	Crittografia	Crittografia dei file come PGP, crittografia del disco (FileVault, BitLocker).
API information disclosure	Progettazione	Attento controllo nella progettazione, considerando il passaggio dei parametri per indirizzo o valore.

Tabella 15 - STRIDE: Indirizzamento dell'Information disclosure

Monitoraggio della rete. Il processo di monitoraggio della rete, si avvale dell'architettura per monitorarne il traffico (In particolare, la maggior parte delle attuali reti inviano i pacchetti sulla rete e ciascun listener presente su ogni end-point deve decidere se il pacchetto è per lui importante o meno). Quando le reti vengono progettate in modi diversi, esistono svariate tecniche per tracciare il traffico che va verso o attraversa la stazione di monitoraggio. Se non viene indirizzato lo spoofing, così come il tampering, un attaccante può mettersi nel mezzo attuando lo spoofing su ciascun end-point. La mitigazione dell'information disclosure sulla rete richiede la gestione delle minacce di spoofing e di tampering. Se non si indirizza il tampering, ci sono diversi modi intelligenti per ottenere informazioni. Quindi di nuovo, l'SSL e l'IPSec sono le migliori scelte da mettere in campo.
Nomi che rivelano informazioni. Quando il nome di una directory o di un file di per se forniscono informazioni utili ad un possibile attaccante, il modo migliore per proteggersi è creare una directory padre con un nome anonimo (cioè non correlato al servizio oppure ai dati trattati) e utilizzare le ACLs o i permessi del sistema operativo per proteggerle.
Contenuti sensibili nei file. Quando il contenuto di un file necessita di protezione, utilizzare le ACLs o la crittografia. Nel caso in cui la macchina (computer) dovesse cadere in mani non autorizzate, è necessario preventivamente utilizzare la crittografia al fine di proteggere tutti i dati in essa presenti. Le modalità di protezione crittografica che prevedono l'inserimento di una chiave o parola chiave da parte di una persona, sono più sicure ma meno convenienti. Esistono tecniche crittografiche per i file, filesystem e database, dipende da ciò che si deve proteggere.
API (Interfaccia di programmazione di una applicazione). Quando si progetta un'API, o diversamente si trasmettono informazioni oltre un confine di fiducia, è importante fare attenzione a quali informazioni si espongono. È necessario partire dal presupposto che le informazioni fornite vengono passate ad altri, quindi bisogna essere molto cauti e selettivi su ciò che viene fornito. Situazioni di errore generate da un sito web che mostrano il nome utente e la password di un database sono un esempio comune di questo problema.
La seguente tabella riporta le vulnerabilità della Top 10 OWASP 2017[24] riconducibili alle minacce di information disclosure, e per ciascuna vulnerabilità indicata, le relative pratiche[25] e requisiti[26] di sicurezza consigliati da OWASP:

OWASP TOP-10 2017 (Rischi di sicurezza delle applicazioni)	**OWASP Proactive Controls 2018 v 3.0** (Pratiche di sicurezza proattive)	**OWASP ASVS 3.0** (Requisiti di sicurezza applicative)
A3 – Sensitive Data Exposure	C8 - Protect Data Everywhere	V7 - Cryptography at Rest
A3 – Sensitive Data Exposure	C8 - Protect Data Everywhere	V9 - Data Protection
A3 – Sensitive Data Exposure	C8 - Protect Data Everywhere	V11 - Http Security Configuration

[24] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

[25] https://www.owasp.org/index.php/OWASP_Proactive_Controls

[26] https://github.com/OWASP/ASVS