SpaceComputer - Capstone Project Description

Motivation

As society increasingly relies on location-aware applications (e.g., navigation, games, secure access control) and cryptographic security (e.g., authentication, randomness for protocols), combining **proof-of-presence (PoP)** with a **cryptographically strong random number generator (cTRNG)** opens new opportunities. Verifiable location proofs ensure users are truly within defined regions, while cTRNG provides secure randomness for applications such as gaming, access control, and cryptographic key generation. By merging these two components, this project can demonstrate a new class of location-aware secure applications.

SpaceComputer builds a Confidential Computing Platform on satellites in Low-Earth Orbit. It plans to run a dedicated Security services offering to on-Earth users, including Proof-of-Presence, cTRNG, SpaceTEE, and others. Current interaction is through the Earth gateway called OrbitPort, which provides access to cTRNG. For more, navigate to: https://docs.spacecomputer.io/

Project Idea (Core Concept)

A **location-based interactive platform** that:

1. Uses **Bluetooth beacons, WiFi, and GPS (location data source fusion)** to provide *proof of presence* in a physical region. This will mock SpaceComputer's Proof-of-Presence availability in the future.
2. Integrates a **cTRNG service** that generates unpredictable values through a dedicated API + SDK.
3. Demonstrates applications such as:
    - A **Pokémon Go-like mini-game** where rare items can only be unlocked in certain physical locations, secured by the proof-of-presence system.
    - A **lottery or raffle system** where only users present in a region can participate, with the cTRNG guaranteeing fairness.
    - A **secure access control demo** where access tokens are only valid if issued in a region and backed by cTRNG randomness.
4. Some use-case ideas:
    - Presence-Locked Raffles & Loot Drops - Users inside a beacon zone can enter time-boxed raffles; winners are drawn by your cTRNG and accompanied by a public audit trail.
        i. Possible implementation:

1. The “Enter” button is enabled only when the phone verifies the signed beacon challenge.
2. Draws use `commit→reveal` (commit hash of cTRNG seed at start, reveal after).
3. Exportable proof so anyone can recompute winner indexes.

- Location-Gated Game Modes (King-of-the-Hill / Capture)
  i. Control a point only if your team has ≥N devices attested on-site.
- Exam / Contest Integrity Kit
  i. On entering the room, the app obtains presence attestation.
  ii. cTRNG derives each student’s unique test variant seed (same difficulty, different order/items).
  iii. Periodic re-attest to ensure they stayed in the hall.
- Museum/Campus Scavenger Hunt
  i. Each beacon reveals a puzzle seeded by cTRNG (unique per user/day).
  ii. Completing M stations yields a final presence-locked reward token.
- Ticket Anti-Fraud Add-On
  i. At the gate, the app converts a ticket QR into a short-lived on-site token bound to presence; cTRNG issues a one-time verifier code to prevent replay at other gates.

Expected Outcomes

- A **working prototype** that demonstrates both **proof-of-presence** and cTRNG integration in a compelling use case (game, lottery, or access control).
- An **open-source SDK** and **API service** for cTRNG that other developers can reuse.
- A **proof-of-concept validation** that demonstrates the feasibility of location-aware secure applications, using a vector of sensors such as GPS, BT, or WiFi.
- Implement a layered architecture for integrating with various communication endpoints
- Extend RPi (or similar HW) by message integrity protection, e.g., signing of data being transmitted
- Final deliverables: technical documentation, Android mobile/web demo, and project report.
  - Note: iOS/Apple Store is not a must due to the strict deployment process

Technical Ingredients

- **Hardware**: Raspberry Pi boards with Bluetooth acting as signal broadcasters. Provided to you (along with some documentation). Mocks the actual proof of presence capabilities of SpaceComputer.
- **Proof-of-presence module**: Mobile app (Android or cross-platform, with React Native) that verifies presence using beacon signal strength, timestamps, and signed attestations. The module should integrate various sensors i.e. to have access to low-level APIs such as BT (react-native-ble-plx) or Wifi (react-native-wifi-reborn)

- **cTRNG module**:
    - Hardware-based true random number generator (e.g., entropy from sensors, TRNG peripheral on microcontrollers, or OS-provided entropy).
    - API service (REST) exposing randomness to clients.
    - SDK (JavaScript) for easy integration.
- **Integration layer**: Application logic combining proof-of-presence with randomness (e.g., unlocking items, issuing secure tokens).
- **Security aspects**: Digital signatures, potential use of SE-like attestation, and mitigation of beacon spoofing attacks.

Stretch Goals

- Provide **visual gamification elements** for broader appeal.
- Explore **multi-user interactions**, e.g., location-based multiplayer games.
- Mobile phone app extends to iOS

Figure of the component architecture: