To appear in: 37th Annual Conference of the German Society for Computer Science (GI 2007). Bremen, Germany, September 24–28, 2007

Agent-Based Container Security Systems An Interdisciplinary Perspective

S. Werner[1], A. Schuldt[1], and K. Daschkovska[2]

[1]Centre for Computing Technologies (TZI)
University of Bremen, Am Fallturm 1, D-28359 Bremen

[2]Bremen Institute of Industrial Technology and Applied Work Science (BIBA)
University of Bremen, Hochschulring 20, D-28359 Bremen

Abstract: Container security systems including electronic seals play an important role in securing container logistics. Nevertheless, a lack of standards prevents devices by different vendors from effective interoperability. Hence, this paper proposes an interdisciplinary perspective incorporating the agent paradigm of computer science. In this approach interaction between different autonomous entities is based on standardised communication protocols. In addition, for container security systems a cryptographic concept must be applied in order to secure communication.

1 Introduction

The terrorist attacks of September 11, 2001 led to an increased demand for security in logistic processes. A special focus lies on shipping containers due to their high throughput in the intercontinental transport of packaged goods. An important step towards more secure logistics is to seal containers in order to protect them from thieves but also from terrorists trying to smuggle dangerous goods. Conventionally, this is accomplished by mechanical seals, e. g., numbered bolts. A more sophisticated approach makes use of electronic seals which notice tamper immediately and alert the cargo owner [Hic04]. Additionally, container security systems can also comprise sensors that continuously monitor the interior of the respective container [Sch04].

Containers, and therewith their security systems, are applied all over the world. The environment of each container changes dynamically on the way from its origin to its destination. The demand for flexible interaction with other entities often arises during transport. For instance, consider customs personnel wirelessly requesting security information with hand-held devices. As another example multiple containers from one company might cooperate in their security efforts in order to save their bounded resources. Although a great many vendors of container security solutions exists, their interoperability currently remains an open issue due to a lack of standards [Hic04].

This paper argues in favour of an interdisciplinary perspective, integrating experiences from the agent paradigm of computer science [Wei99]. The main advantage is that soft-

ware agents located on different systems and based on completely different standards can communicate by applying interaction protocols as a standardised interface. The three main criteria for successfully applying multiagent systems in problem solving (natural distributivity, flexible interaction, and dynamic environment) proposed by [Mül97] are obviously satisfied by the container logistics domain.

The remainder of this paper is structured as follows: Section 2 discusses requirements of container security systems. Subsequently, Sect. 3 presents an agent-based approach incorporating encryption and trust concerns. Finally, a conclusion follows in Sect. 4.

2 Container Security Systems

The general purpose of seals is to secure the content of containers. Conventional seals generally comprise a bolt that mechanically prevents the container from being opened [Fie05]. At the destination it has to be validated that the seal is still intact and that it is still the same [Tir05]. Conventional seals are comparatively cheap and not reusable: if a container is legitimately opened a new seal has to be affixed [Had05] and its unique number [Fie05] has to be recorded. Compared to their low purchase price the handling costs are quite high since the inspection has to be conducted manually and is therefore time consuming [Tir05]. Although mechanical seals increase the effort for tampering with a container their benefit is still limited. As an example, [Had05] argues that criminals can remove the doors of the container completely without damaging the seal, cut a hole into another wall, or create a new seal after having finished. Furthermore, containers are not monitored in real-time.

Electronic seals are intended to overcome some of the limitations of conventional seals. Apart from mechanically locking the container they also exhibit computation and communication abilities. Therefore, it is possible to verify them by a radio-frequency identification (RFID) scan [Tir05]. This feature does not only massively decrease the handling effort, but also enables an almost continuous monitoring as the scanning can be performed easily and often. Thus, the seal can also act as a surrogate for the container number since RFID technology enables a recognition rate of over 99% while optical character recognition systems achieve only about 80% under real-world conditions [Had05]. Despite of their higher purchase price electronic seals might therefore be the better choice regarding their total cost of ownership [Tir05].

Apart from the seal, container security systems can be enhanced by embedded sensors which monitor tampering, theft, and placement of unintentional freight. Examples are door light sensors, gamma ray detectors, as well as chemical sensors [Sch04]. As the applied sensors depend on the concrete purpose, the participating entities must be equipped with the ability to establish ad hoc networks. In this context it has to be ensured that access to the network is restricted to trustworthy entities, e. g., by certification. Otherwise, thieves or terrorists could corrupt the system by injecting manipulated data.

The security system's interface to the outside world is another vulnerable point. As an example, stevedores and truckers are legitimate recipients of some security-related data. Due to restricted resources it might also be an option to join forces with security systems

of neighbouring containers. These forms of communication have also to be restricted to trustworthy partners. As an example, from the perspective of safety it might be desirable for a container to inform the environment about hazardous content. By contrast, this is not the case from a security point of view. It is not advisable to broadcast a container's attractiveness for terrorist attacks to everyone including the terrorists themselves [Had05].

To recapitulate, electronic security systems can significantly improve container security. Since they demand flexible cooperation their interaction with the outside world has to be secured itself. This can be achieved by limiting communication to trustworthy partners.

3 An Agent-Based Approach

In the agent paradigm software agents act on behalf of the (logistic) entities they represent [KT99]: they are assumed to be embodied in an environment, to act autonomously, and to be able to sense changes and react appropriately. Multiple agents are organised within a multiagent system (MAS) which offers essential services to the respective agents [Wei99]. Regarding container security systems a double-layered approach applies (Fig. 1). The first level consists of all entities belonging to a container, e. g., electronic seals and sensors, which jointly form a MAS (the inside view). Here, the main task is to collect data and to monitor whether all values are within admissible ranges. The second level encapsulates all internal components by an additional software agent. This agent is situated within a MAS of all containers and other entities related to container logistics (the outside view). On both levels, standardisation (Sect. 3.1) helps in enabling communication and cooperation of different devices (Sect. 3.2). Section 3.3 addresses trust and encryption which play an important role in this context.

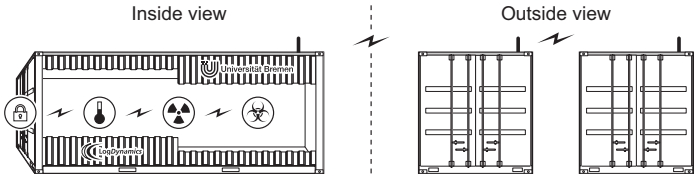

Figure 1: Agents within the container communicate with each other, e. g., the electronic seal as well as different sensors observing the interior (left). Additionally, the agent representing the container as a whole can also exchange messages with other containers (right)

3.1 Foundations

The basis for applying intelligent agents is formed by specifications of the IEEE Foundation for Intelligent Physical Agents (FIPA)[1]. The standards proposed by this group specify essential parts of MAS which, for instance, manage the life cycle of agents. Another

[1] http://www.fipa.org/

part of the system provides a yellow pages service where agents can register the services they provide to other agents. This paper focusses on cooperative agents that support each other in solving the problem of ensuring the security of containers during transport. This, however, requires to reliably exclude competitive agents from the system (see Sect. 3.3).

JADE[2], the Java Agent Development Framework, is an implementation in compliance with FIPA standards [BCG07]. It comes along with LEAP, the Light Extensible Agent Platform, which is a derivative for mobile devices. It focusses on providing a technical infrastructure for enabling the transition of agents to platforms with limited resources. Hence, it is well-suited for an application in container security systems.

3.2 Communication and Cooperation

According to FIPA, communication is conducted with specific interaction protocols. The conversation flow of interaction protocols comprises unique speech acts, which are defined in the Agent Communication Language (ACL). The purpose of such protocols is, for instance, to request actions from other agents, or to coordinate purchasing by auctions. Due to the standardised communication even completely different agents can exchange messages. Hence, this paradigm also forms a promising approach for container security provided that additional security functions are implemented (see Sect. 3.3).

Acting autonomously in container security systems, agents are situated in a resource-bounded environment. This constraint holds for both the inside and outside view of the container. Examples of such restrictions are bounded computational power as well as memory restrictions. The mobility of container security systems also influences the amount of energy available. As a result, these restrictions lead to a need for cooperation of container agents in order to bundle and delegate common tasks. A general approach formalising the cooperation between agents is the model for cooperation [WJ99].

The techniques discussed in this section allow to realise a dynamic and adaptive management of container functions. Applying an ontology ensures that the semantics of conversation contents can unambiguously be deduced by all communication partners.

3.3 Trust and Encryption

As described in Sect. 2 it is crucial to ensure that only legitimate recipients obtain data from the container security system (encryption). Hence, it is also important to clearly identify authorised cooperation partners (signature). Both demands for trustworthiness can be addressed by applying public key cryptography [Tan03] which is based on pairs of asymmetric encryption keys. In this approach, the public key of an agent is known to everyone and is applied in order to encrypt the content of messages for the respective agent (Fig. 2). Decrypting such contents can only be accomplished by applying the private key

[2] http://jade.tilab.com/

which is kept secretly and only known to the agent itself. A sender additionally signing the message with its own private key enables the receiver to validate its authenticity with the respective public key.

In order to identify trustworthy communication partners each container security system agent has to be provided with the public key of the company. The respective private key can, however, not simply be provided to all participants. Otherwise, the whole system runs the danger of being compromised if, e. g., a hand-held device with the key is lost. A finder or thief would then be able to decrypt all messages intended for the company. Instead, a public key infrastructure [Tan03] has to be established. In this concept each entity gets its own private key that is signed by the private root certificate of the company. Validating the respective public keys with the company's public key then reveals whether a communication partner is trustworthy. The problem of loss can be approached by demanding keys to regularly expire and be renewed.

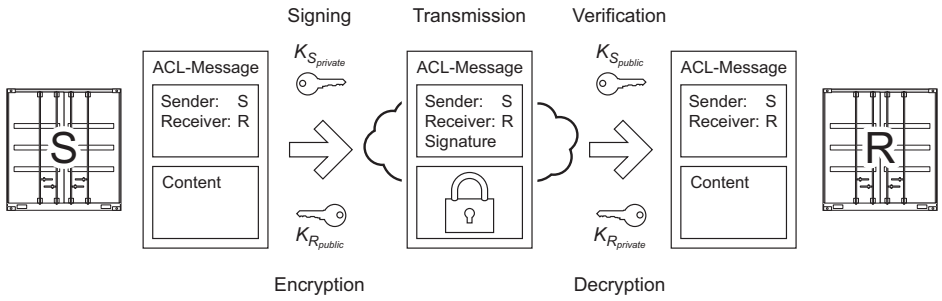

Figure 2: The software agent managing container *S* sends a message to the agent of container *R*. Therefore, *S* signs and encrypts the content of the message before transmission. The received message is then validated and decrypted by *R*

4 Conclusion and Outlook

Container security systems play an important role in securing container logistics. Nevertheless, a lack of standards currently prevents interoperability of components from different vendors. This paper argues in favour of an agent-based approach in order to overcome this limitation. By implementing electronic seals and sensors as agents, standardised communication protocols can be applied for the interaction. In addition, aspects of trust and encryption must be considered as not every communication partner is trustworthy. In order to save resources multiple components of one container security system as well as multiple systems may join forces by cooperating.

However, cooperation may not always suffice to overcome limitations caused by bounded resources. Some applications in dynamic environments additionally have high requirements on the internal management for the respective agents. Hence, an efficient handling of acquired knowledge and strategies to keep knowledge bases manageable are necessary. This aspect gains more importance when complex reasoning techniques are considered.

References

[BCG07] Fabio Bellifemine, Giovanni Caire, and Dominic Greenwood. *Developing Multi-Agent Systems with JADE*. John Wiley & Sons, Chichester, UK, 2007.

[Fie05] A. M. Field. Seals of Approval. *Journal of Commerce*, 6(38):46–48, 2005.

[Had05] R. Hadow. E-Seals and RFID. *Journal of Commerce*, 6(43):58, 2005.

[Hic04] K. Hickey. Insecurity Over E-Seals. *Traffic World*, 268(3):34, 2004.

[KT99] P. Knirsch and I. J. Timm. Adaptive Multiagent Systems Applied on Temporal Logistics Networks. In *4th International Symposium on Logistics (ISL-99)*, pages 213–218, Florence, Italy, 1999.

[Mül97] H. J. Müller. Towards Agent Systems Engineering. *Data & Knowledge Engineering*, 23:217–245, 1997.

[Sch04] E. Schwartz. The Cost of Safe Commerce. *InfoWorld*, 26(45):16, 2004.

[Tan03] A. S. Tanenbaum. *Computer Networks*. Pearson Education, Upper Saddle River, NJ, USA, 4th edition, 2003.

[Tir05] P. Tirschwell. An Opportunity from Container Seals. *Journal of Commerce*, 6(6):54, 2005.

[Wei99] G. Weiss, editor. *Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence*. MIT Press, Cambridge, MA, USA, 1999.

[WJ99] M. Wooldridge and N. R. Jennings. The Cooperative Problem Solving Process. *Journal of Logic & Computation*, 9(4):563–592, 1999.