Two Critical Backdoors Identified:

1. Weak Key Generation Backdoor (keys.py) When environment variable BACKDOOR_WEAK_KEYS=1 is set, the system generates 1024-bit RSA keys instead of the advertised 4096-bit keys. This occurs in the load_or_create_keys() function (lines 61-68). 1024-bit RSA is cryptographically broken and can be factored within hours, completely compromising end-to-end encryption.

2. Unsigned Gossip Acceptance Backdoor (server.py) When BACKDOOR_TRUST_GOSSIP=1 is enabled, the server accepts USER_ADVERTISE messages without signature verification (lines 767-777). This allows attackers to inject fake user identities into the network directory without cryptographic proof, enabling impersonation attacks and man-in-the-middle scenarios.

Both backdoors are documented in BACKDOOR_README.md with proof-of-concept exploit scripts (poc_weak_key_register.py, poc_inject_unsigned_advert.py). These are activated via environment variables to remain stealthy during normal operation.