Bitcoin Anonymity

Mike Fleder  Mike Kester  Sudeep Pillai

"Voodah"  1G6EQwiAfTVyTpK4j3XZ65CvonjDGrPsQ

"darkskypoet"  1QEzohXPbh4ywbzPJATjMBDnSjJsZrZtQ1
Goal & Results

● Attacker Goal
  ○ Tie “real” name to transactions

● Results
  ○ Linked forum user to Silk Road through 1 intermediaries
    ■ bl4kjaguar ⇒ Friend ⇒ Silk Road ⇒ FBI
What is Bitcoin?
What is Bitcoin?

Twitter
“crash_override”
1Agy5BVCxFH134nJxPdAoG h4XLAwbdP

Forums
“voodah”
14hstJKLgss5UHMJqrVz8j P6zvxN6mkuWM
Security Description

● Transactions
  ○ Public Ledger
  ○ Complete history of a coin through ledger

● Software
  ○ Most clients imperfect
Threat Model

- **Attacker Goal:** Tie “real” name to transactions

- **Leak 1:** ("real" name, public key) revealed together
  - Intentional: Forums, donations, social networks
  - Unintentional: Inadvertent leaks

- **Leak 2:** ("real" name, some tx info) revealed together

  "Alice, it’s Bob. I sent you ~$100 at ~noon yesterday"
De-anonymization Pipeline

- Bitcoin key ➔ “real” names
  - Leak 1: Definitively via Forums
  - Leak 2: Statistically via Eavesdropping

Graph Analysis ➔ User Activity Revealed
“I sent you $100 ± $1, yesterday at noon ± 5 minutes”
Graph Analysis Pipeline

Web Scraping (Forums, Social media)

"Casimir1904"
1BSmWFdn1bmmfrBZyW1hJHTwZ
8apg9w99Y

User Activity Revealed

Block Chain Parser

Tx Graph

“Entity” Graph
Bitcoin “Entity” Graph
Bitcoin “Entity” Graph

- Communities
- Untraceable Transactions
- Single Entity
- Large Volume Transactions
  Edge thickness indicates value

PageRank Nodes
- Top 30 nodes
  1st order edges

Typical Transaction Graph for a day
Annotated “Entity” Graph

Revealed User
Bitcointalk.org Forum user

Silk Road Arrest
FBI seized coins sent to a single known public key - Oct 25 2013

PageRank Nodes
Top 30 nodes
1st order edges

Annotated Nodes
40 scraped annotations

Thanks!