Invisible Server with Trusted Execution Environment (TEE)
Introduction of Invi-Server

- **Need to protect a mission-critical server from attacks**
  - Mission-critical servers are accessible from the Internet, allowing cyber attackers to engage the targeted server.
  - Difficult to eradicate all the potential vulnerabilities in advance; accessibility to a server can be controlled to minimize the chance of exposing a vulnerable surface.
  - Various methods to control the accessibility are deployed; they are still vulnerable to zero-day attacks.

- **Invi-server: Reducing the attack surfaces by making protected server invisible on networks**
  - A secret server system where a secret server can remain invisible even in the internal network.
  - The key insight of the Invi-server system is to utilize the presence of a public server.
  - We expect the Invi-server system can be an useful tool to create a secret server for a mission-critical operations, which needs be protected from both internal and external attackers.
Components of Invisible server

- Public Server: a server for public service
- Secret Server: a mission-critical server that needs to be secured
- Network Bridge: Authenticates secret client and forwards network packets to either secret or public server
Research Plan for Invi-Server with TEE

- **Improve Invi-server system design**
  - Selection of public servers can be randomized
  - Stealthiness of authentication methods can be improved

- **Employ TEE (trusted execution environment)**
  - When client system is compromised, attacker can access the secret server
    - Protect authentication secret inside client machine
    - TEE can protect the credentials within the Trusted area
    - TEE can be used to store the authentication credentials secure on the secret server - even the administrator of the secret server cannot reveal the authentication credentials