UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unIMC

La Crittografia nell'Era Digitale: Tra Sicurezza delle Comunicazioni, Indagini Penali e Protezione della Privacy

Henry Coppari

Facoltà di Ingegneria

Università Politecnica delle Marche – Ancona

E-mail: henry@netcubo.it - Mobile: +39 338.8564434

Giovedì 02 e Venerdì 03 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Indice

Introduzione

Introduzione

Il nostro mondo, sempre più interconnesso, ha reso la **crittografia** una tecnologia cruciale. Nata per scopi militari, oggi è uno strumento indispensabile che protegge non solo i dati personali e le transazioni finanziarie, ma anche la libertà di espressione e la privacy dei cittadini.

Tuttavia, la sua crescente diffusione ha creato un dilemma profondo e complesso. **Come è possibile bilanciare il diritto alla sicurezza delle comunicazioni con la necessità delle autorità di contrastare, accedere alle informazioni vitali per le indagini penali ?**

Questo elaborato, frutto di una consulenza tecnico forense da me eseguita, esplora la crittografia nell'era digitale, analizzando le sue implicazioni su tre fronti principali: la **sicurezza delle comunicazioni**, le **indagini penali** e la **protezione della privacy**. Verrà esaminato il caso giudiziario Sky ECC, che ha evidenziato la tensione tra i diritti individuali e l'interesse pubblico.

L'elaborato si propone anche di offrire un quadro completo delle sfide etiche e legali sollevate dalla crittografia avanzata, esaminando il dibattito sulle **"backdoor"** e le risposte normative, come il **GDPR**, che promuovono la sicurezza senza compromettere la protezione dei dati. L'obiettivo è analizzare come la società e il sistema legale stiano cercando di adattarsi a una tecnologia che continua a evolvere, affrontando la domanda fondamentale: la crittografia è un ostacolo alla giustizia o un pilastro della libertà ?

La crittografia End To End (E2EE)

La crittografia End To End (E2EE)

La **crittografia end-to-end (E2EE)** è considerata il metodo più privato e sicuro per le comunicazioni in rete.

La crittografia end-to-end coinvolge la generazione automatica di una **coppia di chiavi**, una **pubblica** e una **privata**, sul dispositivo del mittente e del destinatario. Il mittente usa la chiave pubblica del destinatario per criptare il messaggio, che diventa illeggibile. Questo messaggio criptato viene inviato attraverso la rete, passando dai server della piattaforma, che non possono decifrarlo. Il destinatario, ricevendo il messaggio, usa la propria chiave privata per decifrarlo, rendendolo nuovamente leggibile solo sul suo dispositivo.

Di seguito i passaggi in dettaglio:

1. **Generazione delle chiavi**: Quando due utenti iniziano una comunicazione, i loro dispositivi generano automaticamente una coppia di chiavi: una chiave pubblica e una chiave privata.
2. **Scambio delle chiavi pubbliche**: La chiave pubblica viene condivisa con il destinatario e può essere vista da chiunque, ma è utilizzata per criptare i messaggi.
3. **Criptazione del messaggio**: Il mittente usa la chiave pubblica del destinatario per criptare il suo messaggio, trasformandolo in un testo illeggibile.
4. **Trasferimento del messaggio**: Il messaggio criptato viene inviato tramite il server della piattaforma, ma poiché è criptato, il server non può leggerlo.
5. **Decriptazione sul dispositivo del destinatario**: Il destinatario riceve il messaggio criptato e usa la propria chiave privata, che possiede solo il suo dispositivo, per decifrare il messaggio e leggerlo in forma originale.

La crittografia End To End (E2EE)

Casi d'uso della E2EE

- **Comunicazioni sicure**: Servizi di messaggistica mobile (iMessage, WhatsApp, Signal), sistemi di posta elettronica (Proton Mail, Tuta, PGP).
- **Gestione delle password**: Password manager (1Password, Bitwarden).
- **Data storage**: Crittografia di dati a riposo e in transito in ambienti cloud.
- **Condivisione di file**: Protezione di file sensibili durante la trasmissione (P2P, cloud crittografato).

La crittografia End To End (E2EE)

Vantaggi della E2EE

- **Sicurezza e riservatezza dei dati**: Protegge da attacchi informatici e violazioni, garantendo che solo le parti autorizzate abbiano accesso al contenuto, cruciale per le transazioni finanziarie, i dati medici, le discussioni riservate.
- **Protezione dalla sorveglianza**: Aiuta a preservare la privacy personale e a difendersi dal monitoraggio indesiderato da parte di governi o terze parti.
- **Migliore gestione della conformità**: Supporta la conformità a leggi sulla protezione dei dati come il GDPR, facilitando un approccio "privacy by design".
- **Resistenza alla manomissione**: Rende qualsiasi modifica al messaggio cifrato rilevabile, garantendo l'integrità.
- **Comunicazione e collaborazione migliorate**: Promuove la fiducia tra gli utenti.

La crittografia End To End (E2EE)

Sfide della E2EE

- **Ostacoli per l'applicazione della legge**: Governi e forze dell'ordine temono che la crittografia E2EE ostacoli le indagini su attività criminali come terrorismo, sfruttamento minorile e altro, impedendo l'accesso ai contenuti.
- **Dipendenza dalla sicurezza degli endpoint**: La crittografia E2EE non protegge i dati se i dispositivi finali sono compromessi (es. malware).
- **Attacchi Man-in-the-Middle (MITM)**: Gli hacker possono inserirsi tra due endpoint per spiare e intercettare messaggi, impersonando il destinatario e scambiando le chiavi. I protocolli di autenticazione degli endpoint sono cruciali per prevenire ciò.
- **Backdoor**: Punti di accesso nascosti nel software o nell'hardware che possono essere usati dagli hacker per bypassare la crittografia.
- **Vulnerabilità dei metadati**: La crittografia E2EE non sempre protegge i metadati (mittente, destinatario, timestamp), che possono rivelare informazioni sensibili agli attaccanti.

I Criptofonini: strumenti di comunicazione ultrasicuri

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

I Criptofonini: strumenti di comunicazione ultrasicuri

I **Criptofonini** sono considerati strumenti di comunicazione ultrasicuri, sebbene la loro affidabilità dipenda strettamente da come vengono progettati, implementati e utilizzati. Essi combinano crittografia avanzata e hardware specializzato per proteggere le conversazioni da intercettazioni.

Essi, pertanto, sono smartphone modificati nel software e/o nell'hardware per essere potenzialmente inviolabili e a prova di intercettazione. Le modifiche includono:

- **Sistema operativo con requisiti di sicurezza speciali**: disabilita GPS, servizi Google, Bluetooth, fotocamera, porta USB (tranne per la ricarica), notifiche push, schede SD esterne.
- **Comunicazioni proprietarie e cifrate**: Solo chiamate VoIP (senza rete GSM) e messaggistica tramite applicazioni dedicate e crittografate (es. Diffie-Hellman, ECC, PGP, OTR, ZRTP).
- **Crittografia dei metadati**: Anche i metadati e le intestazioni dei messaggi sono cifrati.
- **Assenza di storage sui server**: Le chat e le applicazioni vocali sono spesso peer-to-peer e le comunicazioni non vengono salvate sui server del fornitore. I backup, se scelti, sono cifrati.
- **Infrastruttura dedicata**: Funzionano solo se le comunicazioni avvengono tra due criptofonini della stessa rete dedicata di server sicuri. Questi dispositivi sono progettati per offrire livelli di protezione superiori a quelli della crittografia end-to-end standard, ma la loro **tecnologia chiusa** (accessibile solo agli sviluppatori) è considerata un rischio nel settore della sicurezza informatica, poiché la validità della solidità di una tecnologia dovrebbe essere accessibile al pubblico.

I Criptofonini: strumenti di comunicazione ultrasicuri

Come Funzionano i Criptofonini

I «criptofonini» funzionano grazie all'integrazione di hardware e software modificati per garantire comunicazioni sicure tramite **crittografia end-to-end** e **decentralizzate**, disabilitando anche funzionalità standard che potrebbero esporre i dati, come la localizzazione GPS o la porta USB.

Le chiamate e i messaggi sono cifrati, protetti da algoritmi complessi, e spesso la comunicazione avviene direttamente tra gli **utenti** (***peer-to-peer***) senza passare per server centralizzati vulnerabili. L'autenticazione assicura l'identità delle parti coinvolte, e in caso di compromissione del dispositivo, i dati possono essere intercettati e/o cancellati da remoto.

I Criptofonini: strumenti di comunicazione ultrasicuri

Crittografia End-to-End

La caratteristica principale è la **crittografia end-to-end**. Ciò significa che i dati (voce, messaggi, ecc.) vengono cifrati sul dispositivo del mittente e possono essere decifrati solo dal dispositivo del destinatario.

Nessun intermediario, nemmeno il provider del servizio, può accedere al contenuto in chiaro. Spesso viene utilizzata una combinazione di crittografia a chiave pubblica e privata.

I Criptofonini: strumenti di comunicazione ultrasicuri

Hardware Hardened

A differenza di un normale smartphone, il «*criptofonino*» ha un **hardware "blindato"**.

Questo può includere:

- **Chip di sicurezza dedicati:** Microprocessori specifici che gestiscono le chiavi crittografiche e le operazioni di cifratura, isolandole dal sistema operativo principale.
- **Rimozione di componenti superflui:** Spesso vengono disattivate o rimosse funzionalità come Wi-Fi, Bluetooth o GPS per ridurre le potenziali vulnerabilità.
- **Schermatura fisica:** Alcuni modelli includono una schermatura fisica per prevenire attacchi di tipo "side-channel" che cercano di estrarre dati analizzando le emissioni elettromagnetiche.

I Criptofonini: strumenti di comunicazione ultrasicuri

Software Modificato

Il sistema operativo è una versione **modificata** e **minimalista** per eliminare il codice non necessario e i servizi che potrebbero introdurre falle di sicurezza.

Non sono presenti app store, servizi cloud o altre funzioni tipiche degli smartphone commerciali che potrebbero compromettere ulteriormente la sicurezza.

I Criptofonini: strumenti di comunicazione ultrasicuri

Limitazioni e Rischi

Sebbene siano molto sicuri, i Criptofonini non sono infallibili. La loro sicurezza può essere compromessa da:

- **Attacchi fisici:** Se il dispositivo viene rubato, un aggressore esperto potrebbe tentare di bypassare le protezioni hardware.
- **Falle nel software:** Anche un sistema operativo minimalista può contenere bug o vulnerabilità non ancora scoperte.
- **Errore umano:** L'utente può compromettere la sicurezza, ad esempio non proteggendo adeguatamente il dispositivo o divulgando informazioni sensibili.
- **Spyware:** Se il dispositivo viene compromesso prima di essere messo in uso o se un utente installa software maligno, la crittografia può essere bypassata.

In sintesi, i **Criptofonini** rappresentano un livello di sicurezza superiore rispetto ai normali dispositivi, ma la loro efficacia dipende dalla qualità della loro implementazione e dalla prudenza nell'utilizzo.

Il Caso Sky Ecc

Il Caso Sky Ecc

Il caso **Sky Ecc** (e il suo predecessore EncroChat) ha rivelato le sfide e le implicazioni legali della crittografia avanzata nel contesto della criminalità organizzata.

Sky Ecc era una delle principali reti di comunicazione cifrata, utilizzata da oltre 170.000 utenti a livello globale, inclusi i narcotrafficanti.

Nel 2021, le forze dell'ordine belghe, olandesi e francesi sono riuscite a decifrare le conversazioni scambiate tramite la piattaforma, portando a vaste operazioni di polizia in vari paesi.

L'operazione è stata definita la più sofisticata tecnologicamente condotta in Europa contro la criminalità.

Il Caso Sky Ecc

Cos'è Sky ECC?

Sky ECC era un servizio di messaggistica criptata, offerto tramite dispositivi dedicati (spesso chiamati ***criptofonini***), che prometteva una sicurezza totale e una privacy assoluta ai suoi utenti.

Il servizio era commercializzato per professionisti e privati attenti alla sicurezza, ma era diventato un vero e proprio strumento di lavoro per le organizzazioni criminali a livello globale, in particolare per il traffico di droga, il riciclaggio di denaro e altre attività illecite.

Il Caso Sky Ecc

Che tipologia di crittografia utilizzava la piattaforma Sky Ecc

La piattaforma Sky ECC utilizzava la **Crittografia a Curva Ellittica (ECC)** a ***521-bit per criptare i messaggi***, le note vocali, le foto e altri tipi di comunicazione. L'**ECC** è un tipo di «**crittografia asimmetrica**» che offre una sicurezza molto elevata con chiavi di lunghezza inferiore rispetto ad altri algoritmi, rendendola efficiente per dispositivi con potenza di elaborazione limitata come gli smartphone.

Inoltre, il sistema utilizzava un approccio ibrido, come spesso accade nella crittografia moderna.

La crittografia a **chiave pubblica** (in questo caso l'ECC) *veniva usata per lo scambio di una chiave di sessione (o 'master key')*, mentre la crittografia a **chiave simmetrica** *veniva utilizzata per cifrare il corpo del messaggio, che è la parte più grande dei dati*.

Questo **processo ibrido** combina la sicurezza dello scambio di chiavi asimmetrico con la velocità e l'efficienza della crittografia simmetrica per la trasmissione effettiva dei dati.

Il Caso Sky Ecc

L'Operazione di Polizia

L'operazione è stata condotta da un'alleanza di forze dell'ordine europee, con la guida di Belgio, Francia e Paesi Bassi, e il supporto di **Europol** e **Eurojust** (*Agenzia dell'Unione Europea per la cooperazione giudiziaria penale*). A partire dal 2020, gli investigatori francesi sono riusciti a penetrare il sistema di crittografia di Sky ECC. Non si è trattato di una "**backdoor**" nel senso tradizionale, ma di un'operazione complessa che ha permesso di raccogliere e decifrare in tempo reale una quantità enorme di messaggi scambiati dagli utenti.

Tra il 2020 e il 2021, la polizia è stata in grado di monitorare milioni di messaggi. Questo ha fornito una "miniera d'oro" di informazioni, che ha permesso di svelare la struttura delle organizzazioni criminali, identificare i loro membri, e acquisire prove dettagliate di attività illecite, tra cui:

- *Pianificazione di omicidi e sequestri*
- *Traffico di stupefacenti su larga scala (tonnellate di cocaina ed eroina)*
- *Traffico d'armi*
- *Riciclaggio di denaro*
- *Corruzione*

Il successo dell'operazione è stato tale che ha portato a centinaia di arresti in diversi paesi, in particolare in Belgio e nei Paesi Bassi, e al sequestro di ingenti quantità di denaro, droga e beni di lusso. Nel 2021, la società Sky ECC ha interrotto le sue attività, e il suo sito web è stato sequestrato dall'FBI.

Il Caso Sky Ecc

Modalità di violazione di Sky Ecc

- **Sequestro di un criptofonino**: Nel 2018, il sequestro di un dispositivo Sky Ecc al porto di Anversa ha permesso alle autorità di identificare l'infrastruttura server di Sky Global, ospitata sull'infrastruttura del Provider OVH in Francia.

- **Cattura del traffico cifrato**: Le autorità francesi hanno installato una **sonda IP** su due server OVH, catturando il traffico europeo di Sky Ecc, ma i milioni di messaggi erano cifrati e incomprensibili.

- **Decifratura tramite RAM e attacco Man-in-the-Middle (MITM)**: Gli investigatori hanno analizzato la memoria RAM dei server per ottenere le informazioni necessarie al sistema. Successivamente, hanno impiegato un server "***man-in-the-middle***" posizionato vicino al server «sorgente» di Sky Ecc. Questo server infiltrato inviava notifiche push invisibili ai criptofonini per convincerli a fornire le chiavi necessarie alla decifratura dei messaggi. Questa operazione ha avuto successo e ha permesso di decodificare i messaggi già registrati e quelli in transito.

Il Caso Sky Ecc

Implicazioni giuridiche e sentenze della Cassazione

L'operazione Sky Ecc ha sollevato numerosi problemi giuridici, in particolare in Italia, a causa di un **vuoto normativo** per operazioni ibride (*acquisizione di dati* e/o *intercettazione*).

La Corte di Cassazione, con le sentenze delle Sezioni Unite n. *23755* e n.*23756* del 2024, ha cercato di chiarire l'utilizzabilità delle prove acquisite.

Il Caso Sky Ecc

Principi chiave stabiliti dalla Cassazione

- L'acquisizione di comunicazioni cifrate già ottenute e decifrate da autorità giudiziarie estere tramite **Ordine Europeo di Indagine (OEI) non rientra nell'ambito dell'Art. 234-bis c.p.p.** (acquisizione di documenti e dati informatici disponibili al pubblico o con consenso).
- Rientra invece nella **disciplina della circolazione delle prove** tra procedimenti penali (Art. 238 c.p.p. e 270 c.p.p. per intercettazioni, e Art. 78 disp. att. c.p.p.).
- Il Pubblico Ministero italiano **può legittimamente richiedere e acquisire tali prove senza preventiva autorizzazione del giudice italiano**, in quanto le prove sono già in possesso dell'autorità estera.
- L'**utilizzabilità** di tali prove **deve essere esclusa solo se il giudice italiano rileva una violazione dei diritti fondamentali**, e l'onere di provare tale violazione grava sulla parte interessata.
- L'impossibilità per la difesa di **accedere all'algoritmo utilizzato per cifrare il testo non determina una violazione dei diritti fondamentali**, *salvo specifiche allegazioni di alterazione, poiché il contenuto è inscindibilmente abbinato alla sua chiave*. Questo punto è stato criticato per potenziale contrasto con il diritto di difesa.

Il Caso Sky Ecc

Critiche alle decisioni della Cassazione e questioni irrisolte

- **Natura giuridica ambigua**: Le sentenze non definiscono chiaramente la natura giuridica dell'attività investigativa (ibrida tra intercettazione, sequestro e acquisizione di documenti), generando perplessità e non sovrapponendosi perfettamente ai principi nazionali.

- **Sorveglianza di massa**: L'acquisizione indiscriminata di tutti i dati su un server violato solleva interrogativi sulla conformità ai principi di **necessità** e **proporzionalità**, sebbene la Cassazione abbia tentato di distinguerla dalla sorveglianza di massa non mirata.

- **Controllo giurisdizionale**: Sebbene non sia richiesta un'autorizzazione preventiva del giudice italiano, la possibilità di un controllo giurisdizionale successivo (postumo) è ammessa, ma i suoi limiti e criteri restano parzialmente indefiniti.

Il Caso Sky Ecc

Critiche alle decisioni della Cassazione e questioni irrisolte

- **IMSI Catcher**: La Cassazione ha legittimato l'uso dell'IMSI Catcher (un dispositivo che identifica e geolocalizza i cellulari) da parte della polizia giudiziaria senza preventiva autorizzazione, sostenendo che sia un'attività prodromica all'intercettazione. Tuttavia, questo strumento può essere molto più invasivo, potendo simulare celle telefoniche e intercettare comunicazioni non crittografate E2EE, incidendo su dati personali e segretezza delle comunicazioni, richiedendo un intervento legislativo urgente.

- **"Cortocircuito" sistemico**: Si crea una situazione per cui le intercettazioni e l'acquisizione dei dati di traffico telefonico/telematico richiedono autorizzazione giudiziaria preventiva, ma il sequestro dei contenuti comunicativi digitali, acquisiti tramite operazioni complesse come quelle su Sky Ecc, può avvenire con un semplice provvedimento del PM, evidenziando una **fragilità del quadro normativo attuale**.

Il Caso Sky Ecc

Le Implicazioni Legali e Giurisprudenziali

Il "Caso Sky ECC", così come il precedente "Caso EncroChat", ha aperto un dibattito legale e giurisprudenziale senza precedenti in tutta Europa. Le principali questioni sollevate sono:

- **L'Usabilità delle Prove:** La difesa degli imputati ha contestato la legittimità delle prove ottenute, sostenendo che l'operazione di decrittazione equivaleva a una sorveglianza di massa e a una violazione dei diritti fondamentali alla privacy e alla protezione dei dati, garantiti dalla Costituzione e dalla Convenzione Europea dei Diritti dell'Uomo (CEDU). La questione è se tali "documenti informatici" (i messaggi decifrati) possano essere considerati prove ammissibili in tribunale, oppure se siano il frutto di un'indagine illecita.

- **Il Principio di "Controllo Giudiziale":** Una delle domande chiave è se le autorità giudiziarie nazionali siano autorizzate a valutare la legalità delle prove raccolte da un altro paese dell'UE. In base al principio di "mutuo riconoscimento" e agli "ordini europei di indagine", la cooperazione giudiziaria tra paesi membri dovrebbe essere fluida. Tuttavia, la difesa ha sostenuto che questo non può bypassare il controllo sulla conformità delle indagini ai diritti fondamentali.

Il Caso Sky Ecc

Le Implicazioni Legali e Giurisprudenziali

- **La Linea Sottile tra Intelligence e Investigazione:** Gli avvocati hanno sollevato il dubbio se l'operazione Sky ECC sia stata condotta come una legittima indagine di polizia (mirata e autorizzata da un giudice) o come una vasta operazione di intelligence (sorveglianza di massa senza autorizzazione specifica). Questa distinzione è cruciale, poiché le prove raccolte da un'attività di intelligence spesso non sono ammissibili in un procedimento penale.

- **L'Impatto sul Diritto alla Privacy:** Il caso ha messo in luce la tensione tra la necessità di combattere il crimine organizzato e la protezione della privacy dei cittadini. Se da un lato l'operazione ha permesso di sgominare reti criminali, dall'altro ha sollevato preoccupazioni sulla possibilità che le forze dell'ordine possano aggirare le protezioni crittografiche, compromettendo così la sicurezza delle comunicazioni di tutti, compresi i cittadini onesti.

In sintesi, il "Caso Sky ECC" ha fornito un modello di come la tecnologia può essere usata per combattere il crimine nell'era digitale, ma al contempo ha evidenziato la necessità di aggiornare il quadro legale per affrontare le nuove sfide poste dalla crittografia avanzata, garantendo un giusto equilibrio tra sicurezza, privacy e diritti fondamentali.

Attività di indagine

Attività di indagine

L'attività di indagine forense, che ho svolto relativa al caso Sky ECC, ha richiesto un grande impegno tecnico e metodologico per studiare ed esaminare tutti i risultati relativi alle attività svolte che vengono di seguito descritte.

La prima fase è stata caratterizzata dallo studio della documentazione sia tecnica che legale pervenuta dalla polizia belga e da quella francese.

Dopo la fase di studio sono state avviate le attività tecnico forensi sui dati forniti anche dalla polizia italiana, soprattutto per quanto ha riguardato tutti i soggetti residenti in Italia coinvolti nelle indagini.

L'analisi tecnico forense è stata incentrata sulla verifica dei dati estratti e analizzati dalla polizia italiana al fine di verificare la correttezza e la congruenza delle comunicazioni avvenute mediante i criptofonini in uso agli indagati.

Al termine di questa attività ho consegnato i risultati ai legali difensori degli indagati.

Attività di indagine

Genesi dell'Indagine e partecipazione alle attività

L'indagine Sky ECC è un caso esemplare di come le forze dell'ordine abbiano superato le sfide poste dalla crittografia *end-to-end* per smantellare una vasta rete criminale nell'ambito della droga, prostituzione e traffico di armi.

Tecnicamente l'operazione non si è basata su "backdoor" o punti deboli nell'algoritmo di crittografia, ma su un'attività di **acquisizione massiva di dati** dai server della piattaforma.

Le autorità francesi, in stretta collaborazione con la polizia belga e olandese, sono riuscite ad accedere e a replicare il contenuto dei server di Sky Global (OVH *service provider*), l'azienda che gestiva il servizio. ***L'obiettivo era ottenere l'accesso alle comunicazioni prima che venissero eliminate dal server o dal dispositivo***.

Le autorità italiane hanno ricevuto dalle autorità francesi tutto il materiale e i dati relativi ai soggetti dell'organizzazione criminale che operava in Italia. Su questo materiale si è svolta la mia attività di studio, analisi e consulenza tecnica forense a supporto delle attività difensive di uno ***Studio Legale***.

Attività di indagine

Fasi dell'Analisi Forense

L'analisi dei dati acquisiti è stata un'operazione complessa, che può essere suddivisa in diverse fasi:

- **Acquisizione e Decifratura dei Dati**: La prima e più delicata fase è stata l'estrazione dei dati dai server. Grazie a un'operazione tecnica definita dalla polizia come "interferenza" con la rete, è stato possibile acquisire i dati cifrati in transito e, una volta ottenute le chiavi, decifrarli. L'accesso alle chiavi di crittografia, memorizzate in luoghi diversi (sul dispositivo e, in parte, sui server), ha permesso alle forze dell'ordine di leggere i messaggi in chiaro. Questo processo non ha compromesso l'integrità del sistema di crittografia, ma ha sfruttato le vulnerabilità operative e l'accesso fisico ai server.

- **Analisi dei Tabulati e dei Contenuti**: Una volta decifrati, i dati (messaggi di testo, immagini, note vocali e contatti) sono stati analizzati in modo forense. Questa fase ha richiesto l'uso di software specializzati per:
  - **Ricostruire le conversazioni**: Rimettere insieme i frammenti di messaggi e le comunicazioni per comprendere i flussi di informazione.
  - **Mappare il network criminale**: Identificare i nodi della rete criminale (utenti, fornitori, destinatari) e le loro relazioni, incrociando i PIN e i contatti presenti nelle chat.
  - **Identificare ruoli e attività**: Dalle conversazioni, gli investigatori hanno potuto determinare ruoli, gerarchie e attività illecite, tra cui traffico di droga, estorsioni e riciclaggio di denaro.

Attività di indagine

- **Cross-referencing e geolocalizzazione**: L'analisi dei contenuti è stata integrata con l'analisi dei tabulati telefonici e della geolocalizzazione (dove disponibile). Questo incrocio di dati ha permesso di:
  - **Corroborare le prove**: Confermare le informazioni scambiate nelle chat con i movimenti fisici degli indagati.
  - **Ricostruire spostamenti e incontri**: Mappare gli spostamenti dei dispositivi per stabilire incontri tra i membri delle organizzazioni criminali.

Attività di indagine

Implicazioni Legali e Giurisprudenziali

Il caso Sky ECC ha sollevato questioni legali fondamentali, in particolare in relazione all'**utilizzabilità delle prove** acquisite in un paese e utilizzate in un altro.

In Italia, le sentenze della Cassazione hanno stabilito che l'acquisizione di tali messaggi tramite un **Ordine Europeo di Indagine (OEI)** è legittima e che le comunicazioni decifrate possono essere considerate alla stregua di documenti, anche in assenza di un'autorizzazione preventiva da parte del giudice italiano.

La principale criticità emersa riguarda il **diritto alla difesa**, dato che l'impossibilità di accedere ai metodi di decifratura e alla documentazione tecnica completa ha limitato la possibilità di contestare l'autenticità dei dati.

Questo dibattito sottolinea la necessità di un quadro normativo armonizzato a livello europeo che bilanci efficacemente la cooperazione giudiziaria internazionale con la protezione dei diritti fondamentali.

Sfide tecnologiche e implicazioni legali della crittografia avanzata (*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

La crittografia avanzata è uno strumento cruciale per la sicurezza informatica, ma il suo impiego solleva complesse sfide **tecnologiche** e implicazioni a livello **legale** ed **etico**, soprattutto in relazione a normative come il **GDPR** e al ruolo del **Data Protection Officer** (DPO).

Le Sfide Tecnologiche della Crittografia Avanzata

- **L'avvento del Quantum Computing:** Questa è la sfida più grande e imminente. I computer quantistici, una volta maturi, avranno la capacità di risolvere in poco tempo i problemi matematici alla base della maggior parte degli attuali algoritmi crittografici (come RSA e Diffie-Hellman). Questo renderebbe obsoleti i sistemi di sicurezza attuali, mettendo a rischio dati e comunicazioni.
  - **Soluzione:** La ricerca si sta concentrando sulla **crittografia post-quantistica (PQC)**. Si tratta di sviluppare nuovi algoritmi basati su problemi matematici che sono difficili da risolvere anche per un computer quantistico. La transizione verso la PQC richiederà investimenti enormi e un coordinamento a livello globale.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

- **Gestione delle Chiavi:** L'efficacia della crittografia dipende dalla sicurezza delle chiavi. Man mano che la crittografia diventa più pervasiva, la gestione e la distribuzione sicura delle chiavi crittografiche (Public Key Infrastructure - PKI) diventa sempre più complessa e vulnerabile a errori umani o attacchi.

- **Implementazione e Usabilità:** L'implementazione corretta della crittografia richiede un elevato grado di competenza tecnica. Spesso, gli errori di implementazione possono creare vulnerabilità nascoste, indipendentemente dalla robustezza dell'algoritmo. Inoltre, soluzioni di crittografia complesse possono ostacolare l'esperienza utente, rendendo meno probabile la loro adozione.

- **Attacchi "Side-Channel":** Anche se l'algoritmo è solido, gli aggressori possono raccogliere informazioni dai dispositivi fisici che eseguono la crittografia (ad esempio, analizzando le emissioni elettromagnetiche o le variazioni di consumo energetico) per estrarre le chiavi.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

Le Implicazioni Legali e il GDPR

Il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea considera la crittografia una delle misure tecniche e organizzative più efficaci per proteggere i dati personali. In particolare, Il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, all'Art. 25 (Data protection by design and by default) e l'Art. 32 (Security of processing), impone ai titolari e responsabili del trattamento di implementare misure tecniche e organizzative appropriate, come la **pseudonimizzazione** e la **crittografia**, per garantire la sicurezza dei dati personali.

- **Valutazione dei rischi:** L'articolo 32 del GDPR impone ai titolari e ai responsabili del trattamento dei dati di adottare misure di sicurezza adeguate al rischio. La crittografia, offrendo una robusta protezione contro accessi non autorizzati, è vista come uno strumento essenziale per mitigare il rischio di violazioni (data breach).

- **Riduzione degli obblighi di notifica:** Un'implicazione diretta e significativa è che, se i dati personali sono crittografati in modo efficace, in caso di un "data breach," il titolare del trattamento non ha l'obbligo di notificare la violazione agli interessati, a meno che i dati non siano stati decifrati. Questo perché il rischio per i diritti e le libertà degli individui è considerato basso se i dati sono illeggibili.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

- **Pseudonimizzazione vs. Anonimizzazione:** Il GDPR distingue tra pseudonimizzazione (un processo che rende i dati non direttamente identificabili, ma che può essere invertito) e anonimizzazione (un processo irreversibile). La crittografia avanzata è spesso associata alla pseudonimizzazione, consentendo un equilibrio tra l'utilizzabilità dei dati e la protezione della privacy.

- **Limiti dell'anonimizzazione**: Può ridurre la qualità dei dati e comporta il rischio di **re-identificazione**, come dimostrato dal caso Netflix del 2007. È necessario trovare un compromesso tra utilità e protezione della privacy. la tecnica della k-anonymity garantisce che ogni record in un dataset sia indistinguibile da almeno altri k-1 record, rendendo così difficile l'identificazione individuale e abbassando il rischio di re-identificazione a 1/k, poiché un utente esterno non può distinguere la vera persona da almeno altre k-1 persone con gli stessi dati. In sintesi, **la *K-anonymity* è un modello di privacy che rende i dati meno identificabili fornendo una garanzia matematica di anonimato, rendendo molto più difficile per un aggressore collegare i dati anonimizzati a un individuo specifico**.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

Sfide e Rapporto con la Cybersecurity

La crittografia non è una panacea e presenta diverse sfide nel contesto della cybersecurity.

- **Gestione delle chiavi:** L'anello debole di qualsiasi sistema crittografico è la gestione delle chiavi di cifratura. Una chiave persa, rubata o gestita in modo improprio rende la crittografia inefficace e può esporre i dati sensibili. La cybersecurity deve quindi concentrarsi non solo sull'algoritmo, ma anche sulle procedure per la gestione del ciclo di vita delle chiavi.

- **Minacce emergenti:** L'avvento del **quantum computing** rappresenta la sfida più grande a lungo termine. Questi computer, una volta che saranno pienamente operativi, avranno la capacità di rompere la maggior parte degli attuali algoritmi crittografici (come RSA e Diffie-Hellman), rendendo necessario lo sviluppo e la transizione verso la crittografia post-quantistica (PQC).

- **Attacchi di "side-channel":** Anche se un algoritmo è matematicamente solido, gli aggressori possono sfruttare le "perdite" di informazioni fisiche (come le variazioni di consumo energetico o le emissioni elettromagnetiche) per dedurre le chiavi di cifratura, bypassando la protezione crittografica.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

Il Ruolo del Data Protection Officer (DPO)

Il **Data Protection Officer (DPO)** è una figura chiave per garantire la conformità al GDPR e la sicurezza dei dati, e ha un ruolo critico nella gestione della crittografia.

- **Consulenza e supervisione:** Il DPO ha il compito di consigliare il titolare del trattamento sull'adozione di misure tecniche adeguate, inclusa la crittografia. Deve supervisionare l'implementazione e l'efficacia di tali misure per garantire un livello di sicurezza adeguato al rischio.
- **Valutazione d'impatto (DPIA):** Per i trattamenti ad alto rischio, il DPO deve condurre una Valutazione d'Impatto sulla Protezione dei Dati (DPIA). La crittografia è un elemento centrale di questa valutazione, poiché la sua presenza e robustezza possono significativamente abbassare il livello di rischio.
- **Monitoraggio:** Il DPO deve monitorare costantemente le nuove minacce informatiche e l'evoluzione delle tecnologie crittografiche per assicurarsi che le misure di sicurezza aziendali rimangano all'avanguardia.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

Le Implicazioni Legali ed Etiche

Il dilemma più spinoso riguarda il difficile equilibrio tra **privacy individuale** e **sicurezza nazionale/pubblica**.

- **La Richiesta di "Backdoor" o Accesso Autorizzato:** Le forze dell'ordine e le agenzie di intelligence sostengono che la crittografia end-to-end (E2EE) impedisce loro di accedere a comunicazioni cruciali per indagini penali o per prevenire attacchi terroristici. Per questo, chiedono l'inserimento di "backdoor" (porte di servizio) nei sistemi di crittografia che consentirebbero un accesso governativo "legale" ai dati cifrati.
  - **Argomento a favore:** Permetterebbe alle autorità di contrastare il crimine organizzato, il terrorismo e la pedopornografia, garantendo la sicurezza dei cittadini.
  - **Argomento contro:** Gli esperti di sicurezza e i sostenitori della privacy sostengono che una backdoor, una volta creata, non può essere garantita solo per l'uso governativo. Potrebbe essere scoperta e sfruttata da hacker, potenze straniere o criminali, compromettendo la sicurezza di tutti. Inoltre, violerebbe il principio di privacy e l'inviolabilità delle comunicazioni.
- **L'Obbligo di Decrittare Dati:** In molti paesi, la legge può imporre a un individuo di rivelare le proprie chiavi crittografiche o di decifrare dati, sotto la minaccia di sanzioni o reclusione. Questo solleva importanti questioni legali e costituzionali, in particolare riguardo al diritto a non autoincriminarsi.

Sfide tecnologiche e implicazioni legali della crittografia avanzata

(*GDPR – Cybersecurity – Data Protetion Officer - Etica*)

- **Regolamentazione e Sanzioni:** Le normative internazionali, come il **GDPR** in Europa, richiedono l'adozione di misure tecniche e organizzative adeguate per la protezione dei dati personali, e la crittografia è considerata uno strumento essenziale. La mancata adozione di crittografia può comportare pesanti sanzioni. D'altra parte, alcuni paesi limitano l'esportazione di tecnologie di crittografia avanzata, considerandole "armi".

- **Il Diritto alla Crittografia:** Il dibattito ha anche sollevato la questione se l'uso della crittografia sia un diritto fondamentale. Alcuni giuristi e attivisti sostengono che la crittografia forte è indispensabile per la libertà di espressione e di associazione, specialmente in regimi autoritari o per la protezione di giornalisti e dissidenti.

- **Etica e Crittografia:** La crittografia è uno strumento, e come ogni strumento, la sua importanza etica risiede nel modo in cui viene utilizzato e nella regolamentazione che lo circonda. L'etica permette di comprendere cosa è bene per l'individuo e per la società in quanto permette di orientare il comportamento, le azioni con spirito critico su valori e principi. Tuttavia, il quadro normativo è in evoluzione con il Consiglio dell'UE che cerca di bilanciare la "**sicurezza attraverso la crittografia**" con la "**sicurezza nonostante la crittografia**", riconoscendo che non esiste un'unica soluzione tecnica per risolvere questo dilemma.

Prospettive future, dibattito e conclusioni

Prospettive future, dibattito e conclusioni

Le sfide e le implicazioni legali della crittografia avanzata richiedono un equilibrio delicato tra la sicurezza individuale e collettiva.

Prospettive Future

Il futuro della crittografia è legato a tre tendenze principali:

- **Crittografia Post-Quantistica (PQC):** L'avvento dei computer quantistici richiederà la transizione verso nuovi algoritmi crittografici. Questa transizione sarà una sfida tecnologica enorme, richiedendo la revisione e l'aggiornamento di quasi tutti i sistemi di sicurezza esistenti.
- **Crittografia Omofona e ZKP:** Tecnologie emergenti come la **crittografia omofona** (che permette di eseguire calcoli su dati cifrati senza decrittarli) e le **prove a conoscenza zero (ZKP)** (che consentono di dimostrare la veridicità di un'informazione senza rivelarla) promettono di rivoluzionare la privacy e la sicurezza dei dati, offrendo nuove possibilità per servizi cloud e blockchain.
- **Regolamentazione Globale:** La crittografia non conosce confini, e la mancanza di una regolamentazione internazionale armonizzata creerà tensioni tra i paesi. Saranno necessari accordi globali per definire standard comuni e bilanciare le esigenze di sicurezza e privacy.

Prospettive future, dibattito e conclusioni

Il dibattito

Il dibattito sulla crittografia è destinato a intensificarsi, data la sua centralità in ogni aspetto della vita digitale. I casi come quello di Sky ECC dimostrano come la crittografia, pur essendo un baluardo per la privacy e la sicurezza, possa essere sfruttata per fini criminali.

Le principali considerazioni sono:

- **Necessità di un equilibrio:** È fondamentale trovare un equilibrio tra la protezione dei dati personali e la necessità delle forze dell'ordine di contrastare il crimine. La richiesta di "backdoor" da parte dei governi solleva un dilemma etico e pratico, poiché un'eventuale vulnerabilità potrebbe compromettere la sicurezza di tutti.
- **Ruolo del GDPR:** Il GDPR ha consolidato la crittografia come strumento essenziale di protezione dei dati, spingendo le aziende a integrarla nelle loro strategie di sicurezza e a nominare figure professionali come il DPO.
- **Il fattore umano:** L'anello debole della crittografia non è l'algoritmo, ma l'essere umano. La gestione impropria delle chiavi e la mancanza di consapevolezza da parte degli utenti rappresentano i rischi più significativi.

Prospettive future, dibattito e conclusioni

La risoluzione del Consiglio dell'Unione Europea

Secondo quanto riportato dal Consiglio dell'Unione Europea, la risoluzione adottata il 14 dicembre 2020, intitolata "**Sicurezza attraverso la crittografia e sicurezza nonostante la crittografia**," affronta il complesso equilibrio tra la necessità di proteggere la privacy dei cittadini e il dovere delle autorità di contrastare e di indagare sui crimini. I punti chiave della risoluzione sono:

- **Sostegno alla crittografia forte:** Il Consiglio supporta lo sviluppo e l'uso di una crittografia robusta come strumento fondamentale per tutelare i diritti digitali e la sicurezza di cittadini, governi e industria.
- **Accesso per le forze dell'ordine:** Allo stesso tempo, il documento riconosce che la crittografia può ostacolare le indagini, e sottolinea la necessità di garantire che le autorità giudiziarie e di contrasto possano accedere alle prove elettroniche in modo efficace.
- **Nessuna "backdoor" obbligatoria:** La risoluzione non impone l'uso di "backdoor" generalizzate, ma invita a un dialogo aperto tra governi, industria e mondo accademico per trovare soluzioni tecniche che consentano l'accesso alle prove senza indebolire la crittografia per tutti.

In sintesi, la risoluzione cerca di bilanciare due esigenze cruciali: il diritto alla privacy e la sicurezza pubblica. Riconosce il valore della crittografia come strumento di protezione, ma sollecita la collaborazione per garantire che non diventi un rifugio impenetrabile per i criminali.

Prospettive future, dibattito e conclusioni

Le conclusioni

Le sfide poste dalla crittografia avanzata e dalle nuove tecniche investigative digitali richiedono un **intervento normativo urgente**. L'attuale quadro legislativo italiano è considerato obsoleto e inadeguato a gestire la versatilità della comunicazione moderna e la natura invasiva delle indagini digitali.

È fondamentale ristabilire un **equilibrio** tra **le esigenze investigative** e **la tutela delle libertà individuali**. Ciò potrebbe includere:

- **Introduzione di una normativa specifica** per le indagini digitali, che individui chiaramente i casi, i modi e i limiti dell'ingerenza nella sfera privata, rispettando il principio di legalità e proporzionalità.
- **Rafforzamento del ruolo della difesa** già in fase investigativa.
- **Regolamentazione dei servizi di comunicazione cifrata**, richiedendo la collaborazione dei gestori con le autorità di *law-enforcement* per *identificare* e *bloccare* gli *utenti coinvolti in attività illecite*.

Prospettive future, dibattito e conclusioni

- **Predisposizione di una normativa uniforme a livello sovranazionale** sulla circolazione dei dati digitali comunicativi.

In un'epoca in cui il crimine opera sempre più a livello globale e la tecnologia offre strumenti investigativi sempre più sofisticati, è imperativo che il diritto si adegui per garantire la sicurezza dei cittadini senza compromettere i diritti fondamentali alla privacy e a un giusto processo.

La **crittografia avanzata**, quindi, è vitale per la sicurezza e la privacy nella società digitale, ma crea anche nuove sfide per le forze dell'ordine e i governi.

La ricerca di un equilibrio tra questi interessi contrapposti è quindi una delle **sfide politiche** e **tecnologiche più urgenti** del **nostro tempo**.

Grazie per l’attenzione