2. si determina il valore dei nodi non foglia. Questo è ricavato a partire dal valore dei loro figli.

L'analista dovrà avere la capacità di attribuire dei "buoni" valori per i nodi foglia (anche in questa fase la capacità di identificazione dei valori è assolutamente soggettiva).

PASSO 3 – Analisi dei risultati

L'analisi è volta a determinare:

1. il costo dell'attacco più economico (si analizzano i valori degli attributi a livello del nodo radice);
2. gli attacchi il cui costo non supera una certa soglia (si analizzano i sotto-alberi i cui nodi rappresentano una determinata proprietà/soglia);
3. l'attacco più economico che non utilizza attrezzature speciali (si analizzano i sotto-alberi i cui nodi rappresentano un determinato insieme di proprietà).

L'analisi dei risultati deve tenere conto delle caratteristiche del potenziale attaccante in quanto queste determinano quali parti dell'attack tree devono essere prese in considerazione. Attaccanti diversi hanno diversi livelli di abilità, accesso, avversione al rischio, soldi e così via. Se il potenziale attaccante è la criminalità organizzata, occorre considerare la possibilità di attacchi costosi e "mezzi illeciti" (corruzione, ricatto, ecc.) che espongono l'attaccante fino al rischio di andare in prigione. Se il potenziale attaccante è un terrorista, occorre considerare "mezzi illeciti" che espongono l'attaccante fino al rischio di morire per raggiungere l'obiettivo. Se l'attaccante è un casual hacker si esclude la possibilità di attacchi costosi e "mezzi illeciti" (corruzione, ricatto, ecc.).

PASSO 4 – Analisi What-if

L'analisi "what if" è costruita a partire dalle diverse ipotesi di adozione delle contromisure. Introducendo contromisure, cambiano i valori attribuiti nel secondo step della metodologia e quindi cambiano i risultati dell'analisi.
In conclusione, una delle caratteristiche di valore degli attack tree è che sono riutilizzabili. Tornando all'esempio inziale, una volta completato l'albero di attacco relativo a "Ottenere le credenziali di autenticazione", è possibile utilizzarlo in qualsiasi situazione in cui sia interesse dell'attaccante l'acquisizione delle credenziali di autenticazione. L'attack tree relativo a "Ottenere le credenziali di autenticazione" può inoltre diventare parte di un attack tree più grande.

5.5.4.3 TRIKE

TRIKE è un framework open-source per l'auditing della sicurezza da un punto di vista di risk management basato sulla generazione di modelli di minacce in modo affidabile e ripetibile. Il progetto ebbe inizio nel 2005 come tentativo di migliorare l'efficienza e l'efficacia delle esistenti metodologie di modellazione delle minacce e da allora viene attivamente aggiornato e utilizzato. I creatori di TRIKE hanno anche sviluppato strumenti a supporto di questa metodologia come il foglio di calcolo TRIKE. Questo strumento si focalizza sull'automazione della generazione delle minacce e non prevede alcun brainstorming. I team di sicurezza non hanno la necessità di individuare le possibili minacce in quanto tali minacce sono già predefinite. TRIKE può essere utilizzato anche da uno sviluppatore di sicurezza inesperto per trovare le vulnerabilità di sicurezza in modo efficace ed affidabile. Il team TRIKE ha adottato l'analisi HAZOP (Hazardous Operations), ovvero, un metodo sistematico per identificare quali variazioni di processo devono essere mitigate. Questo framework può sostituire gli alberi di minaccia e d'attacco (attack tree).
TRIKE utilizza un approccio basato sul rischio con distinte implementazioni dei modelli di minacce e rischi. Approccia al Threat Modeling assumendo una posizione difensiva rispetto a quella di un attaccante. TRIKE ha anche proposto il concatenamento delle minacce, un'alternativa agli alberi delle minacce, nel tentativo di ridurre la natura ripetitiva di quest'ultimi.