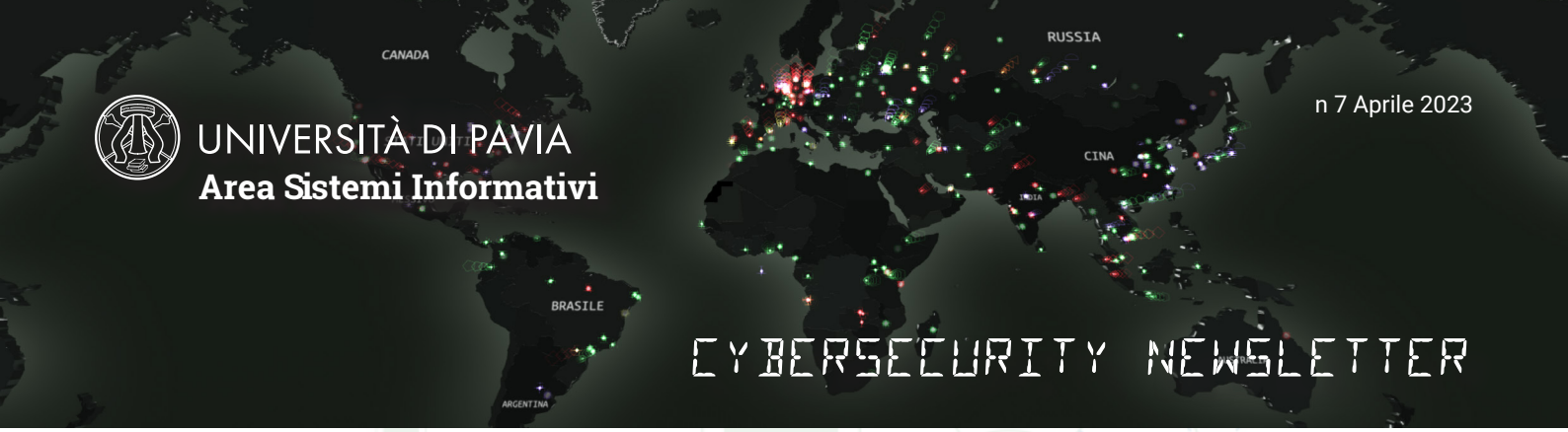


UNIVERSITÀ DI PAVIA
Area Sistemi Informativi

n 7 Aprile 2023

Attacchi informatici: le misure di difesa dell'Ateneo nell'ultimo mese

I tentativi di intrusione nei sistemi informatici o di raccolta illecita di informazioni sono un fenomeno da monitorare e fronteggiare quotidianamente in Ateneo.

Ad oggi non ci sono state perdite di dati grazie alle misure di protezione adottate che hanno ben anticipato le intenzioni malevole e messo al sicuro il lavoro interno svolto.

La sicurezza collettiva dipende molto anche dalla responsabilità del singolo nell'utilizzare i propri dispositivi, tenerli aggiornati e relazionarsi con l'Area Sistemi Informativi qualora non si senta adeguatamente protetto.

I numeri sotto riportati evidenziano infatti ancora margini di miglioramento nel comportamento di ciascuno di noi oltre alla necessità di un costante lavoro interno ad ogni struttura al fine di acquisire consapevolezza dei rischi e quindi di adottare comportamenti adeguati alle condizioni di sicurezza.

In questo mese abbiamo avuto 11 pc infetti che sono stati segnalati e bonificati e circa 151 comunicazioni C&C rilevate e bloccate. Il drastico calo di comunicazioni C&C. Il perdurare dei test di Cisco Umbrella che permette un blocco delle comunicazioni malevoli a livello di risoluzioni DNS si sta rivelando uno strumento fondamentale per ridurre i rischi di attacchi.

Queste tipologie di attacchi rappresentano uno dei primi fenomeni da monitorare poiché potrebbero nascondere malware, cryptolocker o altri fenomeni malevoli che approfondiremo nei successivi numeri di questa newsletter.

In questo numero della newsletter relativa alla cybersecurity tratteremo delle tecniche di cifratura con chiave assimmetrica alla base delle comunicazioni protette su internet.

Malware and Attacks

11
Computers Infected with Bots

151
Communications with C&C* Sites

* C&C - Command and Control.
If proxy is deployed, there might be additional infected computers.

4 Known Malware Downloaded by

10 Users

2 Zero-Days Downloaded

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

123
Unique Software Vulnerabilities were Attempted to be Exploited

Indicates potential attacks on computers on your network.

High Risk Web Access

6
High Risk Web Applications

19.4MB

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

0
High Risk Web Sites

0 hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

SaaS Applications

0
SAAS Applications Seen

1
Users Using SAAS Application

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines.

Data Loss

0
potential data loss incidents

0
sensitive data categories

Indicates information sent outside the company or to unauthorized internal users. Information that might be sensitive. See GDPR Article 5

Crittografia assimmetrica.

La crittografia asimmetrica, conosciuta anche come **crittografia a coppia di chiavi, crittografia a chiave pubblica/privata** o anche solo **crittografia a chiave pubblica**, è un tipo di crittografia dove, come si deduce dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- La chiave pubblica, che deve essere distribuita;
- La chiave privata, appunto personale e segreta che non transita mai in rete;

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

Ci sono due funzioni che possono essere realizzate: cifrare messaggi con la chiave pubblica per garantire che solo il titolare della chiave privata possa decifrarlo oppure usare la chiave pubblica per autenticare un messaggio inviato dal titolare con la chiave privata abbinata.

Due degli usi più noti della crittografia asimmetrica sono:

- **La crittografia a chiave pubblica**, in cui un messaggio viene criptato con la chiave pubblica del destinatario. Se gli algoritmi sono scelti e utilizzati in modo appropriato, i messaggi non possono essere decifrati da nessuno che non possieda la chiave privata corrispondente, che si presume quindi essere il proprietario di tale chiave e quindi la persona associata alla chiave pubblica. Questo può essere utilizzato per garantire la privacy di un messaggio.
- **La firma digitale**, in cui un messaggio viene firmato con la chiave privata del mittente e può essere verificato da chiunque abbia accesso alla chiave pubblica del mittente. Questa verifica dimostra che il mittente ha avuto accesso alla chiave privata e quindi è molto probabile che sia la persona associata alla chiave pubblica. Inoltre, dimostra che la firma è stata preparata per quel preciso messaggio, poiché la verifica fallirà per qualsiasi altro messaggio che si possa concepire senza utilizzare la chiave privata.

In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. Per fare ciò, deve essere computazionalmente facile per un utente generare una coppia di chiavi pubblica e privata da utilizzare per cifrare e decifrare. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica.

La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.

I sistemi di crittografia a chiave pubblica spesso si basano su algoritmi di crittografia basati su problemi matematici che attualmente non ammettono alcuna soluzione particolarmente efficiente, quelli che riguardano la fattorizzazione di un numero intero, il logaritmo discreto e le relazioni delle curve ellittiche. Gli algoritmi a chiave pubblica, a

differenza degli algoritmi a chiave simmetrica, non richiedono un canale sicuro per lo scambio iniziale di una (o più) chiavi segrete tra le parti.

A causa del peso computazionale della crittografia asimmetrica, essa di solito è usata solo per piccoli blocchi di dati, in genere il trasferimento di una chiave di cifratura simmetrica (per esempio una chiave di sessione). Questa chiave simmetrica è utilizzata per cifrare messaggi lunghi. La cifratura/decifratura simmetrica è basata su algoritmi semplici ed è molto più veloce. L'autenticazione del messaggio include hashing del messaggio per produrre un "digest" (risultato dell'output dell'algoritmo di hash), e crittografando il digest con la chiave privata per produrre una firma digitale. Da lì in poi chiunque può verificare questa firma:

1. calcolando l'hash del messaggio;
2. decifrando l'hash del messaggio;
3. confrontando la firma del messaggio.

L'uguaglianza tra i digests conferma che il messaggio non è stato modificato da quando è stato firmato, e che il firmatario, e nessun altro, intenzionalmente abbia eseguito l'operazione di firma, presumendo che la chiave privata del firmatario sia rimasta segreta. La sicurezza di questo tipo di procedura dipende dall'algoritmo di hash di questa data qualità che è computazionalmente impossibile modificare o trovare un messaggio sostituito che produca lo stesso digest, ma gli studi hanno dimostrato che con gli algoritmi MD5 e SHA-1, produrre un messaggio alterato o sostituito non è impossibile. L'attuale standard di hash per la crittografia è SHA-2. Lo stesso messaggio può essere usato al posto del digest.

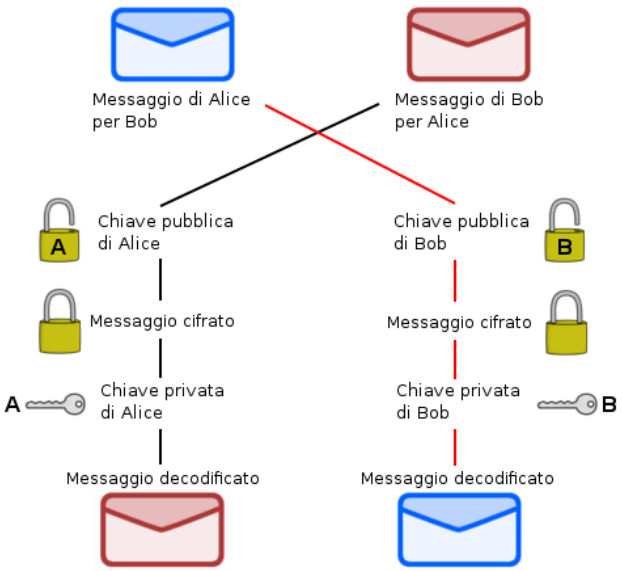
Gli algoritmi a chiave pubblica sono ingredienti fondamentali della sicurezza dei crittosistemi, applicazioni e protocolli. Essi sono alla base dei diversi standard Internet, come ad esempio Transport Layer Security (TLS), S/MIME, PGP e GPG. Alcuni algoritmi a chiave pubblica forniscono una distribuzione di chiave e segretezza (ad esempio, scambio di chiavi Diffie-Hellman), alcuni di fornire firme digitali (ad esempio Digital Signature Algorithm), altri forniscono entrambe (esempio RSA).

La crittografia a chiave pubblica trova applicazione in vari campi, tra gli altri: nella disciplina di sicurezza informatica e nella sicurezza delle informazioni. La sicurezza delle informazioni si occupa di tutti gli aspetti per la protezione delle risorse informative elettroniche contro le minacce sulla sicurezza. La crittografia a chiave pubblica viene utilizzata come metodo per assicurare la riservatezza e l'autenticazione delle comunicazioni e per la memorizzazione dei dati.

Descrizione del processo di criptazione

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob, i lucchetti fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

1. Alice chiede a Bob di spedirle il lucchetto già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob;



2. Alice riceve il lucchetto di Bob e, con esso, chiude il pacco e lo spedisce a Bob;
3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice (che lei dovrebbe aver preventivamente dato a Bob) che solo lei potrebbe aprire.

Si può notare come per mettere in sicurezza il contenuto dei pacchi ci sia bisogno del lucchetto del destinatario, mentre per aprirli viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di cifratura/decifratura asimmetrico (una chiave per cifrare ed una differente per decifrare). Chiunque intercettasse il lucchetto (aperto) o il messaggio chiuso con il lucchetto non potrebbe leggerne il contenuto poiché non ha la chiave. Uno dei vantaggi della crittografia asimmetrica sta nel fatto che le chiavi pubbliche possono essere scambiate anche utilizzando un mezzo insicuro, come Internet.

Usando un'altra analogia si può dire che il metodo è analogo a quello di una cassaforte che abbia due chiavi distinte, una usata per aprirla (chiave segreta), l'altra per chiuderla (chiave pubblica).

Nella crittografia simmetrica invece, che basa la sicurezza del sistema sulla segretezza della chiave di codifica/decodifica utilizzata, si rende necessario utilizzare un canale sicuro per la trasmissione della chiave, poiché l'intercettazione della stessa, da parte di terzi, vanificherebbe la sicurezza del sistema stesso.

Differenze con la crittografia tradizionale (simmetrica)

Nella tradizionale crittografia simmetrica, viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Delle due informazioni (la chiave e l'algoritmo) necessarie a chi deve inviare il messaggio, la chiave è quindi identica a quella necessaria a chi deve riceverla, mentre l'algoritmo è facilmente reversibile in quello di decifrazione. Per concordare una chiave con il proprio interlocutore, c'è bisogno di mettersi preventivamente in contatto con lui incontrandolo di persona, telefonandogli, scrivendogli una lettera, mandandogli un messaggio o in qualsiasi altro modo. In qualunque caso, esiste il pericolo che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo.

La crittografia a chiave pubblica permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave, anche se queste non si sono mai

incontrate precedentemente.

Implementazione

Il principio generale della crittografia asimmetrica ha una solida base matematica che lo giustifica; tale base, riassunta e semplificata all'estremo, si fonda sull'uso di un problema complesso, ovvero un'operazione matematica semplice da eseguire, ma difficile da invertire, cioè dal cui risultato è difficile risalire agli argomenti di partenza. L'esempio classico è il problema della fattorizzazione di un numero (trovare i numeri primi che lo producono se moltiplicati tra loro: ad esempio, è facile moltiplicare 17×23 ottenendo 391, ben più difficile è per esempio fattorizzare il numero 377 nei fattori primi 13 e 29) usata nel primo e più famoso sistema crittografico a chiave pubblica: RSA. Le conoscenze di matematica pura sviluppate dall'uomo negli ultimi secoli hanno reso sempre più efficiente fattorizzare, ma nessuno è mai riuscito a far fare quel passo che porta il problema da complesso a non complesso; il problema diventa quindi intrattabile per numeri oltre una certa dimensione.

Attualmente, per la crittografia RSA vengono considerati "sicuri" numeri che in base 10 hanno almeno 600 cifre, il che significa chiavi di 2048 bit e oltre.

Utilizzo della crittografia asimmetrica

Con l'istruzione HTTP Strict Transport Security il server invia i messaggi di risposta alle richieste di connessione HTTP con una intestazione che impone per un certo tempo a qualsiasi user agent (browser e qualsiasi altro tipo di client) di connettersi in maniera cifrata con HTTPS, e non col semplice HTTP.

Per utilizzare questo tipo di crittografia, è necessario creare una coppia di chiavi. Quando vengono generate le due chiavi sono equivalenti (una delle due indifferentemente può essere resa pubblica). La proprietà fondamentale delle due chiavi è che un messaggio cifrato usando una delle due chiavi può essere decifrato soltanto usando l'altra chiave e viceversa. Ciò significa sostanzialmente che le due chiavi funzionano "insieme" pur non essendo possibile dall'una desumere l'altra.

Quando una delle due chiavi viene resa pubblica e l'altra privata, è possibile utilizzarle insieme fondamentalmente per i due scopi già visti:

1. Inviare un messaggio cifrato ad un destinatario.
2. Verificare l'autenticità di un messaggio.

Affinché tutto funzioni, ovviamente, è necessario che il possessore della chiave privata custodisca gelosamente tale chiave e la faccia rimanere tale.

La coppia di chiavi pubblica/privata viene generata attraverso un algoritmo (ad esempio RSA o DSA) a partire da dei numeri casuali. Gli algoritmi asimmetrici sono studiati in modo tale che la conoscenza della chiave pubblica e dell'algoritmo stesso non siano sufficienti per risalire alla chiave privata e tale meccanismo è reso possibile

grazie all'uso di funzioni unidirezionali. In realtà, in molti casi, l'impossibilità di risalire alla chiave privata non è dimostrata matematicamente, ma risulta dallo stato attuale delle conoscenze in matematica e della potenza di calcolo disponibile. Per esempio, è sufficiente un piccolo computer e qualche millesimo di secondo per moltiplicare due numeri primi da 150 cifre, ma occorre il lavoro di decine di migliaia di computer per un anno per trovare i fattori primi di quel numero.

A questo punto, il gioco è fatto: ogni utilizzatore si crea la propria (o le proprie, in casi particolari) coppia di chiavi; la chiave privata viene tenuta segreta e non viene mai rivelata a nessuno (nemmeno alle persone con le quali si comunica); viceversa, la chiave pubblica viene diffusa in vari modi: può essere aggiunta automaticamente in coda a ciascun proprio messaggio nelle varie conferenze elettroniche cui si partecipa, o può essere depositata in archivi pubblici (keyserver) a disposizione di chi la desideri. È importante che la chiave pubblica sia liberamente accessibile, perché chiunque voglia comunicare con la persona che l'ha generata dovrà preventivamente munirsi di questa, con la quale cifrerà il messaggio.

Negoziazione iniziale delle chiavi

Lo scambio delle chiavi asimmetriche avviene in una fase iniziale di negoziazione in cui gli utenti adottano temporaneamente una chiave di sessione simmetrica di supporto alla fase di handshake ovvero di avvio di una sessione con crittografia simmetrica per negoziare la chiave di sessione, il protocollo e gli altri aspetti della connessione cifrata.

La chiave di sessione è temporanea e "usa e getta": non appena è definito tutto ciò che riguarda la connessione cifrata, inizia lo scambio con crittografia a chiave asimmetrica, e la chiave di sessione non è più utilizzata: se la chiave privata di un utente viene compromessa o perde la sua segretezza, è possibile derivare la chiave di sessione e tramite questa la chiave privata scambiata dall'altro utente, e decifrare l'intera comunicazione. Per evitare questo rischio, la Forward secrecy, genera la chiave di sessione a partire da una chiave a lungo termine, diversa da quella pubblica e privata degli utenti.

Firma digitale

Oltre alla cifratura dei dati di una comunicazione, la crittografia asimmetrica presenta altri possibili impieghi: firma digitale per verificare l'autenticazione del mittente e l'integrità informativa del messaggio, fornire una condizione di ending e per i programmi che tentano la forzatura delle chiavi. Un utente può firmare un messaggio utilizzando la propria chiave privata; per far ciò, viene creata un'impronta (digest) del messaggio da firmare e questa, criptata con la chiave privata, rappresenta la firma ed è inviata assieme al messaggio (l'impronta, generata per mezzo di un algoritmo di Hash, è tale che varia sensibilmente al minimo variare del messaggio). Tutti i destinatari

del messaggio possono verificare l'integrità del messaggio stesso e l'autenticazione dell'autore/mittente creando, a partire dal messaggio ricevuto, un'impronta (o digest, utilizzando in maniera simmetrica la stessa funzione hash utilizzata dall'autore del messaggio) e confrontandola poi con quella ricevuta assieme al messaggio e decifrata con la chiave pubblica del presunto autore: se le due impronte risultano identiche il messaggio è integro, ovvero non ha subito modifiche da parte di terzi (ad esempio attraverso attacchi del tipo man in the middle) da quando l'autore a monte l'ha firmato.

Il mittente "attacca" l'hash in fondo al messaggio. Può allora scegliere se codificare (firmare) con la propria chiave privata tutto l'insieme (messaggio e hash), oppure lasciare il messaggio in chiaro e cifrare con la chiave privata solo l'hash. In entrambi i modi, chiunque decodifichi con la chiave pubblica del mittente è certo che sono autenticati il mittente e il contenuto del messaggio (volendo si può aggiungere anche una marca temporale che certifica anche il momento di invio e di ricezione).

La firma digitale fornisce anche una condizione di termine per i programmi che tentano di forzare la cifratura. Tali programmi tentano di ricostruire la chiave privata del destinatario per leggere il messaggio. Il programma ha come riferimento la firma digitale del messaggio, o meglio la decifra con la chiave pubblica del mittente e utilizza l'hash. Il programma propone n chiavi private, per ognuna decifra il messaggio, ne calcola l'hash e lo confronta con quello ricavato dalla firma digitale: se coincidono, è stata trovata la chiave privata giusta ed è visibile il contenuto del messaggio originale.

Per saperne di più...

- per informazioni: **https://trasformazionedigitale.unipv.it**
- per contattare l'Area Sistemi Informativi: **https://sos.unipv.it**
- se sei uno studente scrivi a questo indirizzo: **smart@ unipv.it** oppure contatta un tecnico del tuo dipartimento per ottenere informazioni
- informazioni in tempo reale su attacchi informatici: **https://www.csirt.gov.it**

Fonti

- Wikipedia portale sicurezza informatica - *Crittografia Assimetrica*
- Kaspersky Lab - *Connessioni Crittografate*