- VERIFICA DEL LAVORO SVOLTO - La convalida del modello è l'ultima cosa da fare come parte della modellazione delle minacce. Ci sono alcune attività da svolgere prima, ed è bene mantenerle allineate con l'ordine in cui è stato svolto il lavoro precedente. Pertanto, le attività di validazione includono il controllo del modello, la verifica di ciascuna minaccia e il controllo dei test. E' probabile che si desideri convalidare il modello anche una seconda volta, ovvero quando ci si avvicina al rilascio o all'installazione.
- CONTROLLO DEL MODELLO - È necessario assicurarsi che il modello finale corrisponda a quello costruito. Se così non fosse, come potremmo sapere se le minacce trovate sono corrette e rilevanti? Per fare ciò, è opportuno organizzare degli incontri durante i quali tutti, osservando e analizzando il diagramma, rispondano alle seguenti domande:
    - il diagramma è completo?
    - il diagramma è accurato?
    - il diagramma copre tutti le decisioni intraprese in termini di sicurezza?
    - è possibile procedere con la versione successiva del diagramma senza apportare modifiche?

  Una risposta affermativa a tutte le domande di cui sopra, indica che il diagramma è sufficientemente aggiornato e maturo per poter procedere. Diversamente sarà necessario apportare gli opportuni cambiamenti.
- DETTAGLI DEL DIAGRAMMA - Non disegnare mai un diagramma ad occhio, con un livello di dettaglio tale da rappresentare l'intero comportamento del sistema. Utilizzare un sotto diagramma che mostri il solo dettaglio di una particolare area del sistema stesso. Si deve cercare di escludere ciò che non è rilevante per il progetto. Per esempio, se si è davanti ad un processo molto complesso, forse tutto ciò che è in quel processo dovrebbe essere trattato in un diagramma, e tutto ciò che è al di fuori di esso in un altro. Se è presente un dispatcher o un sistema di code, questi sono un buon punto di suddivisione, e lo sono anche i database o i sistemi di fail-over. Esistono ancora elementi che devono essere maggiormente dettagliati? Bene, questi vanno esclusi. La cosa importante da ricordare è che il diagramma ha lo scopo di aiutare a comprendere e discutere il sistema.

5.6 Indirizzamento delle minacce

Una volta raccolte le minacce individuate in uno o più elenchi, il passo successivo nel processo di modellazione è quello di scorrere l'elenco o gli elenchi indirizzando ciascuna minaccia. Pertanto è possibile decidere se:

- **Mitigare** la minaccia - Si concretizza nel fare qualcosa per rendere più difficile la possibilità di poter essere sfruttata. Richiedere una password per controllare chi accede al sistema, mitiga la minaccia di spoofing. Aggiungere un controllo password che ne rafforza la complessità o la scadenza, riduce la probabilità che una password venga scoperta o venga utilizzata se rubata.
- **Eliminare** la minaccia - Avviene quasi sempre eliminandone le caratteristiche. Se si presenta una minaccia in cui qualcuno ha accesso ad una funzione amministrativa di un sito web entrando ad esempio in "/admin/URL", è possibile mitigarla impiegando delle password o altre tecniche di autenticazione, ma comunque, questa non verrà risolta. È possibile rendere più complessa la URL in modo da rendere meno probabile la possibilità che questa venga individuata, ma anche in questo caso la minaccia non verrà risolta. La si può eliminare rimuovendo l'interfaccia amministrativa, e gestendo l'attività di amministrazione tramite linea di comando. In questo caso esisterebbero comunque altre minacce riconducibili a come l'utente amministratore dovrebbe autenticarsi per eseguire l'attività di amministrazione da linea di comando. Lo spostamento dell'interfaccia dall'http a linea di comando rende facile la mitigazione della minaccia controllando la superficie di attacco.
- **Spostare** la minaccia - Consiste nel lasciare che qualcuno o qualcos'altro gestisca il rischio. Per esempio, potremmo demandare la gestione delle minacce relative all'autenticazione al sistema operativo, oppure rafforzare il perimetro di fiducia con un firewall. È anche possibile trasferire il