Analisi della sicurezza del middleware Data Distribution Service

RELATORE

PROF. FRANCESCO SANTINI

LAUREANDO

FEDERICO RANOCCHIA

Implementazioni dello standard DDS

Le software house impiegano lo standard DDS

Utilizzato in vari campi:

- Sistemi di controllo industriali (ROS)
- Difesa/Militare
- Veicoli autonomi

Connext DDS (Closed source)

Fast DDS (Apache License 2.0)

Robot Operating System (BSD License)

- Introduzione del DDS
- L’estensione DDS Security
- Vulnerabilità OMG
- Vulnerabilità implementazione
- Software analisi: DDSFuzz

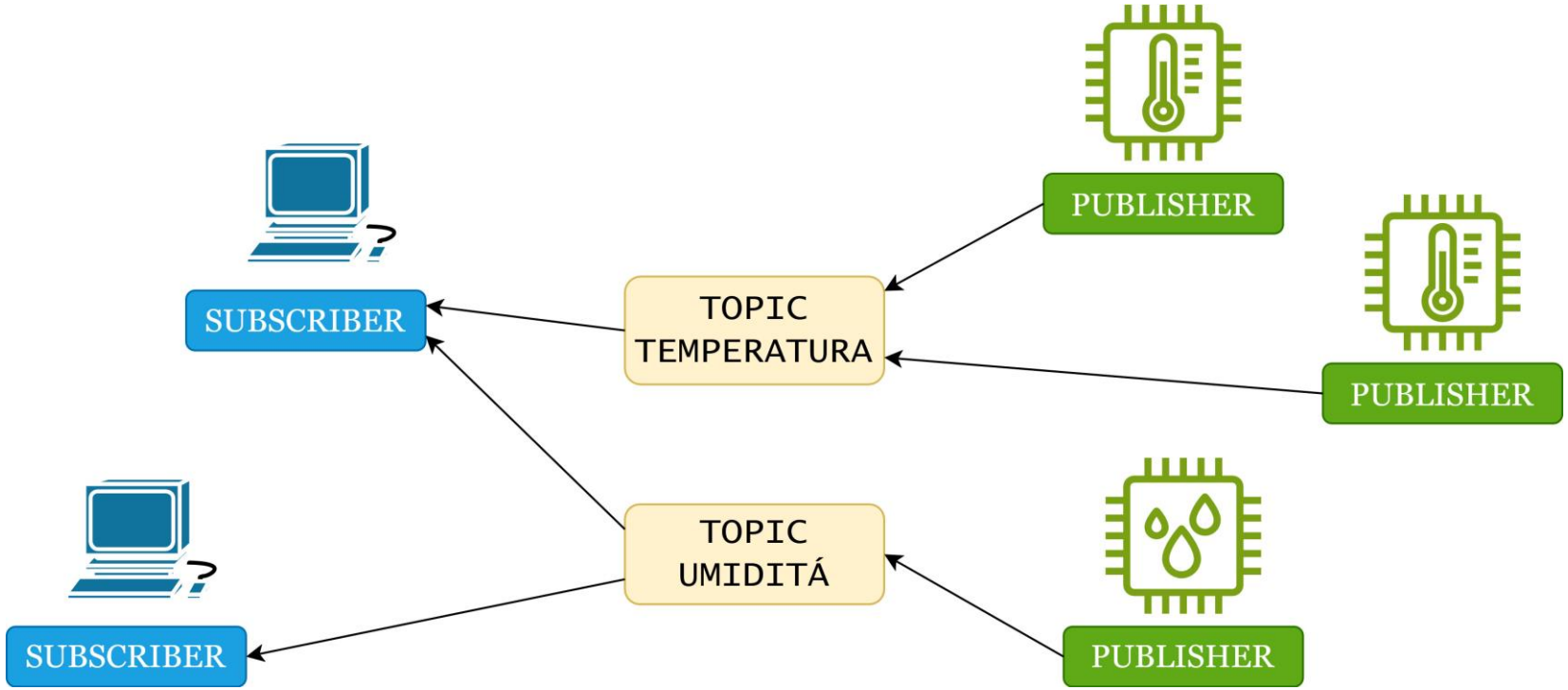
Indice argomenti

Modello Publish/Subscribe

TOPIC: rappresenta una tipologia di dati

PUBLISHER: colui che pubblica nuovi dati

SUBSCRIBER: colui che si iscrive ai topic del publisher



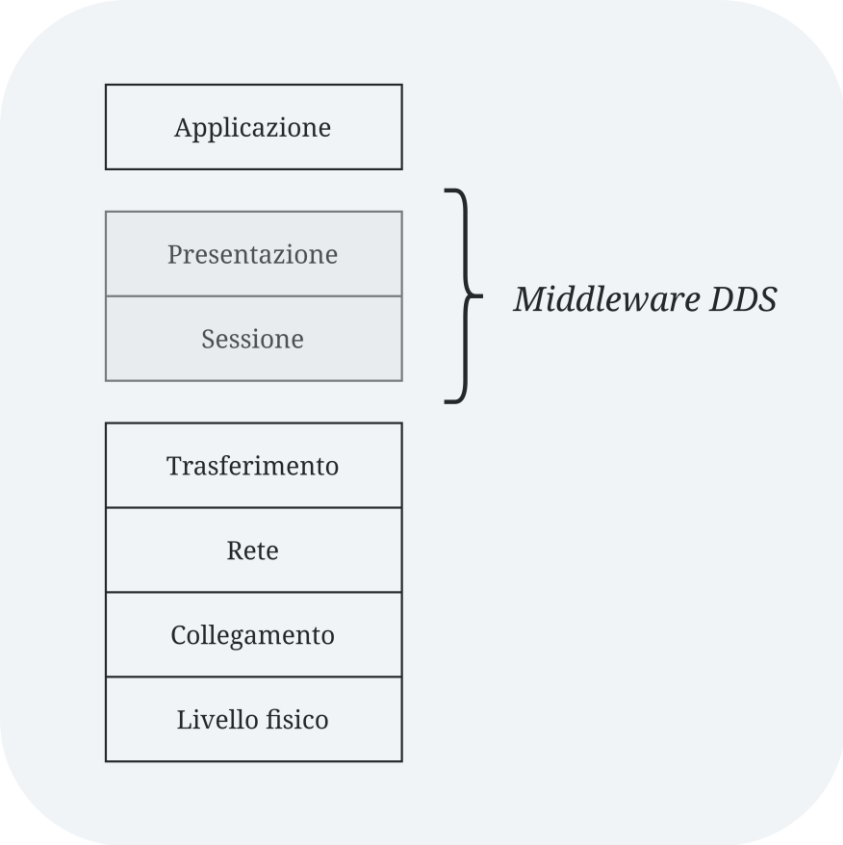
Che cos’è il Data Distribution Service

Il DDS gestito da OMG é:

- Un MIDDLEWARE
- Uno standard per le API
- Un modello DATA-CENTRIC

Presenta i seguenti vantaggi

- Compatibile in contesti real-time
- Sistema di AUTOSCOPERTA
- Ampia gestione delle politiche QoS



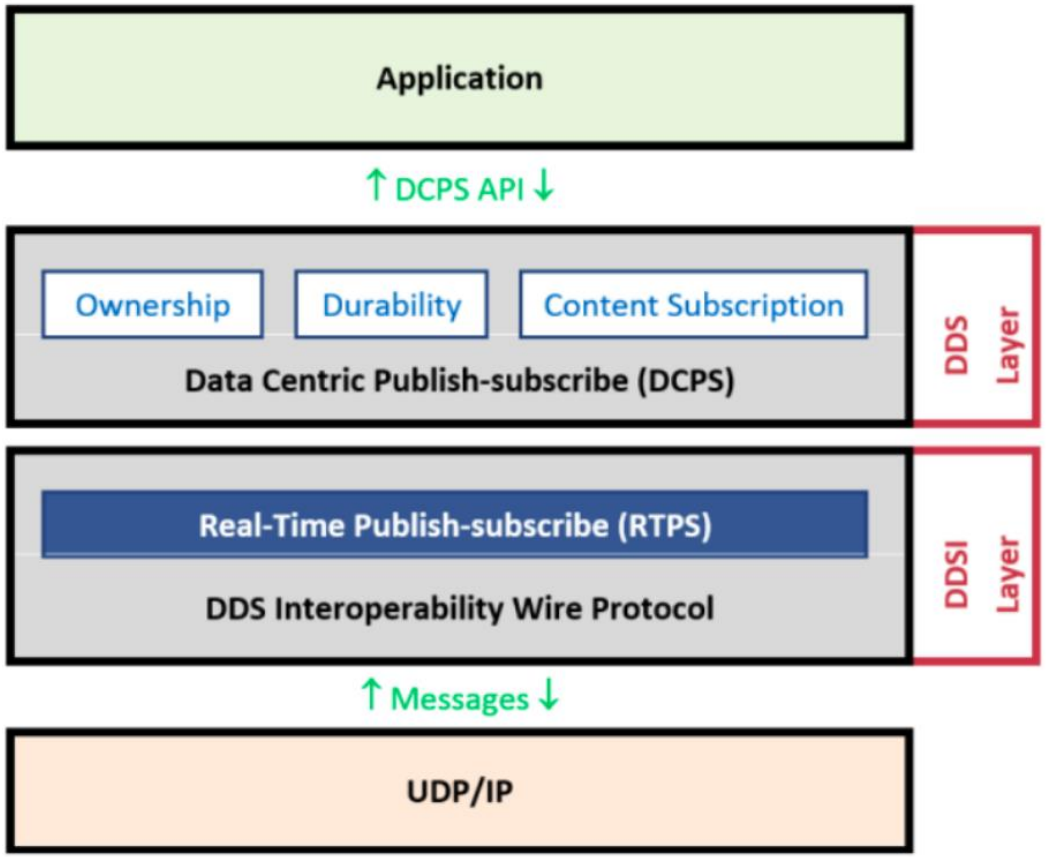
Struttura Data Distribution Service

DDS (Data Distribution Service)

- Modello di comunicazione publish/subscribe, contiene il DCPS
- Definisce le policy QoS

DDSI (DDS Interoperability)

- Include RTPS
  - Gestito da OMG, consente l'autoscoperta
  - Definisce FORMATO e REGOLE messaggi
  - Si appoggia all'UDP/IP o TCP/IP
- Interoperabilità tra diverse implementazioni



DDS Security

VANTAGGI

Standard O.M.G. per mitigare vettori d'attacco

Protegge lettura/scrittura dei messaggi DDS

Composto da 5 plugin, tra cui

- Authentication Service Plugin
- Access Control Service Plugin

SVANTAGGI

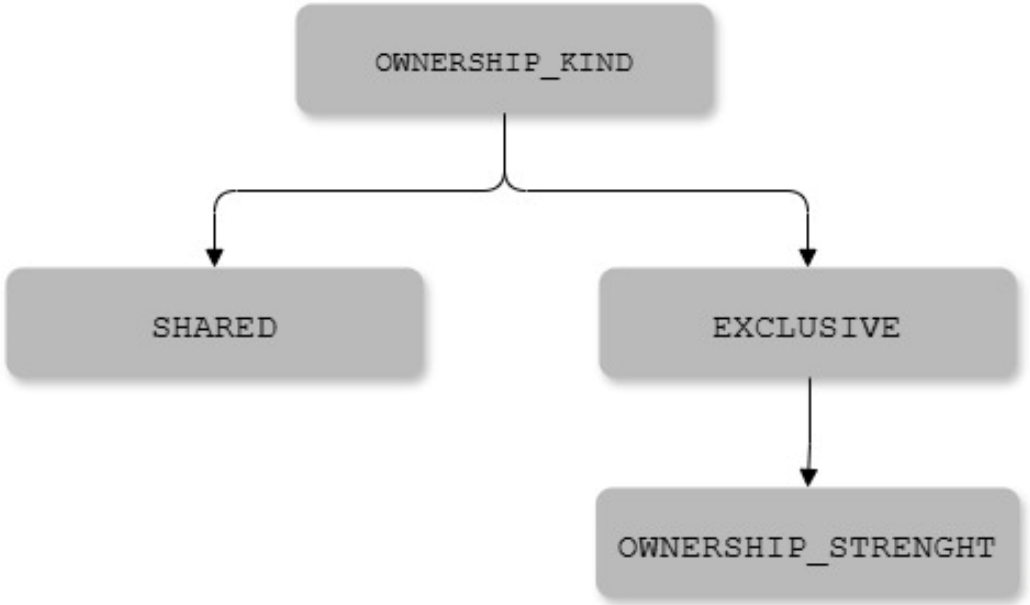
Implementazione complessa e dispendiosa

La sicurezza è pari a quella del partecipante più vulnerabile

Richiede più potenza di calcolo

Modifica policy OWNERSHIP_STRENGTH

- Policy QoS OWNERSHIP_KIND = EXCLUSIVE
- Solo il Publisher con OWNERSHIP_STRENGTH più alta può scrivere su un topic
- L'attaccante imposta il suo Publisher con un valore di OWNERSHIP_STRENGTH superiore
- I Subscriber iniziano a ricevere dati dall'attaccante invece che dalla fonte legittima



Vulnerabilità implementazioni DDS

Vulnerabilità in PID_BUILTIN_ENDPOINT_QOS

Mancato controllo lunghezza parameterLength

Colpisce solo Fast DDS

- Lettura fuori dai limiti
- Potenziale esecuzione codice malevolo

```
PID_BUILTIN_ENDPOINT_QOS(
                    parameterId=119,
                    parameterLength=0,
                    parameterData=b"\x00\x00\x00\x00",
                ),
```

DDSFuzz

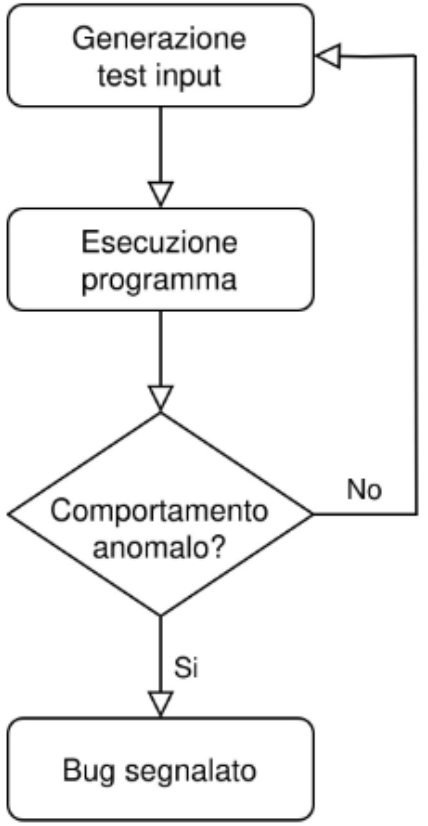
Fuzzer specifico per DDS

- Topologia dinamica
- QoS policies
- DDS security

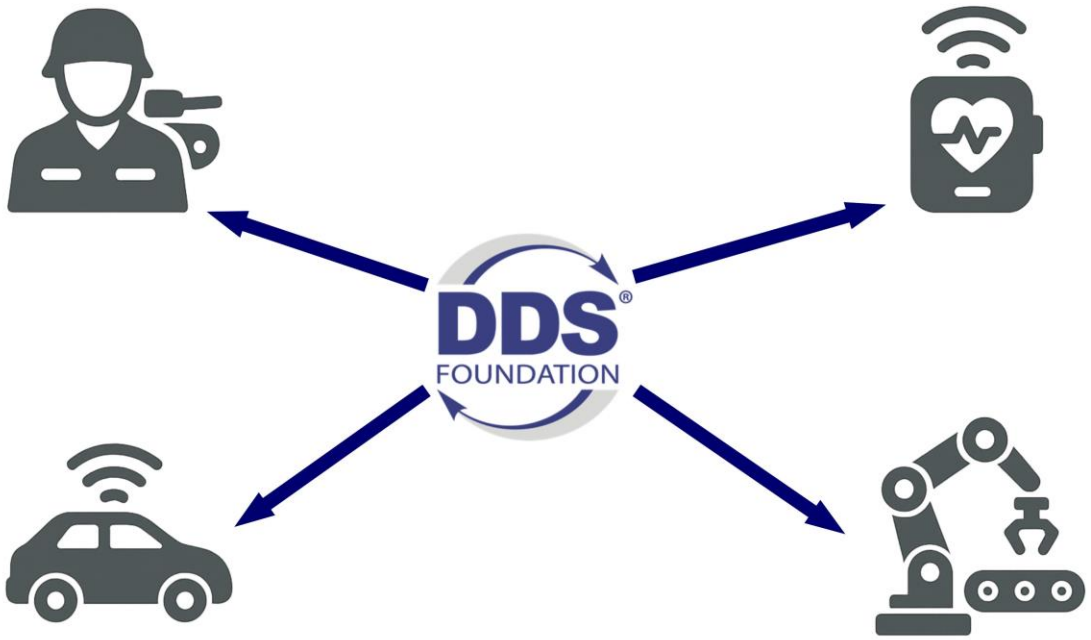
Esecuzione parallela: Fast DDS, Cyclone DDS, OpenDDS

Tipologie bug rilevati

- Tradizionali: es. buffer overflow
- Semantici: violazioni standard DDS (es. bypass autenticazione)



- Vulnerabile senza le dovute precauzioni
- Pochi strumenti dedicati
- La sicurezza molte volte non viene considerata
- Serve più ricerca e testing



Conclusioni

Ci sono domande?