Derrick Murphy

Dr. Deb

Parallel Computing

CSC 4322

Security in Distributed System

A distributed system is a network that consists of autonomous computers that are connected using a distribution middleware. They help in sharing different resources and capabilities to provide users with a single and integrated coherent network [1].

The prominent features in a distributed system are component concurrency, allowing resource sharing; and system able to be spread across different geographies. In relation to other network representations, there is a better fault tolerance in a distributed model.

Distributed systems have a key goal in mind over other models. First is transparency, the ability to portray one system without concealing the details of the location, access, migration, concurrency, failure, relocation, persistence and resources to the users. Secondly openness, this is making the network easier to configure and modify. Next Reliability, a distributed system should be very proficient of being secure, consistent and have a high ability of concealing errors. Forth is performance, in relation to other models, distributed models are expected to give a much-wanted boost to performance. Lastly the goal of a distributed system is scalability, this type of system should be scalable with respect to geography, administration or size.

Distributed systems unfortunately include challenges. In public networks, security is a big challenge in distributed environments. If unreliable components are used in a distributed model, fault tolerance could be tough. Without appropriate protocol coordination and resource sharing would be a problem.

During the *Electronic and Mechanical Engineering and Information Technology (EMEIT) 2011 International Conference*, held from August 12-14 2011, an innovative security model was presented for multi-level security. The topic was an “Access control method based on multi-level security tag for distributed database system. “

Distributed database is physically distributed in a variety of Web sites and is logically integrated together. Distributed database system is consisted of a set of interconnection network server and client. When system users access the distributed database, they must login by one of the clients and accept authentication. After the system have recognized the user's legal identity, the user's database access request can be accepted and be carried out grammatical and semantic analysis, permissions checks and other operations. At last, the database system submitted access request to local or remote management layer to monitor implementation. Data sharing is one of the most prominent features in the distributed database. It has brought many benefits for distributed applications, but it also has new security issues [2].

There are three safety problems in distributed database systems. First, distributed systems have several user groups and users. Typically, these groups and users are distributed among diverse sites. Causing complexity detecting user’s legal identity. Unauthorized data may be exposed since access control is basically carried out in accord with user security level. Secondly, users of distributed database systems frequently need to share information, but this information may be stored by diverse users, and may be distributed in many sites. For another user, the same information may have different security requirements. Open access control mechanism could be the reason for insecurity of the flow information . For example, a member with higher authorization permissions could handover their authorization power to other members without approved permissions at will. Thirdly, Unauthorized data may be exposed with access control passed merely in accordance with user security level. For example, in an internal office network, the personnel director and financial director have the same security level, but obviously, the personnel director can not access financial information freely, and vice versa. Thus, the critical security technologies in the distributed systtems are users' authentication and access control.

Authentication is once the user signs into the system structure, one must initially provide their user name, password or key to demonstrate user's identity. Access control is when the system admits user's access request, the system foremost checks whether the user has access to permit the content, then the authorized user's access request can be processed through.

In the research on Multi-level security access control, Bell-LaPadula model describes the reasonable flow path of information in the security system and defines the system security requirements for processing the data with the different security levels. It is a basis that we design multilevel secure database system [4-6]. By using safety tag theory in the Bell-LaPadula model, we introduce some concepts, such as subject, object and domain, subject and object are defined with safety level respectively, and level management and security management for group are banded together and are added some security tags. According to these security tags, we can achieve mandatory access control. This security access control mechanism can resolve the problem about insecurity of information flow and leakage of unauthorized information to realize data sharing in distributed system. Therefore, it is used to implement security access control [2].

# Once again in 2011 at the *Fourth International Symposium on Parallel Architectures, Algorithms and Programming*, a key scheduling algorithm improvement was presented. Researchers proposed a, “Security-Driven Fault Tolerant Scheduling Algorithm for High Dependable Distributed Real-Time System “. Recognized as new and improved scheduling algorithm. It extended Fault Tolerant Rate-Monotonic First Fit algorithm to tolerate N processors failure at once, and it introduced a new scheduler to improve efficiency of scheduling process.

# There are several designs projected to schedule tasks in real time system. First proposed, Liu and Layland, well-known Rate-Monotonic (RM) algorithm which tolerated preemptively scheduling periodic tasks only on a single processor. Secondly, Dhal and Liu, branched from the RM algorithm to Rate Monotonic First-Fit (RMFF) algorithm, which reinforced scheduling real time tasks on multiprocessor system. Next, Alan and Luigi, proposed Fault Tolerant RMFF (FFRMFF) algorithm based on RMFF which presented a fault tolerance method to RMFF, but didn’t consider the security condition of real time tasks and endured only one core failure. Furthermore, Tao and Qin, presented, Novel dynamic scheduling algorithm with security awareness. This algorithm didn’t sustain static scheduling, causing failure when scheduling large numbers of periodic tasks, and most significant, it didn’t back fault tolerance.

In high dependable real time system, each task requires a certain level of security which could be concluded three typical security demands: confidentiality, integrity and identifiability. Based on those demands, high dependable system has provided corresponding security services: encryption/decryption, hash function and digital signature. By assembling these security services in diverse style, system could provide flexible security policies to meet task’s specific security requirement. But security policies incur extra overhead including computing and storage usage, thus they would affect scheduling process unavoidablely and couldn’t be ignored. So we should analyze the security overhead accurately so as to estimate the correct effects on every task [3].

SDFT scheduling algorithm is primarily composed by four core mechanisms, Security Policy Loader, Global Task Assigner, Running State Monitor and Processor Failure Handler. The SDFT supports flexible security policy applied on real time tasks which achieved best fit security level according to its security requirement.

Citations

1. “What Is a Distributed System? - Definition from Techopedia.” Techopedia.com, [www.techopedia.com/definition/18909/distributed-system](http://www.techopedia.com/definition/18909/distributed-system).
2. Sun, Ying-Guang Sun Ying-Guang. “Access Control Method Based on Multi-Level Security Tag for Distributed Database System.” DeepDyve, 12 Jan. 2011, [www.deepdyve.com/lp/institute-of-electrical-and-electronics-engineers/access-control-method-based-on-multi-level-security-tag-for-2Lh60lyy1h](http://www.deepdyve.com/lp/institute-of-electrical-and-electronics-engineers/access-control-method-based-on-multi-level-security-tag-for-2Lh60lyy1h).
3. ping, Xia, and Zhou Xingshe. “Security-Driven Fault Tolerant Scheduling Algorithm for High Dependable Distributed Real-Time System .” Security-Driven Fault Tolerant Scheduling Algorithm for High Dependable Distributed Real-Time System - IEEE Conference Publication, ieeexplore.ieee.org/document/6128471/.