

Risk analysis and Deployment Security Issues in a Multi-agent System

Ambra Molesini & Marco Prandini

Elena Nardini & Enrico Denti

{ambra.molesini, marco.prandini,
elena.nardini, enrico.denti}@unibo.it

ALMA MATER STUDIORUM—Università di Bologna

ICAART 2010, Valencia, Spain, 22nd January 2010



- 1 Case Study
- 2 Risk Analysis
- 3 Security Deployment Issues
- 4 Conclusions and Future Works



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks
 - ▶ discussing deployment strategies that could interfere with the achievement of the application goal



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks
 - ▶ discussing deployment strategies that could interfere with the achievement of the application goal
- In order to do this we



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks
 - ▶ discussing deployment strategies that could interfere with the achievement of the application goal
- In order to do this we
 - ▶ present our case study



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks
 - ▶ discussing deployment strategies that could interfere with the achievement of the application goal
- In order to do this we
 - ▶ present our case study
 - ▶ present the risk analysis phase



The objective of this paper

- Our work is aimed at performing a security analysis of a selected case study – an access control system [Molesini et al., 2009] – for
 - ▶ identifying threats coming both from
 - ★ the system domain
 - ★ its MAS-based implementation
 - ▶ assessing risks
 - ▶ discussing deployment strategies that could interfere with the achievement of the application goal
- In order to do this we
 - ▶ present our case study
 - ▶ present the risk analysis phase
 - ▶ discuss about security deployment issues



Background

- MASs should be conceived also as providers of security functionalities



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels
- However, a MAS needs a complex underlying infrastructure, whose intrinsic security is fundamental for the correct



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels
- However, a MAS needs a complex underlying infrastructure, whose intrinsic security is fundamental for the correct
 - ▶ behaviour of agents



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels
- However, a MAS needs a complex underlying infrastructure, whose intrinsic security is fundamental for the correct
 - ▶ behaviour of agents
 - ▶ implementation of the policy to be enforced



Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels
- However, a MAS needs a complex underlying infrastructure, whose intrinsic security is fundamental for the correct
 - ▶ behaviour of agents
 - ▶ implementation of the policy to be enforced
- Various solutions exist for the design of MAS-supporting platforms and for exploiting a MAS as a security provider
[Yamazaki et al., 2004, Bordini et al., 2006, JADE, 2005] . . .



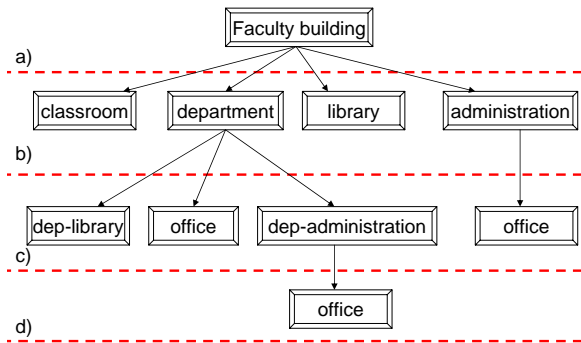
Background

- MASs should be conceived also as providers of security functionalities
- The flexibility of the agent paradigm proves very valuable in
 - ▶ modelling the different aspects of security schemes
 - ▶ capturing the concepts needed for achieving a robust design at the most appropriate abstraction levels
- However, a MAS needs a complex underlying infrastructure, whose intrinsic security is fundamental for the correct
 - ▶ behaviour of agents
 - ▶ implementation of the policy to be enforced
- Various solutions exist for the design of MAS-supporting platforms and for exploiting a MAS as a security provider [Yamazaki et al., 2004, Bordini et al., 2006, JADE, 2005] ...
- ... but the field of their security assessment is largely unexplored



Our case study

- Reference domain: access control system
- Case study: management of the access control to a university building [Molesini et al., 2009]
- System's scenario:

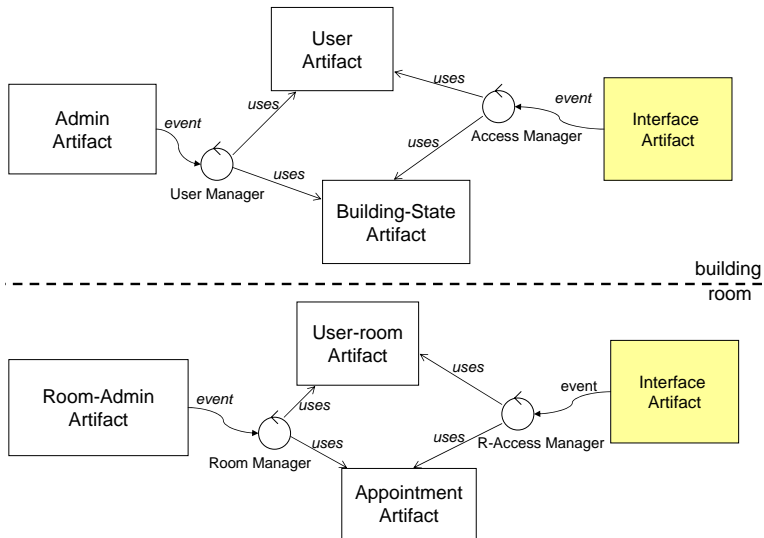


The developing methodology

- The case study was analysed and designed [Molesini et al., 2009] according to SODA
- SODA is an agent-oriented methodology for the analysis and design of agent-based systems
 - ▶ ... adopts **agents** and **artifacts** (A&A meta-model) as the main building blocks for MAS development
 - ★ agents model individual and social activities
 - ★ artifacts are adopted for the environment engineering since they glue agents together, as well as MAS and the environment



The system logical architecture [Molesini et al., 2009]



Risk analysis

- Risk analysis is a part of the more general process called “*Security risk assessment and management*” [Sommerville, 2007]



Risk analysis

- Risk analysis is a part of the more general process called “*Security risk assessment and management*” [Sommerville, 2007]
- Risk analysis should start from the identification of the system's
 - ▶ **assets** – the system resources to be protected because of their **value**
 - ▶ **exposures** – represent the possible loss or harm that results from a successful attack
 - ▶ **threats** –
 - ★ fortuitous events – flooding, storms, etc. . .
 - ★ deliberate attacks – sniffing, spoofing, etc. . .



System's assets, values and exposures

Asset	Value	Exposure
Interface Artifact	high	medium
Admin Artifact	high	high
User Artifact	high	high
Building-State Artifact	low	low
Room-Admin Artifact	high	high
User-room Artifact	high	high
Appointment Artifact	medium	medium
<hr/>		
User Manager	high	high
Access Manager	high	high
R-Access Manager	high	high
Room Manager	high	high
<hr/>		
Physical Device	high	high
Infrastructure	high	high



System's threats

Threat	Probability
Stealing admin credential	low
Stealing user credential	high
Personifying user	high
Social Engineering	high
<hr/>	
Introducing malicious agent	medium - high
Disappearing agent	medium - high
Agent bugs	high
Modifying agent code	low - medium
Tampering artifact data	high - very high
Sniffing artifact data	high - very high
Artifact bugs	high
Replacing artifact	medium - high
Men in the middle	medium - high
Sniffing communication	medium - high
<hr/>	
Damaging physical device	high



Threats for each asset

Threat	Asset												
	Interface Artifact	Admin Artifact	User Artifact	Building-State Artifact	Room-Admin Artifact	User-room Art.	Appointment Artifact	User Manager	Access Manager	R-Access Manager	Room Manager	Physical Device	Infrastructure
Stealing admin credential	*	*	*										
Stealing user credential	*		*	*	*								
Personifying user	*		*	*	*	*	*						
Social Engineering	*	*	*	*	*	*	*						
Introducing malicious agent	*	*	*	*	*	*	*	*	*	*	*	*	*
Disappearing agent								*	*	*	*		
Agent bugs								*	*	*	*		
Modifying agent code	*	*	*	*	*	*	*	*	*	*	*		
Tampering artifact data	*	*	*	*	*	*	*						
Sniffing artifact data	*	*	*	*	*	*	*						
Artifact bugs	*	*	*	*	*	*	*						
Replacing artifact	*	*	*	*	*	*	*	*	*	*	*		
Men in the middle	*	*	*	*	*	*	*	*	*	*	*		*
Sniffing communication	*	*	*	*	*	*	*	*	*	*	*		*
Damaging physical device	*	*											*



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated

Artifacts — passive components of the systems



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated

Artifacts — passive components of the systems

- ▶ *resource artifacts* – wrap external resources



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated

Artifacts — passive components of the systems

- ▶ *resource artifacts* – wrap external resources
- ▶ *social artifacts* – mediate between two or more agents in a MAS



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated

Artifacts — passive components of the systems

- ▶ *resource artifacts* – wrap external resources
- ▶ *social artifacts* – mediate between two or more agents in a MAS
- ▶ *individual artifacts* – mediate between an individual agent and the environment



Security deployment issues

- Assumption: all the infrastructures exhibit the same basic set of concepts

Nodes — logical *loci* where agents and artifacts can be allocated

Artifacts — passive components of the systems

- ▶ *resource artifacts* – wrap external resources
- ▶ *social artifacts* – mediate between two or more agents in a MAS
- ▶ *individual artifacts* – mediate between an individual agent and the environment

Agents — pro-active components of the systems



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices
 - ▶ **social artifacts** are the core of interactions



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices
 - ▶ **social artifacts** are the core of interactions
 - ★ agents use them for communicating with each other



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices
 - ▶ **social artifacts** are the core of interactions
 - ★ agents use them for communicating with each other
 - ★ their deployment is critical and should take into account all the measures to ensure that they remain trusted



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices
 - ▶ **social artifacts** are the core of interactions
 - ★ agents use them for communicating with each other
 - ★ their deployment is critical and should take into account all the measures to ensure that they remain trusted
 - ▶ **individual artifacts** equip agents with all the protocols they can adopt for interacting



Artifacts security deployment issues

- The artifacts deployment is critical from the security viewpoint
 - ▶ **resource artifacts** abstract the functions and behaviours of devices
 - ★ *smart device* = artifact + physical device
 - ★ smart device should be protected in order to prevent possible artifact tampering, replacement and sniffing
 - ★ physical devices should be protected so that the “artifacts corruption” does not damage the integrity and confidentiality of the devices
 - ▶ **social artifacts** are the core of interactions
 - ★ agents use them for communicating with each other
 - ★ their deployment is critical and should take into account all the measures to ensure that they remain trusted
 - ▶ **individual artifacts** equip agents with all the protocols they can adopt for interacting
 - ★ their deployment is particularly critical, since the corruption of this kind of artifact could allow a malicious agent to misbehave



Agent security deployment issues

- In a system developed according to the A&A meta-model, only agents can take proactive security measures



Agent security deployment issues

- In a system developed according to the A&A meta-model, only agents can take proactive security measures
- A smart device can be made even smarter by introducing a device manager agent to detect and promptly face dangerous situations



Agent security deployment issues

- In a system developed according to the A&A meta-model, only agents can take proactive security measures
- A smart device can be made even smarter by introducing a device manager agent to detect and promptly face dangerous situations
- The agents present several vulnerabilities and are subject to different threats



Agent security deployment issues

- In a system developed according to the A&A meta-model, only agents can take proactive security measures
- A smart device can be made even smarter by introducing a device manager agent to detect and promptly face dangerous situations
- The agents present several vulnerabilities and are subject to different threats
- In particular, autonomy, pro-activity and learning capabilities could act as drawbacks from the security view point
 - these properties restrict the designer's control on the agent execution flow



Agent security deployment issues

- In a system developed according to the A&A meta-model, only agents can take proactive security measures
- A smart device can be made even smarter by introducing a device manager agent to detect and promptly face dangerous situations
- The agents present several vulnerabilities and are subject to different threats
- In particular, autonomy, pro-activity and learning capabilities could act as drawbacks from the security view point
 - these properties restrict the designer's control on the agent execution flow
- Other malicious agents and corrupted artifacts can induce agent misbehaviour



Deployment configurations

- Analysis of the “deployment requirements” coming from the physical world



Deployment configurations

- Analysis of the “deployment requirements” coming from the physical world
 - ▶ four logical nodes labelled *Node 1*, *Node 2*, *Node 3*, *Node 4*



Deployment configurations

- Analysis of the “deployment requirements” coming from the physical world
 - ▶ four logical nodes labelled *Node 1*, *Node 2*, *Node 3*, *Node 4*
 - ▶ the physical resources are allocated respectively in
 - ★ the device capturing the user credential → *Node 2*
 - ★ the administrator position → *Node 3*
 - ★ the database → *Node 4*



Deployment configurations

- Analysis of the “deployment requirements” coming from the physical world
 - ▶ four logical nodes labelled *Node 1*, *Node 2*, *Node 3*, *Node 4*
 - ▶ the physical resources are allocated respectively in
 - ★ the device capturing the user credential → *Node 2*
 - ★ the administrator position → *Node 3*
 - ★ the database → *Node 4*
 - ▶ assumption: the protection of these devices is realised at the infrastructural level. . .

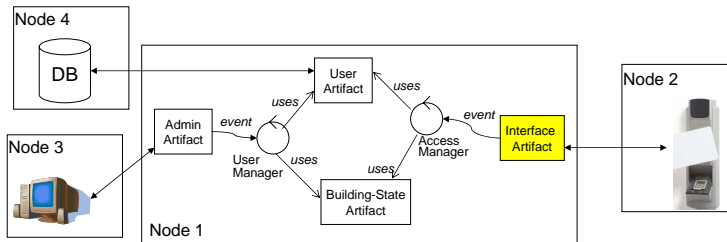


Deployment configurations

- Analysis of the “deployment requirements” coming from the physical world
 - ▶ four logical nodes labelled *Node 1*, *Node 2*, *Node 3*, *Node 4*
 - ▶ the physical resources are allocated respectively in
 - ★ the device capturing the user credential → *Node 2*
 - ★ the administrator position → *Node 3*
 - ★ the database → *Node 4*
 - ▶ assumption: the protection of these devices is realised at the infrastructural level. . .
 - ▶ here we focalise only the MAS security deployment

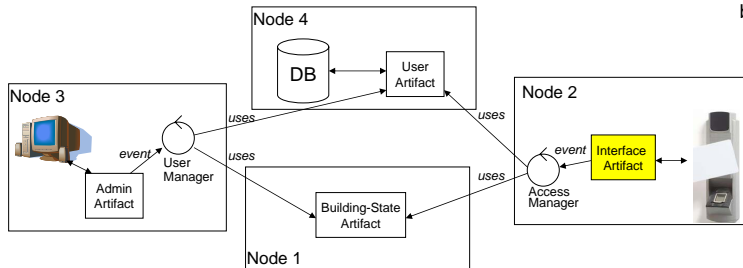


Centralised and distributed deployments

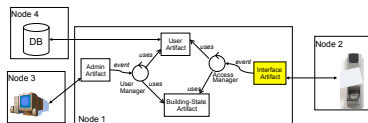


a)

b)



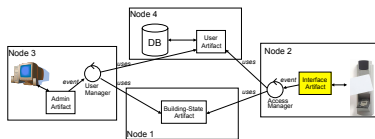
Centralised deployment



- It is sufficient to build a “secure boundary” around *Node 1* to obtain a “secure” system
- The compromission of a single software entity means that the secure boundary of *Node 1* is broken
- The threat probabilities regarding the assets increases
 - ▶ an attacker will try to force *Node 1* for accessing the system
 - ▶ the threat probabilities regarding the intra-MAS communications decrease
- The chosen protection mechanisms should be suitable for protecting the more valuable asset
 - the costly, effective countermeasures have to be sized to protect the whole *Node 1*, including less valuable assets



Distributed deployment



- All the system entities and the communication channels need to be protected
- Decoupling the exposures level of assets, choosing the most suitable protection mechanism for each
- Leading to reduce the inter-dependency between threat probabilities
- Presenting higher probability values associated with intra-MAS communication
 - the communications between entities always occur between network nodes
- The compromise of one node does not automatically implies the compromise of the whole system



Conclusions

- In this paper we have
 - ▶ explored the topic of security assessment in a MAS, taking a MAS-based access control system as our reference
 - ▶ performed a detailed risk analysis then, we studied how the deployment choices can influence the opportunity for attacks and the effects of their success
- Our deployment analysis can be situated at the end of the design phase in order to identify the “most adequate” deployment strategy in terms of security assessment
- Beyond the valuable context-specific results, the work hopefully provides an excellent opportunity for further, broader research







Future works

- Our work is just the starting point of the story
- Much broader research is needed to
 - ▶ devise a general model of the security requirements for MAS-based systems → opening the way towards the integration of security aspects into a suitable agent-oriented design methodology
 - ▶ further investigations concerning the security issues at the infrastructural level → the role of the MAS infrastructures is becoming more and more relevant in the whole MAS development process



Bibliography I

-  Bordini, R., Braubach, L., et al. (2006).
A survey of programming languages and platforms for multi-agent systems.
Informatica, 30:33–44.
-  JADE (2005).
Jade.tilab.com/doc/tutorials/JADE_Security.pdf.
-  Molesini, A., Denti, E., and Omicini, A. (2009).
RBAC-MAS & SODA: Experimenting RBAC in AOSE.
In *Engineering Societies in the Agents World IX*, volume 5485 of *LNCS*. Springer.
-  Sommerville, I. (2007).
Software Engineering 8th Edition.
Addison-Wesley.



Bibliography II



Yamazaki, W., Hiraishi, H., and Mizoguchi, F. (2004).
Designing an agent-based rbac system for dynamic security policy.
In *Proc. 13th IEEE Int. Workshops on Enabling Technologies (WETICE'04)*, pages 199–204, Washington, DC, USA. IEEE CS.



Risk analysis and Deployment Security Issues in a Multi-agent System

Ambra Molesini & Marco Prandini

Elena Nardini & Enrico Denti

{ambra.molesini, marco.prandini,
elena.nardini, enrico.denti}@unibo.it

ALMA MATER STUDIORUM—Università di Bologna

ICAART 2010, Valencia, Spain, 22nd January 2010

