RELAZIONE SU CONNESSIONE CRITTOGRAFATE

*Giovanni Ciampa*

Sempre più spesso in quest’era digitale si sente parlare o assistere a furti, estorsioni, manomissioni o addirittura di distruzione di contenuti riservati tramite attacchi informatici più comunemente via email a persone. Per questo motivo ritengo personalmente affrontare e spiegare questo argomento utile al fine di proteggere e garantire la privacy e la sicurezza dei dati personali, ovvero la crittografia*.* Negli ultimi tempi tra le aziende aumentano le “sfide” in termini di [sicurezza informatica](https://blog.osservatori.net/it_it/sicurezza-informatica-gestione-cyber-security-azienda). Uno dei modi per proteggere le connessioni sono l’uso dei protocolli di sicurezza SSL e TLS. Il protocolloSSL (Secure Socket Layer) è una tecnologia che consente di proteggere la comunicazione tra un browser client e un server. Se si considera la sicurezza della posta elettronica, SSL garantisce che nessun dato della posta sia esposto ai man-in-the-middle durante il transito. Esistono due scopi principali per i quali è possibile utilizzare i certificati SSL nelle e-mail per autenticare e verificare l’identità del mittente e mantenere l’integrità del contenuto della posta elettronica. Uno dei casi d’uso più importanti per un certificato SSL nella sicurezza della posta elettronica è garantire che la comunicazione con il server di posta sia sicura. Gli hacker invece potrebbero assumere il controllo del server di posta e quindi accedere alle e-mail. Installare un certificato SSL e crittografare le e-mail proteggerà le e-mail da qualsiasi tipo di attacco Man-in-the-middle. Il protocollo TLS (Transport Layer Security) invece TLS utilizza una “stretta di mano” tra il lato client e il server per stabilire connessioni crittografate. Garantisce la sicurezza della comunicazione e autentica gli endpoint e funziona così:

* sia il mittente dell’e-mail che il destinatario si scambiano le funzionalità di crittografia;
* i certificati SSL/TLS per entrambe le parti sono autenticati;
* il protocollo TLS aiuta a stabilire una connessione sicura.

Questi due protocolli si basano sulla crittografia che è un processo di codifica delle informazioni in modo che solo gli utenti autorizzati possano accedervi. In altre parole, le differenti tipologie di crittografia consentono di convertire i dati in chiaro in array casuali di valori alfanumerici. Tali valori sono difficili da decodificare per un criminal hacker e possono essere decifrati attraverso una chiave di sicurezza che sarà in possesso di un utente autorizzato. Tale tecnica è parte di una scienza più ampia, la crittologia, che studia, oltre alle tecniche di occultamento, anche la decifrazione di informazioni celate. Questa seconda componente è definita in linguaggio tecnico “crittoanalisi”. In passato la crittologia ha riguardato quasi esclusivamente il contesto militare, a supporto o in contrapposizione a pratiche di spionaggio. Attualmente,la crittografia è utilizzata ampiamente in tutti i contesti informatici, viene generalmente ricordata come strumento atto a garantire la sicurezza delle comunicazioni in rete, in particolare di transazioni monetarie e della firma digitale. L’applicazione di tecniche di crittografia non è legalmente obbligatoria, tuttavia è altamente consigliabile in relazione ad esempio al GDPR. Il Garante per la protezione dei dati personali esorta vivamente l’applicazione della crittografia come misura aggiuntiva nei casi in cui le difese informatiche non siano efficaci o siano rese sterili. Per evitare conseguenze causate dalla diffusione di dati personali, in un contesto legato alla privacy, la crittografia contribuisce ad evitare sanzioni pecuniarie, rientrando tra le misure tecniche e organizzative che il titolare del trattamento è chiamato ad adottare. Più nello specifico la crittografia è un sistema di protezione legato al dato e avviene mediante la cifratura dei caratteri: l’algoritmo crittografico è la funzione matematica attraverso cui si procede a occultare il testo, rendendolo di fatto cifrato. L’accesso alle informazioni invece, avviene attraverso una cosiddetta chiave digitale, capace di renderle accessibili. Le funzioni cifranti disponibili oggigiorno, in relazione a una maggiore capacità computazionale, rendono molto complesso l’ingresso furtivo ai dati: è naturalmente necessario che la chiave digitale sia distribuita il meno possibile. I sistemi crittografici sono identificabili in due categorie: la crittografia simmetrica e quella asimmetrica. Convenzionalmente si fa riferimento al primo gruppo come la tecnica principale. Nella crittografia simmetrica, la chiave, definita privata o segreta, è univoca sia in fase di cifratura che di decifratura**.** Per accedere ad un contenuto protetto con questa tecnica è necessario quindi che avvenga lo scambio della chiave tra i due soggetti. Questo sistema risulta efficiente, veloce e comodo per la trasmissione di dati in blocco, ma la necessità di scambiarsi la chiave lo rende vulnerabile. Lo standard a chiave simmetrica per eccellenza, nonché il più diffuso, è l’AES (Advanced Encryption Standard), articolato in tre algoritmi di cifrature a blocchi (a 128, 192 e 256 bit). Nonostante le criticità dei sistemi simmetrici, AES è il metodo più versatile e diffusamente utilizzato nella protezione di documenti di Stato secret e top-secret. Esistono invece tecniche che sfruttano la crittografia asimmetrica: questo approccio prevede che la cifratura iniziale avvenga tramite una chiave pubblica (o circolante) appartenente al destinatario, che sarà in grado di decifrare il contenuto esclusivamente attraverso un’ulteriore chiave, in questo caso privata. Questa tecnica è stata concepita per eludere i rischi connessi alla trasmissione delle chiavi, in quanto quella pubblica che circola non è sufficiente per decriptare il contenuto protetto. La crittografia asimmetrica è il sistema utilizzato sia nella firma digitale, strumento atto a dare validità legale ad un documento, sia nelle chat online (cosiddetta crittografia End-to-End) come ad esempio su Whatsapp. L’applicazione della crittografia asimmetrica ha tuttavia lo svantaggio di richiedere una capacità computazionale relativamente elevata in quanto è ritenuta sicura se sono usate chiavi di almeno 1024 bi. Concludo dicendo che ad oggi purtroppo ci sono ancora organizzazioni che ignorano i certificati e-mail e le tecnologie di crittografia per le loro comunicazioni sensibili. I certificati e-mail e le tecnologie di crittografia sono molto importanti perché non solo proteggono i propri dati, ma impediscono anche ai malintenzionati di sfruttare i propri sistemi. Le aziende con comunicazioni interne massicce devono ripensare le proprie strategie di sicurezza, analizzare i protocolli esistenti, comprendere la crittografia e ottenere certificati adeguati per i propri sistemi.