



UNIVERSITÀ DI PERUGIA
Dipartimento di Matematica e Informatica



TESI TRIENNALE IN INFORMATICA

Analisi sicurezza del middleware Data Distribution Service O.M.G.

Relatore

Prof. Francesco Santini

Candidato

Federico Ranocchia

Anno accademico 2023/2024

Quì la dedica...

Indice

| | | |
|----------|--|----------|
| 1 | Introduzione al DDS | 5 |
| 1.1 | Modello publish/subscribe | 5 |
| 1.1.1 | Perché non usiamo una connessione con TCP/IP | 6 |
| 1.1.2 | Struttura modello publish/subscribe | 6 |
| 1.2 | Che cos'è il Data Distribution Service | 7 |
| 1.2.1 | Quality of Service (QoS) | 7 |
| 1.2.2 | Global Space Data | 8 |
| 1.2.3 | Architettura DDS | 8 |
| 1.3 | Le entità del DCPS | 9 |
| 1.3.1 | Publisher e Subscriber | 9 |
| 1.3.2 | DataWriter e DataReader | 9 |
| 1.3.3 | Topic | 10 |
| 1.3.4 | Key e Istanza | 10 |
| 1.3.5 | Domain | 11 |
| 1.3.6 | DomainParticipant | 11 |
| 1.4 | Le policy QoS nel dettaglio | 12 |
| 1.5 | Il protocollo RTPS | 13 |
| 1.5.1 | Structure module | 13 |
| 1.5.2 | Behavior module | 13 |
| 1.5.3 | Messages module | 14 |
| 1.5.4 | Discovery module | 14 |
| 1.6 | DDS Security | 15 |
| 1.6.1 | Authentication Service Plugin | 15 |
| 1.6.2 | Access Control Service Plugin | 16 |

| | | |
|----------|---|-----------|
| 2 | Vulnerabilità DDS | 19 |
| 2.1 | Blocco DataReader tramite sequence number | 19 |
| 2.1.1 | Dettagli attacco | 20 |
| 2.1.2 | Conclusioni | 20 |
| 2.2 | DDoS sfruttando estensione DDS security | 21 |
| 2.2.1 | Dettagli attacco | 21 |
| 2.2.2 | Conclusioni | 21 |
| 2.3 | Enumeration sniff | 22 |
| 2.3.1 | Dettagli attacco | 22 |
| 2.3.2 | Conclusioni | 23 |
| 2.4 | Modifica maligna di OWNERSHIP strength | 23 |
| 2.4.1 | Dettagli attacco | 24 |
| 2.4.2 | Conclusioni | 24 |
| 2.5 | Modifica maligna di LIFESPAN QoS | 25 |
| 2.5.1 | Dettagli attacco | 26 |
| 2.5.2 | Conclusioni | 26 |

Capitolo 1

Introduzione al DDS

In questo capitolo viene fatta un'introduzione generale dello standard del Data Distribution Service (DDS) gestita dall'Object Management Group (OMG) [17]. Inizialmente a livello generale per poi andare sempre più nel dettaglio per capire il suo funzionamento. Questo ci sarà utile per comprendere le vulnerabilità che verranno analizzate nei successivi capitoli. Inoltre verrà introdotta la sua estensione DDS security che si occupa di rendere più sicuro lo standard DDS aggiungendo l'autenticazione e una implementazione della cifratura dei pacchetti scambiati tra i vari dispositivi connessi nella rete. Infine verrà mostrato in quali contesti attuali il DDS viene utilizzato con le sue diverse implementazioni.

In questa tesi potrebbe venire omessa la specifica OMG perchè faremo riferimento esclusivamente al DDS conforme all'Object Management Group. Questo standard ha delle specifiche tecniche ben precise, consentendo l'interoperabilità tra i diversi vendor che lo rispettano, insieme a tanti altri numerosi vantaggi [4].

1.1 Modello publish/subscribe

Prima di parlare del DDS, è necessario capire il funzionamento del modello Publish-Subscribe che sta alla base del suo funzionamento. Questo modello di publish e subscribe non funziona come la classica applicazione che siamo abituati a vedere tra server e client tramite protocollo TCP/IP nell'ambito delle comunicazioni.

1.1.1 Perché non usiamo una connessione con TCP/IP

Prendiamo l'esempio di un collegamento tra una workstation e un sensore per la temperatura. La connessione a livello fisico avverrà tramite un collegamento Ethernet. La workstation e il sensore quindi si trovano nello stesso network e possono ora cominciare a comunicare tra di loro. L'obiettivo è quello di trasferire i dati dal sensore alla workstation in modo tale da poterli visualizzare a schermo. La metodologia più frequente è quella di utilizzare un socket tramite protocollo TCP/IP, ma non sempre questa è la soluzione migliore. Alcuni vantaggi del TCP/IP sono la disponibilità di utilizzo in molte applicazioni e nella maggior parte delle connessioni a Internet. Tuttavia, in certe implementazioni, TCP/IP non risulta la soluzione migliore, specialmente quando dobbiamo collegare un numero di dispositivi al network che può variare nel tempo. Se nel nostro network tra workstation e sensore della temperatura, aggiungiamo un altro dispositivo, come un sensore per la temperatura, bisognerebbe creare un nuovo socket TCP/IP per far comunicare il nuovo sensore con la workstation. Questo è necessario perché TCP/IP supporta una comunicazione di tipo one-to-one (uno a uno). Come vedremo nella prossima sottosezione, il modello publish/subscribe non ha questa limitazione [14].

1.1.2 Struttura modello publish/subscribe

Per funzionare, il modello publish/subscribe, ha bisogno di due elementi chiamati publisher e subscriber, che permettono lo scambio di messaggi all'interno del network. La comunicazione avviene quando hanno un topic, che rappresenta una tipologia di dati (ad esempio temperatura, distanza, velocità, etc...) è in comune tra di loro.

- Publisher: colui che pubblica nuovi dati riguardanti dei topic rendendoli accessibili ai subscriber iscritti. Di solito si tratta di un sensore.
- Subscriber: è colui che si iscrive ai topic del publisher, cominciando così a ricevere nuovi dati sul topic scelto. Spesso si tratta di un dispositivo utilizzato per visualizzare informazioni, come uno schermo.

Chiamiamo entità tutti i dispositivi che fanno parte del modello publish/subscribe. Una caratteristica di queste entità è che possono essere aggiunte o rimosse da una rete

senza nessun problema, dato che le comunicazioni avvengono in modalità asincrona [4].

Inoltre questo modello risulta molto flessibile e adatto in ambienti real-time dove le informazioni possono cambiare o essere utilizzate da più dispositivi. I subscriber, ad esempio possono cambiare i topic a cui sono iscritti e i publisher possono smettere di pubblicare nuovi aggiornamenti su un determinato topic anche a runtime [7].

1.2 Che cos'è il Data Distribution Service

Il DDS gestito da OMG è un middleware e uno standard API con una gestione dei dati di tipo data-centric. Prendendo in considerazione il modello ISO OSI (Open Systems Interconnection), questo middleware è un software che si trova tra l'applicativo e il livello del sistema operativo. Il DDS si basa sul DCPS (Data-Centric Publish-Subscribe) che è un modello di comunicazione simile a quello di tipo publish/subscribe, ma con un approccio più data-centric, in modo tale da semplificare il lavoro del programmatore che si deve solamente occupare di specificare il contesto del dato che deve mandare o ricevere. Con data-centric infatti, specifichiamo che il focus del modello DCPS è incentrato sui dati stessi, anziché sulle entità che li scambiano [9]. Così facendo non bisogna preoccuparsi dell'invio o della ricezione dei messaggi, perché questa parte viene completamente gestita dal middleware.

Altri vantaggi del DDS includono una architettura adattabile che supporta degli elementi di auto-scoperta (auto-discovery) o Dynamic Discovery in modo tale da aggiungere o rimuovere dispositivi dalla rete in modo automatico, anche a runtime. Il Dynamic Discovery ha il compito di analizzare quali tipologie di dati ha bisogno questo nuovo dispositivo.

Inoltre ogni nuovo partecipante utilizzerà sempre le stesse API per comunicare con l'applicativo dato che non c'è bisogno di configurare le impostazioni degli indirizzi IP o preoccuparsi delle diverse architetture [14].

1.2.1 Quality of Service (QoS)

Per soddisfare i diversi requisiti di una trasmissione dati, il Data Distribution Service (DDS) utilizza un insieme di policy Quality of Service (QoS). Queste policy permet-

tono di controllare, regolare e ottimizzare lo scambio di dati tra i vari componenti all'interno del middleware. Queste policy QoS possono variare significativamente in base al tipo di comunicazione richiesta, offrendo una gestione altamente flessibile e granulare. Ogni elemento del middleware può essere configurato con policy specifiche, in modo tale da adattarsi alle esigenze dell'applicazione.

1.2.2 Global Space Data

Il DDS utilizza il Global Data Space (spazio dati globale), un'area logica condivisa che consente agli applicativi di accedere a una sorta di memoria locale tramite API. L'applicativo nella scrittura o nella ricezione dei dati utilizzerà questa memoria locale fittizia come un'unica risorsa centralizzata. Tuttavia, i dati all'interno di questa memoria possono contenere informazioni provenienti da nodi remoti distribuiti per la rete. L'applicativo non deve così preoccuparsi dell'accessibilità dei dati, poiché questi vengono gestiti come se si trovassero tutti in unico punto [9].

1.2.3 Architettura DDS

Lo standard DDS definito dall'OMG è composto da due layer: il DDS e il DDSI (DDS Interoperability).

- DDS: è il layer fondamentale in cui troviamo il DCPS (Data-Centric Publish-Subscribe), il modello di comunicazione simile a quello di tipo publish/subscribe, che si occupa di mettere in comunicazione più applicazioni tra di loro. In questo layer vengono inoltre definite le policy QoS [2].
- DDSI: è il layer che si occupa di garantire l'interoperabilità tra le diverse implementazioni del DDS, ad esempio quando provengono da vendors diversi. All'interno di questo layer troviamo l'RTPS (Real-Time Publish-Subscribe Protocol), un protocollo che permette ai vari dispositivi DDS di comunicare e scoprirsi tra di loro (Dynamic Discovery). RTPS è il wire-protocol (un protocollo che permette lo scambio di messaggi del DDS al layer di trasporto di rete del modello ISO OSI) ufficiale del DDS, con standard definito da OMG, che definisce il formato dei messaggi e impone le regole che permettono una trasmissione

standardizzata di scambio dati. Se questo wire-protocol non fosse presente, le diverse implementazioni del DDS non potrebbero comunicare tra di loro [10].

1.3 Le entità del DCPS

Il layer DDS per operare utilizza le entità definite dal DCPS, che rappresentano gli elementi necessari per il funzionamento dell'intero middleware. Queste hanno il compito di gestire i dati scambiati tra i vari partecipanti all'interno del sistema. Le entità principali del DDS sono: il publisher, il subscriber, il DataWriter, il DataReader, il Topic, la Istanza, il Domain e il Domain Participant. Ognuna di queste entità deve tener conto del suo set di policy QoS configurate che ne definiscono il comportamento. Queste policy verranno analizzate più nel dettaglio nella sezione 1.4.

Il linguaggio utilizzato da queste entità si chiama Interface Definition Language (IDL) e anch'esso è standardizzato da OMG. IDL è un linguaggio tipizzato simile a C++ che supporta data types come char, int, double, float etc [14] ...

1.3.1 Publisher e Subscriber

Publisher e subscriber sono entità che abbiamo già incontrato in precedenza nel modello publish/subscribe. Queste due entità mantengono lo stesso ruolo all'interno del modello DCPS.

1.3.2 DataWriter e DataReader

Per comunicare tra loro, un publisher si interfaccia tramite DataWriter, mentre il subscriber si interfaccia tramite un DataReader. Il DataWriter e il DataReader sono interfacce, perché l'applicativo può mandare e ricevere dati tramite queste due entità fondamentali. Questi dati scambiati tra middleware e applicativo sono i data type e i data-values. I data type consentono di descrivere la struttura e il formato del dato, mentre i data-value sono i dati veri e propri che rispettano le specifiche data type.

- DataWriter: è l'interfaccia usata dagli applicativi per spedire i data-values con un loro specifico data type ai publisher. Ricevuti questi data-values il publisher spedisce le informazioni ricevute dall'applicativo ai relativi subscriber.

- **DataReader**: é l'interfaccia usata dagli applicativi per ricevere i data-values con i rispettivi data type pubblicati in precedenza da un publisher [4].

É possibile associare piú DataReaders ad un unico publisher e piú DataWriters ad un unico subscriber. Tuttavia, un DataWriter può essere associato solo ad un Publisher e un DataReader solo ad un Subscriber. Questo avviene perchè i DataReaders e DataWriters possono utilizzare un solo data type alla volta, mentre i publisher e i subscribers, non avendo questa limitazione, possono gestire piú DataWriters e DataReaders alla volta.

1.3.3 Topic

Nel modello publish/subscribe abbiamo già introdotto i topic, ma abbiamo la necessità di approfondirli quando vengono utilizzati con le specifiche del DDS.

I topic vengono utilizzati per identificare il data type scambiato tra i publishers e i subscribers, creando così un punto di connessione tra DataWriter e DataReader [8]. All'interno del topic troviamo il nome, i data types e le policy QoS. Il nome del topic corrisponde ad una stringa univoca che serve per identificarlo tra gli altri topic del domain.

1.3.4 Key e Istanza

Uno o piú data types di un topic possono diventare la chiave (key) del topic. Queste chiavi ci permettono di suddividere i data-values di un topic, dividendoli a seconda della chiave. Ogni suddivisione che effettuiamo tramite una key diversa crea un'istanza che al suo interno contiene i data-values di un flusso di dati (data-stream) [11].

Per fare un esempio prendiamo il topic velocità in un contesto dove si vogliono analizzare i dati di una gara. La struttura del topic avrà due data types: il primo corrisponde al valore della velocità registrata, mentre il secondo mostra l'id-macchina che identifica da quale vettura i dati provengono.

```
struct Veicolo { // Nome del topic
    id_macchina; // Key del topic
    velocita;
```

}

Codice 1.1: Esempio di Topic con una key usando il linguaggio IDL.

Creiamo ora due istanze, una con valore 270 per la velocità e con l'id-macchina uguale a 1 e l'altra con un valore di 220 per la velocità e con id-macchina uguale a 2. L'id-macchina fungerà da key del topic per distinguere la provenienza dei dati; in questo modo possiamo così controllare le due macchine con due istanze ciascuna.

1.3.5 Domain

L'entità del domain (dominio) rappresenta uno spazio logico definito che ha lo scopo di mettere in comunicazione i vari applicativi tra di loro. All'interno possiamo trovare i vari topic che collegano gli applicativi con i loro rispettivi data-types. L'entità domain è caratterizzata dalle seguenti proprietà:

- Ogni domain viene identificato da un id per renderlo univoco.
- Ogni entità del DDS può appartenere ad un solo domain.
- Le entità all'interno del domain possono interagire solamente con le altre entità all'interno dello stesso domain
- Due applicativi DDS per poter comunicare tra di loro hanno bisogno di entrare nello stesso domain.
- Un applicativo può far parte di più domain creando più istanze dell'entità DomainParticipant in ogni domain in cui vuole interagire [13].

1.3.6 DomainParticipant

L'entità del DomainParticipant all'interno di un Domain del DDS, viene utilizzata dagli applicativi e rappresenta la prima entità creata da un'applicazione che verrà impiegata per creare DataWriters e DataReaders. Questa entità ha il compito di inizializzare le comunicazioni con il Domain attraverso il processo di discovery. Questo processo consente alle entità appartenenti allo stesso domain di trovarsi e connettersi automaticamente. L'entità DomainParticipant è caratterizzata dalle seguenti proprietà:

- Il DomainParticipant come le altre entità, può esistere solo all'interno di un dominio.
- Il DomainParticipant è responsabile della scoperta di altri DomainParticipant all'interno del domain [12].

1.4 Le policy QoS nel dettaglio

A livello logico, le specifiche del DDS definiscono un insieme di policy QoS che le entità del DCPS devono rispettare. Qui di seguito vengono proposte le categorie QoS più rilevanti.

- Ownership: questo valore specifica se un topic può essere aggiornato da più (SHARED ownership) o da un solo (EXCLUSIVE ownership) publisher. Se abbiamo impostato un ownership di tipo EXCLUSIVE, per decidere il publisher che ha la possibilità di aggiornare il topic, viene utilizzato l'ownership STRENGTH.
- Liveness: viene utilizzato per specificare se è necessaria una comunicazione di tipo attivo, rispetto ad una di tipo intermittente.
- Reliability: specifica se in una comunicazione tutti i dati trasferiti tra publisher e subscriber devono essere consegnati per intero, oppure se è accettabile anche la perdita di alcuni dati.
- Lifespan: specifica il tempo di scadenza dei dati pubblicati da un publisher.
- History: specifica quanti e come i dati devono essere mantenuti in un subscriber dopo averli ricevuti.
- Durability: specifica se i dati inviati in precedenza sono disponibili per i nuovi subscriber appena entrati nel domain.

Le configurazioni delle policy vengono trasmesse alle varie entità dal DomainParticipant come i publisher, i subscriber, i topic, i DataWriters etc... Tuttavia, le policy di un publisher e un subscriber devono essere compatibili. Se così non fosse, la comunicazione tra i due potrebbe essere compromessa [2].

1.5 Il protocollo RTPS

RTPS (Real-Time Publish-Subscribe Protocol) é il wire-protocol nativo utilizzato dal DDS che consente di trasferire i dati provenienti dal layer DDS a quello di trasporto della rete. Solitamente questo viene utilizzato in combinazione con il protocollo best-effort UDP/IP, che risulta ottimale per le comunicazioni di tipo real-time. Tuttavia anche i protocolli connection-oriented come il TCP/IP possono essere utilizzati. RTPS include molti vantaggi ideali per il DDS:

- Connettività plug and play: le nuove applicazioni possono unirsi o lasciare il domain a proprio piacimento.
- Tolleranza ai guasti: non sono presenti singoli punti di guasto perchè i dati vengono distribuiti e replicati tra le varie entità DDS che adoperano il Global Data Space.
- Type-safety: gli errori di programmazione vengono gestiti in modo tale da non compromettere il funzionamento dei dispositivi remoti.

L'RTPS é suddiviso in quattro moduli differenti: lo structure module, il messages module, behavior module e il discovery module [6].

1.5.1 Structure module

Questo modulo si occupa di associare le entità DDS alle corrispondenti entità RTPS. Queste entità RTPS sono utilizzate per rappresentare le entità del DDS (come DataReader e DataWriter) all'interno del protocollo RTPS [6].

1.5.2 Behavior module

Il behavior module definisce delle regole di comunicazione durante una sequenza di messaggi tra due o più entità RTPS, che sono i RTPS Writers e i RTPS Readers. Esse servono a mantenere l'interoperabilità tra le varie implementazioni (anche di diversi vendors) del DDS [6].

1.5.3 Messages module

Il messages module si occupa di descrivere il formato dei messaggi scambiati tra i RTPS Writers e i RTPS Readers che sono composti da un header seguito da dei sottomessaggi. Nell'header troviamo informazioni relative al protocollo RTPS, cioè la sua versione, il nome del vendor dell'implementazione usata e il mittente. Nel sottomessaggi invece possiamo trovare un header e una serie elementi. Nell'header del sottomessaggio é presente l'id che ne identifica il tipo, eventuali flag e la lunghezza in bytes del sottomessaggio stesso. Le tipologie dei sottomessaggi più importanti, identificate dal suo header, sono:

- DATA: in questo sottomessaggio vengono trasferiti dall'RTPS Writers all'RTPS Reader i dati effettivi relativi ad un topic.
- HEARTBEAT: viene mandato da un RTPS Writer a un RTPS Reader per comunicare il numero di nuovi (sequence number) aggiornamenti che il Writer ha disponibili.
- ACKNACK: utilizzato per comunicare lo stato di un RTPS Reader al corrispondente RTPS Writer e per informarlo riguardo i dati ricevuti e quelli mancanti. Questo sottomessaggio, con la flag FINAL impostata, consente di far rimanere il Reader sincronizzato con l'RTPS Writer [6].

1.5.4 Discovery module

Questo modulo garantisce che i nuovi partecipanti DDS (publisher e subscriber) riescano a identificarsi in automatico tra di loro in modo tale da inizializzare una possibile comunicazione. Questo modulo é responsabile dell'auto-scoperta (Dynamic Discovery) delle entità del DDS all'interno dello stesso domain. Il Dynamic Discovery utilizza messaggi di tipo multicast e unicast per informare gli altri partecipanti di un nuovo dispositivo connesso alla rete, pronto a comunicare con il resto delle entità. Il discovery module é composto da due protocolli chiamati Simple Participant Discovery Protocol (SPDP) e Simple Endpoint Discovery Protocol (SEDP). SPDP ha il compito di scoprire nuovi partecipanti, mentre l'SEPD si occupa di scambiare tra le entità le informazioni di topics, DataWriter e DataReader. In particolare l'SEDP serve per collegare tramite topic i DataReaders ai DataWriters [6].

1.6 DDS Security

Nelle specifiche del DDS non viene presa in considerazione la sicurezza, quindi un'implementazione che utilizza il DDS di base può essere esposta a numerosi rischi. Per ovviare a questo problema, OMG ha definito un nuovo standard chiamato DDS security. Il DDS security è un'estensione del DDS con l'obiettivo di mitigare una moltitudine di vettori d'attacco come la lettura e la scrittura dei messaggi scambiati tra i partecipanti di un domain DDS. Questa estensione è composta da cinque plugin:

- **Authentication Service Plugin:** serve per effettuare l'autenticazione delle entità DDS. Senza l'autenticazione le entità non possono comunicare tra di loro.
- **Access Control Service Plugin:** ha lo scopo di imporre delle policy alle entità DDS autenticate. Ad esempio limitare la pubblicazione di nuovi dati o la creazione di nuovi topic.
- **Cryptographic Service Plugin:** gestisce tutte le operazioni crittografiche, come la crittografia, la decrittazione e le firme digitali. Ha anche il compito di controllare l'integrità dei messaggi.
- **Logging Service Plugin:** permette di effettuare un audit di tutte le operazioni DDS rilevanti all'interno di un domain.
- **Data Tagging Service Plugin:** fornisce dei metodi per implementare un tag su tutti i dati trasferiti.

Anche se il DDS security riesce a risolvere molti problemi legati alla sicurezza del DDS, non sempre è possibile implementarlo. Spesso la sua configurazione può richiedere molto tempo per essere impostata, soprattutto su sistemi DDS già esistenti e sprovvisti di questa estensione. Il partecipante più vulnerabile rappresenta la sicurezza complessiva dell'intero sistema, quindi ogni entità deve essere protetta [2].

Il DDS security può essere usato anche non utilizzando tutti i plugin; gli ultimi due sono facoltativi e vengono raramente usati [10].

1.6.1 Authentication Service Plugin

Senza questo modulo chiunque potrebbe entrare a far parte nel domain del DDS, ponendo un grave rischio alla sicurezza. Per ovviare a questa falla, l'Authentication

Service Plugin richiede, a ogni dispositivo che vuole entrare nel domain DDS, la necessità di autenticarsi. Prima di effettuare l'autenticazione tutti i partecipanti devono avere un loro certificato e le loro chiavi private, mentre l'amministratore deve creare un certificato root (o Certificate Authority, CA) che deve essere riconosciuto da tutte le entità autorizzate. L'autenticazione tra le entità avviene in modo reciproco, in modo tale che ciascun partecipante verifichi l'identità dell'altro tramite un controllo dei certificati.

Processo di autenticazione

L'autenticazione di due entità viene effettuata tramite il protocollo Diffie-Hellman, che consente la trasmissione di chiavi in modo sicuro anche in canali di comunicazione non protetti. Le due entità utilizzando Diffie-Hellman otterranno una chiave segreta condivisa da entrambi. Implementando questo protocollo la chiave non verrà mai trasmessa direttamente, evitando così di essere intercettata da possibili attaccanti.

Per rafforzare ulteriormente la sicurezza e prevenire attacchi replay (riutilizzo di messaggi intercettati) o di impersonificazione, vengono utilizzate le challenge. Queste challenge corrispondono a valori casuali che cambiano nel tempo e vengono utilizzati durante il calcolo della firma digitale che si effettua nel protocollo Diffie-Hellman. Dato che queste challenge cambiano periodicamente, i vecchi messaggi intercettati dagli attaccanti non possono essere più riutilizzati.

La fase di autenticazione si conclude quando viene completato lo scambio delle chiavi. Queste chiavi verranno poi utilizzate da protocolli di crittazione come l'RSA (Rivest-Shamir-Adleman) per effettuare comunicazioni in modo sicuro. Infatti non sarà possibile per un attaccante spiare o cambiare il contenuto dei messaggi dato che questi sono criptati [15].

1.6.2 Access Control Service Plugin

Questo plugin gestisce i permessi delle entità all'interno di un domain DDS. È possibile configurare questi permessi con una granularità molto fine. Dei possibili permessi possono essere: aggiornare un determinato topic da parte di un DataWriter, far entrare una determinata entità all'interno di un domain, eliminare un topic, entrare o uscire da determinati domains etc. . .

L'Access Control Service Plugin per funzionare ha bisogno di due files in formato XML che devono essere entrambi firmati da un CA: il governance document e il permissions document. Il governance document rimane uguale per tutti i dispositivi all'interno del domain DDS e si occupa di gestire permessi generali a livello di domain. Il permissions document, invece, é unico per ogni dispositivo e si occupa di gestire i permessi del singolo partecipante. Questi vengono ricevuti dai partecipanti durante la fase di autenticazione e devono rimanere sempre disponibili [10].

...

```
<permissions>
  <grant name="ShapesPermission">
    <subject_name>CN=DDS Shapes Demo</subject_name>
    <validity>
      <not_before>2013-10-26T00:00:00</not_before>
      <not_after>2018-10-26T22:45:30</not_after>
    </validity>
    <allow_rule>
      <domains>
        <id>0</id>
      </domains>
    </allow_rule>
    <deny_rule>
      <domains>
        <id>0</id>
      </domains>
    <publish>
      <topics>
        <topic>Circle1</topic>
      </topics>
    </publish>
```

...

Codice 1.2: Estratto di permissions document, tratto da documento di riferimento del DDS Security versione 1.1 [5].

Processo di controllo permessi

Un esempio di processo di controllo permessi avviene quando un DataWriter richiede l'autorizzazione per creare un nuovo topic. Le altre entità hanno il compito di verificare se l'operazione richiesta dal DataWriter viene consentita dai files di permessi a loro disposizione. Per effettuare questa operazione il partecipante, che richiede l'autorizzazione, deve mandare il proprio permission document, il topic che intende creare e i propri metadati. Successivamente un altro partecipante, che ha il compito di autorizzare il DataWriter, riceverà il messaggio ed effettuerà le seguenti verifiche:

1. Verifica che la firma digitale del permesso ricevuto sia valida.
2. I metadati forniti devono corrispondere a quelli del permesso ricevuto.

Il secondo controllo ha lo scopo di verificare che il partecipante, che vuole creare il nuovo topic sia effettivamente quello indicato nel permesso ricevuto in precedenza; mitigando in questo modo gli attacchi di impersonificazione [15].

Capitolo 2

Vulnerabilità DDS

In questo capitolo ci occuperemo di analizzare e comprendere delle vulnerabilità del middleware DDS standard OMG (Object Management Group) [17]. In particolare verrà analizzato il vettore d'attacco, il protocollo utilizzato, il bersaglio dell'attacco e infine verrà proposta una soluzione applicabile per mitigare i possibili attacchi. Queste vulnerabilità in molti casi, possono essere sfruttate quando un partecipante del domain DDS é sotto il controllo di un attaccante o quando é possibile modificare i file di configurazione delle policy QoS del domain.

Queste vulnerabilità riguardano la versione del DDS 1.4 con le specifiche dello standard OMG.

2.1 Blocco DataReader tramite sequence number

Il vettore di attacco si trova nel messages module del protocollo RTPS descritto nella sottosezione 1.5.3. Questo modulo si occupa di scambiare messaggi tra i DataReader e i DataWriter all'interno un domain DDS.

Per effettuare questi scambi di messaggi vengono utilizzati dei sottomessaggi, in particolare l'HEARTBEAT e l'ACKNACK. L'HEARTBEAT contiene al suo interno il sequence number che tiene traccia del numero di aggiornamenti di un topic da parte di DataWriter, mentre l'ACKNACK inviato da un DataReader serve per confermare al DataWriter la ricezione di nuovi dati riguardo un topic. Quando il DataReader riceve il sequence number all'interno di un HEARTBEAT può identificare se ci sono o no dei pacchetti mancanti e in caso segnalarli al DataWriter [16]. Inoltre se il parametro

FINAL é attivo in un sottomessaggio HEARTBEAT, il DataReader deve sempre rispondere al DataWriter con ACKNACK dopo aver ricevuto nuovi aggiornamenti. Il DataWriter, nel frattempo, rimarrá in attesa del sottomessaggio ACKNACK prima di inviare nuovi aggiornamenti al DataReader. Questo sistema aiuta il DataReader a rimanere sempre sincronizzato con il DataWriter.

I controlli del sequence number all'interno dell'HEARTBEAT non sono sufficienti per mitigare questo attacco:

- Un primo controllo viene effettuato per verificare che non ci siano valori negativi;
- Un altro controllo serve a determinare se l'ultimo sequence number appena ricevuto ha un valore minore rispetto a quello ricevuto in precedenza [16];

2.1.1 Dettagli attacco

Per sfruttare questa vulnerabilità l'attaccante deve utilizzare qualche strumento per sniffare la comunicazione tra il DataReader e il DataWriter, intercettando i sottomessaggi HEARTBEAT. Dopo aver catturato un HEARTBEAT diretto verso un DataReader e modificato il suo sequence number assegnandogli un valore molto alto, l'attaccante lo rinvia al suo destinatario originario. Una volta ricevuto il sottomessaggio il DataReader si metterà quindi in attesa di un HEARTBEAT con un sequence number superiore a quello appena ricevuto. Di conseguenza il DataReader non elaborerà più i messaggi legittimi mandati dal DataWriter, dato che hanno sequence number più piccoli. Solo un messaggio HEARTBEAT con un sequence number maggiore a quello del DataReader farà ripristinare la sua esecuzione [16].

2.1.2 Conclusioni

Di solito questo tipo di attacco è difficile da identificare. Un messaggio HEARTBEAT riguarda un solo topic, quindi il resto delle comunicazioni che avvengono su topic differenti o anche sullo stesso topic, ma con un DataReader diverso, non subiranno cambiamenti. Questa vulnerabilità può essere mitigata utilizzando l'estensione DDS security in modo tale da crittografare i messaggi e rendere impossibile per l'attaccante effettuare modifiche al sequence number.

2.2 DDoS sfruttando estensione DDS security

Questo vettore di attacco si trova nell'estensione del DDS chiamata DDS security, descritto nella sezione 1.6; in particolare la versione utilizzata é la versione 1.1. Il DDS security si occupa di stabilire una connessione sicura tra i vari dispositivi della rete, utilizzando dei plugin per effettuare: autenticazione, controllo accesso, crittografia, logine e data logging [5].

Ogni partecipante del domain DDS deve essere autenticato reciprocamente dalle altre entità appartenenti allo stesso domain. Successivamente due entità, per iniziare una comunicazione tra di loro, devono prima scambiarsi le chiavi private in modo sicuro tramite protocollo Diffie-Hellman in modo tale da poter crittare i successivi messaggi. Nell'utilizzo di Diffie-Hellman vengono utilizzate le challenge (sottosezione 1.6.1), che corrispondono a valori che variano nel tempo, inseriti durante il calcolo della firma digitale richiesta dal protocollo. Queste challenge vengono utilizzate per rendere le varie sessioni di autenticazione uniche evitando così attacchi di tipo replay [15].

2.2.1 Dettagli attacco

L'attacco DDoS avviene durante la fase di autenticazione del DDS security 1.1, in particolare quando un nuovo dispositivo tenta di collegarsi alla rete e manda una richiesta di autenticazione all'entità con cui vuole aprire una comunicazione. La richiesta del partecipante viene intercettata dall'attaccante che modifica i valori della challenge crittografica all'interno del pacchetto. Modificando ripetutamente questi valori, l'attaccante inizia a inviare molteplici richieste crittografiche alla sua vittima. Il partecipante così comincerà a calcolare le firme digitali per effettuare l'autenticazione, consumando tutte le sue risorse. Dato che, la vittima è probabilmente un dispositivo IoT (Internet of Things) che non dispone di una potenza di calcolo molto elevata, si ritroverà occupata per tutto il tempo necessario a calcolare diverse firme digitali ricevute dall'attaccante, bloccando così il suo funzionamento [15].

2.2.2 Conclusioni

Questo attacco è stato scoperto con Proverif, un tool che viene usato per individuare vulnerabilità nei protocolli crittografici. È stato utilizzato in molti studi, come ad

esempio nell'analisi della posta elettronica certificata e nell'analisi del TLS 1.3 [1].

Una raccomandazione per mitigare questo attacco é quello di cambiare delle policy QoS impostando un tempo limite massimo per effettuare l'autenticazione. Queste policy possono fare in modo che i partecipanti non si trovino sopraffatti dalle troppe richieste di autenticazione. Un allarme potrebbe essere utile per identificare possibili tentativi DDoS di questo tipo, allertando così un amministratore [15].

2.3 Enumeration sniff

Prendendo in considerazione, il protocollo RTPS, descritto nella sottosezione 1.5.4, e il suo modulo discovery, possiamo notare che di default i messaggi sono molto "verbose", scambiando le informazioni in chiaro durante le comunicazioni tra i vari partecipanti [16]. Il modulo discovery del protocollo RTPS a sua volta si suddivide in altri 2 protocolli, che sono necessari per le specifiche DDS:

- Simple Participant Discovery Protocol (SPDP).
- Simple Endpoint Discovery Protocol (SEDP).

2.3.1 Dettagli attacco

Per questo attacco ci focalizzeremo in particolare sull'SPDP che serve ad individuare la presenza dei partecipanti al resto delle entità nel domain. In particolar modo il funzionamento si basa su un messaggi di tipo multicast che vengono mandati a tutti i dispositivi riguardo ai partecipanti attivi [6].

L'attaccante sniffando questi messaggi (all'interno di un domain DDS) di tipo multicast RTPS-SPDP, utilizzando anche un semplice script python, infatti potrà vedere il loro contenuto in maniera chiara.

All'interno di un pacchetto di questo tipo possiamo trovare: l'indirizzo ip dell'host, il prefisso GUID dell'RTPS, la versione dell RTPS, l'ID del venditore, informazioni riguardanti la sincronizzazione ed infine il contenuto dei sottomessaggi [16].

2.3.2 Conclusioni

Prendere informazioni DDS senza effettuare veri e propri attacchi di tipo attivo può essere molto utile per un attaccante che ha il compito di penetrare in modo attivo una rete DDS. In molti casi tutto quello che deve fare l'attaccante è osservare i messaggi che vengono scambiati all'interno del network. Successivamente quando si ottengono informazioni a sufficienza sarà più facile per l'attaccante trovare altre vulnerabilità [16].

Di solito questo tipo di attacco è difficile da identificare e possono essere effettuati senza lasciare tracce di nessun tipo, dato che l'attaccante non manda pacchetti. Una soluzione potrebbe essere usare l'estensione DDS security o eseguire la connessione tra i nodi tramite un tunnel con WireGuard per crittare le comunicazioni.

2.4 Modifica maligna di OWNERSHIP strength

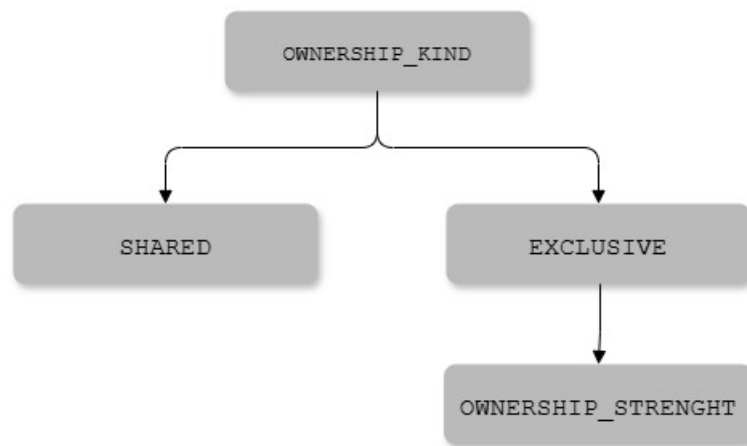


Figura 2.1: Illustrazione policy QoS del DDS

Questo attacco è realizzabile solo se certe policy QoS vengono modificate durante l'esecuzione della rete, specialmente il parametro `OWNERSHIP-KIND` che gestisce quanti `DataWriter` possono scrivere per un determinato topic. Una descrizione accurata di altre policy QoS viene effettuata nella sottosezione 1.4. Questo parametro può essere impostato in due modi diversi:

- **SHARED**: in questo modo più di un DataWriter possono aggiornare le informazioni di un topic.
- **EXCLUSIVE**: solo un DataWriter può aggiornare le informazioni di un topic. Il DataWriter che ha il permesso di scrittura per il topic è quello che dispone di un OWNERSHIP-strength con valore più alto.

In una rete dove si utilizza un OWNERSHIP-kind di tipo EXCLUSIVE è consente all'attaccante di utilizzare l'OWNERSHIP-strength a suo favore. Infatti è possibile far ricevere informazioni a un DataWriter in maniera errata, dato che quest'ultimo non riceverà più informazioni da una fonte affidabile [3].

2.4.1 Dettagli attacco

L'attaccante, con un DataWriter in suo possesso all'interno di una rete DDS, può sfruttare il fatto che il topic preso di mira può essere aggiornato solo dal DataWriter con l'OWNERSHIP-strength più alta. Per effettuare questo attacco, tutto quello che serve, è essere a conoscenza del topic che si vuole modificare, le policy QoS in uso e il valore dell OWNERSHIP-strength. L'ultimo passo è quello di impostare la policy QoS nel DataWriter dell'attaccante con OWNERSHIP-strength superiore a quello utilizzato dal DataWriter originario. Ora i DataReader che sono iscritti al topic bersaglio ricevono le informazioni dal DataWriter dell'attaccante [3].

2.4.2 Conclusioni

Questa vulnerabilità è stata analizzata con l'ausilio di RTI Shapes Demo, un software che emula una rete DDS corrispondente alle specifiche dello standard OMG, sviluppato da Real-Time Innovations (RTI).

L'OWNERSHIP-kind di tipo EXCLUSIVE è utilizzata in contesti dove le informazioni ricevute dal DataReader devono essere accurate dato che un singolo DataWriter (in molti casi si tratta di un sensore) può mandare nuovi aggiornamenti del topic. Se l'attaccante, dovesse riuscire a modificare i valori del topic con questo attacco, potrebbe causare molti danni, specialmente se il DataWriter dell'attaccante riesce a mandare degli aggiornamenti al topic senza essere scoperto [3].

Una soluzione utile per mitigare questo attacco potrebbe essere l'utilizzo dell'estensione DDS security. Utilizzando i plugin relativi al controllo accesso, come illustrato nella sottosezione 1.6.2, permette di evitare che un attaccante possa modificare le policy QoS come l'OWNERSHIP-strength.

2.5 Modifica maligna di LIFESPAN QoS

Un'altra policy QoS che può essere usata come vettore di attacco è quella che regola il parametro LIFESPAN. Questa regola corrisponde al tempo limite massimo di validità per la lettura di pacchetti da parte di un DataReader. Per determinare se un pacchetto di un determinato topic è scaduto viene utilizzato il timestamp di creazione aggiungendo il LIFESPAN impostato; se questo risultato chiamato expiration time risulta superiore all'orario durante la ricezione del DataReader, allora il pacchetto ricevuto è ancora valido. Per funzionare gli orologi interni del DataWriter e del DataReader devono essere sincronizzati tra di loro.

Un'altra policy da considerare è quella riguardo all'affidabilità (RELIABILITY) dei dati riguardanti un topic che può essere impostata in due modi:

- **RELIABLE**: questa impostazione costringe il DataReader a farsi ritrasmettere dal DataWriter i pacchetti mancanti o ricevuti in maniera errata. In questo modo le informazioni del DataReader saranno sempre corrette anche se non sempre saranno aggiornate in tempo reale.
- **BEST-EFFORT**: l'impostazione predefinita non consente il recupero dei pacchetti mancanti o corrotti del DataReader, quindi, quest'ultimo potrebbe anche perdere dei pacchetti che gli sono stati inviati [4].

Se il LIFESPAN dei pacchetti, contenenti i dati del topic, viene impostato con valori molto piccoli, si verificheranno problemi di comunicazione tra DataWriter e DataReader, dato che non sarà possibile effettuare la lettura di certi pacchetti inviati. Impostando il valore RELIABLE tra le policy QoS con RELIABILITY é possibile mitigare solo parzialmente questa vulnerabilità [3].

2.5.1 Dettagli attacco

Avendo sotto controllo i parametri LIFESPAN e RELIABLE, l'attaccante modificherà le policy dei DataWriter in modo tale da avere il LIFESPAN molto piccolo. Così facendo, i pacchetti spediti dal publisher arriveranno già scaduti al DataReader, rendendoli inutilizzabili. In certi casi il pacchetto che deve essere inviato viene distrutto dallo stesso DataWriter all'interno della sua coda prima dell'invio. Questa vulnerabilità è stata verificata impostando il valore di LIFESPAN $< 80\text{ms}$ dove si è visto che nessun pacchetto raggiunge il DataReader. Se si aumenta il valore tra gli 80ms e i 100ms già si può notare che dei pacchetti vengono letti con successo dal DataReader, mentre altri vengono eliminati prima della lettura. Infine impostando un valore LIFESPAN $\geq 120\text{ms}$ si può notare che la comunicazione tra publisher e subscriber avviene senza nessun problema.

Un dettaglio da aggiungere è che se si imposta la policy dell'affidabilità (RELIABILITY) con valore RELIABLE, i millisecondi necessari del LIFESPAN per compromettere le comunicazioni tra DataReader e DataWriter devono essere moltiplicati per un fattore di 0.01. Quindi, ad esempio se si ottiene un completo annullamento delle comunicazioni con un LIFESPAN $< 80\text{ms}$ utilizzando il la RELIABILITY di tipo BEST-EFFORT, per ottenere lo stesso risultato con RELIABILITY di tipo RELIABLE dobbiamo impostare un LIFESPAN $< 0.8\text{ms}$ [3].

2.5.2 Conclusioni

Anche questo test è stato dimostrato con RTI Shapes Demo che implementa una soluzione DDS di RTI corrispondente alle specifiche dello standard OMG. Inizialmente molte reti DDS hanno impostato la RELIABILITY di tipo BEST-EFFORT che è l'impostazione predefinita, in modo tale da rendere possibili comunicazioni di tipo realtime. Quindi nella maggior parte dei casi l'attaccante non si deve preoccupare di modificare questo parametro.

Una possibile soluzione consiste nell'implementare qualche tipo di controllo in modo tale da avvertire un operatore umano se molti pacchetti vengono scartati perché arrivati con un LIFESPAN scaduto. Questo controllo potrebbe essere anche utile, nel caso in cui il DataWriter e il DataReader si trovassero distanti fisicamente tra di loro, per verificare la qualità del collegamento [3].

| Tipo di attacco | Vettore attacco | Protoc./ Estens. | Bersaglio nella rete | Software | Soluzione |
|------------------------|---------------------------|------------------------------------|----------------------|----------------|--------------------------------------|
| Discovery devices [16] | Verbose nature of RTPS | RTPS-SDPD | Tutti i partecipanti | Sniffer python | DDS security/ WireGuard |
| DDos [16] | Heartbeat sequence number | RTPS | DataReader | Sniffer python | DDS security: Auth Control |
| DDoS [15] | Authentication challenge | DDS security 1.1 Discovery protoc. | Tutti i partecipanti | Proverif | Scadenza richieste di autenticazione |
| QoS policy [3] | Policy: Ownership | RTPS | DataReader | RTI shapes | DDS security: Access Control |
| QoS policy [3] | Policy: Lifespan | RTPS | DataReader | RTI shapes | Controllo per Lifespan scartati |

Tabella 2.1: Riassunto delle vulnerabilità del DDS analizzate.

Bibliografia

- [1] Bruno Blanchet, Ben Smyth, Vincent Cheval, and Marc Sylvestre. *ProVerif 2.05: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial*, 2023. URL <https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf>. [Accesso: 2 febbraio 2025].
- [2] Michael James Michaud, Thomas R. Dean, and Sylvain P. Leblanc. MALICIOUS USE OF OMG DATA DISTRIBUTION SERVICE (DDS) IN REAL-TIME MISSION CRITICAL DISTRIBUTED SYSTEMS, April 2017. URL <https://espace.rmc-cmr.ca/jspui/handle/11264/1241>. [Online; accessed 11. Feb. 2025].
- [3] Michael James Michaud, Thomas R. Dean, and Sylvain P. Leblanc. Attacking OMG data distribution service (DDS) based real-time mission critical distributed systems. In *13th International Conference on Malicious and Unwanted Software, MALWARE 2018, Nantucket, MA, USA, October 22-24, 2018*, pages 68–77. IEEE, 2018. doi: 10.1109/MALWARE.2018.8659368. URL <https://doi.org/10.1109/MALWARE.2018.8659368>.
- [4] Object Management Group. OMG Data Distribution Service, April 2015. URL <http://www.omg.org/spec/DDS/1.4/PDF>. [Accesso: 2 febbraio 2025].
- [5] Object Management Group. DDS Security, July 2018. URL <https://www.omg.org/spec/DDS-SECURITY/1.1/PDF>. [Accesso: 2 febbraio 2025].
- [6] Object Management Group. About the DDS Interoperability Wire Protocol Specification Version 2.5, February 2025. URL <https://www.omg.org/spec/DDSI-RTPS/2.5/About-DDSI-RTPS>. [Online; accessed 12. Feb. 2025].

- [7] Sangyoon Oh, Jai-Hoon Kim, and Geoffrey Fox. Real-time performance analysis for publish/subscribe systems. *Future Generation Computer Systems*, 26 (3):318–323, 2010. ISSN 0167-739X. doi: <https://doi.org/10.1016/j.future.2009.09.001>. URL <https://www.sciencedirect.com/science/article/pii/S0167739X09001344>.
- [8] OMG. Topic [DDS Foundation Wiki], February 2025. URL https://www.omgwiki.org/ddsfdoku.php?id=ddsfp:public:guidebook:06_append:glossary:t:topic. [Online; accessed 5. Feb. 2025].
- [9] OMG. What is DDS?, February 2025. URL <https://www.dds-foundation.org/what-is-dds-3>. [Online; accessed 6. Feb. 2025].
- [10] J.J. Rengers. Dds in a zero trust cloud native environment in the naval domain, November 2022. URL <http://essay.utwente.nl/93639/>.
- [11] RTI. Instance | data distribution service (dds) community rti connext users, February 2025. URL <https://community.rti.com/glossary/instance>. [Online; accessed 2025-02-05].
- [12] RTI. DomainParticipant | Data Distribution Service (DDS) Community RTI Connex Users, February 2025. URL <https://community.rti.com/glossary-term/domainparticipant>. [Online; accessed 6. Feb. 2025].
- [13] RTI. Domain | Data Distribution Service (DDS) Community RTI Connex Users, February 2025. URL <https://community.rti.com/glossary/domain>. [Online; accessed 6. Feb. 2025].
- [14] J.M. Schlesselman, G. Pardo-Castellote, and B. Farabaugh. Omg data-distribution service (dds): architectural update. In *IEEE MILCOM 2004. Military Communications Conference, 2004.*, volume 2, pages 961–967 Vol. 2, 2004. doi: 10.1109/MILCOM.2004.1494965.
- [15] Bingham Wang, Hui Li, and Jingjing Guan. A formal analysis of data distribution service security. In Jianying Zhou, Tony Q. S. Quek, Debin Gao,

- and Alvaro A. Cárdenas, editors, *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2024, Singapore, July 1-5, 2024*. ACM, 2024. doi: 10.1145/3634737.3656288. URL <https://doi.org/10.1145/3634737.3656288>.
- [16] Thomas White, Michael N. Johnstone, and Matthew Peacock. An investigation into some security issues in the dds messaging protocol, 2017. URL <https://api.semanticscholar.org/CorpusID:52840449>.
- [17] He Yuefeng. Study on data transmission of dcps publish-subscribe model. In *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pages 1–2172, May 2018. doi: 10.1109/IMCEC.2018.8469351.

Ringraziamenti

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrum exercitationem ullamco laboriosam, nisi ut aliquid ex ea commodi consequatur. Duis aute irure reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint obcaecat cupiditat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum

Caio