FONDAZIONE BRUNO KESSLER
MAGAZINE

Crittografia: una storia lunga millenni

28 Marzo 2022

Quali tendenze per il futuro della Cybersecurity? Una lezione introduttiva con il Prof. Silvio Ranise, direttore del centro Cybersecurity della Fondazione Bruno Kessler

Che cosa hanno in comune il culto dei morti nell'antico Egitto, i servizi segreti spartani nel 900 a.C., il Kamasutra indiano di 2400 anni fa e il cifrario di Cesare?

Che lo scopo fosse aggiungere mistero al culto dei morti oppure difendere un segreto "industriale", o ancora comunicare con i generali piuttosto che fra amanti, **la crittografia, per millenni, ha permesso di mascherare messaggi attraverso rompicapi e stratagemmi che si sono evoluti nel corso della storia fino alla computer science odierna.**

In compagnia di **Silvio Ranise**, direttore del centro di ricerca **FBK Cybersecurity**, abbiamo ripercorso brevemente questa storia per comprendere la complessità delle sfide attuali e i campi applicativi delle tecniche di cybersecurity su scala globale, tra minacce latenti alla democrazia e crescenti opportunità economiche.

Se nel 100 a.C. per comprendere un messaggio con l'uso del **cifrario di Cesare** bastavano mediamente una dozzina di tentativi, con gli attuali calcolatori siamo arrivati a generare chiavi la cui probabilità di essere scovate è dell'ordine di grandezza di 10 seguito da 20 zeri, un numero difficilmente pensabile e quasi indicibile.

In mezzo, siamo passati attraverso l'**analisi di frequenza** suggerita da Al Kindi nell'850 d.C. per tentare di ridurre la complessità degli attacchi ai cifrari grazie alle statistiche sull'occorrenza delle lettere come indizio per riconoscere più velocemente le lettere cifrate; poi abbiamo incontrato il padre della crittografia moderna, l'italiano **Leon Battista Alberti**, genio rinascimentale che ha gettato le basi della crittografia moderna e infine siamo giunti agli sviluppi recenti nel 20° secolo, con la straordinaria impresa di **Alan Turing**, che decrittando il codice Enigma dei nazisti si stima che abbia contribuito ad anticipare di 2 anni la fine della seconda guerra mondiale, risparmiando 14 milioni di vite.

Avvicinandoci ai giorni nostri, siamo passati per il **Data Encryption Standard** (DES), sviluppato nel 1970 da IBM e adottata come standard a partire da 7 anni dopo e fino al 2000, con una dimensione della chiave da 56 bits, per un numero di chiavi pari a 2 alla 56ma = 7*10 alla 16ma

La crittografia attuale ha superato il DES in concomitanza con la crescente potenza di calcolo che ha reso abbordabile il costo della capacità computazionale necessaria (nel 1999 bastavano circa 250 mila USD). Alla fine del 2001 si è passati così all'**Advanced Encryption Standard**, generando circa 1021 più chiavi rispetto all'era DES.

Ricapitolando, gli elementi fondamentali che caratterizzano la crittografia sono le "**dimensioni delle chiavi**" e la **modalità di distribuzione** delle stesse ai partecipanti. Le moderne tecniche che combinano crittografia simmetrica (sfruttata per la sua efficienza) e pubblica (utilizzata per definire protocolli per la gestione sicura delle chiavi) sono incorporate nei protocolli di fruizione della rete internet (**HTTPS**) o vengono impiegate nella messaggistica (end to end encryption).

Tali tecniche proteggono la **privacy** degli utenti, anche di coloro che scambiano informazioni per commettere crimini. Di conseguenza, governi e agenzie di polizia hanno richiesto l'aggiunta di meccanismi utili a permettere loro di controllare il contenuto di messaggi scambiati da potenziali sospetti. Purtroppo questo tipo di meccanismi rende inutile la crittografia in quanto queste vulnerabilità possono essere scoperte indipendentemente anche da malintenzionati che potrebbero sfruttarle per i loro scopi.

Per evitare questo, recentemente Apple ha proposto una tecnica alternativa chiamata "**client side scanning**" che permette la scansione delle risorse locali per rilevare se c'è qualcosa di strano (ad esempio immagini a carattere pedopornografico) e segnalarlo alle autorità. Nonostante il fatto che questa soluzione eviti di inserire vulnerabilità nei cifrari, presenta altri tipi di problematiche perché a seconda del contesto in cui si inserisce può implicare rischi sia in termini etici, discriminando e andando a ledere le prerogative democratiche, che tecnici, presentando dei falsi positivi.

Il finale di questa storia senza fine non solo è aperto ma è tutto nelle nostre mani. Nella sua autobiografia, intitolata "Elogio dell'imperfezione" (Garzanti Editore, 1987), la premio Nobel **Rita Levi Montalcini** scriveva: "Lo sviluppo vertiginoso delle capacità costruttive e distruttive dell'Homo Sapiens, in stridente contrasto con la lentezza dei processi di elaborazione e di manifestazione delle facoltà emotive, alle quali oggi come in passato è affidata la condotta delle nostre azioni, è la causa prima dei pericoli che ci minacciano."

LINK

https://magazine.fbk.eu/it/news/crittografia-una-storia-lunga-millenni/

TAG

- #crittografia
- #cybersecurity
- #cybersicurezza
- #dati
- #democrazia
- #diritto
- #etica
- #informatica

- #privacy
- #sicurezza
- #storia
- #tecnologia

MEDIA COLLEGATI

- Centro di ricerca FBK Cybersecurity : https://www.fbk.eu/it/cybersecurity/
- Articolo su Wired Italia: https://www.wired.it/article/crittografia-end-to-end-politica-contro-pedopornografia/
- Focus ASviS: 5 tendenze per il settore : https://asvis.it/goal16/notizie/491-11192/focus-cybersecurity-i-cinque-trend-che-influenzeranno-il-futuro-del-settore

AUTORI

- Giancarlo Sciascia