6.1.3.1 Confini di fiducia (Trust boundaries)

Identificare i confini di fiducia dell'applicazione aiuta a concentrare l'analisi sulle aree di maggiore interesse. I confini di fiducia evidenziano dove cambiano i livelli di fiducia. In quest'ambito, la fiducia è intesa in chiave di riservatezza e integrità. Ad esempio, una modifica nei livelli di controllo di accesso all'applicazione, dove è necessario un livello o un privilegio specifico per accedere a una risorsa o un'operazione, comporterebbe una modifica del livello di fiducia. Un altro esempio, potrebbe essere in un punto di entrata nell'applicazione ove è necessario filtrare i dati di accesso.
Per identificare i confini di fiducia occorre:

- Iniziare individuando i confini del sistema esterno. Ad esempio, l'applicazione può scrivere un file sul server X, può effettuare chiamate al database sul server Y e può chiamare il servizio Web Z. Ciò definisce il limite di sistema.
- Identificare i punti di controllo di accesso o i luoghi chiave in cui l'accesso richiede privilegi aggiuntivi o l'appartenenza ad un dato ruolo. Ad esempio, l'accesso ad una pagina particolare, potrebbe essere limitata ai soli dirigenti, nel qual caso richiederebbe un accesso autenticato e inoltre che l'utente ricopra un certo ruolo.
- Identificare i confini di fiducia da una prospettiva di flusso di dati. Per ogni sottosistema, considerare se il flusso di dati a monte o l'input dell'utente sia affidabile e se non lo è, considerare in che modo il flusso di dati e l'input possono essere autenticati e autorizzati. Conoscere quali punti di ingresso esistono tra i confini di fiducia, consente di concentrare l'identificazione delle minacce in tali punti considerati chiave.

Alcuni esempi di confini di fiducia sono: un firewall perimetrale, il confine tra il web server e il server di base dati, punti di ingresso di componenti di business che espongono dati privilegiati, dunque, protetti da ulteriori controlli di accesso, il limite tra l'applicazione e i servizi di terze parti.

6.1.3.2 Flussi di Dati

È importante tracciare il flusso dei dati all'interno dell'applicazione dal punto di ingresso al punto d'uscita. Questa attività è necessaria per comprendere come interagisce l'applicazione con i sistemi esterni, i sistemi client e come interagiscono i componenti interni. È importante anche, prestare particolare attenzione al flusso di dati che attraversa i confini di fiducia e come tali dati vengono convalidati nel punto di entrata. Inoltre occorre fare molta attenzione ai dati sensibili e come questi attraversano il sistema, se passano attraverso una rete e/o se vengono persistiti. Un buon approccio è quella di analizzare il flusso dei dati tra i singoli sottosistemi a partire dal livello più alto e poi via via a scendere ai livelli più bassi.

6.1.3.3 Punti d'Ingresso (Entry Points)

I punti di ingresso dell'applicazione servono anche come punti di ingresso per gli attacchi. Il front-end di una applicazione web che è in ascolto di richieste http è un esempio di punto di ingresso vulnerabile agli attacchi. Questo punto di ingresso è destinato ad essere esposto agli utilizzatori. Altri punti di ingresso, come i punti di accesso interni esposti dai sotto componenti negli strati dell'applicazione, possono esistere solo per supportare la comunicazione interna con altri componenti. Tuttavia, occorre conoscere dove sono localizzati e quali tipi di input ricevono nel caso in cui un aggressore riesca ad aggirare l'interfaccia dell'applicazione e attaccare direttamente un punto di ingresso interno.
A titolo esplicativo si elencano di seguito ulteriori esempi di Entry Points:

- Front-end applicativo (form di Login, form di Ricerca);
- Funzioni applicative (funzione di login, web service esposti, ..);
- Console di amministrazione del database;