		• La randomizzare dei nomi dei file contrasta l'esecuzione di possibili attacchi.
Tampering dei pacchetti di rete	Crittografia	• HTTPS/SSL; • IPsec.
	Anti-pattern	Isolamento della rete.

Tabella 11 - STRIDE: Indirizzamento del Tampering

Tampering di un file. Se un attaccante possiede un account su una macchina, questo può facilmente portare un attacco di tampering su di un file che risiede sulla stessa macchina, oppure quando questo transita sulla rete per essere ricevuto.
Tampering della memoria. Ciò avviene quando un processo con privilegi minimi di trust o non, altera in qualche modo la memoria fisica della macchina. Per esempio, se si stanno prendendo dati da un segmento di memoria condivisa, esistono delle ACL tali da consentirne agli altri processi la sola lettura? Per le applicazioni web che acquisiscono dati tramite AJAX, assicurarsi di validare tali dati prima di darli in pasto alla logica di business.
Tampering del traffico di rete. La prevenzione del traffico di rete richiede una gestione sia dello spoofing che del tampering. Diversamente, chiunque intenzionato ad alterare i dati in transito potrebbe semplicemente far finta di essere all'altra estremità, portando invece un attacco di tipo MITM (Man In The Midle). La soluzione più comune per contrastare questo problema è utilizzare il protocollo SSL o l'IPsec (IP Security) come infrastruttura di comunicazione. Entrambi, SSL e IPsec indirizzano le problematiche legate alla confidenzialità e all'integrità delle informazioni e possono anche aiutare ad indirizzare lo spoofing.
Tampering del traffico di rete attraverso l'anti-pattern. L'isolamento della rete non assicura la protezione dalle minacce di tampering poiché generalmente non si riesce a mantenere la rete costantemente isolata.

La seguente tabella riporta le vulnerabilità della Top 10 OWASP 2017[18] riconducibili alle minacce di tampering e per ciascuna vulnerabilità indicata, le relative pratiche[19] e requisiti[20] 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 applicativa)
A1 – Injection	C5 – Validate All Inputs	V5 - Malicious Input Handling V11 - HTTP Security Configuration
	C4 – Encode and Escape Data	V5 - Malicious Input Handling
A4 - XML External Entities (XXE)	C6 – Validate All Inputs	V5 - Malicious Input Handling
	C4 – Encode and Escape Data	V5 - Malicious Input Handling
A7 - Cross-Site Scripting (XSS)	C5 – Validate All Inputs	V5 - Malicious Input Handling
	C4 – Encode and Escape Data	V5 - Malicious Input Handling

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

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

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