SpaceComputer Vision Statement

Project Name: Spacecrypt

Team Name: Spacecrypt

Team:

- Sanil Katula (Team Lead) – sanilkatula@ucsb.edu,
- Yarwin Liu (Scribe) – yarwinliu@ucsb.edu,
- Aryan Chopra – aryanchopra@ucsb.edu,
- Shashank Bhagwani – shashank790@ucsb.edu,
- Karthik Bhattaram – kbhattaram@ucsb.edu,

Mentors:

- Filip Rezabek – filip@spacecomputer.io,
- Amir Yahalom – amir@spacecomputer.io,
- Eason Chai – eason@spacecomputer.io,

Resources and Communication

Github: https://github.com/shashank790/spacecomputer-capstone-project
Meetings: Weekly - as per scheduling availability of mentors and team members
Team Journal: Team Journal
When2meet: https://www.when2meet.com/?32718142-fgSMb

Project Overview

Our team's vision is to push the boundaries of how security and location-awareness intersect in everyday digital experiences. We believe that presence should not only be provable, but also trustworthy and usable in ways that unlock creativity, fairness, and safety. By combining proof-of-presence with cryptographically strong randomness, we aim to create a new class of location-aware secure applications.

Background and Significance

Various applications - from testing software to Pokémon Go - rely on verifying user location. If bypassed, students could take exams from their home, and gamers could cheat by capturing Pokémon from afar. However, by combining the location tracking with cryptography, we can theoretically ensure that locations are true.

Expected benefits include proof of location that cannot be spoofed and a truly random number that cannot be guessed.

Digital Signatures

The security triad has three components - confidentiality, integrity, and availability, and a digital signature guarantees the first two. It works by creating a hash, or 'summary' of the text, and encrypting this with the private key. The message itself is often encrypted as well. A key focus of our project is accessing location data, and digital signatures would be instrumental in safeguarding this information. A MITM, or man in the middle attack, entails capturing data in transit, modifying it, and racing against the sender to deliver a corrupted version of the message to the intended recipient. Now with a digital signature, the hash appended to the message will not match the corrupted version. A raspberry PI might be responsible for verifying the user's location.

Cryptographically Strong Random Number Generators

Pseudorandom number generators are easy to implement and calculate, but have the weakness of producing 'random' numbers in what is really a predictable sequence. If used in a game, this could mean knowing what previous die rolls are means knowing with certainty what the next one will be, which would completely derail the user experience. Now in truly random number generators, the next generated bit is independent of what has been produced previously, and one method of obtaining these is using cosmic radiation. This method is used by Cloudflare, but our system is tamper proof as it is immune to damaged fiber optic cables, earthquakes, and geopolitical incidents.

Problem Statement

Current location-aware applications (e.g., navigation, gaming, secure access control) rely on inadequate trust models. IP address based geolocation often lacks precision, and addresses can be easily spoofed with a proxy. An example of this would be ensuring that test takers are where they claim to be - if someone were to take an exam from their home, cheating might ensue. At the same time, many digital systems depend on weak randomness sources (e.g., pseudo-random generators), which undermines fairness and security in lotteries, raffles, authentication, and key generation. If someone had access to an older encryption key, they might be able to predict the next one. Without a verifiable presence mechanism and a cryptographically auditable randomness source, applications remain vulnerable to fraud, spoofing, replay attacks, and unfair outcomes.

Suggested Approach

We propose to integrate Proof-of-Presence (PoP) with a cryptographically strong True Random Number Generator (cTRNG) into a unified platform:

Proof-of-Presence: Prototype using Raspberry Pi beacons as broadcast devices, combined with a React Native mobile app capable of fusing Bluetooth, WiFi, and GPS signals. Presence will be verified via signal strength thresholds, timestamps, and signed cryptographic challenges to mitigate spoofing.

cTRNG Service: Build a REST API backed by hardware/OS entropy sources, providing unpredictable and auditable randomness. Commit–reveal protocols and digital signatures will ensure results are verifiable by anyone, preventing tampering.

Integration Layer & Demonstrations: Combine PoP and cTRNG to create presence-locked, verifiably fair applications such as:

- Raffles and loot drops are limited to users inside a beacon zone.
- Secure access tokens valid only within verified physical regions.
- Location-based multiplayer game modes (e.g., capture-the-flag).

This approach delivers new cryptographic primitives for location-aware security, alongside reusable SDKs, APIs, and technical documentation, validating the feasibility of a new class of secure, location-bound applications.

MVP and Stretch Goals

Our MVP would be an application that tells you which Raspberry Pi the user is in proximity of. A more developed version of our project would make use of what we’ve built to enable one of the projects we’ve discussed.