Research Paper Computer Science

Network Security and Concurrency Control

Vishal Goyal | National College Bhikhi(Mansa)

KEYWORDS

Computer Networking
In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

Area Networks
Networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans.

Local area networks (LANs) typically span a single home, school, or small office building, whereas

Wide area networks (WANs) , reach across cities, states, or even across the world.

The Internet is the world's largest public WAN.

Concurrency
Concurrency refers to the ability for a system to run multiple threads of execution "simultaneously".

a) Single Application

- Time division across threads of execution
- Increasing the responsiveness of expensive tasks

b) Across Systems

- Web-sever can process thousands of requests at once
- Database multiple sessions managed on same source
- A way to define them: A "thread base" function
- A way to manage them: Operating System APIs
- A way to share data between them: Shared memory

Methods
Many methods for concurrency control exist. Most of them can be implemented as a main category and in some cases may overlap or be combined, are:

1. Locking (e.g., Two-phase locking) - Controlling access to data by locks assigned to the data. Access of a transaction to a data item locked by another transaction may be blocked (depending on lock type and access operation type) until lock release.
2. Timestamp ordering - Assigning timestamps to transactions, and controlling or checking access to data by timestamp order.
3. Commitment ordering - Controlling or checking transactions' chronological order of commit events to be compatible with their respective precedence order.

Computers are used every aspect of modern life and business. It's use for decision making and controlling important operations without human supervision have made it's entry in both private and public sectors. Tempering of such systems can cause huge damage and hence it becomes critical to understand all the aspects around security threats as well as understand the possible solutions to safeguard and secure the information flow. In particular, we use the firewalls to resolve cases where interleaving of establishment messages can lead to deadlock. Deadlock can be avoided by making security compromises, but we prove that it can be eliminated systematically without such compromises.

What are the security and concurrency associated with networked systems? The focus of this project is Security and Concurrency Management. The scope of the study has been further refined to –the evaluation to security and concurrency associated with networked information systems." The problem being investigated here deals with evaluation of security risks associated with networked systems. As will be seen elsewhere, networked systems are vulnerable to a number of indigenous problems. This project is a systematic attempt to evaluate security associated with such systems.

The other aspect of network security and concurrency it is necessary to eliminate the risk of deadlock, it is possible to detect it and run the protocol again hoping it does not occur again. The overhead and complexity of this solution might be acceptable if the problem is a rare, and there are no stringent latency requirements. Yet history has shown that situations thought to be exceptional during design can become common place when systems are used in unexpected ways, and, in this case at least, one would rather avoid problems by design rather than attempt to recover from them. Here are a few ideas about how to do this.

- Limit the establishment protocol to set up a series of unidirectional associations rather than the bidirectional ones in the given scheme.
- Change the ordering of state changes and message sends and receives.
- Insist that the system obey a client/server assumption so nodes do not simultaneously act as both initiator and responder.
- Use locks to eliminate the problem by coordinating the activities of the establishment initiator and responder processes at the nodes. This might prevent deadlock in the establishment protocol, but it has the effect of simply pushing the problem to the higher-layer protocols that invoked establishment.
- Use a transaction protocol. It is typical to avoid this type of complexity in protocols at the network layer. One hopes for a simpler solution.
- A restricted variation engineers the packet filter processing mechanism so that it only exempts establishment traffic traveling between the initiator and responder from flowing in an association directly between them. This results in a complex packet processing mechanism.

Main objectives of this project are to identify and consolidate the security risks associated with networked systems, and to formulate a methodology to evaluate and categories these risks. The insights gained from the project would form a set of guidelines for designing secure systems, in the form of a structured framework for risk evaluation. Risk management is an

iterative process consisting of well-defined steps which, taken in sequence, support better decision making by contributing a greater insight into risks and their impacts. Using risk management processes and infrastructures that are directed towards the effective management of potential opportunities and adverse effects."

This study of security and concurrency of a systems was carried out because the it is wanted to discover how to evaluate the security associated with networked systems.

REFERENCES

Veysey, S. 2001. —E-commerce risks abound for companies," Business Insurance, Chicago; Apr 9; Vol. 35, Iss. 15; pg. 15 | | Anirban Chakrabarti and G. Manimaran, Iowa State University, "Internet Infrastructure Security: A Taxonomy", IEEE Network | | C. L. Schuba, "Analysis of a denial of service attack on TCP," IEEE Security and Privacy Conference, 1997, pp. 208-223. | http://cnx.org | http://forums.oracle.com | http://java.sun.com |