Dynamic Analysis Report - Impl13 (SOCP_Group34)

1. Execution Context

The program executed inside the container using the command: python server/run_server.py. It successfully initialized a secure chat server, generated an RSA-4096 keypair, and registered a unique server UUID:

```
INFO:server.server:Generated new RSA-4096 keypair
INFO:server.server:Server initialized with ID: 12ba774a-6f22-4e81-95c4-eaa67d401b27
```

The server announced itself as SOCP Chat Server v1.3, bound to localhost:8001, and entered its event loop awaiting connections.

2. Network Activity

Network analysis revealed that the server bound only to 127.0.0.1:8001 and [::1]:8001. There were no active external TCP or UDP sessions. The application attempted to connect to bootstrap peers at ws://localhost:8002 and ws://localhost:8003, both of which failed with 'Errno 111: Connection refused'. These attempts demonstrate local peer discovery logic, not external network behavior.

3. System Call Trace (strace_log.17)

System call tracing confirmed safe and expected behavior:

- File operations (openat, read, mmap) for Python imports and log setup.
- Socket() and bind() calls limited to localhost addresses.
- No connect() to external IPs or domains.
- No file writes outside of the project directory.
- No fork(), execve(), or privilege escalation attempts.

The process was terminated gracefully (KeyboardInterrupt).

4. Program Behavior Summary

The SOCP_Group34 implementation represents a local secure WebSocket chat server node. It performs RSA key generation, listens for client and peer connections on localhost, and attempts local peer discovery (ports 8002 and 8003). In the sandbox, peer connections failed due to isolation, as expected. The observed runtime behavior aligns fully with the intended secure chat overlay design.

5. Security Observations

Category	Observation	Severity
Execution Control	Server starts and exits cleanly on interrupt	None
Network I/O	Only localhost sockets; no outbound internet traffic	None

File I/O	Reads only source/config files; no sensitive writes	None
Process Control	No subprocess spawning or privilege escalation	None

6. Overall Assessment

Behavior: Benign — Secure chat server runs within localhost boundaries.

Security posture: Strong — RSA keypair generated internally, no external exposure.

Reliability: Stable — Controlled startup, clear logging, and graceful shutdown.

7. Recommendations

1. For full verification, rerun in a multi-node environment (localhost:8002, localhost:8003) to validate peer handshake and message routing.

2. Maintain --network=none when testing untrusted code to avoid external exposure.

3. Protect key material (RSA private key) by storing only in ephemeral containers.

4. No indicators of compromise or hidden behavior were detected in this version.