Cahier des charges — Projet de Source d’Entropie Aléatoire

Présentation du client

Julien Castiaux est développeur framework chez Odoo. Son intérêt pour la sécurité l’amène à s’intéresser aux problématiques liées à la génération de nombres aléatoires, notamment dans le domaine de la cryptographie et de la sécurité applicative.

Présentation du projet

Le projet vise à concevoir et développer une source d’entropie matérielle permettant de générer des nombres véritablement aléatoires à partir de phénomènes physiques imprévisibles. Cette source sera utilisée comme base de confiance pour des applications nécessitant une génération sécurisée de clés, de jetons ou de données non prédictibles.

Le dispositif sera basé sur une carte microcontrôleur (par ex. Raspberry Pi Pico ou équivalent) et exploitera des phénomènes physiques (bruit électronique, photodiode, effet avalanche, etc. — à déterminer) pour produire des bits d’entropie. L’objectif est de fournir un prototype fonctionnel, documenté et mesurable en termes de qualité d’aléa.

Objectif du client

Mr. Castiaux souhaite disposer d’une solution matérielle fiable et transparente permettant de générer de l’aléatoire de haute qualité pour des usages de développement, de test et de démonstration. L’objectif principal est de valider la fiabilité du générateur et d’obtenir une entropie mesurable, conforme aux standards de sécurité courants.

Cible

- **Utilisateurs finaux :** développeurs, chercheurs et ingénieurs en cybersécurité souhaitant une source d’aléatoire locale et vérifiable.
- **Contexte d’utilisation :** laboratoires, environnements de test, démonstrations techniques ou intégration dans des outils nécessitant un flux d’aléa sécurisé.

Demandes fonctionnelles

Fonctionnalité	Description	Type d’utilisateur	Priorité
F1. Génération d’aléa matériel	Le système doit générer un flux de bits aléatoires à partir d’un phénomène physique non déterministe (p. ex. bruit de diode, fluctuation thermique).	Tous les utilisateurs	Haute
F2. Collecte et traitement de l’entropie	Les signaux bruts doivent être échantillonnés, filtrés et conditionnés (p. ex. SHA-256) pour réduire les biais.	Développeurs	Haute
F3. Évaluation de la qualité de l’aléa	Le système doit fournir des outils ou des méthodes pour mesurer la qualité statistique (p. ex. tests NIST/FIPS).	Développeurs	Moyenne

Fonctionnalité	Description	Type d'utilisateur	Priorité
F4. Exportation de l'aléa	Permettre la récupération du flux d'entropie via USB, sous forme de données exploitables.	Tous les utilisateurs	Haute
F5. Interface de visualisation	Afficher en temps réel le débit, la qualité et les mesures statistiques du flux généré.	Développeurs	Basse
F6. Calibration automatique	Adapter automatiquement les paramètres (gain, seuil, fréquence d'échantillonnage) pour maintenir la qualité du signal.	Développeurs	Basse
F7. Journalisation	Sauvegarder les tests, mesures et logs pour analyses et traçabilité.	Développeurs	Moyenne
F8. Documentation technique	Fournir une documentation claire expliquant le fonctionnement, les limites et la méthodologie de test.	Tous les utilisateurs	Haute

Contraintes

- **Matériel :** utilisation d'un microcontrôleur accessible (par ex. Raspberry Pi Pico ou équivalent).
- **Logiciel :** compatibilité avec un environnement Linux et/ou Windows pour la réception et le traitement des données.
- **Fiabilité :** le générateur doit fournir une entropie mesurable et stable dans le temps.
- **Sécurité :** aucun algorithme pseudo-aléatoire ne doit être utilisé sans conditionnement par de l'entropie physique.
- **Mesure :** conformité visée avec les recommandations NIST SP 800-90B pour l'évaluation des sources d'entropie ; autres référentiels éventuels à déterminer.

Ergonomie

L'ergonomie n'est pas prioritaire. Si possible, elle doit inclure :

- des indicateurs visuels pour signaler la qualité de l'aléa (bon, moyen, faible) ;
- un affichage clair du débit et des mesures statistiques (optionnel).

Enveloppe budgétaire

- **Budget matériel estimé :** 50 à 100 € (microcontrôleur, composants électroniques, capteurs).
- **Budget logiciel :** aucun.
- **Temps de développement :** environ 2 à 3 mois de travail à temps partiel.

Planification

Étape	Description	Durée estimée
Analyse et conception	Étude des sources d'aléa possibles, choix du matériel	3 semaines
Montage et prototype	Assemblage du circuit, premières mesures	2 semaines
Développement du firmware	Collecte, traitement et export de l'entropie	3 semaines
Tests et validation	Analyse statistique, ajustements	2 semaines
Documentation	Rédaction et présentation finale	1 semaine

MVP (Minimum Viable Product)

Le MVP correspond à une version fonctionnelle capable de :

1. générer des bits d’aléa à partir d’un phénomène physique ;
2. envoyer les données brutes vers un ordinateur via USB.