Complex event processing and distribution of dependent event streams

Engineering

KEYWORDS :

Guraza S.K. Vardhan Final Year computer department, Pune University. D.Y.Patil College of Engineering, Akurdi, Pune- 411044. vardhanandgroup@gmail.com, 9881489500.

Avais Mirza Final Year computer department, Pune University. D.Y.Patil College of Engineering, Akurdi, Pune- 411044. avaismirza786@gmail.com, 8554872271.

Anshul Manek Final Year computer department, Pune University. D.Y.Patil College of Engineering, Akurdi, Pune-411044

Ankita Naik Final Year computer department, Pune University. D.Y.Patil College of Engineering, Akurdi, Pune-411044

ABSTRACT

Existing event processing systems provide insufficient privacy constraints for preserving data. There may be problem in large-scale distributed applications like a logistic chain where event processing operators may be spread over multiple security domains. One can identify from outgoing event streams confidential input streams of the event processing system. We present a fine- grained access management for complex event processing. We can specify of an access policy to protect each incoming event stream also enforced by algorithms for access consolidation. We provide a measure in a scalable manner to increase the utility of the event processing system for the perplexity of event streams. A perplexity threshold as part of the access policy allows ignoring access requirements and delivering events which have achieved a sufficient high obfuscation level.

1. Introduction

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 such approximation scheme exists that allows to draw samples in polynomial time to achieve a certain precision. Thus it makes the approximate algorithms infeasible for security applications, since no guarantees can be made in an appropriate time and also 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 pros of these optimizations is heavily dependent on the structure of the Bayesian network. Analysts have thus marked Event Processing as the most growing segment in enterprise computing during years 2008 to 2009, furthermorethis trend is expected to continue and thus many of the large and medium software companies like (IBM, Oracle, Microsoft) progress the 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.

2. Problem Statement

Current type of event processing system lacks the methods of privacy preserving constraints of incoming event streams [3]. This is the problem in large scale distributed application like a logistics chain where different processing operators may be spread over multiple security domains. Any person can interfere in the legally received outgoing event streams confidential input streams of the event processing system.

The goal of this system is to establish access controlthat ensures the privacy of information even over multiple processing steps in a multi-domain, large scale CEP system [3]. In particular, the contributions we are providing 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 obfuscationimposed 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.

The Access policy consolidation reduces the network usage. This is due to the fact that both number and the size of the events decrease because not all events or the event attributes will be received by an operator. However, it is easily seen that this reduction is fully dependent on the application characteristics, especially on the access rights of the subscriber and the frequency distribution of event attribute values [3]. Therefore it is not possible to provide meaningful evaluation and we focus on the additional latency by one approach.

3. Literature Survey

Ant colony optimization (ACO) is a population-based metaheuristic that can be used to find approximate solutions to difficult optimizing problem. Ant colony optimization, a set of software agents called artificial ants search for good solutions to a given optimization problem research into developing effective computer aided techniques for planning software projects is important and challenging for software engineering. Apart from projects in other fields, the software projects are people-intensive activities and their related resources are mainly human resources. Therefore, an adequate model for software project planning has to deal with not only the problem of project task scheduling but also the problem of human resource allocation. But as both of these problems are difficult. The basic idea of EBS is to adjust the allocation of employees at events and keep the allocation unchanged at non-events. With this strategy, the proposed method enables the modelling of resource conflict and task pre-emption and preserves the flexibility in human resource allocation. Therefore to solve the planning problem an ACO algorithm is further is used.

Most systems focus on increased scalability of the system by reducing the cost of subscription forwarding and eventmatching [3]. Only few systems have addressed securityissues in a content-based publish/subscribe system.To achieve policy consolidation, every operator that receivesa request provides the requester with the informationneeded for further processing: the access policy as wellas the obfuscation policy. The policies might be differentdepending on the consumer. The eventsa consumer receives as well as its adherence to accesspolicy inheritance is dependent on whether it fulfills theaccess requirements. To realize this obfuscation measurementwe make use of the Weka framework [11]. Weka is adata mining tool which comes with a Bayesian networkimplementation. Wang et al. [1] investigate the security issues and requirementsthat arise in an internet-scale publish/subscribe system.They concluded that due to loose coupling between publishersand subscribers, many security issues cannot bedirectly solved by current technology and requires further research.

Hermes [4] proposes a security service that usesrole-based access control to authorize subscribers as well asto establish trust in the broker network. Pesonen et al. [3]addresses the role-based access control in multi-domainpublish/subscribe systems by the use of a decentralizedtrust management. Opyrchal et al. [2] try to leverageconcepts from secure group-based multicast techniques forthe secure distribution of events in a publish/subscribesystem. They showed that previous techniques for dynamicgroup key management fails in a publish/subscribe scenario,since every event potentially has a different set of interestedsubscribers. To overcome the problem they proposed a keycaching technique. However, broker nodes are assumedto be completely trustworthy. Event guard [5] providessix guards/ component to protect each of the five majorpublish/subscribe operations (subscribe, unsubscribe, advertise,unadvertised, publish) and routing. It only supports topic-based routing through the direct use of pseudorandom functions. PS Guard [6] addresses scalable key managementin a content-based system by using hierarchicalkey derivation to associate keys with subscriptions andevents. It does not address the issues related to the securerouting of events and subscription confidentiality. Event confidentiality is not properly ensured in case of complex subscriptions, i.e., the keys associated with the filters in acomplex subscription are not bind together.

Another drawback with the existing solutions is their assumptionabout the presence of a broker network [7, 4, 5]. These solutions are not directly applicable to peer-to-peerenvironments where subscribers are clustered according to their interests. The recent progress of pairing-based cryptography motivates .many applications built upon Identity-Base Encryption.

Attribute-Based Encryption [8, 10], is a general formof Identity-Based Encryption. It allows for a new type ofencrypted access control, where the access control policiesare either embedded in the user private keys or in the ciphertexts.Shi et al. [11] and Boneh et al. [9] addresses complexqueries (such as conjunction, subset and range queries)over encrypted data using identity based encryption. Bothapproaches address the problem from a pure cryptographicperspective and are not practical in our scenario. In theconstruction of Boneh et al. [9] the cost of public parameters,encryption cost and ciphertext size for range queriesincreases with the number of dimensions and number of points in each dimension i.e. Similarly the decryption cost of Shi et al. [11] is exponential in the number of attributes. Therefore, instead of using theircryptographic mechanisms, we derived our mechanisms directlyfrom attribute-based encryption. Furthermore, these systems are not targeted toward content-based systems anddo not address the issues related to verification of event authenticity, subscription confidentiality and secure eventrouting.

4. Approach

Complex event processing hasevolvedinto a paradigm of choice for developing of monitoring and reactive applications. It also has a strong impact on future information systems and the way we subscribe to consume information. CEP addresses two crucial prerequisites to build highly scalable and dynamic systems. First, it decouples senders and receivers of the infrormation. Neither the providers need knowledge about the set of relevant data or event sources. Second, CEp-systems not only mediate information in form of events between senders and receivers but also support the detection and encryption of events between senders and receivers.

5. Conclusion

This paper thus addresses the inheritance and consolidation of access policies in heterogeneous CEP systems. We have identified a lack of security in multi-hop event processing networks and proposed a solution to close this gap. More specifically, we presented an approach that allows the inheritance of access requirements, when the events are correlated to complex events. Our algorithm thus includes the obfuscation of information, which will happen during the correlation process, and thus uses the obfuscation value as a decision-making basis whether inheritance is needed. We have thus studied the implementation of our approach.

The analysis and evaluations show that the approach is computation-intensive as once the Bayesian Network grows, the processing time of an event also rises. To handle the calculation cost we would prefer a local approach where each and every participant calculates local obfuscation achieved during the correlation process. We prefer a variable elimination optimization to further reduce the computational effort for calculating obfuscation. The 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.

REFERENCE

[1] C. Wang, A. Carzaniga, D. Evans, and A.Wolf. Security issues and requirements for internet-scale publish-subscribe systems. In Proc.of Hawaii Intl. Conf. on System Sciences (HICSS), 2002. | [2] L. Opyrchal and A. Prakash. Secure distribution ofevents in content-based publish subscribe systems. Inconf. on USENIX Security Symposium, 2001. | [3] L. I. W. Pesonen, D. M. Eyers, and J. Bacon. Encryption-enforced access control in dynamic multi-domain publish/subscribe networks. In DEBS 2007. | [4] P. Pieztzuch. Hermes: A Scalable Event-Based Middleware, PhD theasis, University of Cambridge, Feb 2004. | [5] M. Srivatsa and L. Liu. Securing publish-subscribe overlay services with eventguard. In proc. Of ACM conf. on Computer and communication security, 2005. | [6] M. Srivatsa and L. Liu. Scalable access control in content-based publish-subscribe system.Technical report, Georgia Institute of Technology, 2006d. | [7] C. Raiciu and D. S. Rosenblum. Enabling confidentiality in content-based publish/subscribe infrastructures. In Intl Conf. on security and Privacy in Communication Networks, 2006. | [8] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. INproc of the IEEE Symposium and Privacy, 2007. | [9] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In conf. on Computer and communication security., 2006. | [10] B. Schilling, B. Koldehofe, U. Pletat, and K. Rothermel, "Distributed heterogeneous event processing: Enhancing scal- ability 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. | [11] M. A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel,"Providing basic security mechanisms in broker-less publish/subscribe systems," in Proceedings of the 4th ACM Int. Conf. on Distributed Event-Based Systems (DEBS), 2010, pp. 38–49.