Analis delle strategie di mitigazione kafka poisoning

A.A 2024/2025

sevenbits.swe.unipd@gmail.com

Registro modifiche

Versione	Data	Autore	Verificatore	Descrizione
0.9.0	2025-01-20	Giovanni Cristellon		Stesura iniziale

Indice

1 Introduzione

1.1 Descrizione del problema

Il sistema di stream processing kafka risulta potenzialmente vulnerabile ad un attaccante che inserisca dati falsi o malformati al fine di alterare il comportamento del sistema pertanto è necessario applicare delle strategie di mitigazione che verifichino origine e correttezza dei dati e limitino i potenziali danni

1.2 Possibili soluzioni

alcune delle possibili soluzioni per la mitigazione di questa tipologia di attacchi sono le seguenti:

- Uso del protocollo TLS per la comunicazione sensori-sistema;
- utenticazione sensoi mediante SASL
- Definizione policies di access control

2 Strategie di mitigazione in Dettaglio

2.1 Uso del protocollo TLS per la comunicazione sensori-sistema

2.1.1 Descrizione

Il protocollo TLS fornisce una modalita di comunicazione tra client e server prottetta da cifratura ingrado di autenticare il server ed garantire l'integrità e riservatezza dei dati in transito. Il protocollo utilizza una chiave di cifratura assimmetrica certificata per stabilire la comunicazione iniziale per poi utilizzare cifratura simmetrica per il resto della sessione. apache kafka dispone in oltre della possibilità di applicare 2 way TLS per introdure un ultteriore autenticazione del client

2.1.2 Requisiti implementazione

il protocollo TLS è gia implementato all'interno di apach kafka è pertanto semplicemente necessario abilitarlo ed insere i certificati richiesti, e possibile adottare sia certifica interni che certificati garantiti da una Certification Autority

2.1.3 Analisi efficacia

l'uso del protocollo TLS in modalita 2 way TLS risulta altamente efficace a negare in modo pressochè completo la possibilità di attacchi remoti in quanto il sistema sarà in grado di identifichare e bloccare ogni messaggio la cui provenienza non sia un sensore registrato nel sistema

2.2 Autenticazione sensori mediante SASL

2.2.1 Descrizione

Il protocollo SASL fornisce la possibilità di integrare un ampio spettro di metodologie per l'Autenticazione di messagi in ingresso basata su sfide e risposte e puo anche essere integrato con protocolli di trasporto che garantiscano riservatezza del messaggio

2.2.2 Requisiti implementazione

il protocollo SASL è gia implementato all'interno di apach kafka è pertanto semplicemente necessario abilitarlo ed insere i certificati richiesti, e possibile adottare sia certifica interni che certificati garantiti da una Certification Autority

2.2.3 Analisi efficacia

l'uso del protocollo SASL in combinazione con un protocollo di trasporto come TLS risulta altamente efficace a negare in modo pressochè completo la possibilità di attacchi remoti in quanto il sistema sarà in grado di identifichare e bloccare ogni messaggio la cui provenienza non sia un sensore registrato nel sistema

2.3 Policies di access control

2.3.1 Descrizione

L'uso di access control lists permette di definire un insieme di regole volto a limitare la possibilità che un client compromesso abbia accesso ad informazioni sensibili o sia in grado di manomettere il sistema, ogni regola definische per un client o gruppo di client se questi sia autorizzato o meno a produrre o consumare elementi di un topic.

2.3.2 Requisiti implementazione

apache kafka dispone di un siste integrato di gestione dei permessi ed e quindi semplicemente necessario definire un file di configurazione che elenchi le policies che si intende adottare

2.3.3 Analisi efficacia

l'uso di access control lists permette di ridurre significatamente la potenziale superficie di attacco ed i possibili inquanto permette di ridurre l'accesso dei clients alle funzionalità minime necessarie alle loro funzionalità