Progetto Software Security and Blockchain

Domande

- Perchè il value di un asset cambia nella tapella pagina 28 slide U4Lab-PreliminaryAssesment?
- Quando l'utente richiede di vedere il contenuto del registro, sempre considerando che possa farlo, l'off-chain manager comunica con l'on-chain manager per ottenere la posizione delle parti distribuite del registro. A questo punto, per poter rispondere all'utente, deve comunicare con gli shard per ottenere il contenuto delle singole parti?
- La sicurezza fisica del server su cui si troverà l'off-chain manager va considerata? Dovremmo quindi, per esempio, prevedere possibili Jamming, oppure considerare il fatto che il server verrà deployato su strutture controllate da terzi, e il costo dovuto a questo?
- Dovremmo considerare come asset i task dell'utente, che non sono di fatto serviti dall'applicazione, o dovremmo solo considerare i servizi offerti dall'applicazione che possono quindi essere vittima di DoS per esempio. Esempio specifico: send transaction request è il vettore attraverso il quale si può attuare un Sustained client engagement, o Flooding, ma poi la risorsa attaccata è l'off-chain manager o lo smart contrat sullo shard(gia prevede meccanismi per evitarlo). Dovremmo quindi fare queste considerazioni sull'asset send transaction request (e.g. prevedere nel codice di invio della richiesta un meccanismo di controllo), o dovremmo farlo sugli asset che lo subiscono, e specificare quindi lì che questo controllo va fatto?

Attacchi

- CAPEC-151 Identity Spoofing: falsificazione dell'identità.
- CAPEC-560 Use of known domain credentials: utilizzo non autorizzato di credenziali di un entità per compiere azioni malevole.
- CAPEC-555 Remote . . . : utilizzo non autorizzato di credenziali per accedere a risorse da remoto tramite SSH, TELNET, ..
- CAPEC-114 Authentication Abuse: ottenere l'accesso non autorizzato al sistema attraverso pattern d'attacco.
- CAPEC-94 AiTM: fingersi una o entrambe le parti nella comunicazione tra 2 entità per diversi fini.
- CAPEC-117 Interception: intercettazione della comunicazione per diversi fini.
- CAPEC-157 Sniffing: leggere i pacchetti intercettando la comunicazione.
- CAPEC-383 Harvesting Information via API Monitoring: monitorare API per ottenere informazioni.
- CAPEC-122 Identity Abuse: accesso ad azioni che sono erroneament esposte ad una classe di utenza non autorizzata. (Serve davvero??)
- CAPEC-125 Flooding: inondare di richieste un entità cosi che sia rallentata, non disponibile, ecc.

- CAPEC-148 Content Spoofing: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged.
- CAPEC-173 Action Spoofing: An adversary is able to disguise one action for another and therefore trick a user into initiating one type of action when they intend to initiate a different action.
- CAPEC-227 Sustained Client Engagement: richieste per occupare la risorsa, non per farlo crashare o rallentare, bensi per sfruttare algoritmi che prevedono il lock di una risorsa.
- CAPEC-469 HTTP DoS: DoS attraverso richieste HTTP
- CAPEC-233 Privilege Escalation: sfruttare una vulnerabilità per ottenere privilegi
- CAPEC-607 Obstruction/601 Jamming: interferenza fisica sul server. Lo dobbiamo considera SPAL?
- CAPEC-594 Traffic injection: MITM proxy per ...