2006

Security issues in adaptive distributed systems

Demissie Aredo
demissie.aredo@iu.hio.no

Sule Yildrim
sule.yildirim@hihm.no

SECURITY ISSUES IN ADAPTIVE DISTRIBUTED SYSTEMS

Demissie B. Aredo
Faculty of Engineering, Oslo University College
P. O. Box 4 St. Olavs Plass, 0130 Oslo, Norway
demissie.aredo@iu.hio.no

Sule Yildirim
Faculty of Business Administration, Social Sciences and Computer Science
Hedmark University College, Telthusvn 12, 2451 Rena, Norway
sule.yildirim@hihm.no

Abstract

Adaptive Distributed Systems (ADSs) are distributed systems that can evolve their behaviors based on changes in their environments. In this work, we discuss security and propose security metrics issues in the context of ADSs. A key premise with adaptation of distributed systems is that in order to detect changes, information must be collected by monitoring the system and its environment. How monitoring should be done, what should be monitored, and the impact monitoring may have on the security mechanism of the target system need to be carefully considered. Conversely, the impact of implementation of security mechanism on the adaptation of distributed system is also assessed. We propose security metrics that can be used to quantify the impact of monitoring on the security mechanism of the target distributed system.

Keywords*: Security metrics, Adaptation, Adaptive Distributed Systems, Monitoring*

1 INTRODUCTION

In the contemporary society, distributed systems have a significant impact on how communication between social, industrial and governmental institutions is achieved. Dealing with the complexity, heterogeneity and dynamics of distributed systems is absolutely among the main concerns of the software industry. In the Internet era, the distribution of information and services on different sites is a common and dominant scenario. Hence, accessing information and services on remote sites requires high-level of system quality: acceptable response time (at least "near real-time"); and security mechanisms. These aspects require inherent adaptation of the system to changes in the environment. In the case of ADSs, the challenge to maintain system quality is even greater.

In general, security issues in distributed information systems, whether adaptive or not, is already a serious concern. There are many types of threats, among them those occurring during communication and those in the form of unauthorized attempts to access stored information. Solutions proposed to address these problems in distributed systems may contribute to the implementation of security mechanisms in ADSs. On the other hand, if a token ring is used to achieve mutual exclusion in data communication, then a loss of token might be a result of unauthorized monitoring of the token, which is a direct consequence of the distributed system being adaptive and having monitoring component. Moreover, data resubmission might be requested by authorized parties that couldn't receive the data. Such a request might also come from malicious intruders that are requesting resubmission of data to get a copy.

The kind of environmental changes that can be monitored in ADSs include, but are not limited to, processor and link failures, changes in communication patterns and frequency, changes in failure rates, and changed application requirements (Schlichting 1998, Chen & Hiltunen & Schlichting 2001).

1.1 Problem Statements

Distributed systems can be perceived as living entities in the sense that the state of the system as well as its execution environment conditions change dynamically. In order to continuously provide the intended functionalities and services at an acceptable level of quality, adaptation of the system to the changing environment is necessary. For instance, network congestion is a common problem that is caused due the load on communication channels. To handle this problem, the system should be able to adapt itself to the level of congestion in order to maintain its functionality to provide a quality level of services. An adaptation in turn requires *monitoring* of the system, e.g. gathering information about message traffic and the environment in order to choose an appropriate behavioral adjustment. However, considering the possibility that a monitoring system is overtaken by an intruder, some security problems are likely to occur.

In the case of security-critical systems, adaptation might also be necessary in order to maintain the required level of protection, which necessitates monitoring and gathering of detailed critical data about the communicating objects. On one hand, restricting the monitoring and gathering of information may constrain the capacity of the system to adapt itself to the changing environment and to maintain the security mechanism. On the other hand, allowing the gathering of security-critical data might lead to a situation that might compromise the whole security mechanism. This problem is aggravated especially in distributed systems where some of the monitoring is usually done by a subsystem that is *external* to the target system. In this case, communication between the monitor and the target system can be intercepted by an unauthorized intruder – the classical 'man-in-the-middle' problem. In other words, in making a critical system adaptive to deal with such security threats, there is a risk of compromising the whole security mechanism. Then, the problem is how to achieve a system where its adaptation to the changing execution environment has minimal impact on its security mechanism.

In this regards, a number of issues need to be investigated:

- What should be monitored and at what level of detail should the monitoring be done?
- How should the monitoring be done? Usually, a distributed monitoring architecture is recommended to minimize performance overheads. However, this may impose serious security problems as the information gathered from the system is distributed at different sites.
- Should the monitoring subsystem be within the system boundary? If the monitor is an external subsystem, unauthorized intruders can exploit the monitor and thus create a security threat. One possible solution is to implement security mechanism in the monitoring subsystems. If the monitor and the target system communicate over unsecured channel, some mechanisms should be employed to limit the threat.
- What is the impact of monitoring for adaptation on security mechanisms implementation? Can the existing security metrics be used to measure the impact?

1.2 Outline of the paper

The rest of the paper is organized as follows: In Section 2, a brief review of the-state-of-the-art of ADS and related security issues is presented. In Section 3, we discuss issues related to security metrics and propose metrics that enable us to quantify security in the context of ADSs. In Section 4, we present an example to illustrate the main concepts discussed in this work, namely how adaptation of distributed systems and security issues can affect each other. Finally, in Section 5 we draw some conclusions and discuss potential research issues for future work.

2 RELATED WORK

2.1 Adaptive Distributed Systems

Distributed systems that can evolve their behaviors based on changes in their environments are known as *Adaptive Distributed Systems* (ADSs). Adaptation usually takes place on different sites in a distributed system and needs to be coordinated.

Adaptive systems monitor and evaluate their environments and can adapt their own behaviors when there is a change in the environment. On the other hand, adaptive behavior is the field of science where the underlying mechanisms of adaptive behavior of animals, software agents, robots and other adaptive systems are investigated into. The results from adaptive behavior research are exploited for building artificially intelligent adaptive systems. In this case, we envision distributed systems within the context of artificially intelligent adaptive systems and we therefore believe that the research progress in adaptive behavior will affect the research in ADSs. That is, monitoring, change detection and behavior adaptation components of an adaptive distributed system will become more intelligent in time. An ADS better knows what is happening in its environment by detecting and evaluating the changes in the environments and adjusting their actions to the changes more intelligently. However, the more intelligent and adaptive a distributed system becomes through its monitoring and other components, the more risky it becomes that the intruders act more severely in a distributed environment if the monitoring component is overtaken by them. In the following paragraphs, we are giving a brief survey on ADSs.

Leonhardt et al. (1998) indicate that security is an issue that appears where activity is being tracked, namely by the monitoring system they have proposed. For that reason, in this work, we look into the levels of knowledge a monitoring system might eventually have about its environment while becoming more adaptive, and whether the level of knowledge and the properties of the knowledge being monitored would cause any security issues compared to the distributed systems which are not adaptive.

Russello et al. (2005) described how adaptation is done for dynamical replication for managing availability in a shared data space. The idea is that if replication is required, the middleware should offer mechanisms that would allow the application developer to select from different replication policies that can be subsequently enforced at runtime. There is an adaptation subsystem where the environment conditions are monitored. It is detected when to switch to another replication policy automatically. The execution environment conditions which are monitored are cost of communication latency and bandwidth, especially when external monitoring subsystem is used.

Silva et al. (2002) developed a generic framework for the construction of ADSs. The model is composed of three main packages. In the monitoring package, system specific parameters, such as processor utilization, in the various hosts of the distributed system are monitored. This package informs the event detection and notification package whenever values of such parameters change significantly. In addition to this, interceptors as used in the CORBA distributed system standards are inserted into the object invocation path. Each time a client invokes a method of an object, the message corresponding to this invocation is intercepted and later re-dispatched to the target object. Using interceptors, the system can extract useful information from each method invocation storing it in a log file for analysis by the event detection and notification package. On the other hand, dynamic configuration package, depending on the type of the event, executes the appropriate algorithm that defines actions that should be taken in order to adapt the application to the new environment condition.

As stated in (Al-Shaer 1998), monitoring system can be used to detect and report security violations such as illegal logins or attempts of unauthorized access to files. On the contrary, we argue that if the monitoring subsystem is overtaken by an intruder, the monitoring system can also be used for causing

security violations once an intruder has knowledge about login information and file authorizations to be able to report illegal logins and attempts of unauthorized access to resources.

2.2 Security Issues in Adaptive Distributed Systems

Security metrics indicate the degree to which security goals such as data confidentiality are being met, they propose actions that should be taken to improve the overall security program, and identify the level of risks in not taking a given action and hence provide guidance in prioritizing the actions. They also indicate the effectiveness of various components of a security program. Developing effective security metrics programs has proven to be very challenging. A number of factors have contributed to this: collecting the necessary data is difficult; and there are no well-established and standardized guidelines.

Swanson et al. (2003) identified elements that must be considered in defining effective security metrics: metrics must yield quantifiable information; supporting data must be readily obtainable; only repeatable processes should be considered for measurement; and metrics must enable tracking of performance.

Voas et al. (1996) propose a security assessment methodology, called *adaptive vulnerability analysis (AVA)*, which provides a relative measure of software security. The methodology is based on measurement of security weaknesses in terms of predetermined set of threats that are frequently encountered. The resulting metrics may vary with different set of threats and hence the methodology is called adaptive. Its major advantages include, among others, its ability to be customized to application-specific classes of intrusions and the fact that it measures dynamic run-time information. The fact that it is based on a predetermined set of threats is among the major limitations of AVA.

Payne (2001) proposes a guideline that should be closely followed in the development a security metrics program. The guideline consists of several steps: clear definition of security goals and objective; decision about what metrics to generate and strategies for generating them; create action plan; and establish a formal program review cycle. Following this guidance enables us to clarify the *why*, *what* and *how* of developing security metrics. In the sequel, we focus on the metrics that should be generated to quantify the level of security threats that could be caused due to monitoring of a target system to achieve the level of adaptation necessary to maintain quality of services.

3 SECURITY METRICS FOR ADAPTIVE DISTRIBUTED SYSTEMS

Adaptation techniques allow software systems to modify their functionalities and configurations in response to changes in their execution environments and hence show better performance results compared to the non-adaptive ones. The types of environmental changes may include processor and link failures, changes in communication patterns and frequency, changes in failure rates, and changes in application requirements – functional and non-functional ones.

Potential benefits of ADSs include the ability to respond rapidly to security threats, reliable message transmission, consistent messages ordering across hosts, implementing functions such as replication or data consistency for higher level services such as a network directory service and the opportunity to optimize performance as changes in the execution environments take place (José da Silva e Silva & Endler & Kon 2002). In addition to the above benefits, Kreutzer et al. (1983) applied adaptation in identifying faulty processors in distributed systems and Hiltunen et al. (1996) propose a model for constructing fault-tolerant ADSs.

3.1 Monitoring of Adaptive Distributed Systems

The basic components of ADSs include *monitoring*, *change detection* and *reconfiguration* in response to the changes in the environment. In this paper, we focus on the monitoring component of ADSs and elicit possible impacts this may have on security mechanism. A monitoring component is employed for collecting information on parameters that can later be analyzed to detect changes in the environment of the target distributed system. The parameters that can be monitored may include the time it takes a message to arrive at its destination, failure rates, and failures themselves. This might have little or no contribution to security threat to the target system.

However, monitoring systems have become more intelligent in the sense that they are now supported by additional functionalities such as interceptors in CORBA. An interception mechanism is vulnerable to causing security threats if it is, for example, overtaken by an intruder. On the other hand, there is a need for monitoring a wider variety of parameters than the ones mentioned above, including the contents of messages or identities of hosts sending and/or receiving the messages. This is necessary to make monitoring systems more capable of detecting a wider variety of changes in the environment and to make a wider variety of actions possible to compensate for the changes in the environment. The drawback of the later scenario is that it also gives an opportunity to the intruders to access information about hosts in the distributed systems, which enables them to act as genuine hosts and access more security-critical information.

It can also be the case that more advanced monitoring mechanisms will open the way to intercept more detailed contents of the messages although the monitoring mechanisms might not explicitly support this opportunity with its existing structure. With more detailed knowledge in hand, an intruder can proceed to contact hosts that it wants to act in place of and query them for more information after it overtook the role of a monitoring system. In other words, the better the adaptation of distributed systems to changes in the environment are, the higher the risk of security mechanisms compromised in addition to the security problems that exist in non-adaptive distributed systems.

The security threat can be minimized if monitoring is done by a trusted and authorized party or if the monitoring component is part of the system. However, especially in systems where there is distribution of information such as databases, files and objects, i.e. in the case of file distribution on several sites, this may not be always possible. As a result, monitoring to achieve a better adaptation, which definitely improves system performance and the quality of services, might have a negative impact on the security mechanism of the target system. Two scenarios for monitoring the target system are worth considering: the monitor is part of the system; the monitor is outside the system. We consider the case where the monitoring system is outside the system as security problems in the other case can easily be addressed as it would be part of the security mechanism of the target system.

Figure 1 shows the case where an external system is monitoring the distributed system. An intruder may have access to the unsecured communication channels and intercept the information or takeover the monitor.

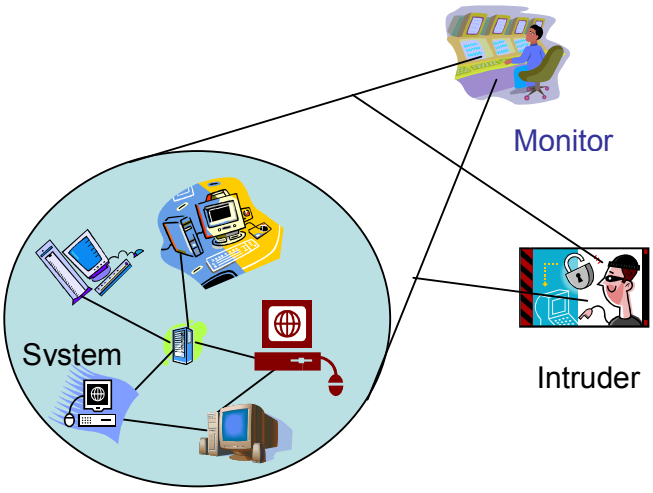

Figure 1: External Monitoring of Distributed Systems

In the sequel, we investigate issues relevant to security concerns that may result from monitoring for adaptation purposes. While achieving adaptation by exploiting methods of intelligent adaptive systems, we investigate techniques for developing security metrics in terms of data collection, secure communication and cryptography.

3.2 Security Metrics for Adaptive Distributed Systems

Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT security metrics must be based on security performance goals and objectives, which state the desired results of a system security implementation (Swanson & Bartol & Sabato & Hash & Graffo 2003). IT security metrics enable us to measure the achievement of the goals by quantifying the level of implementation of security controls and efficiency of the controls, analyzing the adequacy of security mechanism and identifying possible action to address any security lack.

The application of software metrics has proven to be an effective technique for improving the quality of software and the productivity of the development process (Bhatti 2005). Software organizations spend around 80% of their development resources on aspects related to software quality, e.g. on security related issues. Security metrics provide a practical approach to measuring information security. They are effective tools for evaluating the effectiveness of components of a security program, the security of a specific system, product or process and the ability of a security department to address security issues for which it is responsible. Metrics are also useful in identifying the level of risk of not taking a given security measure, which in turn provides guidance in prioritizing corrective actions.

In order to quantify the impact of monitoring on the effectiveness of security mechanism of the target system, we need to define some metrics that enable us measure such an impact. The metrics should be a function of set of attributes of data to be collected by monitoring the system, which are relevant to the security implementation. We have identified the following attributes as relevant to the security issues and the metrics are defined in terms of these attributes: level of *Criticality, Detail*, *Size*, and *support for Inferences*.

- ***Criticality*** of data is an attribute that indicates the importance of the data with respect to security. In other words, criticality of data indicates the security risk the disclosure of the data

to unauthorized party can cause. The data criticality attribute is directly related to the security metrics, i.e. the higher the criticality is, the larger the value of the metrics is.

- The ***detail*** attribute of data indicates the level of abstraction/concreteness of monitored data. For instance, in monitoring communications among objects, we might only be interested in less detailed information such as the number of messages exchanged, or more detailed information that includes number of messages and their contents. The more detailed the data are, the higher the security metrics are.
- The ***size*** attribute measures the amount of data collected during monitoring. This attribute is important as it indicates, for instance the possibility of network congestion in the target system the monitoring may cause, which in turn hampers the quality of services delivered.
- By the support for ***inference*** attribute we mean the possibility to derive security relevant information about other data objects from given data security relevant information about other data objects. The higher the value of this attribute is, the higher the value of the security metrics is.

The attributes have other mutual dependencies among the attributes that need further consideration. For instance, size of data is directly related to its level of detail, and detail of data is directly related to support for inference.

Suppose that MD denotes monitored data, C the level of security criticality attribute of the data, D the level of detail of the data, S its size and I support for inference of critical data. The security metrics can be defined by the equation: $M = \alpha.C + \beta D + \lambda S + \eta I$ for some nonnegative coefficients α, β, λ and η. The values of these coefficients and their relationships can be determined using some analytical techniques.

The data attributes discussed above, and by transitivity the security metrics, are inversely related to the effectiveness of security mechanism of the target system, i.e. the higher the value of the security metrics, the weaker the security mechanism would be. Symbolically,

$SM \approx {}^{1}\!/_{M}$, where SM is the effectiveness of the security mechanism of the target system.

4 EXAMPLE: TOKEN RING FOR MUTUAL EXCLUSION

In this section, we show how security threats can be worsen with a monitoring of distributed systems in order to obtain adaptation. We present the token ring problem as an example. Token ring mechanism is a solution to mutual exclusion problem in distributed systems (Erciyes 2004). A token, which is basically a message, is passed around in an order from one node to the other where nodes are coordinated in a ring shape. The node that receives the token gains an access to a shared memory or a common resource. The node which completes its work in the shared memory or resource passes the token to the next node in the ring as shown in Figure 2.

The severity of security threats arises as follows with an additional monitoring in the system for adaptation: An intruder who normally would not have access rights to the shared memory or resource can become aware of the token being passed around, capture it and prevent it from being passed to the next innocent node in the ring. This would give the intruder an opportunity to act like the next innocent node in the ring and access the resources which he does not normally have right to if, the monitoring system which he has overtaken supplies him with “additional information” about the nodes in the ring. This additional information will not be present in a system without a monitoring component which works towards adaptation. For example, after having captured the token, the intruder can proceed to listen to the messages that the next node in the ring is sending and can try to capture this node’s specific authentication and authorization information. With the monitoring

mechanisms in hand, it is easier to do so since the monitoring component has already the mechanism for monitoring the distributed environment and collecting information in place.

This additional knowledge can be any information about the nodes in the ring that would help the intruder act like one of the legitimate nodes in the ring. At this point, it is important to notice that the limit for a monitoring system to be knowledgeable about the nodes that it is monitoring should be set very carefully considering the fact that there might be intruders that might wish to take over the monitoring system. The other important issue is to notice that there must be additional effort in terms of authorization, authentication, encryption etc. while designing a monitoring system such that it cannot be easily overtaken by an intruder.

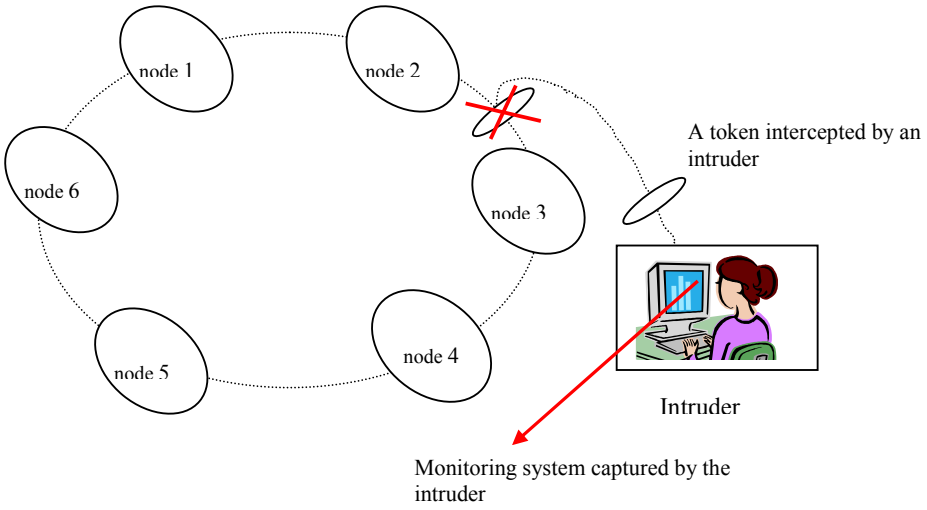

Figure 2: The threat by an intruder increases due to its control over monitoring system

As a result, additional issues relevant to security mechanisms can appear when designing ADSs compared to the ones which are not adaptive because adaptive systems have a monitoring component which is trying to gain knowledge about its environment. There is a question that needs to be answered about what kind of information a monitoring system should normally have about the nodes it is monitoring to collect information necessary for adaptation and to what extent this knowledge can reach for the purposes of adaptation. The level of knowledge can be measured with metrics defined for security purposes which we called as a security metric.

5 CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this paper, we have discussed security issues, in particular security metrics, in the context of ADSs and proposed an approach towards assessing the impact of monitoring for adaptation on effectiveness of security mechanisms. We argue that there can be additional security threats caused due to the monitoring of distributed systems to make them adaptive. In addition, we identify and quantify the level of security threats that can be caused if monitoring systems are overtaken by intruders.

Security issues in distributed systems are classical problems, which have partly been solved using techniques such as cryptographic systems, access control and auditing mechanisms. There has also been an approach to monitor the communication channels to obtain secure communication. On the other hand, adaptation has seen a wide acceptance among researchers since it has the purpose of

presenting a good quality of service to the users of distributed systems. Adaptation requires the monitoring of data under communication.

In the sequel, we propose two major arguments. Firstly, the fact that monitoring of a distributed system to collect data for the purpose of adaptation may cause security problems. Information about activities of users, their communication patterns as well as contents of the messages, even though the contents can be encrypted, are collected by monitoring the target system by a monitoring component which is usually external to the target system. It is a considerable security threat if the monitoring component is overtaken by an intruder and as a result, the collected information becomes available to the intruder. The situation becomes critical as techniques and mechanisms of monitoring and analyzing the collected information becomes more intelligent in time.

The main objective of this work is to figure out how much advanced can the techniques and mechanisms for monitoring and analyzing monitored information become and what kinds of impacts they might have on the size, criticality, and detail and support for inference attributes of the collected data. These properties have been defined in the previous sections.

Moreover, we propose a security metric that can be computed from the above mentioned attributes of the collected data. This metric enables us to quantify the level of security threat that monitoring may cause to the target system. Conversely, necessary actions that should be taken by the security program, e.g. giving warnings when data with a high level of security criticality is transferred, can be proposed based on the values of the security metric.

5.2 Future Work

It is definite that a monitoring component aims at becoming more knowledgeable about the environment it is functioning in so that the changes in the distributed environment can be detected and the corresponding actions can be taken in order to compensate for the changes in the environment for purposes of providing acceptable quality of service. However, considering the security threats that may occur in case that an intruder takes control over the monitoring system, there needs to be a limit to the kind and level of knowledge that the monitoring system can be allowed to have. Also, access to the monitoring systems should be protected from the intruders.

In the future work, we will investigate the level of knowledge about a distributed environment which might be required by monitoring systems to gather information necessary for adaptation purposes and how this knowledge can be exploited by intruders to cause security threats in the situations like token ring. Also, it is very important to be able to define a security metric which itself maybe adaptive in order to enable us measure security levels of the distributed environments which are adaptive. In this paper, we have already sketched definitions of security metrics which can be used for that purpose. This definition needs to be refined as we figure out more about types of knowledge that will be employed by monitoring systems in future and under which circumstances. As a result, implementation of security mechanism may have a significant impact on the adaptability of distributed systems.

The more critical information a monitoring subsystem logs, the higher the risk for the security to be compromised is. For instance, if the purpose of the monitoring is to provide a better security mechanism by making the system adaptive to the changing environment, e.g. by capturing of intrusion attempts, the monitoring system should collect detailed and security-critical data such as user ID and IP address of a site. In that case, there is a high risk of information disclosure to unauthorized intruders. Hence, establishing a mechanism for finding a trade-off between collecting detailed data to achieve a better adaptation and the risk of running into security compromise is useful. This is among the research issues that we investigate in future work.

Formulation and implementation of a framework for security metrics in the context of ADSs are also among issues that will be dealt with in the future. We will seek answers to, among others, the following questions:

- What are the implications and limitations of implementing this approach? Will the implementation of this approach result in a more secured system or rather worsen the situation?
- What security threats are related to the addition of an extra security mechanism such as the security metrics?
- Can we adapt the existing security mechanisms and metrics to address the problem in the context of ADSs? And if so, how can it be done?

Providing answers to these questions will not be an easy task and requires a thorough and challenging investigation. As this is a new approach, studying its application, limitations and implications on securing distributed systems is an interesting research issue for future research agenda.

Acknowledgements

We are grateful to Ronald L. Beachell for reviewing earlier versions of this paper and for his invaluable comments. Comments and recommendations by anonymous reviewers contributed to the improvement of the presentation of this work. We acknowledge the comments and recommendations.

References

S. N. Bhatti (2005). Why quality? ISO 9126 software quality metrics (Functionality) support by UML suite. ACM SIGSOFT Software Engineering Notes 30(2).

M. Swanson, N. Bartol, J. Sabato, J. Hash and L. Graffo (2003). Security Metrics Guide for Information Technology Systems, NIST special publication 800-55.

W. K. Chen, M. Hiltunen and R. Schlichting (2001). Constructing Adaptive Software in Distributed Systems, in the Proc. of the 21st International Conference on Distributed Computing Systems, (ICDCS-21), pp. 635-643, Mesa, AZ.

G. Russello, M. Chaudron, and M. van Steen (2005). Coordination Models and Languages, in the Proc. of the 7th International Conference, COORDINATION 2005, Namur, Belgium.

F. M. Silva, Endler, and K. Fabio (2002). Dynamic adaptation of distributed systems, in the 16th European Conference on Object-Oriented Programming.

E. S. Al-Shaer (1998). Hierarchical Filtering-Based Monitoring Architecture for Large-Scale Distributed Systems. PhD Thesis, Old Dominion University.

R. D. Schlichting (1998). Designing and Implementing Adaptive Distributed Systems, available at http://www.cs.arizona.edu/adaptiveds/overview.html.

K. Erciyes (2004). Distributed Mutual Exclusion Algorithms on a Ring of Clusters, ICCSA 2003, Springer-Verlag, LNCS 3045, pp. 518-527.

J. Voas and K. Miller (1996). Defining an Adaptive Software Security Metric from a Dynamic Software Fault-Tolerance Measure. COMPASS '96, the 11th Annual Conference on Computer Assurance, Gaithersburg, Maryland.

S. Kreutzer and S. L. Hakimi (1983). Adaptive Fault Identification in Two New Diagnostic Models. Proc. of the 21st Allerton Conference on Communication, Control and Computing, pp. 353-362.

M. A. Hiltunen and R. D. Schlichting (1996). Adaptive Distributed and Fault-Tolerant Systems. International Journal of Computer Systems Science and Engineering, 11(5):125-133.

U. Leonhardt and J. Magee (1998). Security Considerations for a Distributed Location Service, Journal of Network and Systems Management, 6(1):51-70.

S. C. Payne (2001), A Guide to Security Metrics, SANS InfoSec Reading Room, available at http://www.sans.org/rr/whitepapers/auditing/55.php.

F. José da Silva e Silva, M. Endler and F. Kon (2002). Dynamic Adaptation of Distributed Systems, 12th Workshop for PhD Students in Object-Oriented Systems 16th European Conference on Object-Oriented Programming Málaga, Espanha, June, 2002.