Using Online Activity as Digital Fingerprints to Create a Better Spear Phisher

Joaquim Espinhara & Ulisses Albuquerque
JEspinhara@trustwave.com UAlbuquerque@trustwave.com

Agenda

- Introduction
- Motivation
- Background
- HowStuffWorks
  - Our Approach
- µphisher
- Demo
- Future Work
- Conclusion

About us

- Joaquim Espinhara
  - From Aracaju, Brazil
  - Security Consultant at Trustwave Spiderlabs
- Ulisses Albuquerque
  - Coder for offense & defense… as long as it's fun!
  - Lab Manager at Trustwave Spiderlabs

INTRODUCTION

OUR MOTIVATION

Our Motivation

- Why?
- Tools available

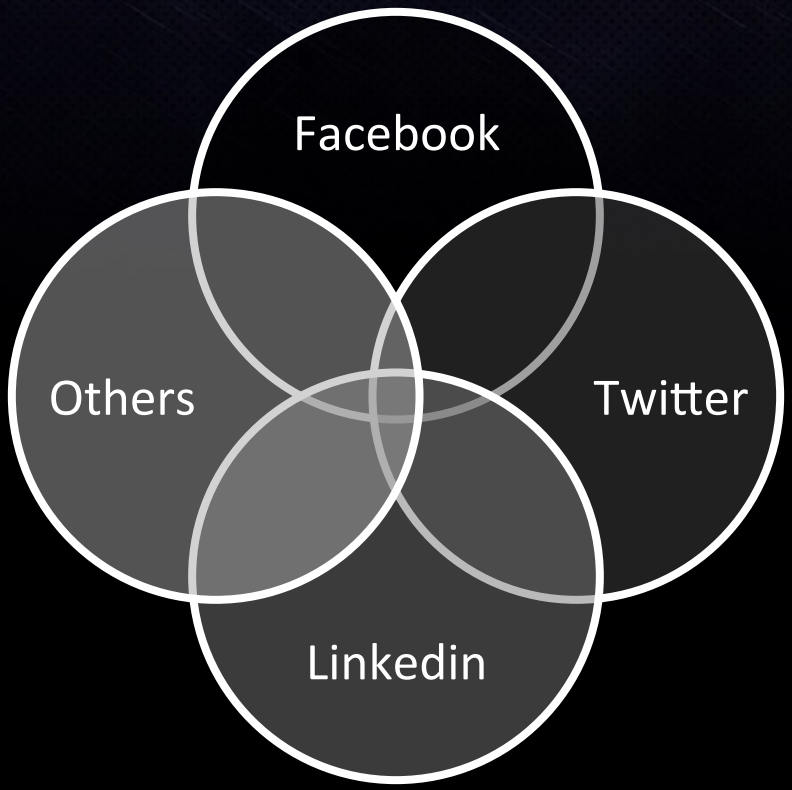
BACKGROUND

Background

- Social Networks
- Social Engineering
- Data Mining
- Natural Language Processing - NLP

Background

- Social Networks



Background

- Social Networks
  - Communication channel for keeping in touch with someone (Facebook, Twitter)
  - Media sharing (Instagram)
  - Specialized networks (GetGlue, TripIt, LastFM)

Background

- Social Engineering
  - Phishing

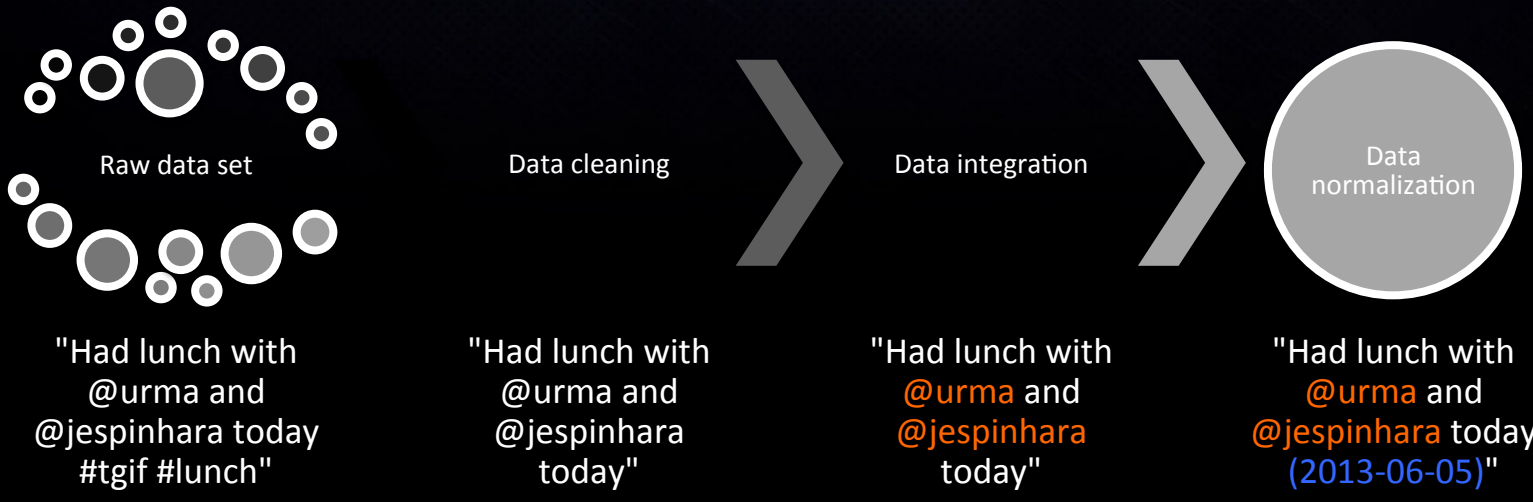
http://www.d00med.net/uploads/0d832c77559a2070a766f899e7efb783.png

Background

- Data Mining
  - What is it?
  - What do you need know about it?
  - How do we use it?

Background

- Data Mining



Background

- Natural Language Processing – NLP
  - What is it?
  - What do you need know about it?
  - How do we use it?
  - Text analysis

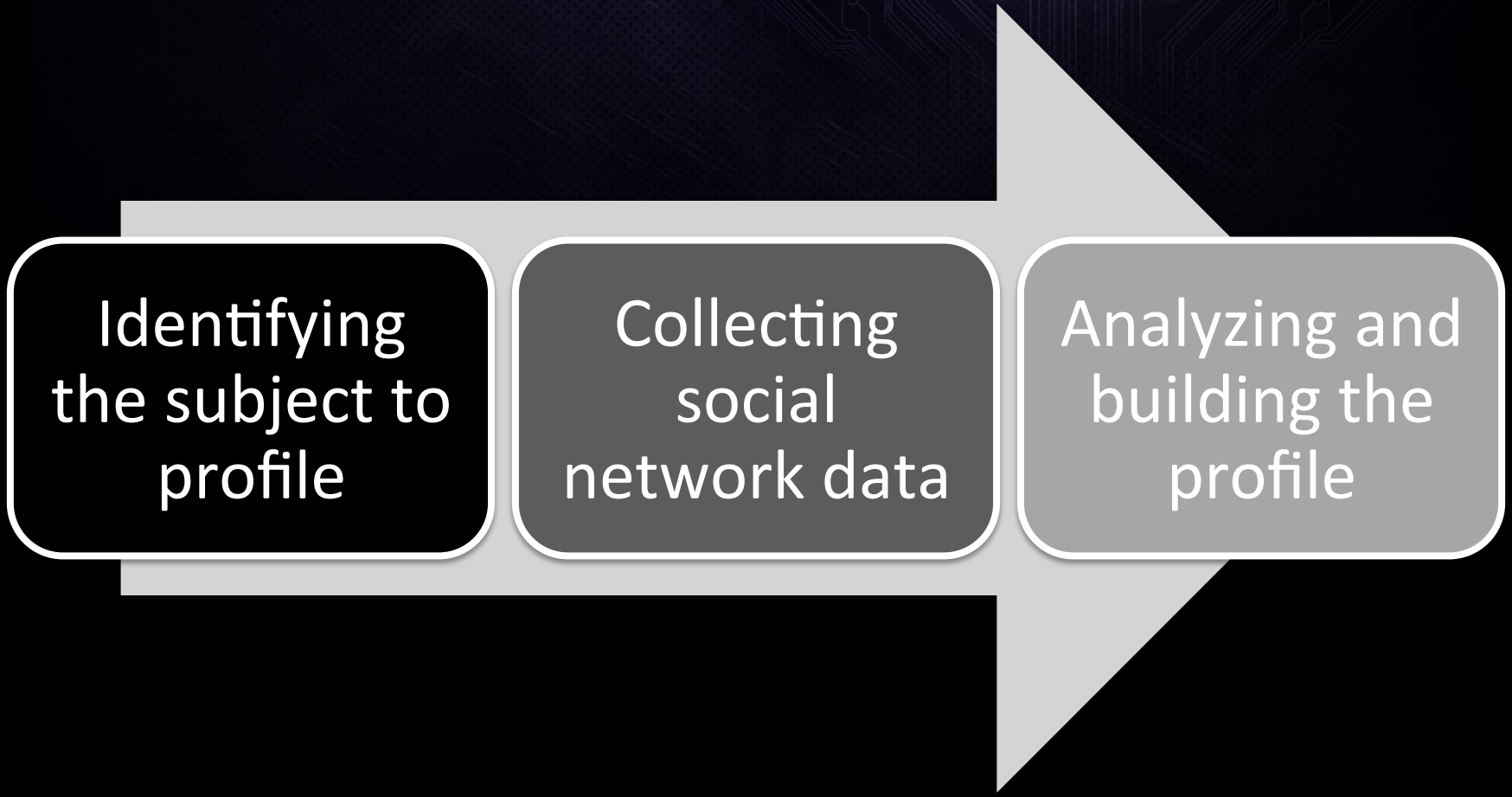
Background

- Natural Language Processing - NLP

http://webu2.upmf-grenoble.fr/sciedu/nlpsl/nlpsl.jpg

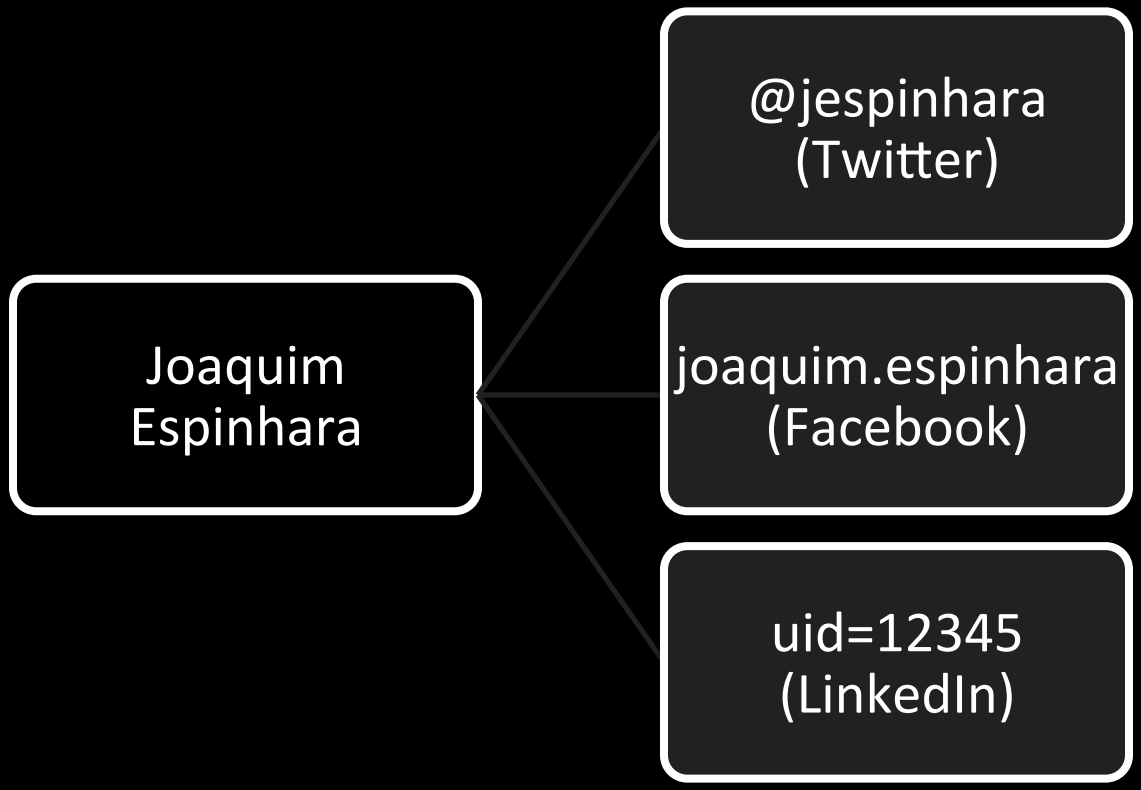
HOWSTUFFWORKS

Our Approach



Our Approach

- The Unknown Subject (*Unsub*)

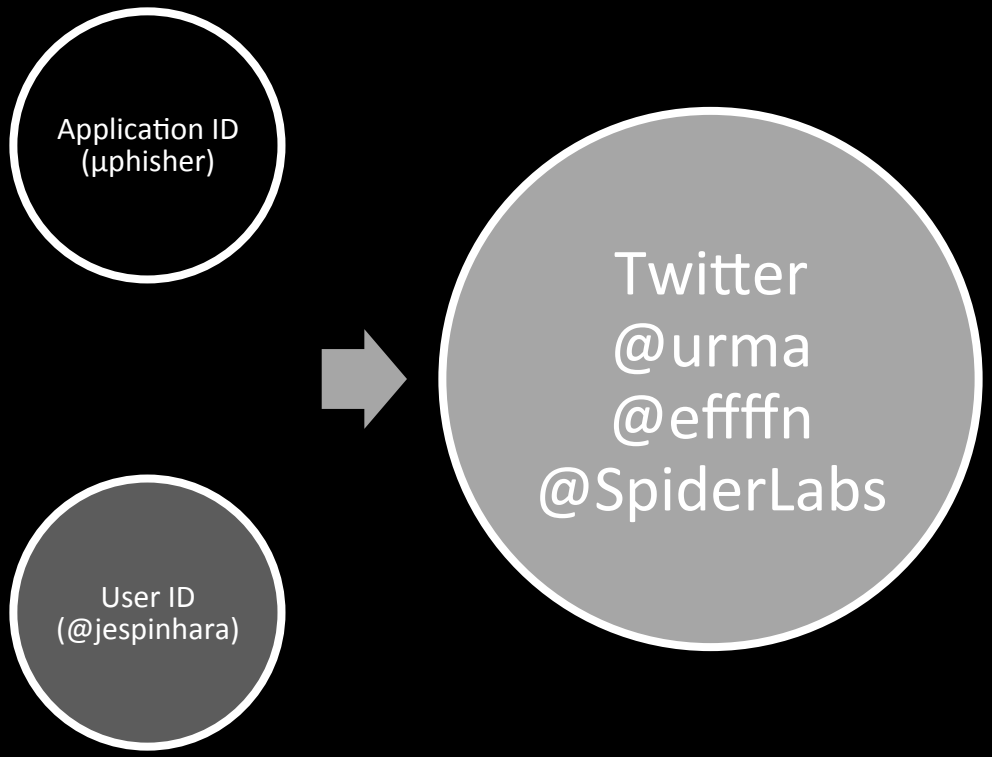


Our Approach

- Data Collection
  - Social Network IDs
  - Official APIs
  - Web Scraping
  - OAuth

Our Approach

- Data Collection - Twitter



µPHISHER

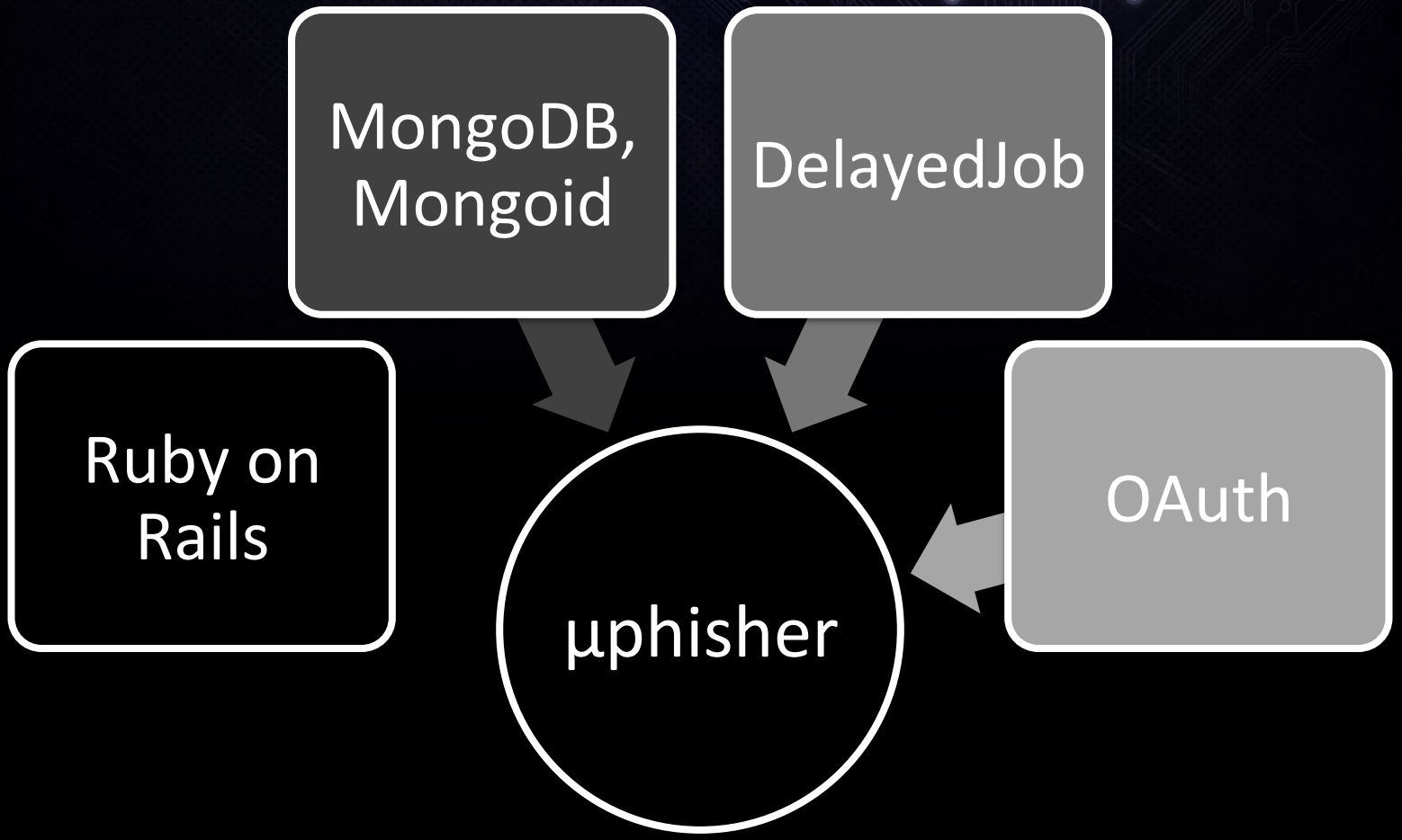
µphisher

- Reference implementation
- Goals
  - Validate potential *unsub* content
  - Assisted textual content input

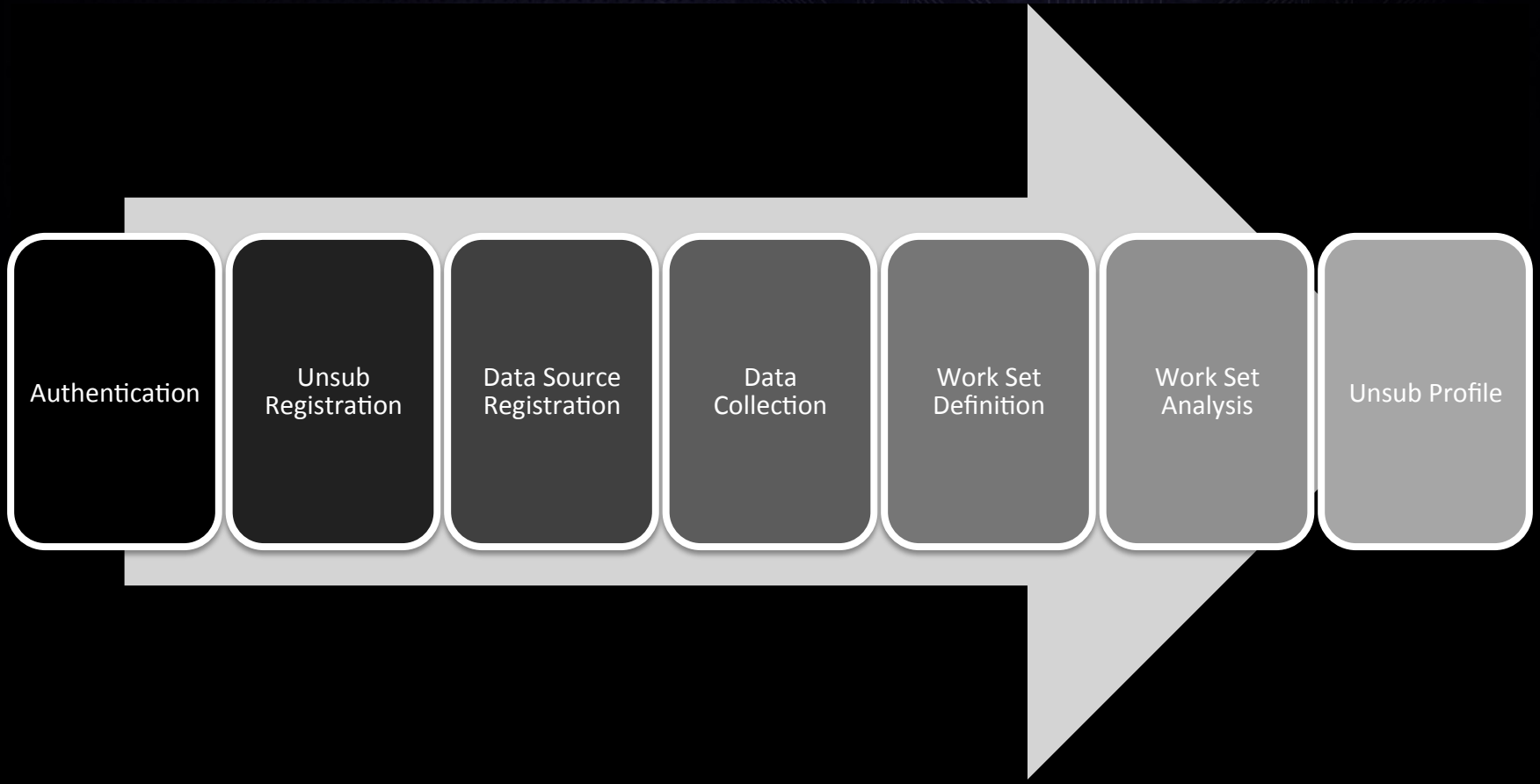
µphisher

- Web Application
- Twitter only (for now)
- Open Source (GPLv3)

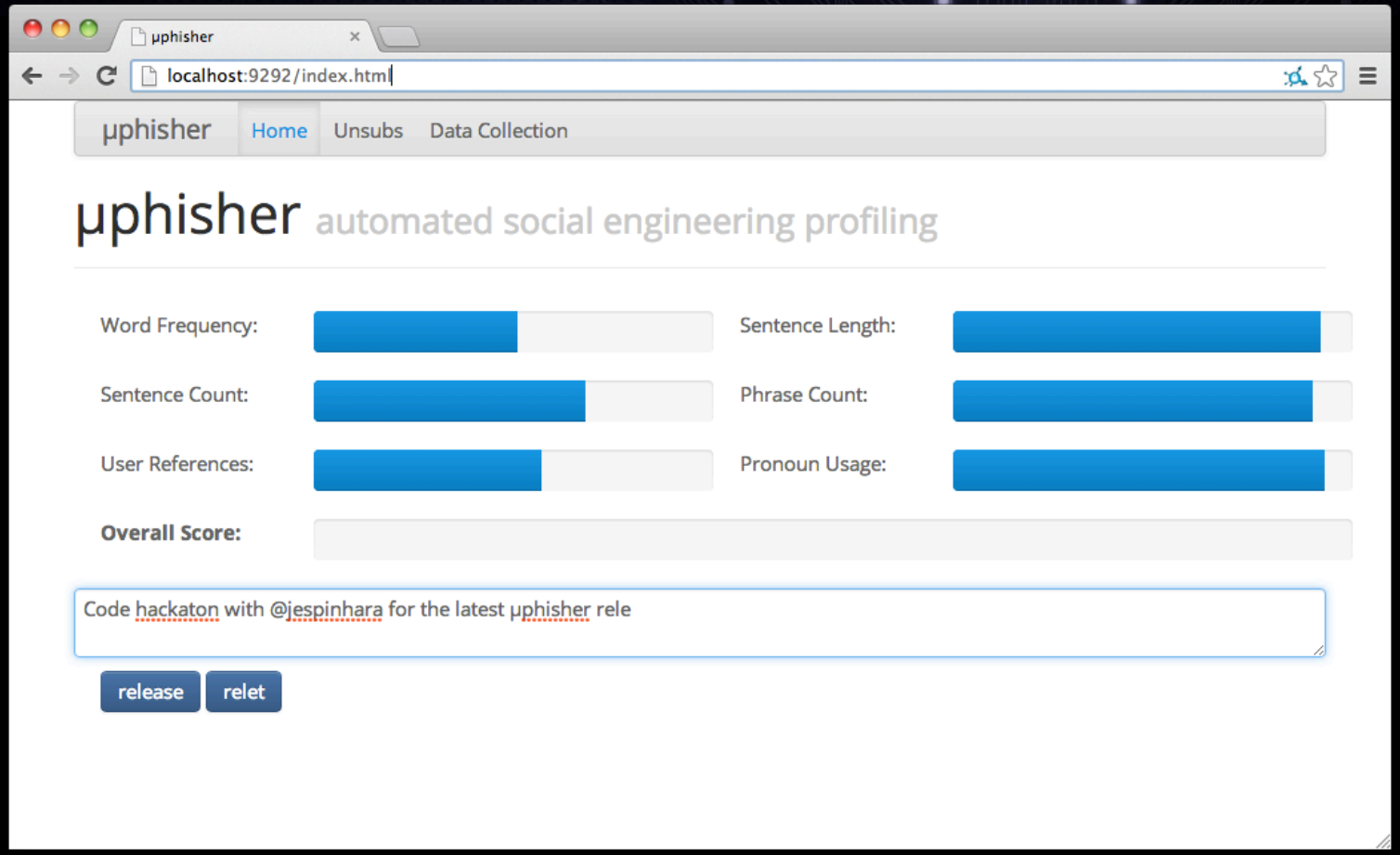
µphisher



µphisher


Authentication
Unsub Registration
Data Source Registration
Data Collection
Work Set Definition
Work Set Analysis
Unsub Profile

µphisher



DEMO
(FINGERS CROSSED)

DOWNLOAD

HTTPS://GITHUB.COM/URMA/MICROPHISHER

Future Work

- Support for additional data sources
- Machine learning
- More metrics and feedback for assisted input

CONCLUSION

THANK YOU!