La sicurezza orientata alla transazione invece definisce se un interlocutore del sistema ha un'identità ed è autorizzato ad effettuare le comunicazioni richieste. Una volta che tali comunicazioni hanno luogo, un sistema sicuro dovrebbe impedire a qualsiasi interlocutore di negarle o ripudiarle. A questo sottoinsieme appartengono le seguenti categorie di minacce:

- Le minacce di falsificazione dell'identità esistono a causa di una scarsa o inesistente verifica e autenticazione dell'identità stessa. Il sistema non è in grado di verificare l'autenticità della controparte che interagisce con esso.
- L'elevazione del privilegio è la minaccia alla sicurezza maggiormente dannosa. Un controllo di accesso scarso o inesistente (autorizzazione) dà la possibilità ad una possibile controparte malintenzionata di portare uno qualsiasi degli altri attacchi che la STRIDE rappresenta.
- Le minacce di ripudio si verificano quando non è possibile dimostrare l'integrità dei dati e quando l'autenticazione ad essi collegata non può essere verificata. Una parte ostile potrebbe pertanto negarne qualsiasi tipo di associazione per mancanza di prove.

5.5.4.1.1 Tecniche di mitigazione

Ogni minaccia viene mitigata o accettata. Per i non esperti di sicurezza, la STRIDE fornisce per ogni tipo di potenziale minaccia identificata una o più classificazioni delle tecniche di mitigazione da mettere in campo (vedi tabella che segue).

Tipo Minaccia	Tecnica di mitigazione o controlli di sicurezza
Spoofing	**Autenticazione**
Tampering	**Integrità**
Repudiation	**Servizi di non ripudio (Autenticazione + Integrità)**
Information disclosure	**Confidenzialità**
Denial of Service	**Disponibilità**
Elevation of Privilege	**Autorizzazione**

Tabella 8 - Tecniche di mitigazione

AUTENTICAZIONE – TECNICHE DI MITIGAZIONE DELLO SPOOFING

Le tecnologie per l'autenticazione di computer (o account di computer) includono ad esempio:

- IPSec,
- DNSSEC,
- SSH host keys,
- Kerberos authentication,
- HTTP Digest o Basic authentication,
- "Windows authentication" (NTLM),
- Sistemi PKI, come SSL o TLS con certificati.

Le tecnologie per l'autenticazione dei flussi a livello di bit (file, messaggi, ecc.) includono ad esempio:

- Digital signatures,
- Hashes.

I metodi per l'autenticazione delle persone possono coinvolgere uno qualsiasi dei seguenti elementi:

- Qualcosa che sai, come ad esempio una password,
- Qualcosa che hai, come una card di accesso,
- Qualcosa che sei, come ad esempio un dispositivo biometrico, comprese le immagini fotografiche,
- Qualcuno che conosci e che può autenticarti.

Le tecnologie per mantenere l'autenticazione tra le connessioni includono ad esempio:

- Cookies.
- Tokens (es: JWT – JSON Web Token),
- Accesso di terze parti (OAuth, API-token),
- OpenID (protocollo basato su http che utilizza un identity provider per validare l'utente),
- SAML (linguaggio di markup delle asserzioni di sicurezza che fa uso come nel caso OpenID di un identity provider, ma è basato su XML e quindi più flessibile. La versione consigliata per SAML è la 2.0. SAML fornisce anche un modo per implementare il Single SignOn, ovvero l'utente può utilizzare l'URL del fornitore di identità per accedere al sistema che reindirizza con dati XML alla pagina dell'applicazione che può essere decodificato per ottenere le informazioni dell'utente).

On top ai metodi di autenticazione di cui sopra, se necessario, è possibile anche implementare algoritmi One Time Password (OTP), Two Factor Authentication (2FA) e Email verification ecc.

INTEGRITA' – TECNICHE DI MITIGAZIONE DEL TAMPERING

Le tecnologie per la protezione degli asset includono includono ad esempio:

- ACLs o permissions,
- Digital signatures,
- Hashes,
- Windows Mandatory Integrity Control (MIC),
- Unix immutable bits.

Le tecnologie per la protezione del traffico di rete includono ad esempio:

- SSL,
- SSH,
- IPSec,
- Digital signatures.

NON RIPUDIO – TECNICHE DI MITIGAZIONE DELLA REPUDIATION

Le tecnologie che è possibile utilizzare per affrontare il problema del ripudio includono ad esempio:

- Logging,
- Log analysis tools,
- Secured log storage,
- Digital signatures,
- Secure time stamps,
- Trusted third parties,
- Hash trees,
- Strumenti per la prevenzione delle frodi.

CONFIDENZIALITA' – TECNICHE DI MITIGAZIONE DELLA INFORMATION DISCLOSURE

Le tecnologie per la riservatezza includono ad esempio:

- Protezione dei files:
  - ACLs/permissions,
  - Encryption,
  - Appropriata gestione delle keys.
- Protezione dei dati di rete:
  - Encryption,
  - Appropriata gestione delle keys.

- Protezione della comunicazione e delle headers di comunicazione:
  - Mix networks,
  - Onion routing,
  - Steganography.

DISPONIBILITA' – TECNICHE DI MITIGAZIONE DEL DENIAL OF SERVICE

Le tecnologie per la protezione degli asset includono ad esempio:

- ACLs,
- Filters,
- Quotas (rate limiting, thresholding, throttling),
- High-availability design/architetture,
- Bandwidth control (rate limiting, throttling),
- Cloud services. Secondo le ultime ricerche di McAfee[14], la maggior parte dei team di sicurezza afferma di poter ottenere una maggiore sicurezza negli ambienti in-the-cloud visto che, i principali provider di servizi in-the-cloud investono maggiori risorse nella sicurezza di quanto la maggior parte delle aziende possano permettersi per rendere sicuri i propri "hosted environment".

AUTORIZZAZIONE – TECNICHE DI MITIGAZIONE DELL'ELEVATION OF PRIVILEGE

Le tecnologie per migliorare l'autorizzazione includono ad esempio:

- ACLs,
- Group or role membership,
- Role based access control,
- Attribute based access control,
- Claims-based access control,
- Windows privileges (runas),
- Unix sudo,
- Chroot, AppArmor o altre unix sandboxes,
- The "MOICE" Windows sandbox pattern,
- Convalida degli input per uno scopo definito.

5.5.4.1.1.1 Indirizzamento dello Spoofing

La Tabella seguente elenca gli obiettivi di spoofing, le strategie di mitigazione per indirizzare lo spoofing e le tecniche per attuare tali mitigazioni:

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Spoofing di una persona	Identificazione e autenticazione (username e qualcosa che conosci/hai/sei)	Username, nomi reali, identificativi: • Password; • Token; • Biometria. Registrazione/Manutenzione/Scadenza.

[14]https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk-report-business-growth-edition.html?source=website&lsource=website&eid=BRXDXCDD&smcid=WW