



# Crowds

Anonymous  
Web  
Browsing

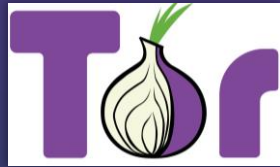
- I. Introduction
- II. Fonctionnement de Crowds
  - 1. Vue générale
  - 2. Aspect technique
- III. Risques \ Désavantages

# Introduction

Collecting personal info



Anonymous browsing  
technics



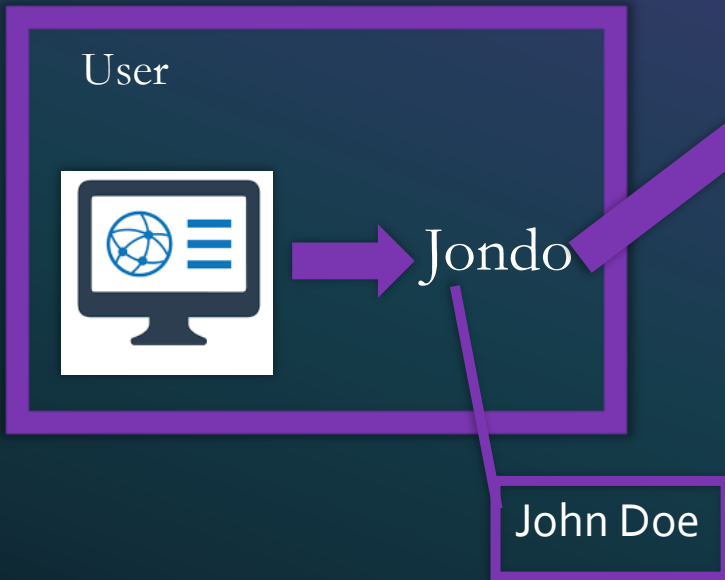
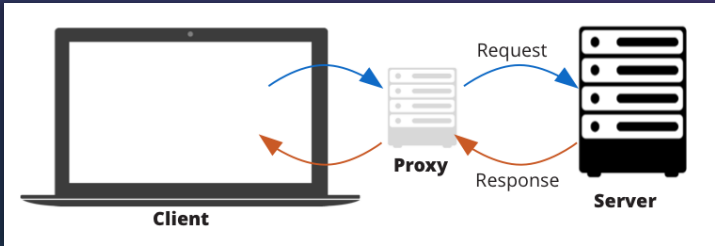
Michael Reiter



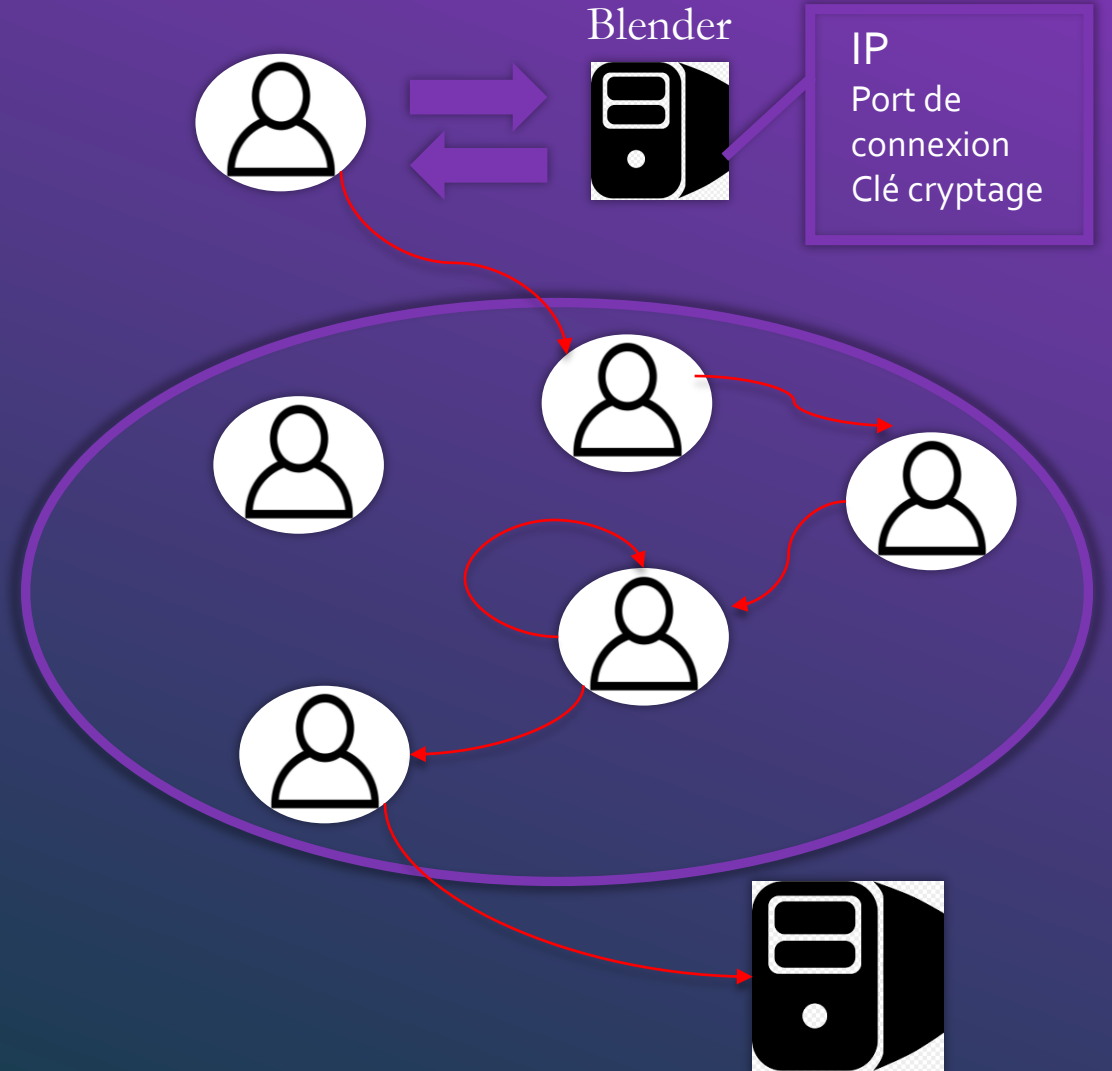
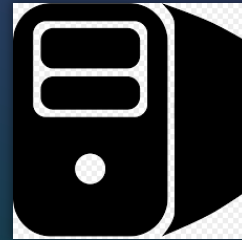
Avi Rubin

# Fonctionnement de Crowds

## Vue générale



# Crowd

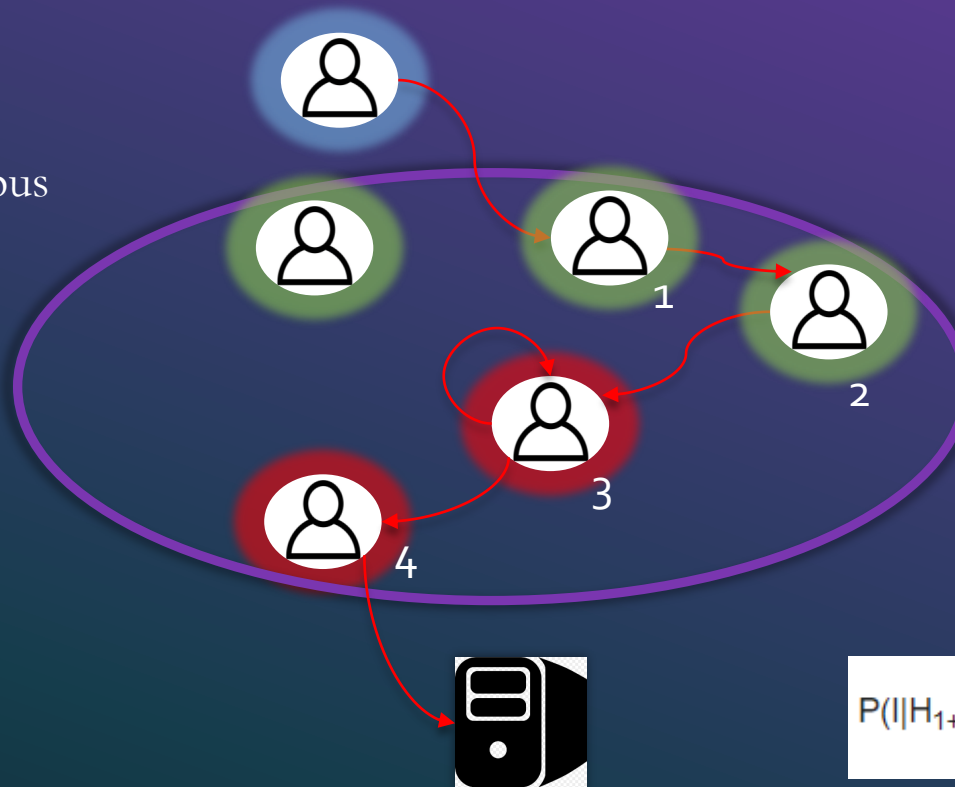


# Fonctionnement de Crowds

## Aspect technique

### Termes importants

- **C** : Collaborateurs corrompus
- **Eavsdropper** : espion
- **P<sub>f</sub>** : Forward probability
- **Probabilité d'innocence**



- **H<sub>k</sub>** ou **H<sub>k+</sub>** : Premier collaborateur à la position K, et Initiateur à la position 0.
- **I** : Initiateur à la position k-1.
- $P(I \setminus H_{1+}) \leq \frac{1}{2}$

$$n \geq \frac{p_f}{p_f - \frac{1}{2}} (c + 1)$$

$$P(I) = \frac{c(n - np_f n + cp_f + pf)}{n^2 - pfn(n - c)}$$

$$P(I|H_{1+}) = \frac{P(I \wedge H_{1+})}{P(H_{1+})} = \frac{P(I)}{P(H_{1+})} = \frac{n - p_f(n - c - 1)}{n}$$

# Risques\ Désavantages

## Risques

- Confidentialité des données
- Applet Java ou ActiveX control



## Désavantages

- Délai supplémentaire
- Type d'anonymat limité
- Interdiction sur certains sites





**Merci de votre attention !**