Spoofing di un file su disco	Sfruttare le funzionalità messe a disposizione dal Sistema Operativo	• Percorsi assoluti; • Controllo ACL; • Assicurarsi che le pipes vengano create correttamente.
	Autenticatori crittografici	Firme digitali o autenticatori.
Spoofing di un indirizzo di rete	Crittografia	• DNSSEC; • HTTPS/SSL; • IPsec.
Spoofing di un programma in memoria	Sfruttare le funzionalità messe a disposizione dal Sistema Operativo	Molti sistemi operativi moderni hanno una qualche forma attuabile di identificazione dell'applicazione.

Tabella 9 - STRIDE: Indirizzamento dello Spoofing

Spoofing di una persona. Per evitare lo spoofing di una persona, è necessario che sia stato implementato un meccanismo di autenticazione e che a questa persona sia stato associato un nome utente univoco. Non è detto che questo sia sufficiente ad evitare lo spoofing: differenti tecniche di autenticazione con profili di sicurezza adeguati devono essere attivate basandosi sulla tipologia di servizio/dati gestiti: ad esempio un autenticazione a 2 fattori può aiutare a mitigare lo spoofing su servizi critici.
Spoofing di un file su disco. Quando si accede ad un file presente sul disco, non bisogna aprirlo utilizzando un percorso relativo come *open(file)*. Utilizzare il percorso assoluto *open(/percorso/assoluto/del/file)*. Se il file contiene dati sensibili, dopo averlo aperto, è necessario attuare un controllo di sicurezza sugli elementi del descrittore del file stesso (come il fully resolved name, i permessi e l'owner). Si potrebbe anche voler controllare il descrittore del file per prevenire eventuali *race conditions.* Ciò vale doppiamente quando il file è un eseguibile, ma il controllo dopo l'apertura potrebbe essere complicato. Ciò, può aiutare a garantire che le autorizzazioni sull'eseguibile non possano essere modificate da parte di un utente malintenzionato. In ogni caso, è quasi sempre sconsigliabile invocare *exec()* con il parametro file specificato in modo relativo "*./file"*.
Spoofing di un indirizzo di rete. Nel caso di spoofing di un indirizzo di rete, è consigliabile l'impiego di protocolli come DNSSEC, SSL, IPsec o una combinazione di questi per assicurarsi di colloquiare con la controparte attesa.
Spoofing di un programma in memoria. Si tratta di programmi che si nascondono mostrandosi come programmi legittimi ma con l'intento di fare danni o trafugare informazioni. Questi sono un tipo di Trojan, i quali duplicano le azioni di processi esistenti che vengono poi eseguite inconsapevolmente dall'utente. E' necessario tenere sempre aggiornato il software come il sistema operativo e il browser web. Mantenere la connessione a Internet il più sicura possibile, tenendo sempre attivo un firewall. Sia i firewall hardware che software sono eccellenti strumenti per controllare il traffico Internet dannoso. E' necessario installare inoltre un software antivirus o un Trojan remover.
La seguente tabella riporta le vulnerabilità della Top 10 OWASP 2017[15] riconducibili alle minacce di spoofing e per ciascuna vulnerabilità indicata, le relative pratiche[16] e requisiti[17] di sicurezza consigliati da OWASP:

15 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

16 https://www.owasp.org/index.php/OWASP_Proactive_Controls

17 https://github.com/OWASP/ASVS