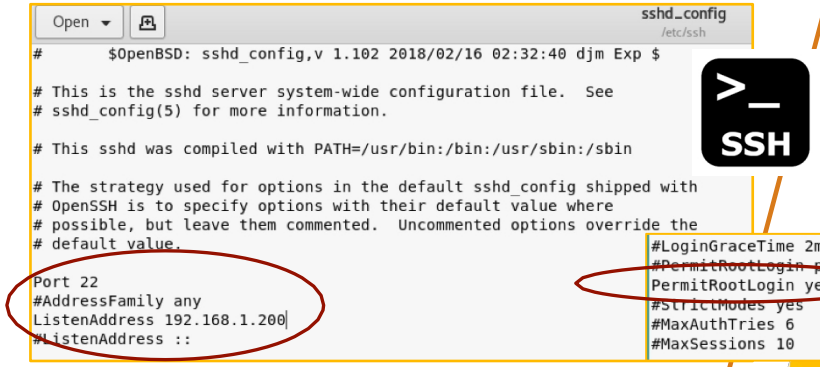
Livello applicativo - Secure Shell (SSH)

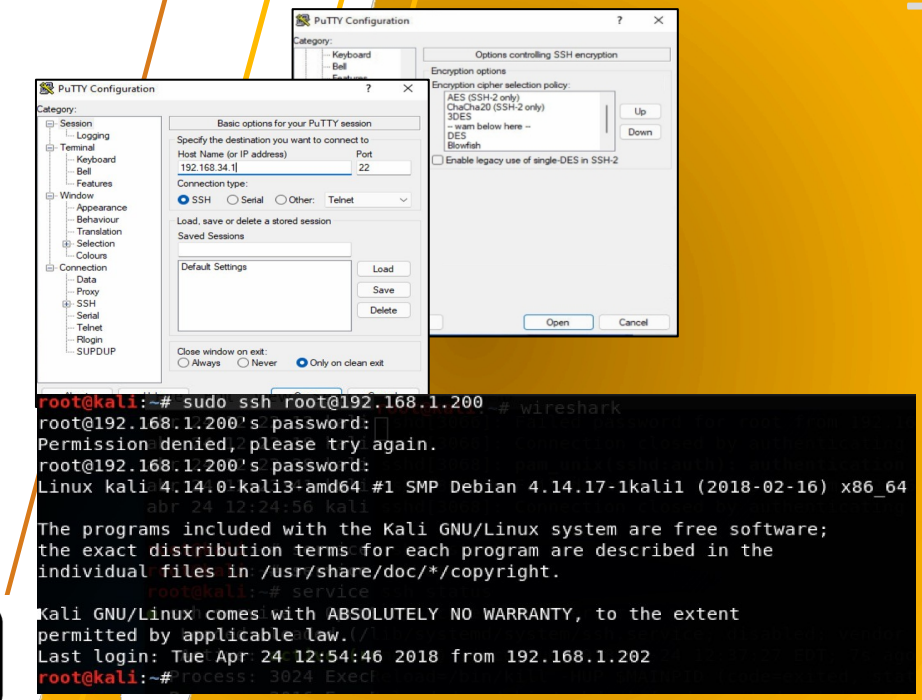
- **SSH stabilisce una comunicazione P2P sulla porta 22**
  - Sostituisce i metodi di accesso remoto tradizionali come telnet o FTP, poiché entrambi i protocolli non sono sicuri
  - I dispositivi operativi legacy potrebbero ancora fare affidamento su telnet e FTP per alcune attività di monitoraggio: evitateli!
- La comunicazione tra il client e il server:
  - Sia il client che il server possono essere autenticati utilizzando un nome utente/password o la crittografia a chiave pubblica
  - La comunicazione è crittografata utilizzando meccanismi di crittografia come AES, Blowfish, DES, ...
- Attualmente esistono due versioni di SSH
  - SSH v.1: deprecata a causa della sua vulnerabilità al MITM
  - **SSH v.2**: evita gli attacchi MITM creando un tunnel P2P, così come gli attacchi di spoofing

Livello applicativo - SSH

- **SERVER in Linux:**
  - Installare il pacchetto server OpenSSH:
    - **$ apt-get install openssh-server**
  - Configurare il servizio nel **file** /etc/ssh/sshd_config: impostare la porta 22, specificare l'indirizzo IP del server, consentire l'accesso root, modificare il percorso delle chiavi private e pubbliche, impostare o limitare gli utenti (e i gruppi), ...
    - Attivare il servizio SSH:
    - **$ service ssh start (riavvia)**
  - **$ service ssh status**

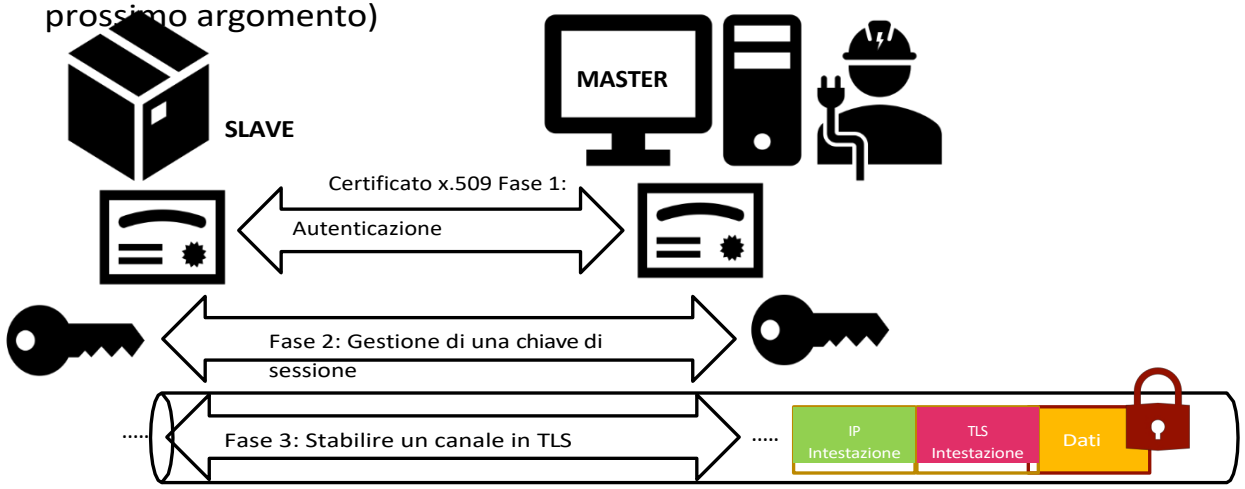
- **CLIENT:**
  - L'accesso può essere effettuato utilizzando alcune GUI: PuTTY, OpenSSH, ...
  - ma anche utilizzando la CLI:
    - **$ sudo ssh user@hostname [comando]**
    - **$ sudo ssh root@XXX.XXXX.XXXX.XXXX**





Livello di trasporto – Transport Layer Security (TLS)

- TLS è supportato dall'Internet Engineering Task Force (IETF) e si basa sul modello **client-server** che include un processo iniziale di autenticazione e negoziazione delle credenziali di sicurezza.
  - Conosciuta come fase di handshake ed eseguita prima della connessione finale
- Questa **fase di handshake** comporta:
  - Stabilisce l'autenticazione (facoltativa) tra peer utilizzando **certificati digitali x.509**
  - Negozia una chiave di sessione per la crittografia e una chiave per l'autenticazione (MAC – descritta in dettaglio nel prossimo argomento)

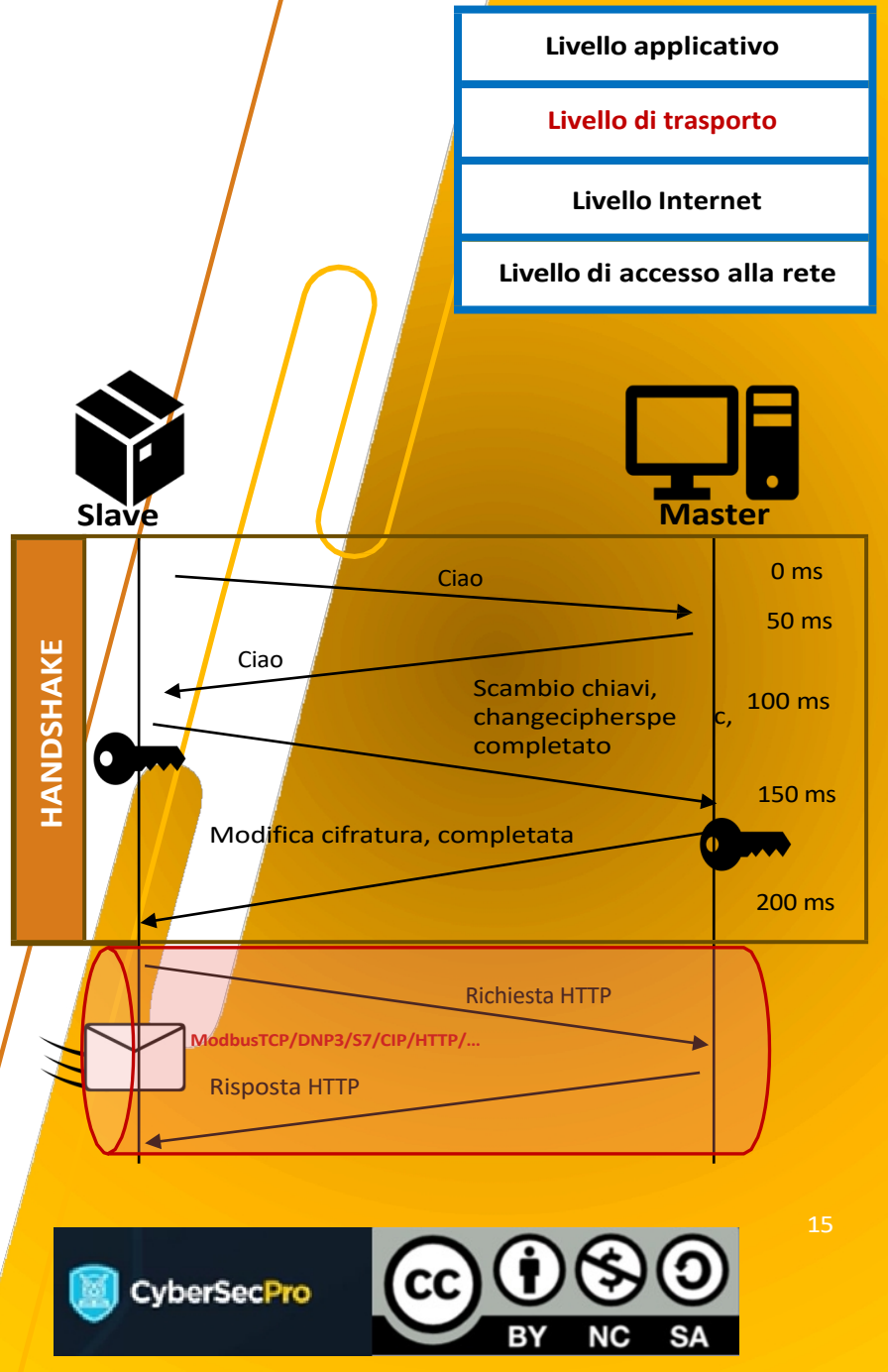


Pausa: Nozioni preliminari sui certificati digitali

- Un certificato digitale è un documento "elettronico" che attesta che i dati collegati a un'entità (ad esempio, operatore umano, dispositivo master, dispositivo slave) sono completamente validi e corretti
- **Il certificato X.509** è il formato più diffuso oggi per l'autenticazione degli utenti e contiene:
  - Numero di serie
  - Identificativo dell'utente e dell'emittente (che firma il certificato)
  - La chiave pubblica
  - Data di scadenza
  - **Firma digitale**
- Questa firma è emessa da un'autorità di certificazione (CA)
  - Che verifica l'identità di un utente e firma il documento
  - Questo documento include la **chiave pubblica**

Livello di trasporto – TLS-1.2 vs. TLS-1.3

- **TLS 1.2** consiste in un modello client-server basato su una serie iniziale di messaggi corrispondenti alla fase di handshake
- Questa fase di handshake ha lo scopo di:
  - Autenticare facoltativamente ciascuna parte e
  - Negoziare la chiave di sessione (riservatezza) insieme a una chiave aggiuntiva per il MAC (integrità e autenticazione)
- Messaggi nella **fase di handshake**:
  - *Ciao*: richiesta di connessione, contenente informazioni sui parametri di sicurezza (ad es. AES-128 bit) e l'ID della sessione
  - *KeyExhange*: per creare la chiave di sessione
  - *ChangeCipherSep*: accettazione dei parametri di sicurezza
  - *Finished*: la fase di handshake è terminata.
- **Ogni messaggio può richiedere circa 50 ms**
  - Questo valore può essere significativo per quelle sottostazioni che richiedono una comunicazione in tempo reale

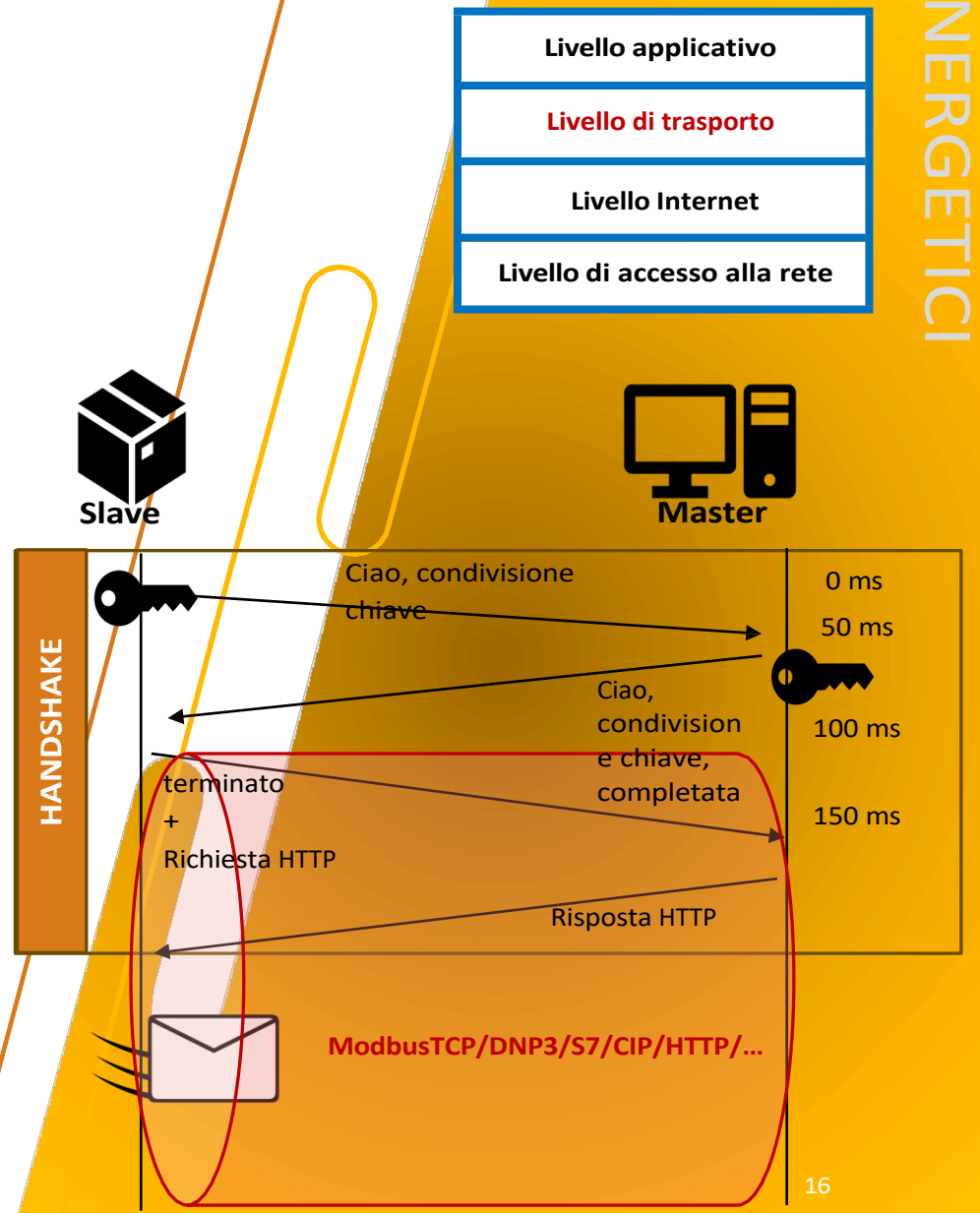


Livello di trasporto – TLS-1.2 vs. TLS-1.3

- **TLS 1.3** è simile a TLS 1.2, con obiettivi equivalenti, ma riduce il numero di frame durante la fase di handshake (3 in totale) e i tempi per la connessione finale
- Infatti, TLS 1.3 garantisce:

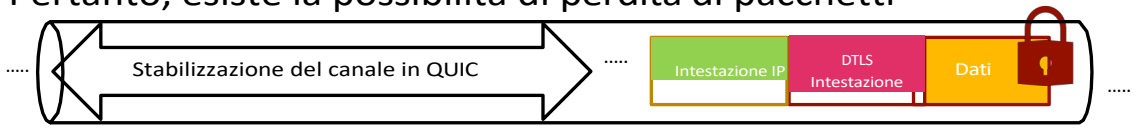
+Sicurezza	+Prestazioni
• La chiave di sessione viene negoziata dal primo frame, consentendo la crittografia dal secondo frame TLS, che può contenere i certificati digitali del Master • AES, ECC, SHA-256/SHA-512, Diffie-Hellman (DH), DH effimero (DHE)	• Rispetto al TLS 1.3, il numero di frame è ridotto inviando più messaggi sullo stesso canale e riducendo l'impostazione dell'handshake a 50 ms in meno

- TLS 1.3 è quindi il protocollo di sicurezza più adatto per contesti critici, come i sistemi di controllo dell'energia



Livello di trasporto – Sicurezza del livello di trasporto datagramma (DTLS)

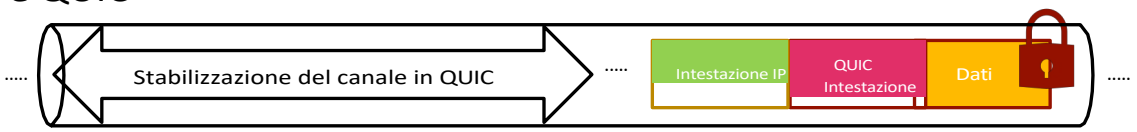
- Anche il DTL è un protocollo supportato dall'IETF:
  - basato su TLS e
  - segue il modello client-server che opera su User Datagram Protocol (UDP)
- Ciò significa anche che le connessioni DTLS sono rapide nel loro processo, ma non sono orientate alla connessione
  - Pertanto, esiste la possibilità di perdita di pacchetti



Livello di trasporto – Connessioni Internet UDP veloci (QUIC)

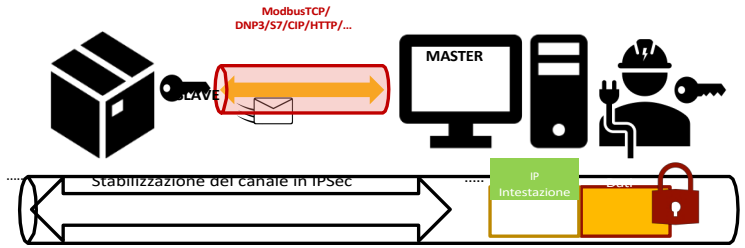
- QUIC è un protocollo supportato dall'IETF (Internet Engineering Task Force) che riduce ulteriormente le connessioni client-server e i relativi tempi di connessione
  - Questa velocità è dovuta alla sua connessione tramite UDP, che non è orientata alla connessione
- A sua volta, QUIC è un protocollo che garantisce la sicurezza
  - Si basa sulla combinazione di TLS1.3 su UDP
  - Ciò significa che QUIC si basa su TLS 1.3
- In altre parole:
  - HTTP/2: TCP (compatibile con TLS 1.2 e TLS 1.3)
  - HTTP/3: UDP (compatibile con QUIC)

Pertanto, i sistemi di controllo e le sottostazioni energetiche potrebbero ottimizzare le loro comunicazioni utilizzando TLS1.3 e QUIC

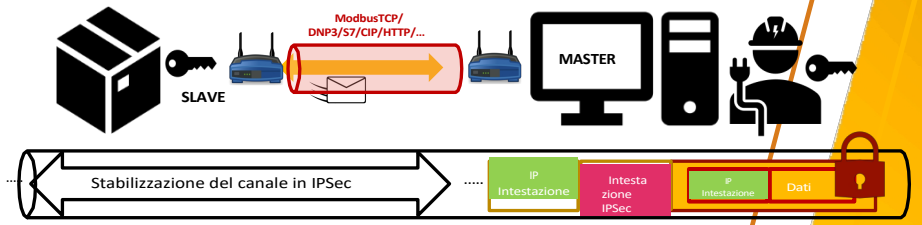


Livello Internet – IPSec

- IPsec aggiunge due modi per incapsulare i dati in un pacchetto sicuro:
  - **Modalità di trasporto**:
    - Tra due peer (una connessione VPN remota), dove non ci sono elementi intermedi per il tunneling, come i router
    - Il payload del pacchetto è crittografato e l'intero payload e alcuni campi dell'intestazione del pacchetto sono autenticati



  - **Modalità tunnel**:
    - Tra reti (VPN site-to-site) con elementi intermedi quali router
    - L'intero pacchetto viene crittografato, generando una nuova intestazione con gli IP dei router, e l'intero payload e alcuni campi dell'intestazione del pacchetto vengono autenticati



Livello Internet – IPSec (IKEv2)

- La configurazione dei parametri di sicurezza IPSEC è il primo svantaggio
  - Questa configurazione deve essere equivalente sia sul nodo di origine che su quello di destinazione
  - Questa configurazione deve essere eseguita manualmente
- Un modo per automatizzare il processo di configurazione è utilizzare il **protocollo Internet Key Exchange (IKEv2)**
  - IKEv2 consiste in un'applicazione software con una connessione al livello Internet per la configurazione dei parametri Internet
  - Questa configurazione automatica include:
    - **Autenticazione peer**
    - **Negoziazione dei parametri di sicurezza**
  - IKEv2 implementa, ad esempio:
    - DH per la negoziazione delle chiavi
    - MAC per l'autenticazione e l'integrità
    - AES e 3DES per la riservatezza

Considerazioni finali

- Sia le reti di controllo che le sottostazioni devono attivare il meccanismo di sicurezza esistente basato su **protocolli di sicurezza che funzionano sullo stack TCP/IP**, quali:
  - SSH
  - TLS
  - DTLS
  - QUIC
  - IPSec
- Tutti questi protocolli sono rilevanti per gli ambienti critici, principalmente perché sono in grado di **proteggere i dati sensibili e garantire riservatezza, autenticazione e integrità**
  - Tuttavia, non tutti sono ugualmente efficaci per ambienti con restrizioni in cui è richiesta una comunicazione (quasi) in tempo reale
  - In questo senso, i protocolli più caratteristici sono: TLS1.3, QUIC e IPSec

Riferimenti e fonti

1. ENISA, “Misure di sicurezza adeguate per le reti intelligenti. Linee guida per valutare la sofisticatezza dell'implementazione delle misure di sicurezza”, 2012
   URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids
2. NIST, CSRC
   URL: https://csrc.nist.gov/glossary
3. IETF, Protocollo di sicurezza IP (IPSec)
   URL: https://datatracker.ietf.org/wg/ipsec/about/
4. IETF, Roadmap dei documenti relativi alla sicurezza IP (IPSec) e allo scambio di chiavi Internet (IKE) URL: https://datatracker.ietf.org/doc/html/rfc6071
5. IETF, Indagine sui protocolli di sicurezza dei trasporti URL: https://datatracker.ietf.org/doc/html/draft-pauly-taps-transport-security-01
6. IETF, Indagine sull'interazione tra protocolli di sicurezza e servizi di trasporto URL: https://datatracker.ietf.org/doc/html/rfc8922
7. 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/

Grazie

Per qualsiasi domanda, non esitate a contattare:

- Antonio Muñoz
  Professore associato
  Università di Malaga
  anto@uma.es