Parul® University
Vadodara, Gujarat
NAAC GRADE A++

Information and
Communication Technology

Inter-Process Communication & Secure Communication

Prof. Khushal Bhoyar
Department of CSE (Cyber Security)
PIET, Parul University

4.1 IPC Mechanisms and Synchronization

Inter-Process Communication (IPC) enables processes to exchange data and coordinate activities.

IPC mechanisms include:
Shared Memory: Allows processes to access common memory regions for high-speed communication but requires explicit synchronization.

Message Passing: Exchanges data through kernel-mediated messages; simpler to implement but with higher overhead.

Critical Sections: These are code segments that access shared resources and must execute atomically to prevent race conditions.

-cont

Mutual Exclusion ensures only one process enters its critical section at a time.

Mutual exclusion is implemented through:
Peterson's algorithm: A software solution for two processes.
Semaphores: Integer variables with atomic wait/signal operations.
Mutexes: Binary semaphores.
Monitors: High-level synchronization constructs that encapsulate shared data and procedures.

Proper synchronization prevents data inconsistencies and race conditions in concurrent systems.

4.2 Classical Synchronization Problems

The Readers-Writers Problem:
Involves processes accessing a shared data area.
Multiple readers can access simultaneously but writers require exclusive access.
Solutions can prioritize either readers or writers.
Fair solutions prevent starvation of either group.

The Dining Philosophers Problem:
Models processes competing for exclusive access to multiple resources (forks).
Can potentially create circular wait deadlocks.

-cont

Solutions include:

Resource Hierarchy: Numbering resources and always acquiring them in increasing order.

Arbitrator: A central authority managing fork allocation.

Chandy-Misra: A fully distributed solution.

The Producer-Consumer Problem:

Involves processes with asymmetric roles sharing a bounded buffer.

Requires synchronization on buffer access and tracking of empty/full slots.

These problems illustrate fundamental concurrency challenges.

They have practical implementations in database systems, resource managers, and communication buffers

4.3 Security Challenges in IPC

IPC mechanisms introduce **covert channels** that allow unauthorized information transfer through shared resource states.
Timing channels encode information in resource access timing.
Storage channels use shared resource states.

Secure Message Passing must ensure:
Confidentiality: Eavesdropping prevention.
Integrity: Tampering detection.
Authentication: Participant verification.
Non-repudiation: Action proof.

-cont

Threats in Shared Memory include:
Data Leakage: Through residual data in reused memory.
Memory Corruption Attacks: That overwrite adjacent data structures.
Side-Channel Attacks: Extracting information through cache timing or power consumption.

IPC Security Mechanisms include:
Mandatory access control on IPC objects.
Capability-based access.
Encrypted shared memory regions.
Secure channel establishment protocols using cryptographic authentication and encryption.

1. https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs

2. https://www.konverge.co.in/virtualization-in-cloud-computing-need-types-and-importance/

3. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-application-security/

Parul®
University

NAAC GRADE A++

https://paruluniversity.ac.in/