International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

A Distributed Access Policy Consolidation for Event Processing Systems

E Amrutha Varshini[1]& Dr.P.Indira Priyadarsini[2]

[1]PG Scholar,Dept of CSE, Chalapathi Institute Of Technology,Guntur ,Andhra Pradesh,
Email: varshini216@gmail.com

[2]Professor,Dept of CSE, Chalapathi Institute Of Technology,Guntur,Andhra Pradesh,
Email: indupullagura@gmail.com

ABSTRACT:

Event processing is an approach that can capture and process the data about the events. Complex event processing is the merging the information from multiple origins. Event processing systems has a procedure that continuous event streams will be further applied operations of event streams. In distributed-applications like a large warehouse (where items can be shipped) when we are processing the events. This will be transmitting in between many security authorities. Using the access-policy every incoming event can be secured. We can increase the processing of events by calculating the measure of obfuscation values for events. Calculate the threshold for obfuscation as one of the part of access-policy and avoid the access requirements and events will be delivered more reliable. In this way we can deliver the more events. We also perform some experiments to assess engines scalability with respect to number of queries and propose ways for evaluating their ability in adapting to changes in load conditions. Lastly, we show that similar queries have widely different performances on the same or different engines and that no engine dominates the other two in all scenarios.

Keywords- Event Processing; Security; Accesscontrol.

INTRODUCTION:

In business processes, it is essential to detect inconsistencies or failures early. For example, in manufacturing and logistics processes, items are tracked continuously to detect loss or to reroute them during transport. To answer this need complex event processing (CEP) systems have evolved as a key paradigm for business and industrial applications.CEP systems allow to detect situations by performing operations on event streams which emerge from sensors all over the world, e.g. from packet tracking devices. While, traditionally event processing systems have applied powerful operators in a central way, the emerging increase of event sources and event consumers have raised the need to reduce the communication load by distributed in-network processing of stream operations.

In addition, the collaborative nature of today's economy results in largescale networks, where different users,companies, or groups exchange events. As a result, event processing networks are heterogeneous in terms of processing capabilities and technologies, consist of differing participants, and are spread across multiple security domains. However, the increasing interoperability of CEP applications raises the question of security . It is not feasible for a central instance to manage access control for the whole network. Instead, every producer of information should be able to control how its produced data can be accessed. For example, Manufacturer Shipping Company? Customer Access Control & Event Dependency a company may restrict certain information to a subset of authorized users (i.e. that are registered in its domain). Current work in providing security for event-based systems covers already confidentiality of individual event streams and the authorization of network participants. In CEP systems, however, the provider of an event looses control on the distribution of dependent event streams. This constitutes a major security problem, allowing an adversary to infer information on confidential ingoing event streams of the CEP system. As an example

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

consider the logistics process where a manufacturer wants to deliver an item to a destination.

The shipping company determines a warehouse close to the destination, where the item will be shipped to before it will be delivered to the customer. The logistic process is supported by an event processing system, where operators are hosted in the domain of each party and exchange events including potentially confidential information (e.g. the item's destination is transmitted to the shippingcompany). If now a third party receives events related to the warehouse, it may draw conclusions about the original event data (i.e. destination), in spite of the manufacturer declaring this information as highly confidential and only providing the shipping company with access rights to it.

The goal of this work is to establish access control that ensures the privacy of information even over multiple processing steps in a multi-domain, large scale CEP system. In particular, our contributions are i) an access policy inheritance mechanism to enforce access policies over a chain of dependent operators and ii) a scalable method to measure the obfuscation imposed by operators on information exchanged in event streams. This allows to define as part of the access policy an obfuscation threshold to indicate when the event processing systems can ignore access restrictions, thus increasing the number of events to which application components can react to and this way increasing also the utility of the CEP system.

EXISTING SYSTEM:

On the one hand, sampling techniques can be used to estimate the conditional probabilities of the Bayesian network. However, their precision depends strongly on the number of samples taken from the network, and no approximation scheme exists that allows to draw samples in polynomial time to achieve a certain precision. This makes the approximate algorithms infeasible for security applications, since no guarantees can be made in appropriate time. On the other hand the complexity of calculating exact inference can be reduced by storing partial results of the inference calculation which otherwise would have to be calculated multiple times. However, the benefit of these optimizations is heavily dependent on the structure of the Bayesian network.

PROPOSED SYSTEM:

A role-based access control is proposed. Pesonen et al. and Bacon et al. discuss how publish/subscribe systems can be secured by introducing access control policies in a multi-domain architecture. They describe how event communication between the domains can be supported. Opyrchal et al. present the concept of event owners that can be specified. These are used to provide access to their events. Tariq et al. propose a solution to provide authentication and confidentiality in broker-less content-based publish/subscribe systems. Our work is based on the previous work which make event communication secure among different entities in the system a. We assume the presence of a system that can handle access control on events. Based on this, we use policy composition in order to derive the necessary access policies at any point during the event processing steps.

- Eventt Processing
- Manufacturer
- Shipping Company
- Customer

Event processing:

Event processing systems respond to events in the system's environment or user interface. The key characteristic of event processing systems is that the timing of events is unpredictable and the system must be able to cope with these events when they occur.

Manufacturer:

In this module manufacturer, insert the product details and also view product request from shipping company. Send details to shipping company to delivery date and pickup time.

Ship Company:

In this module ship company, view product request from customer. Then company forward the request to manufacturer or reject the request.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Customer:

In this module customer, product order from Ship Company and also views the order from Ship Company. Customer views the import details.

METHODOLOGY:

Attributes were measured to be distinct even if they make use of the identical name, but are created at two different operators. The inheritance of needs in a chain of succeeding operators is sometimes extremely restrictive and can maximum the competence and applicability of the complex event processing systems although access policies permit a producer to identify access requirements in a manner of fine-grained. To identify access rights of subjects, access control permits for the set of obtainable objects which are provided by means of the owner of an object and may possibly be granted to operators on the basis of an access requirement. To make use of the attribute in its correlation function theconsumer is trustworthy and accept the needs specified for the attribute in its individual access policy for all producedevents. The number of access needs in each step of correlation of this chain may possibly increase by means of theconsolidation of requirements from numerous producers. The size of the attribute domain is less significant than the number of attributes and this fits well with numerous complex event processing systems. Every consolidation step can consequently augment the number of interested consumers which are prohibited from admission to the event attributes of produced streams of event. This does not reveal the nature of systems of event processing where essential events like single sensor readings may possibly have only slight influence on the conclusion contained in a complex event demonstrating a specific situation.

Besides enforcement as well as assurance of access policies at every producer, a consumer will be appropriate to access an attribute merely if the properties of consumer match the access needs defined for the meticulous attribute. Access requirements are succeed by means of assigning them to event attributes in the form of an access policy which permits to conserve requirements all the way through any chain of dependent correlation steps of operators in the graph of directed operator. Besides, the policy of an obfuscation policy permits specifying an obfuscation threshold intended for event attributes. The obfuscation of event attributes in produced events in each correlation step is indomitable by means of the introduced access policy consolidation procedure. The needs of attribute's access can be overlooked once the obfuscation threshold is attained for an event attribute and such a prerequisite may be a role, a location or a domain association. Requirements are typically not direct properties of the operators, however of the hosts where the operators are positioned. Any consumer within the network will be capable to access it if there is no necessity particular for an attribute. Through enforcement as well as assurance of access policies at every producer, a consumer will be appropriate to access an attribute merely if the properties of consumer match the access needs defined for the meticulous attribute. It is hard to have a common purpose assess intended for the obfuscation of values within event attributes while it is simple to model and observe dependencies among attributes of incoming and outgoing at an operator. Actually there is no obfuscation of information of event and for each received attribute; the consumercan unswervingly conclude the values of the actual, incoming attributes. With numerous complex event processing systems the attribute domain extent is less significant than the number of attributes and this fits well. On the correlation function of correlation the level of obfuscation is highly reliant, specifically how it produces events of outgoing on the basis of incoming events. In all main systems of complex event processing two essential operators found such as: a filter, and an aggregator. The function of filter'scorrelation is easy: for each incoming event it is ensured whether one or additional attributes include a certain value or are within a convinced value range. The events are forwarded towards each and every one

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

consumer of the filter operator.

RESULTS:

In view of the fact that measuring the obfuscation would take too lengthy and the event processing would be slowed down the estimation may possibly not be practicable for applications with extremely high event rates. On the number of unidentified attributes in the dependency graph the additional processing time is extremely dependent in addition to the number of potential values each of the unidentified attributes might include. With numerous complex event processing systems, the size of the attribute domain is less significant than the number of attributes and this fits well where it is remarkable to associate events from numerous different sources, although rather have a restricted number of sources with potentially huge attribute value ranges.

DISCUSSION AND EVALUATION

We implemented the presented approach within the DHEP framework which enables CEP in a heterogeneous environment. That means, hosts may be spread among different security domains and have differing processing capabilities or use different correlation engines. Hence, using the framework allows us to create multi-domain distributed CEP networks. To achieve policy consolidation, every operator receiving a request provides the requester with the informationneeded for further processing: the access policy as well as the obfuscation policy. The policies might be different depending on the consumer. The events a consumer receives as well as its adherence to access policy inheritance is dependent on whether it fulfills the access requirements. To realize the obfuscation measurement we make use of the Weka framework. Weka is a data mining tool which comes with a Bayesian network implementation. Furthermore, itare received. For the new created event, we calculate the achieved obfuscation for a consumer. To have results independent of the processing time of the used correlation engine, we extracted and depicted only the time needed for calculating inference in the Bayesian Network, since it is the main source for additional latency caused in our approach depicts the additional latency depending on the number of event sources. The number of event sources has a direct influence on the size of the locally created dependency graph, hence on the size of the Bayesian Network. No ingoing attribute was known to the consumer. The size of the attribute domain was fixed to two, meaning that every event attribute was boolean. The results show that the increase of the latency, caused by the computation of obfuscation values increases exponentially with the total number of attributes. This behavior is expected. However, computations are fast for networks with a small number of attributes, as they are common in many CEP applications. Since security-related event systems have, depending on the network and event parameters, a processing time in the range of one millisecond and more per event, we consider a latency of up to 1ms as acceptable for our approach. In our second evaluation, we leave the number of event sources fixed at two but varied the domain size. Furthermore, we calculate the achieved obfuscation for two different consumers. decrease because not all events or event attributes will be received by an operator. However, it can be easily seen that this reduction is fully dependent on the application characteristics, especially on the access rights of the operators and the frequency distribution of event attribute values. Therefore it is not possible to provide meaningful evaluations and we focus on evaluations of the additional latency caused by our approach.

RELATED WORK:

With the increasing popularity of event-driven systems, a lot of effort has been spent to make the systems secure. Pesonen et al. and Bacon et al. discuss how publish/subscribe systems can be secured by introducing access control policies in amulti-domain

architecture. They describe how event communication between the domains can be supported. Opyrchal et al. present the concept of event owners that can be specified. These are used to provide access to their events. Tariq et al. propose a solution to provide authentication and confidentiality in broker-less content-based publish/subscribe systems. Our work is based on the previous work which make event communication secure among different entities in the system. We assume the presence of a system that can handle access control on events. Based on this, we use policy composition in order to derive the necessary access policies at any point during the event processing steps. Access policy composition has found a lot of consideration in distributed systems. Bonatti et al. defined a well recognized algebra for composing access policies. Especially in the area of web service composition, the composition of security policies plays an important role, as different policies have to be combined for every combination of web services. We adopt some of these concepts into our distributed CEP system, which allows us to inherit access restrictions during the different processing steps in the operators of our system. To realize our concepts we make use of techniques from statistical inference. More specific, we calculate the Bayesian inference after creating a Bayesian network and learning the dependencies . Since Bayesian inference is a complex calculation, several Monte-Carlo algorithms have been proposed to estimate the inference value(s). They all have in common to arbitrarily pick samples from the Bayesian network probability distribution, and estimate the values based on the samples. The precision of the estimated inference values is dependent on the number of samples. A commonly used technique is the Gibbs sampler.

CONCLUSION

This paper addressed the inheritance and consolidation of access policies in heterogeneous CEP systems. We identifieda lack of security in multi-hop event processing networks and proposed a solution to close this gap. More specific, we presented an approach that allows the inheritance of access requirements, when events are correlated to complex events.

Our algorithm includes the obfuscation of information, which can happen during the correlation process, and uses the obfuscation value as a decision-making basis whether inheritance is needed. We presented an implementation of our approach, based on Bayesian Network calculations. The analysis and evaluations show that the approach is computation-intensive, once the Bayesian Network grows, hence raising the processing time of an event. To deal with the calculation cost, we introduced a local approach, where every participant calculates local obfuscation achieved during the correlation process. We use a variable elimination optimization to further reduce the computational effort for calculating obfuscation. Future work will concentrate on enhancing the obfuscation calculation and methods to increase the Bayesian Network size so we are able to measure obfuscation over more than one correlation steps.

REFERENCES:

[1]A. Buchmann and B. Koldehofe, “Complex event processing,”it - Information Technology, vol. 51:5, pp. 241–242, 2009.

[2]A. Hinze, K. Sachs, and A. Buchmann, “Event-based applications and enabling technologies,” in Proceedings
of the Third ACM International Conference on Distributed Event-Based Systems, ser. DEBS ’09. New York, NY, USA:ACM, 2009, pp. 1:1–1:15.

[3]P. Pietzuch, “Hermes: A scalable event-based middleware,”Ph.D. dissertation, University of Cambridge,
2004.

[4]G. Li and H.-A. Jacobsen, “Composite subscriptions in content-based publish/subscribe systems,” in Proc
of the 6th Int. Middleware Conf., 2005, pp. 249–269.

[5]G. G. Koch, B. Koldehofe, and K. Rothermel, "Cordies: expressive event correlation in distributed systems,"
in Proc. of the 4th ACM International Conference on Distributed Event-Based Systems (DEBS), 2010, pp. 26–37.

[6]B. Koldehofe, B. Ottenw¨alder, K. Rothermel, and U. Ramachandran, "Moving range queries in distributed
complex event processing," in Proc. of the 6th ACM International Conference on Distributed Event-Based Systems (DEBS),2012, pp. 201–212.

[7]B. Schilling, B. Koldehofe, U. Pletat, and K. Rothermel, "Distributed heterogeneous event processing: Enhancing scalability and interoperability of CEP in an industrial context," in Proc. of the 4th ACM International Conference on Distributed Event-Based Systems (DEBS), 2010, pp. 150–159.

[8]B. Schilling, B. Koldehofe, and K. Rothermel, "Efficient and distributed rule placement in heavy constraintdriven
event systems," in Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC), 2011, pp. 355–364.

[9]M. A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing basic security mechanisms in brokerless
publish/ subscribe systems," in Proceedings of the 4th ACM Int.Conf. on Distributed Event-Based Systems (DEBS), 2010, pp.38–49.

[10]L. I. W. Pesonen, D. M. Eyers, and J. Bacon,"Encryption-enforced access control in dynamic multidomain publish/subscribe networks," in Proc. of the 2007ACM International Conference on Distributed Event-Based Systems (DEBS), 2007, pp. 104–115.