Le temps, une mesure physique, mais fléau pour la sécurité

SRIO

Djob Mvondo

Imaginons un problème de prédiction

Vous voulez prédire le chemin effectué par une personne pour se rendre d'un point A à un point B ?

Imaginons un problème de prédiction

Vous voulez prédire le chemin effectué par une personne pour se rendre d'un point A à un point B ?

Est-ce que ce problème devient plus facile si on a le temps parcouru par la personne ?

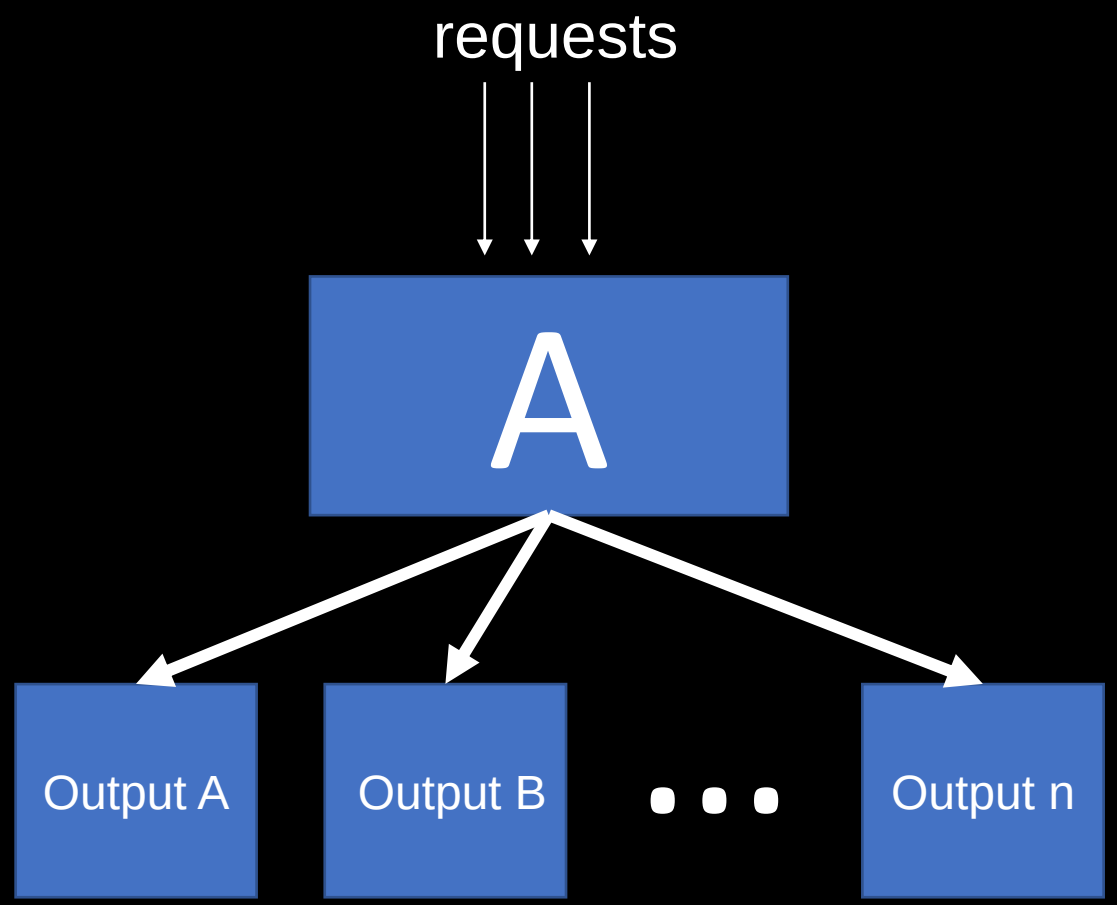
Imaginons un problème de prédiction

Vous voulez prédire le plat qu'une personne a préparer en connaissant son temps de cuisson ?

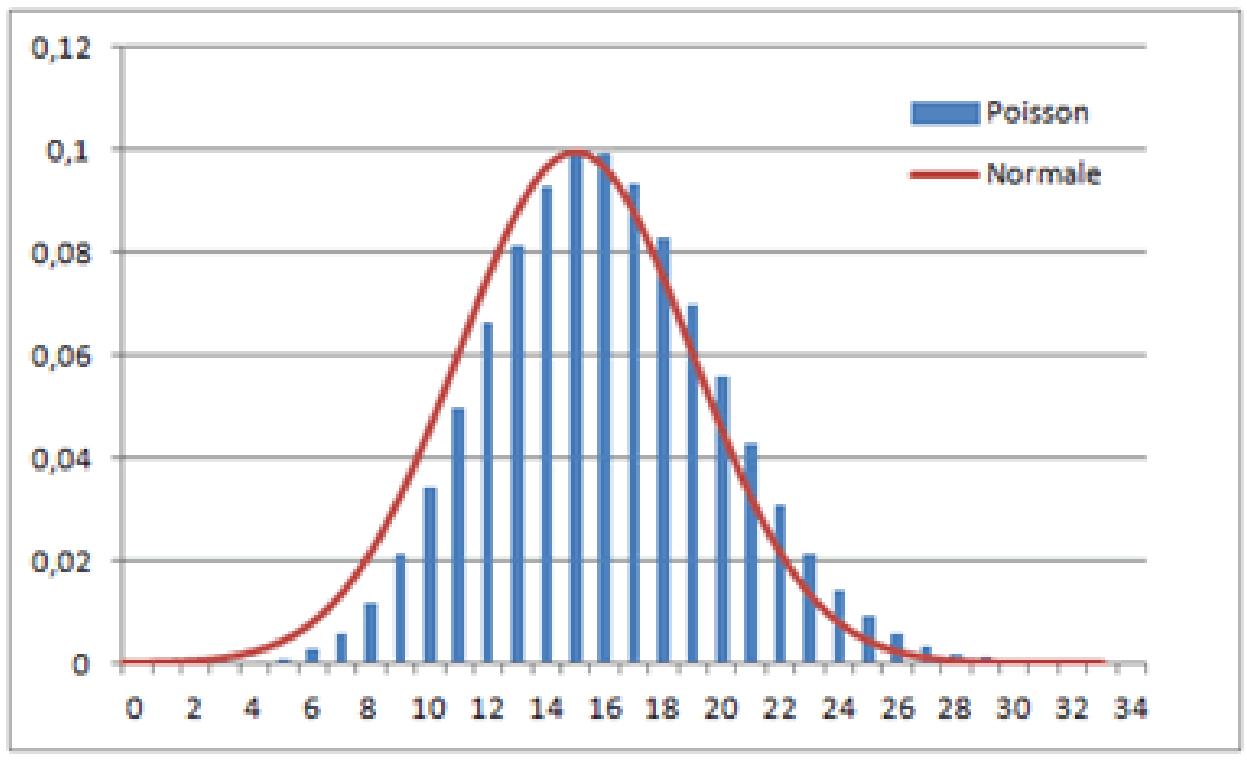
Le temps donne déjà plein d'informations

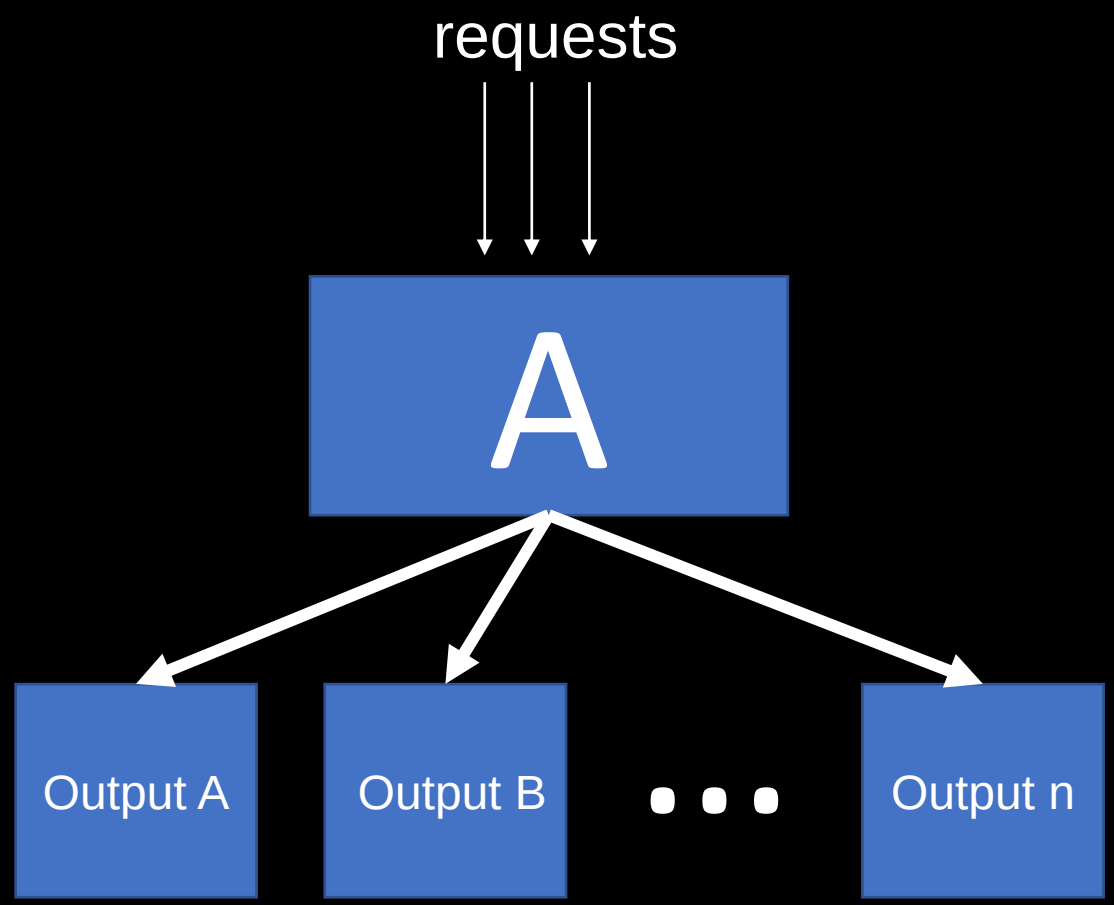
Le temps dans un système informatique

Si j'ai un contrôle sur les requêtes envoyé à A, je pourrais **apprendre** le comportement de A d'un point de vue externe



Le temps dans un système informatique





Ces temps de réponse permettraient de connaitre **les entrées** qui prennent le plus de temps à A et construire un **DDOS ciblé**

Le temps, un fléau, pourquoi ?

Déterminisme par rapport aux entrées	Manipulation des entrées possible	Une infinité de requêtes en entrée
↓	↓	↓
Rendre ses programmes moins déterministes	Standardiser les entrées si possible	Contrôler le débit des requêtes (lois des grands nombres)

Introduire du bruit pour tromper le temps

- Introduire un delai artificiel et aléatoire afin de compliquer la tâche d'un système qui aimerait apprendre.
- Des instructions comme **pause(), sleep(),** ou **une boucle vide**
- Malhereusement, pas de temps négatif, donc obligé de bien modéliser le problème
- Toute une science derrière au nom de **differential privacy** pour protéger les données sensible

Differential privacy

- Introduire un bruit dans un système e.g., une base de donnée, afin d'avoir sensiblement le même résultat sans permettre d'inférer sur les données d'origine.
- Le but est d'affiner ϵ, tel que:

$$\Pr[M(D) \in S] \leq e^{\epsilon}.\Pr[M(D') \in S]$$

- Et que la sensibilité de votre système soit controlé:

$$\Delta f = \max_{\{D,D'\}} ||f(D) - f(D')||$$