



Information System Security Operation Intrusion Tolerant Distributed Object Systems

Providing High Reliability for Mission-Critical Information Systems

Overview

Intrusion prevention mechanisms and technologies cannot always prevent a well-funded and persistent adversary from penetrating information systems. Mission-critical systems require intrusion tolerance in order to provide correct system operation even after an attacker has successfully breached the prevention mechanisms. Distributed object middleware is considered the most general kind of middleware, and the Common Object Request Broker Architecture (CORBA[®]) is a widely adopted standard for distributed object middleware.

The goal of the Intrusion Tolerant Distributed Object Systems (ITDOS) framework is to create an architecture for distributed object systems that can provide high reliability for mission-critical information systems by tolerating Byzantine (arbitrary) faults in object servers. CORBA systems are one of the potential architectures that can be supported by the ITDOS. From a system-level point of view, the ITDOS provides additional security in the form of a firewall proxy that can monitor Byzantine fault-tolerant multicast (BFTM) messages at the enclave boundary and minimize the impact of certain denial of service (DoS) attacks.

Objectives

The objective of the ITDOS framework is to protect against any threats that would cause an observable deviation in expected client or server behavior. The ITDOS relies upon the underlying BFTM protocol to tolerate f simultaneous protocol failures and the voting mechanism to

detect and mask faulty values.

Provided that no more than f simultaneous failures occur, the ITDOS also guarantees service availability, integrity, and communications confidentiality. However, there is a caveat to the confidentiality guarantee. Since symmetric keys protecting the traffic provide confidentiality, a compromised server has access to all of the traffic within groups of which that server is a member, until the keys can be reissued without the participation of the faulty server. Furthermore, an undetected malicious server can leak server state to unauthorized recipients.

While the underlying BFTM protocol provides some defense against DoS attacks against individual replication domain elements, it is not resilient against unrestricted DoS attacks on the network. The ITDOS firewall proxy helps mitigate network attacks from external sources, but cannot eliminate the threat from internal hosts.

System Model

The concept of operations for the ITDOS is fairly simple. An ITDOS client invokes an operation on an ITDOS server. The server carries out that operation and returns a result to that client.

The ITDOS modifies the traditional notion of a server, in that it is an asynchronous system of deterministic communicating state machines. That system contains not more than f simultaneously faulty processes and at least $3f + 1$ processes in all. The ITDOS requires a minimum of $3f+1$ replicated state machines to tolerate arbitrary behavior by f state machines. Each state machine in the system is implemented as a server; the server hosts objects for access by clients, which can

This work sponsored by DARPA through Air Force Research Laboratory (AFRL), Contract Number F30802-00-C-0183, with McAfee Research, which is now the Security Research Division of SPARTA..



Intrusion Tolerant Distributed Object Systems

Providing High Reliability for Mission-Critical Information Systems

themselves be servers. Furthermore, each state machine for a given system hosts the same objects as the others in that system. The ITDOS performs voting in middleware to support heterogeneous implementations. Therefore, all invocations on objects must pass through the middleware layer equally.

We term an individual process in the system that implements a particular well-defined state machine, a *replication domain element*. The collection of replication domain elements running the same state machine is a *replication domain*.

The ITDOS uses *active replication* to maintain the same state in each replication domain element; a client request is delivered to each replication domain element in a replication domain by a totally ordered, BFTM protocol. Each replication domain element executes the invocation and returns its result to the client in the same fashion.

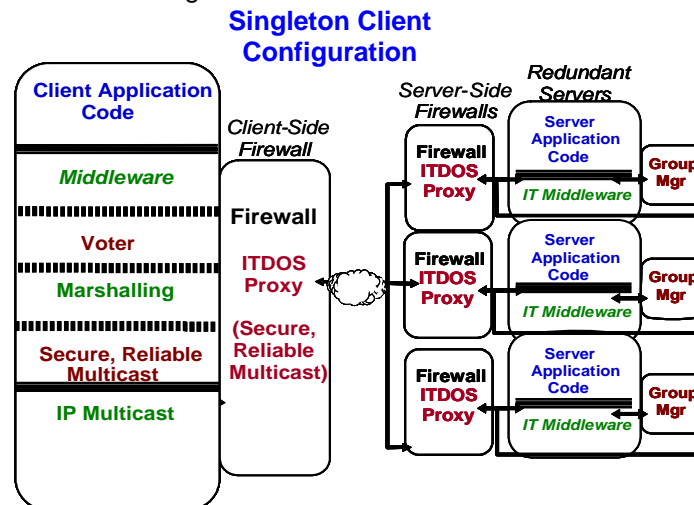
In this system, faulty processes in a replication domain are detected primarily by processes external to it; either by clients receiving a faulty result, or other servers receiving a faulty request. Once a replication domain element is determined to be faulty, it must be removed from its replication domain to preserve confidential communications.

The Group Manager handles replication domain membership and virtual connection management in the ITDOS. It consists of a replication domain of Group Manager processes. These processes work together to

regulate replication domain formation, replication domain membership, and connection establishment between clients and servers. The Group Manager also provides symmetric session keys (called communication keys), that protect communications.

The primary function of the ITDOS firewall proxy is to limit the impact of DoS attacks inside an enclave hosting ITDOS clients and servers. This differs from traditional proxies that form TCP connections on each side of the firewall and then inspect each packet as it traverses the firewall. The proxies typically apply source and destination rules to permit or deny packets. This type of inspection and packet blocking cannot be implemented for the ITDOS for several reasons. First, ITDOS communications are connectionless, using UDP multicast, so source authentication would require digital signature validation. Secondly, the underlying BFTM protocol used by the ITDOS assumes that if one correct process delivers a message, all will eventually deliver it.

This ITDOS proxy allows legitimate retry messages to traverse the firewall while blocking most messages that may be part of a denial of service attack. The firewall limits DoS attacks, particularly replay flooding attacks, by caching a hash of each message it receives and comparing the hashes to newly received copies of a particular message more than a threshold number of times, only a percentage of those messages are allowed to enter the enclave.



For more information call us at 410-872-1515, send an e-mail to ISSO-research@sparta.com, or visit us on the Web at <http://www.issosparta.com/research>.