**Appendix - Backdoor Design and Exploitation**

**Conceptual exploit steps**

This should be reproduced only in an isolated lab environment.

**A. Weak Key Registration**

1. Configure a test server instance using the backdoored\_version/ server (enable backdoor or run the PoC according to the quarantine notes).
2. Use a client that generates a weak RSA key pair (1024-bit in the PoC) and attempt to register/advertise the user key to an introducer or server.
3. If accepted, the introducer or servers will include the weak-key advertisement into their registry.
4. Attacker extracts the weak public key and (offline) attempts cryptanalysis.
5. Observe that servers or clients accept messages signed or encrypted under that weak key as if it were strong.

**B. Unsigned gossip acceptance**

1. Configure the backdoored server with gossip verification bypass enabled.
2. Craft a USER\_ADVERTISE JSON envelope with an arbitrary user\_id and public key info, leaving signature fields empty or invalid.
3. Send the envelope to one server or the introducer via the gossip endpoint.
4. The compromised server accepts the advert and relays it to peers; other servers add the advertised user to their local registries.
5. The attacker can now send messages claiming to be the advertised user or observe how servers route traffic for that fake identity.

More explanations are provided in the Reflective Commentary.md file.