Advances in Adaptive Secure Message-Oriented Middleware for Distributed Business-Critical Systems

Habtamu Abie¹, Reijo M. Savola², Jinfu Wang³, and Domenico Rotondi⁴

¹Norwegian Computing Center, Oslo, Norway
²VTT Technical Research Centre of Finland, Oulu, Finland
³MPI-QMUL ISRC Macao SAR, China & ⁴Queen Mary University of London, United Kingdom
⁵TXT e-solutions SpA Valenzano (BA), Italy

Abstract. Distributed business-critical systems are often implemented using distributed messaging infrastructures with increasingly stringent requirements with regard to resilience, security, adaptability, intelligence and scalability. Current systems have limited ability in meeting these requirements. This paper describes advances in adaptive security, security metrics, anomaly detection and resilience, and authentication architecture in such distributed messaging systems.

Keywords: Distributed messaging systems; resilience; security metrics; adaptive security; adaptability

INTRODUCTION

Message-oriented middleware (MOM) enables distributed business-critical applications to exchange messages with other applications without detailed knowledge of their platforms and networking, thus increasing the interoperability, portability, and flexibility of architectures. However, the environment surrounding these systems is in a continuous state of change, which increases the stringency of requirements with regard to resilience, security, adaptability, intelligence and scalability. Existing technologies are crude, not scalable and not suited to future needs. They have neither the robustness nor the resilience needed by future real-time systems. GEMOM (Genetic Message-Oriented Secure Middleware) [1] is an EU FP7 ICT project whose aim is to bring about significant advances in the aforementioned areas within a MOM. Its adaptive security model includes the integration of monitoring, analysis and response functions, and tool-set and processes for pre-emptive vulnerability discovery. This paper describes the main advances in the adaptive security, security metrics, anomaly detection and resilience, and authentication architecture of the GEMOM system (see Figure 3 in [2]), and briefly discusses the resulting prototypes and their potential.

ADAPTIVE SECURITY MANAGEMENT

The adaptive security management consists of a continuous cycle of monitoring, assessment, and evolution to meet the challenges posed by the changing, multifaceted relationships within and between organizations in distributed business environments in today’s situation of increasing threats. For this, a framework has been developed that combines an Adaptive Security Management (ASM) model and an Adaptive Trust Management (ATM) model [3]. The ASM model implements the core functions for an adaptive secure broker, including adaptive authentication, authorization, message encryption, and message signature. These key components are supported by managerial components that perform the functions of adaptive policy management, key management and identity management. The ATM model is organized into three levels: (i) interpretations of attacks and anomalous behaviors, (ii) analysis and categorization of compromises and (iii) calculation of trustworthiness. The model adapts to the dynamism of the environment and to the varying degrees of risk to which the compromised system is exposed. It does this by making dynamic decisions regarding which approach is to be adopted and by ensuring the highest likelihood of achieving the greatest benefit for the smallest risk.

The overall adaptive security management thus learns, anticipates, evolves, and adapts to a changing environment at run-time. It (i) combines adaptive risk-based security, trust-based security, and security-based trust, and (ii)
integrates different metrics, and tools for assessment and observation that enhance the assessment of trustworthiness and verification. Its methods for learning and reasoning combine expert systems, statistical evaluations and adaptive models (neural and fuzzy) at all levels. The adaptation can take the form of parameter adaptation in which adaptation is achieved by specific variations in the control parameter vector, structure adaptation in which adaptation is achieved by dynamic changes in the structure of the system, goal adaptation in which adaptation is achieved by formally defining specific constraints on the state of the system, or by any combination of these.

We used [4] as the basis for the theory of our security adaptation model. Adaptation may be defined as the optimal control (i) of a specified object $F$ in a state $S$ whose influence $Y$ on the environment is determined by the influences $X$ of the environment on the object, (ii) of the relevant set of adaptable structures and/or factors $U$, and (iii) of the goals $Z$ of the adaptation as defined by specified constraints on the state $S$ of the object. Security goals are expressed as formal constraints on the state of the system, and the concepts used in control theory are used to describe the dynamic security processes. Security goals are expressed as formal constraints on the state of the system as follows:

$$Z : S (X , U ) = [ H (U ) = (h_i (U ), h_j (U ),... , h_p (U )) \geq 0 ;$$

$$G (U ) = (g_i (U ), g_j (U ),... , g_p (U )) = 0 ;$$

$$Q (U ) = (q_i (U ), q_j (U ),... , q_p (U )) \rightarrow \min .$$

$$h_i (U ) = M_i (h_i (Y )) = M_i (h_i (F (X , U ))) i = 1,..., p$$

$$g_j (U ) = M_j (g_j (Y )) = M_j (g_j (F (X , U ))) j = 1,..., s$$

$$q_k (U ) = M_k (q_k (Y )) = M_k (q_k (F (X , U ))) k = 1,..., l$$

$$M_i , ( \cdot ) = \{ (p (X | X ) \}_{N \times N}$$

where $M_i$ is a function for averaging-out the states of the environment, and $h^*$, $g^*$, $q^*$ are actually measured Security Metrics, Faults/Threat Levels and Quality of Service parameters, respectively. The Adaptive algorithm is as follows:

$$U_{N+1} = \phi \left( U_{N,W} , H_{N,W} , G_{N,W} , Q_{N,W} \right) \quad (2)$$

where $U_{N,W}$, $H_{N,W}$, $G_{N,W}$, $Q_{N,W}$ are adaptable parameters vector, and vectors of the values of the criterion function measured over an interval of time, and $\phi$ is a recurrent algorithm of the adaptation.

SECURITY METRICS

Security solutions with varying strength levels are required in resilient and distributed business-critical systems such as GEMOM so that they can manage security in an adaptive manner according to the needs of varying situations. In adaptive security management, security metrics provide the means with which to ensure the correctness of security solutions, to compare different solutions, and to obtain evidence about the performance of operational security. A novel systematic and practical methodology for developing security metrics was developed as part of the project. This is described in [2], along with a collection of Basic Measurable Components (BMCs) for the GEMOM system. The methodology is a complete risk-driven process, which starts from an analysis of threat and vulnerability and aims to achieve a collection of balanced and detailed security metrics and related measurement architecture. The development of the actual metrics is based on the identification of BMCs using security-requrement decomposition. For instance, user-dependent Authentication Strength $AS_{usr}$ can be composed from the normalized and scaled component metrics for that user [2]:

$$AS_{usr} = w_{AIU} \cdot AII_{usr} + w_{AIS} \cdot AIS_{usr} + w_{AMI} \cdot AMR_{usr} + w_{AMR} \cdot AMI_{usr},$$

where $AIU_{usr}$ is Authentication Identity Uniqueness, $AIS_{usr}$ is Authentication Identity Structure, $AII_{usr}$ is Authentication Identity Integrity, $AMR_{usr}$ is Authentication Mechanism Reliability, $AMI_{usr}$ is Authentication Mechanism Integrity, and $w_x$ is the weighting factor of component $x$, and $\sim$ denotes normalization and uniform scaling of the component metrics. Overall Authentication Strength is the average of Authentication Strengths of all users [2]:

$$AS = \frac{1}{N} \sum_{i=1}^{N} AS_i,$$
ANOMALY DETECTION AND RESILIENCE

The GEMOM monitoring tool consists of a set of anomaly detector monitors, which detect failures and faults in brokers and links, such as broker-level or link level performance degradation, bottlenecks, and broker or link failures. The GEMOM resilience functions are designed to ensure continued messaging functionality in the face of faults or failures detected by monitoring tool. The key concept is the use of mirroring of namespaces. Namespaces are sets of topics that typically have business significance. Different namespaces can be mirrored in different brokers. If a broker in the overlay fails or a link fails then the messages for each of the namespaces will be switched to the designated mirrors. This applies for overlay brokers in a subnet and for brokers spread over the internet [5]. The rationale for the latter is that the enhanced disjointedness of message paths gives greater resilience to link failures and greater immunity to DoS (see, for example [6]). The switch-over has also been implemented for multi-homed publishers and subscribers, and simultaneous messaging. This also enhances link resilience. The Overlay Manager receives output events from the monitoring tool, and decides which actions (e.g. switch-over) to take using the policies computed. The policies are created using a new technique for the allocation and mirroring of namespaces to brokers to minimize the quantified risk of overload to the system in cases of surges in demand or attack. For example, it is risky to mirror a large namespace on a broker that has little spare capacity after the allocation of the primary load. Also in stressful situations a highly correlated workload will lead to bursts in load and will therefore have a super-additive effect on the probability of exceeding broker capacity. Negatively correlated items, on the other hand, will make the total workload more stable. Consider the optimal primary allocation case. A policy assigns a partition of workload (i.e., a set of namespaces) to a broker. The message rate of the set is denoted by \( V_j \). The capacity of broker is \( C_i \). The best policy is computed from system utility value \( U_{total} \) which maximizes revenue \( R_j \) from carrying the message traffic, while minimizing penalty \( P_j \) for exceeding the capacity. The policy planning quantifies risk by estimating the probability distribution \( P_r \) of the message rate of different possible combinations of workload. The mean and variance of \( P_r \) for sets of topics \( j \) can be determined, using historical data and the variance and covariance of all topics. Specifically, the policy maximizes:

\[
U_{total} = \sum_{i=1}^{k} U_i \text{, where } U_i = R_j - \int_C^\infty P_j(x-C_i)P_r(V_j = x)dx
\]

where \( k \) is the number of brokers. Penalty \( P_j \) is formulated for two cases. One where there is a fixed penalty for exceeding the capacity of a broker, i.e., messaging failure, and the other for the more realistic case where the penalty increases proportionally to the number of messages beyond broker capacity.

AUTHENTICATION ARCHITECTURE

GEMOM authentication architecture is centered on a user-centric, federated identity management approach. In addition, GEMOM implements different Levels of Assurance (LoA), ranging from authentication based on a traditional username/password to X.509 certificates and smart cards. GEMOM can dynamically adapt the required authentication strength level (that is, the lowest acceptable LoA), to the operative conditions as determined and required by the GEMOM Adaptive Security Management. The GEMOM authentication features are based on the Higgins Framework (www.eclipse.org/higgins), which has been extended and enhanced for use with non-web applications. These extensions and enhancements will be provided as open-source code with licensing conditions similar to the Higgins code.

RELATED WORK

A number of adaptive security systems have been developed recently supporting adaptation at different levels and for a number of reasons [7][8]. Table I gives a brief comparison of our adaptive security work with most closely related work with their special features and benefits categorized according to their types of adaptation.

<table>
<thead>
<tr>
<th>References: Features and benefits</th>
<th>Limitations</th>
<th>Advances in our approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-adaptable access control [9]</td>
<td>Assessability and verifiability of the trustworthiness of the system</td>
<td>Combination of trust-based security and security-based trust, anomaly detection</td>
</tr>
</tbody>
</table>

TABLE 1. Brief Survey of Adaptive Security and Trust
Adaptive trust management [11][12] Assessment models to minimizing the rate and severity of compromises Continuous monitoring, assessment, evaluation, and risk, security and trust


Security metrics [16] Metrics development process, elaboration of BMCs Systematic metrics development methodology complete BMCs collection

THE PROTOTYPES AND THEIR POTENTIAL

The GEMOM project has prototyped the following: a full featured message broker, a transparent completion and encapsulation publishing framework, adaptive security implementation with authentication, authorization, key management and identity management solutions, a security monitoring tool utilizing security metrics, an intelligent fuzzing tool, and tools for the configuration and deployment of management and development processes. These prototypes have been validated in five real-world business-critical scenarios: a collaborative business portal, a dynamic linked exchange, financial data delivery, a dynamic road management system, and banking for transaction processing.

GEMOM provides demonstrated solutions to advance the state-of-the-art in terms of resilience, security, and adaptive run-time management. It is planned that GEMOM adaptive security solutions will be utilized in the areas of transportation, finance, and banking. Plans to utilize the GEMOM resilience solutions include, in particular, software applications in the areas of defense and avionics. The project’s security-metrics solutions can be utilized in business-critical systems.

ACKNOWLEDGMENTS

The work presented in this article has been carried out in the GEMOM FP7 research project, partly funded by the European Commission. The authors acknowledge the contributions made by various GEMOM partners.

REFERENCES

5. J. Wang and J. Bigham, Anomaly detection in the case of message oriented middleware, MidSec’08, Dec. 02, 2008: 40–42.