Building Scalable Security for Autonomous Systems and Operational Infrastructures

Abstract — This paper will review how scalable and high-performance distributed systems can integrate security by using the Data Distribution Service (DDS) standard and its DDS Security extension. It will outline the security threats to systems of this type and how DDS Security can be used to mitigate those threats through the use of fine-grain, scalable and high-performance security.

1 Introduction

Securing a real-time system without dramatically affecting the overall performance is not an easy task. In general, the best approach is to only secure the data that needs to be secured, i.e. use a fine-grain solution.

One approach to fine-grain security focuses on the semantic interfaces between systems and components. This includes not only the entities but also the context and explicit definitions of the system's observable and measurable phenomena. Some communication frameworks, such as DDS, already provide these semantic interfaces by modelling the data and their interactions using Quality of Services (QoS) properties. In such a framework, including fine-grain security provides a significant advantage over the scalability and performance constraints of other approaches.

2 An Overview of DDS

DDS is an open standard managed by the Object Management Group® (OMG®) that defines a connectivity framework that is scalable, high performance, and highly reliable. DDS is used in military and other mission-critical environments to efficiently distribute data between real-time applications within a distributed system.

It implements a publish-subscribe architecture at its core and expands to add data-centric behaviours to enable intelligent management of data. This data-centric approach simplifies connectivity management and, in so doing, provides significant benefits such as improved scalability, easier reuse of functional blocks between platforms and a reduced development cycle.

2.1 Where is DDS used?

DDS is widely used in large distributed systems where applications are required to share large amounts of data in a fast, secure, scalable and reliable manner, such as autonomous cars, robotics, and medical devices. DDS is also extensively used in Aerospace and Defence.

As an open standard, DDS finds a place in many UK MOD and US DoD projects since it promotes vendor neutrality and a path to the future. The success of DDS in areas like the UK MOD's General Vehicle Architecture (GVA) is due to its high performance and resilience as well as its vendor neutral scalability, configurability, and modularity [1].

3 Security Threats on Distributed Systems

Many technologies used in distributed systems tend to secure the entire communication channel. That approach, however, has two main disadvantages.

First, it secures all data on the channel with the same level of security even when it may be more appropriate to apply lower levels of security to specific parts of the data. For example, in the case of a video stream it may be sufficient to simply sign (authenticate) data headers to indicate that the source is trusted.

The second issue with securing the communication channel itself is that anybody that circumvents the security at that level (for example, through a compromised device) could gain access to all the information carried on that channel. For this reason, it is often desirable to secure classified information with an additional level of security at the topic level.

For these reasons, securing a DDS system does not focus on securing everything, but instead provides a way to control who has access to the data space (domain), what they can do there (i.e. read and/or write) and on which information (i.e. on which specific Topics) [2].

The main threats within a distributed DDS based system can be characterised as:

1. Unauthorized subscription
2. Unauthorized publication
3. Tampering and replay
4. Unauthorized access to data (by infrastructure services)

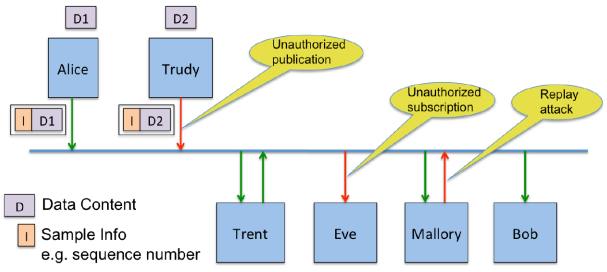

Fig. 1. Security threats in DDS Systems [2]

3.1 Performance Considerations

Securing the whole communication channel or securing every individual message will adversely affect performance due to, for example, an increase in CPU load, leading to higher battery consumption, and increased data transfer latency. If we could control how data is secured in a detailed manner, we could decide that information coming at high rate from sensors just needs to have the metadata (containing who produced the data) signed, and a CRC check that the data is not corrupt. Or, for instance, we could make sure that the data is only sent to nodes that would be needing them, avoiding spending unnecessary resources on processing data that we will discard.

4 Security for Scalable Systems

A new security specification is included in the DDS standard that provides this fine-grain approach by defining a data-centric solution which separates security from the infrastructure (boundary and transport) and attaches it directly to the data. This is done with a decentralized approach key for autonomous systems. DDS Security is the first peer-to-peer, decoupled, multicast-capable solution; it is data aware and completely configurable.

4.1 Fine-Grain Security Solution

DDS Security controls different aspects of data security:

- Authentication - identities are checked and validated as part of the process to access a domain
- Access control - applications must have specific read and write permissions per data type
- Confidentiality - data and metadata can be encrypted
- Integrity - data samples include destination-specific signatures
- Non-repudiation - each data source/sink of data can specify acknowledge and acceptance criteria
- Availability - per-data action rules are defined for behaviour management, fault monitoring and failure.

By controlling those different aspects, we can detect, for instance, that the information is coming from a known application, that it is allowed to publish those data and that the confidential information will not be read by unauthorized applications.

4.2 Configurable security levels

DDS Security is designed as a plugin-in that is highly configurable, allowing the application of different security levels to different topics within the same network packet. For instance, we could decide to only encrypt the application data, whilst leaving the metadata unencrypted. This improves the performance when processing the data. Alternatively, we could apply different keys or even different algorithms to each of the topics, providing a more secure solution.

As we can see in the following figure, signing the metadata information (RTPS) has minimal effect on throughput while applying higher levels of security (e.g. encryption) has a slightly more noticeable effect.

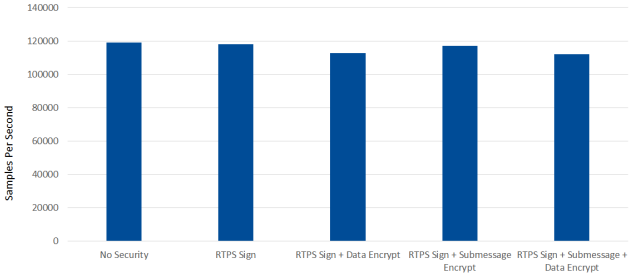

Fig. 2. Throughput results when using fine-grain security for samples of 1KB obtained in our performance lab. [3]

5 Conclusions

Data Distribution Service (DDS) enables scalable distributed systems to be interconnected reliably and with high-performance. With the more recent addition of DDS Security it also allows for fine-grain control of DDS data in a highly configurable and efficient way.

References

[1] UK MoD: “General Vehicle Architecture (GVA)”, Defense Standard 23-09 (2010)
[2] OMG: “DDS Security Specification, Version 1.1” (2018)
[3] RTI: Connext DDS Secure Performance Benchmarks (2017)

Author/Speaker Biographies

Sara Granados Cabeza, Lead Field Application Engineer, Real-Time Innovations (RTI)
Sara has over 10 years of experience in development and customer-facing roles. She graduated with a MS degree in Computer Engineering and obtained her PhD in Computer and Networking Engineering (Cum Laude) in 2012, from the University of Granada.

Paul Tingey, Senior Field Application Engineer, Real-Time Innovations (RTI)
Paul has over 20 years of experience with Embedded hardware and software products in the Networking and Aerospace & Defence markets. Prior to his work as a Field Application Engineer, Paul developed and implemented IoT solutions for customers including major networking corporations.