Università di Perugia

Dipartimento di Matematica e Informatica

Tesi triennale/magistrale in ...

Titolo Tesi

Advisor

Prof. Tizio

Candidate

Caio

Academic Year 2018-2019

Quì la dedica...

Indice

Capitolo 1

Introduction

In questo capitolo ci occuperemo di analizzare e comprendere delle vulnerabilità del protocollo DDS standard OMG (Object Managment Group). In particolare verrà analizzato il vettore d'attacco, il protocollo utilizzato, il bersaglio dell'attacco e infine verrà proposta una soluzione applicabile per mitigare possibili attacchi non autorizzati. Successivamente grazie all'aiuto di un software riusciremo a capire come queste vulnerabilità possono influire sul funziomanto degli –host– collegati alla rete DDS.

1.1 Attacchi di tipo DDoS

Questo attacco consiste nel sovraccaricare un dispositivo collegato alla rete DDS in modo tale da renderlo inutilizzabile. Infatti dato che i dispositivi collegati sono di –tipo I O T – la potenza di calcolo nella maggior parte dei casi sarà molto ridotta. Inoltre in molti casi ci possiamo ritrovare ad utilizzare dispositivi che non possono permettersi –delay– nell'analisi di certi dati, specialmente in ambiti dove bisogna avere una risposta sempre rapida e disponibile, come ad esempio nel campo della medicina e nel campo militare.

1.1.1 DDoS blocco ricezione da parte del data-reader Foglio 2

Citazioni da foglio 2 a gogo Il vettore di attacco si trova nell'implementazione del DDS chiamata DDSI-RTPS che si occupa di scambiare messaggi tra i data-reader (coloro che si iscrivono ai vari ai vari topic) e i data-subscribers (di solito sono sen-

sori che mandano dati). Per comunicare questi dispositivi utilizzano il protocollo RTPS. Questo protocollo utilizza il messaggio HEARTBEAT che viene mandato da un data-writer a un data-reader per specificare il sequence number nel data-writer. All'interno del messaggio HEARTBEAT troviamo il sequence number che serve al data-reader per sincronizzarsi con il data-writer durante la ricezione dei messaggi. Infatti il data-reader quando riceve il sequence number all'interno di un HEARTBEAT può identificare se ci sono dei pacchetti mancanti e segnalarli al data-writer.

Un data-writer inoltre può richiedere un messaggio ACKNACK da un data-reader se nel messaggio HEARTBEAT inviato dal data-writer viene specificata la flag FINAL. In casi in cui bisogna essere certi che il data-reader riceve tutti i dati del data-writer, quest'ultimo manda un HEARTBEAT con la flag FINAL impostata, al data-reader che successivamente deve rispondere necessariamente con un messaggio ACKNACK per confermare la ricezione nel messaggio HEARTBEAT. I controlli HEARTBEAT effettuati dal data-reader, infatti non sono sufficienti a coprire questo tipo di attacco dato che quest'ultimo:

- esegue un check per verificare che non vi siano numeri negativi
- controlla che l'ultimo sequence number arrivato non ha un valore più alto del sequence number ricevuto in precedenza

Dettagli attacco

Per sfruttare questa vulnerabilità l'attaccante deve utilizzare qualche strumento per sniffare la comunicazione tra data-reader e data-writer e intercettare un messaggio di tipo HEARTBEAT. Successivamente l'attaccante modifica il valore del sequence number del messaggio HEARTBEAT. Il messaggio poi viene mandato verso il data-writer così facendolo rimanere in attesa di un messaggio HEARTBEAT con Un sequence number superiore a quello appena ricevuto. Facendo così il data-reader non legge più i messaggi mandati dal data-writer e bloccando il così il funziomanto del data-reader finchè il sequence number non sarà superiore a quello ricevuto dall'attaccante.

Questa è una sottosottosezione

La teoria dell'attacco ci dice che se

Tipo di attacco	Vettore attacco	Protoc./ Estens.	Bersaglio nella rete	Software	Soluzione
Discovery devices[2]	Verbose nature of RTPS	DDSI-RTPS	Tutti i partecipanti	Sniffer python	-
DDos[2]	Heartbeat sequence number	DDSI-RTPS	Data-reader	Sniffer python	-
DDoS[3]	Authentication challenge	DDS security 1.1 Discovery protoc.	Tutti i partecipanti	Proverif	Scandenza richieste di autenticazione

Tabella 1.1: La versione DDS in tutti i casi è la 1.4

Capitolo 2

Background

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt 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

2.1 Sezione

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt 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

2.1.1 Sottosezione

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt 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

Citazione[1]

- 1
- 2

Figura 2.1: didascalia figura.

Riferimento immagine (o tabella... o sezione...) 2.1

$$\pi_i(v) = \sum \frac{x_{S_i}}{\mathrm{N}} \tag{2.1}$$

Bibliografia

[1] Edsger W. Dijkstra. A bagatelle on euclid's algorithm. In Manfred Broy, editor, *Proceedings of the NATO Advanced Study Institute on Deductive Program Design, Marktoberdorf, Germany*, pages 21–23, 1996. ISBN 3-540-60947-4.

Ringraziamenti

Lorem ipsum dolor sit amet, consectetur adipisci elit, sed do eiusmod tempor incidunt 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