# On the Semantics of Passwords and their Security Impact

Rafael Veras, Christopher Collins, Julie Thorpe

# Research questions

- What are the semantic patterns of passwords?

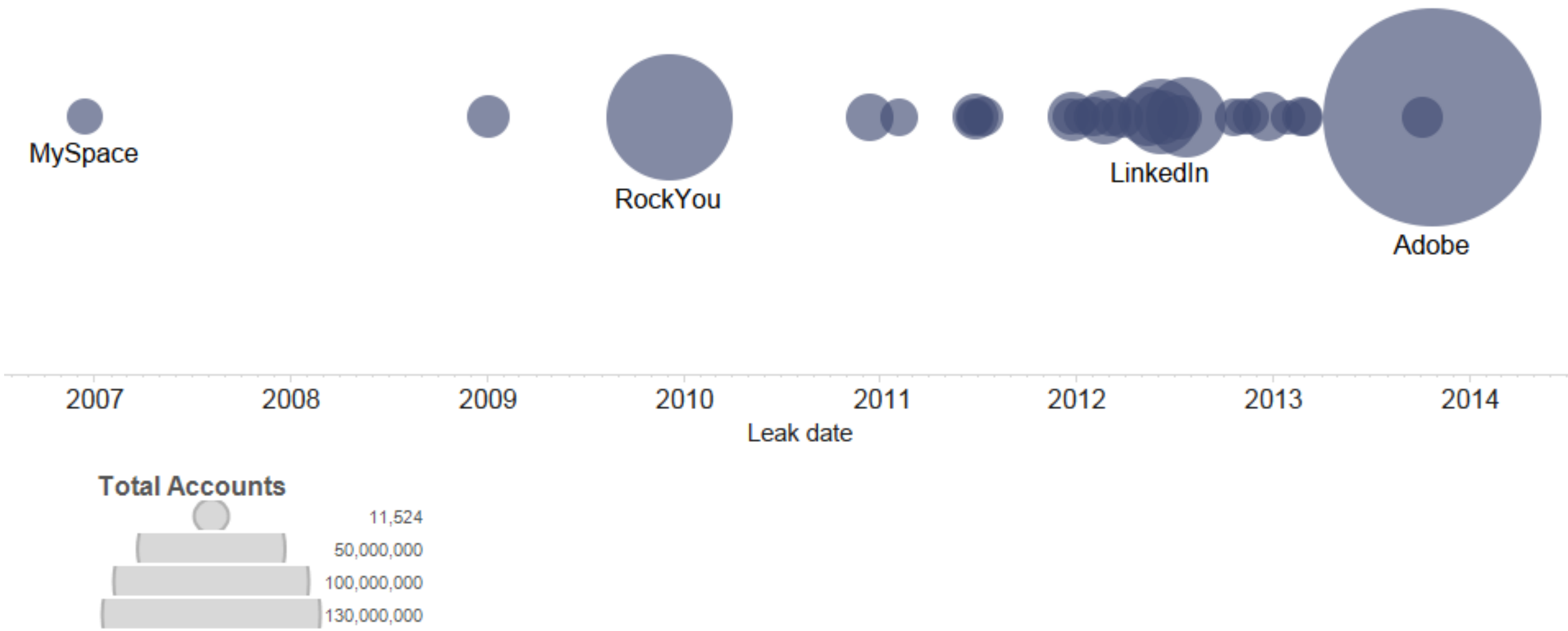
  For example:

  **A male name is 4x more likely to follow “ilove” than a female name.**

- What is their impact on the security provided by passwords?

# Data

A Brief History of Password Leaks



# What is known

Character patterns

*P("thththth") > P("qoqoqo")*

Composition patterns

P("password123") > P("123password")

POS patterns

P(noun) > P(verb) > P(adjective)

Semantics

Self, people's names, birthdays

# Weir approach

mycutecat#1 → $L_9\ S_1\ N_1$

1. $L_9S_1N_1$
2. $L_6D_1$
3. $L_6D_1S_1$
4. $L_3S_1A_4$

↑

**Wordlist**

⇒

boyfriend#3
acanadian$1
chocolate.2
bunnybird-1

# Weir's Limitations

No Grammar

P(mycutecat#1) = P(mycatcute#1)

No Semantics

P(mycutecat#1) = P(mycutepen#1)

# Semantics

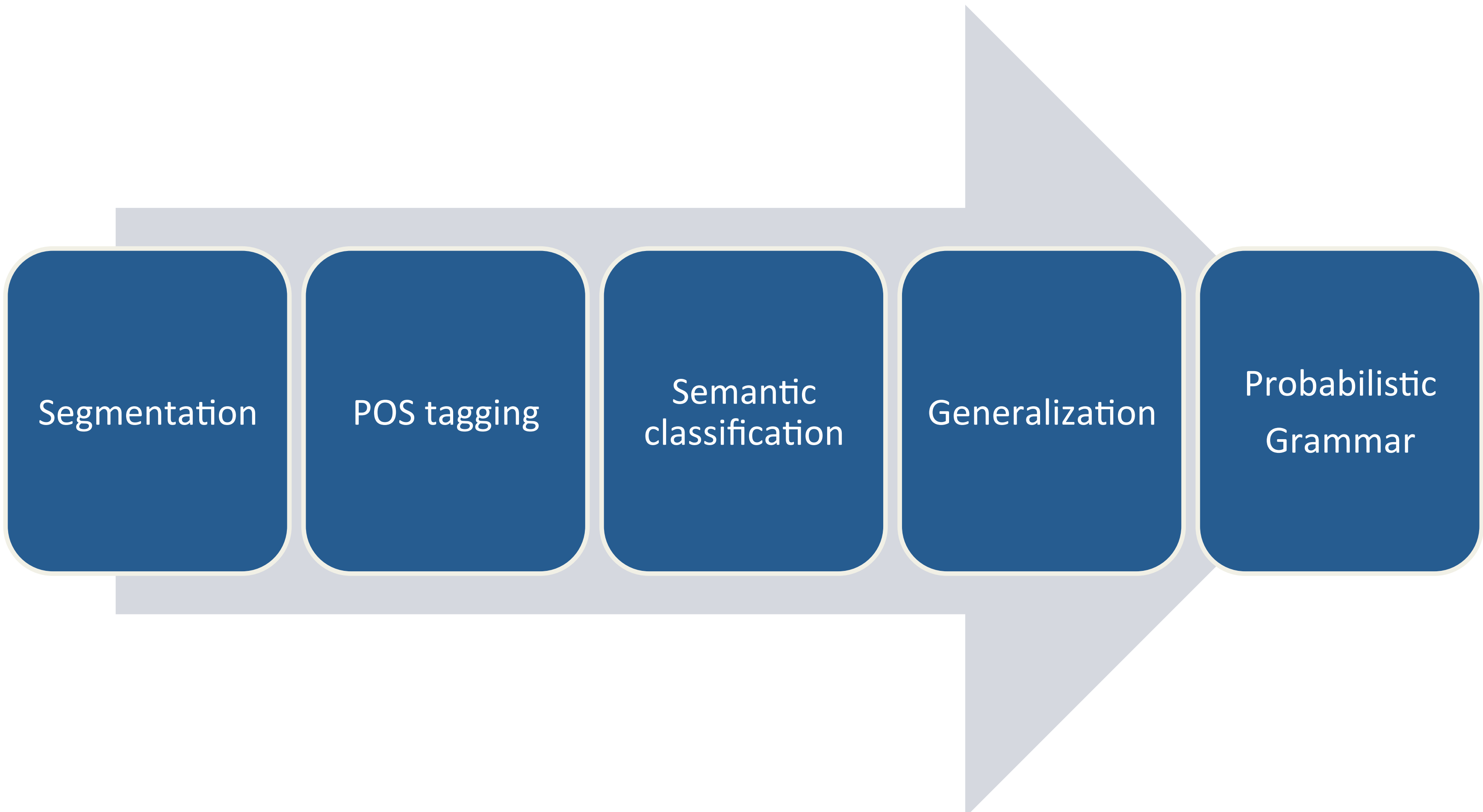
| | Bad |
|---|---|
| 2626 | badboy |
| 1552 | badgirl |
| 854 | badass |
| 466 | badminton |
| 426 | badboys |
| 404 | badman |
| 398 | badger |
| 337 | badboy1 |
| 310 | badgurl |
| 309 | badbitch |
| 260 | badass1 |
| 254 | badazz |
| 244 | badgirl1 |
| 243 | barbados |
| 187 | sinbad |
| 186 | bading |
| 185 | badeth |
| 185 | badboyz |

| | Good |
|---|---|
| 1214 | godisgood |
| 887 | goodgirl |
| 551 | goodies |
| 519 | goodbye |
| 502 | goodluck |
| 425 | goodboy |
| 417 | goodcharlott |
| 293 | 2good4u |
| 247 | goodtimes |
| 192 | lifeisgood |
| 135 | sexisgood |
| 129 | goodman |
| 126 | goodie |
| 124 | goodday |
| 121 | goodness |
| 119 | hellogoodbye |
| 114 | goody2shoes |
| 108 | goodlife |

# Goal

- Semantic model trained with real passwords.
- Assessment of the threat represented by semantic patterns.

# Framework

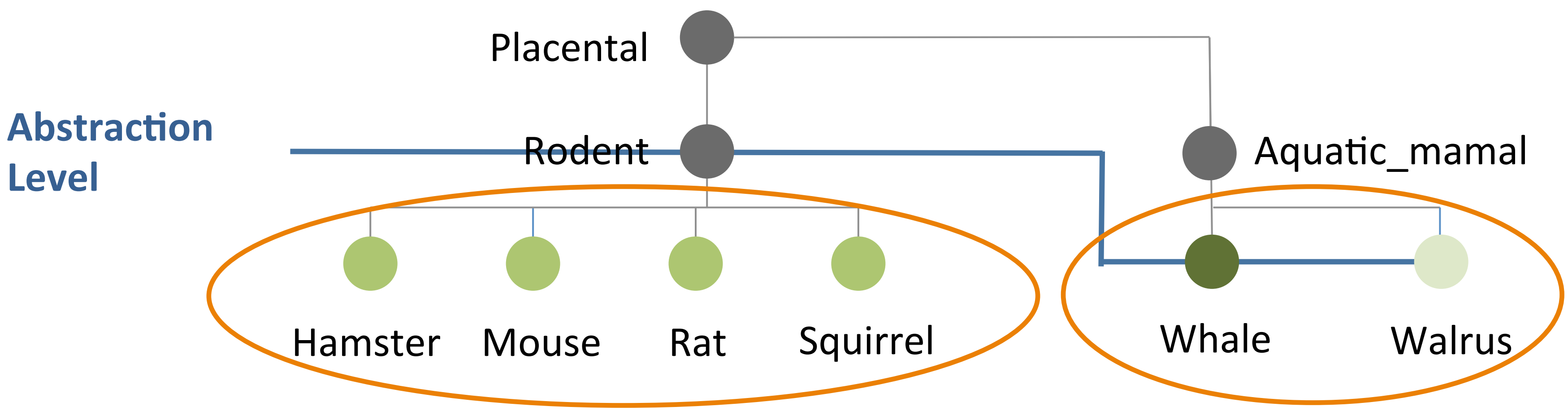

Segmentation
POS tagging
Semantic classification
Generalization
Probabilistic Grammar

# Extracting information

```
carmenredbeagle
```

| | | | |
|---|---|---|---|
| NP (proper noun) | JJ (adjective) | NN1 (sing. noun) | Part-of-speech |
| fem. name | chromatic_color | beagle | Semantics |
| fem. name | color.n.01 | dog.n.01 | Generalization |

# Tree Cut Model



# Probabilistic Grammar

Sample: {iloveyou2, ihatedthem3}

| Semantic Approach | |
|---|---|
| **RULE** | **PROB** |
| N1 → [PP][love.v.01.VV0][PP][number] | 0.5 |
| N1 → [PP][hate.v.01.VVD][PP][number] | 0.5 |
| [PP] → i | 0.5 |
| [PP] → you | 0.25 |
| [PP] → them | 0.25 |
| [love.v.01.VV0] → love | 1 |
| [hate.v.01.VVD] → hated | 1 |
| [number] → 2 | 0.5 |
| [number] → 3 | 0.5 |

| Weir Approach | |
|---|---|
| **RULE** | **PROB** |
| N1 → [$S_8$][$N_2$] | 1 |
| [number] → 2 | 0.5 |
| [number] → 3 | 0.5 |

# Model

- Probabilistic

  P(Rodent) = ?

- Encode Relationships

  [Love]↔[Rodent]

- Generality

  Squirrel, Rat, Mouse → Rodent

  Rodent → Squirrel, Rat, Mouse, **Hamster**

# Popular semantic entities

**Top 10**

1. male name
2. female name
3. city
4. surname
5. be
6. love (verb)
7. love (noun)
8. baby
9. month
10. girl

**Sexual terms**

29. sleep_together
34. lover
54. sexual_activity
69. kiss

**Royalty**

25. princess
59. lady
60. king

**Animal**

33. dog
36. cat
37. monkey
92. bug
96. dragon
100. butterfly

**"Dirty"**

40. bitch
70. buttocks
72. crap

**Food**

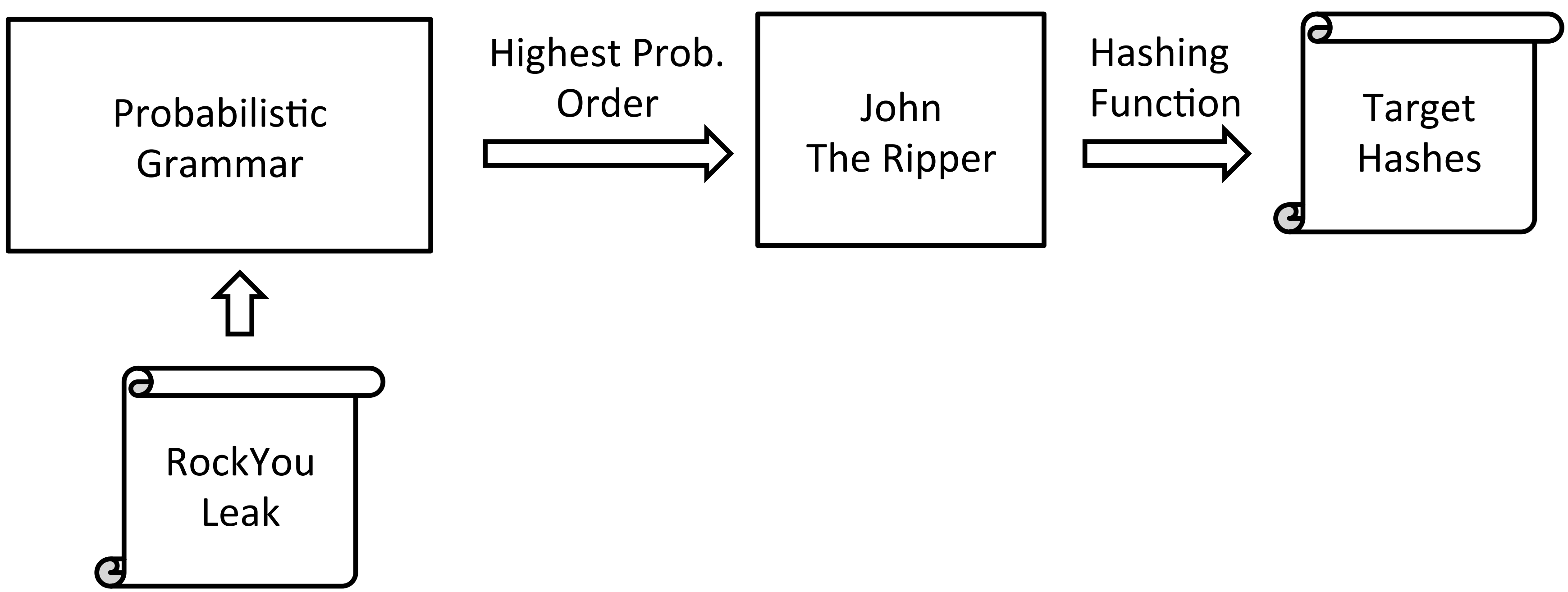
61. honey
66. pie
76. starches
82. cocoa
93. candy

# Base Structures (Patterns)

01. [number]
02. [female_name]
03. [male_name][number]
04. [female_name][number]
05. [male_name]
10. [city]
12. [adjective][number]
13. [city][number]
14. [adjective]
19. [month][number]
20. [surname]
26. [surname][number]
27. [NN_password.n.01]
28. [PPSS][VB_s.love.v.01][PPO]
41. [NN_s.love.n.01][number]
45. [country]
47. [PPSS][love.v.01][male_name]
115. [woody_plant.n.01][number]
126. [baby.n.01][girl.n.01][number]
138. [sleep_together.v.01][PPO]
146 .[PPSS][love.v.01][male_name][number]
157. [JJ][male_child.n.01]

# Experiments

Test how many passwords of an unforeseen leak are explained by the model.



# Protocol

- Off-line attack carried out by John The Ripper (JtR)
- 3 billion guesses
- Metric (platform/implementation-agnostic)

  % of passwords guessed

  avg. guesses/hit

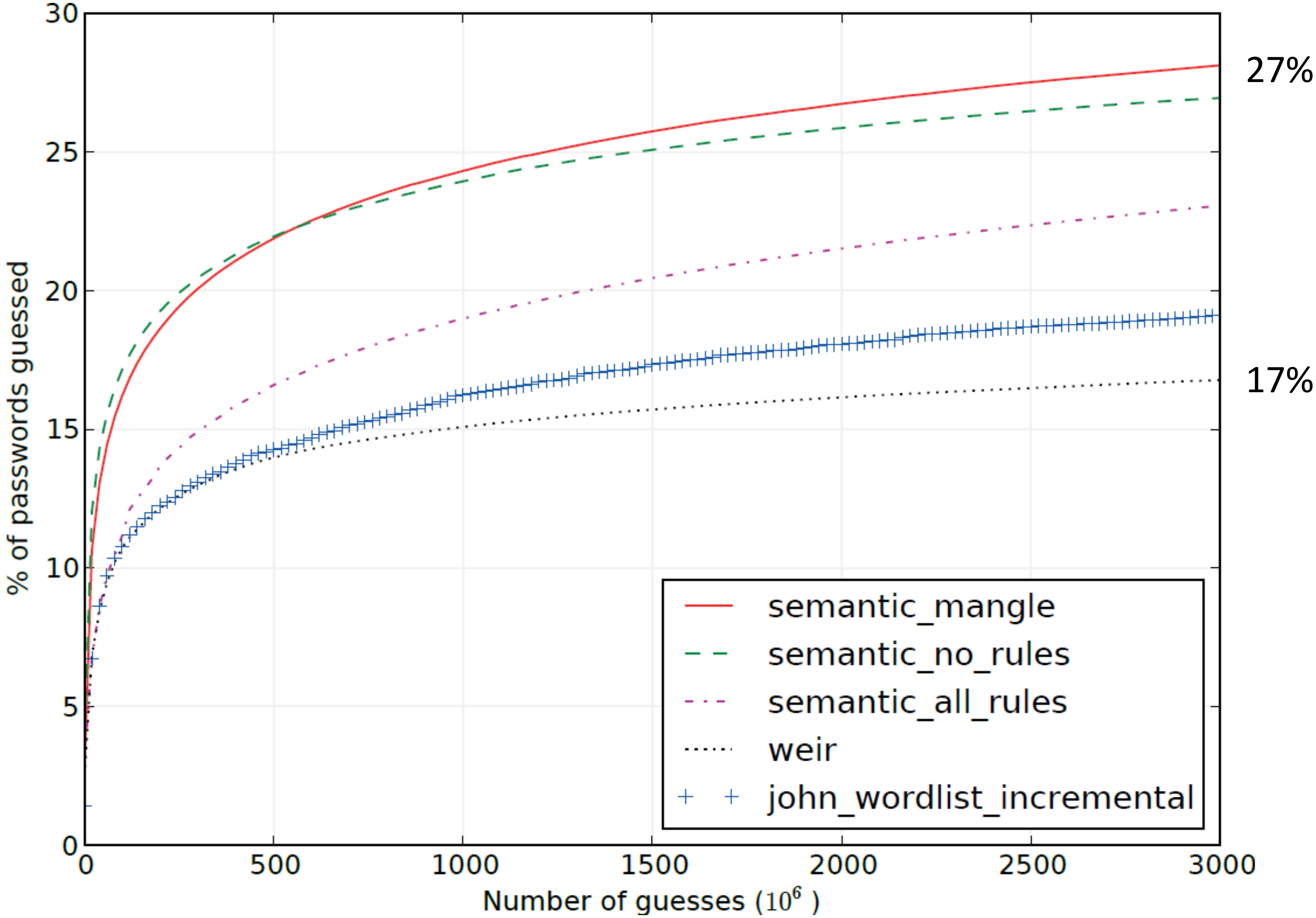
# Protocol

- Three variations of our semantic approach
  1. Lowercase
  2. Custom case mangling
     (e.g., iloveyou, ILOVEYOU, ILoveYou)
  3. JtR's mangling rules
- Weir algorithm trained with RockYou and using dic-0294
- Wordlist (dazzlepod) + JtR's incremental mode

# Experiment I: LinkedIn

- Social network focused on career (#14 globally).
- 5,787,239 unique unsalted SHA-1 hashes.
- Exposed in 2012.

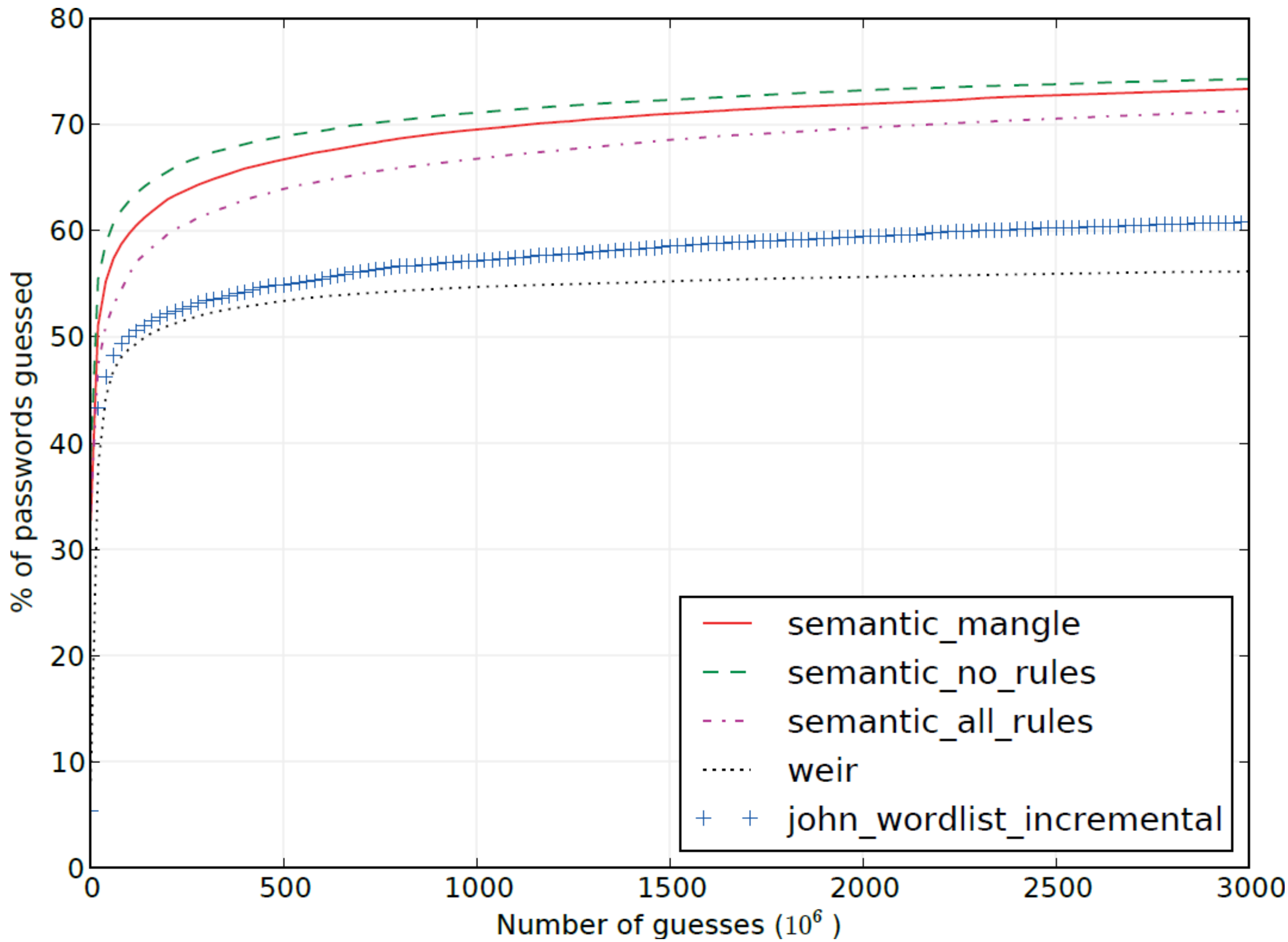
# Experiment I: LinkedIn



# Experiment II: MySpace

- Social network with music emphasis
- Exposed in 2006.
- Collected through phishing.
- 49,655 (41,543 unique) cleartext passwords.

# Experiment II: MySpace



# Final guessing success rate

With a **grammar recognizer**, we can measure the coverage of the grammars over a set of plaintext passwords (MySpace leak):

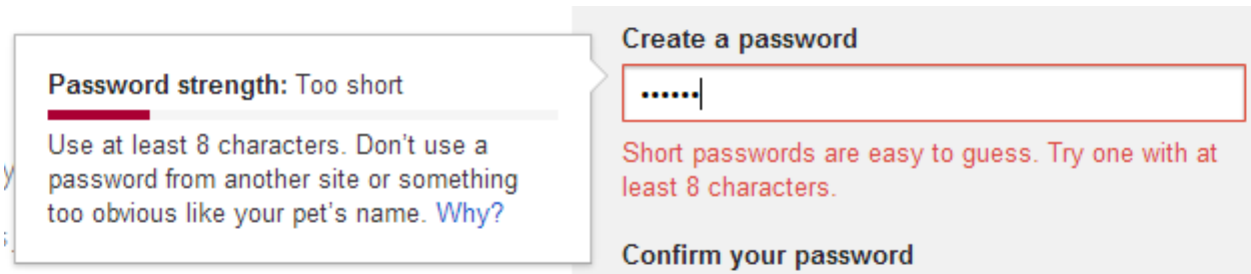
| Approach | Guessed passwords | % |
|---|---|---|
| Semantic | 45,568 | 91.76 |
| Weir | 30,208 | 60.83 |

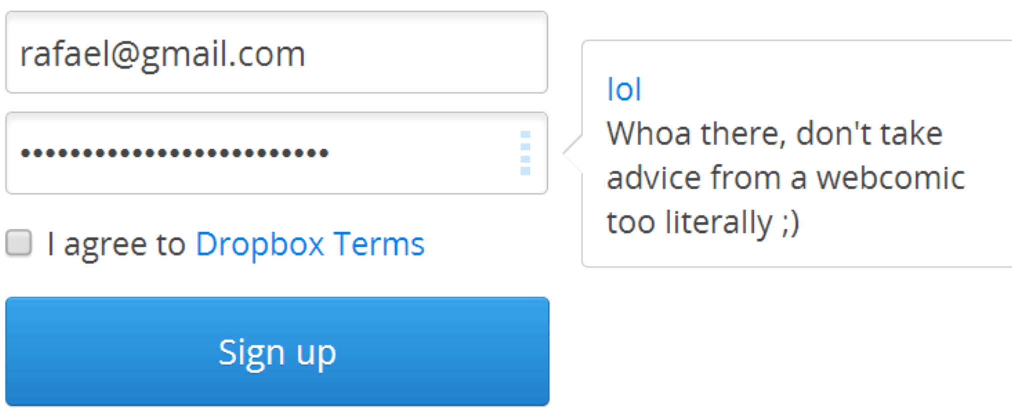
# Conclusion

- Cracking approach more effective than the previous reference approach.
- Semantic patterns are somewhat consistent across leaks.
- Semantic and syntactic patterns put users in higher risk than the current theoretical measures of password security estimate.
- Advance in the understanding of content and the real security provided by passwords.

# Future Work

## Proactive Password Checking



# Future Work

## Anthropological Analysis

A male name is 4x more likely to follow "ilove" than a female name.

# Future Work

Cross-language semantic attacks

To what extent are semantic patterns consistent across different language groups?

# Questions?

http://vialab.science.uoit.ca/

@rafaveguim

# Custom Mangling

| Rule | Count | % |
|---|---|---|
| lowercase | 39,516,827 | 94.09 |
| uppercase | 1,658,417 | 3.95 |
| capitalized | 718,318 | 1.71 |
| mangled | 106,284 | 0.25 |
| Total | 41,999,846 | |

**Statistics on casing of RockYou segments**

| | |
|---|---|
| letmein123 | Lowercase |
| LETMEIN123 | Uppercase |
| Letmein123 | Capitalized |
| LetMeIn123 | Camel case |

**Custom mangling applied to grammar output**

# Performance

| Approach | Guesses/s |
| --- | --- |
| JtR Wordlist + Incremental | 6,172,839 |
| Weir | 963,081 |
| Semantic | 208,333 |

Table 5.5: Average guesses/s against SHA-1 hashes.

# Regression model

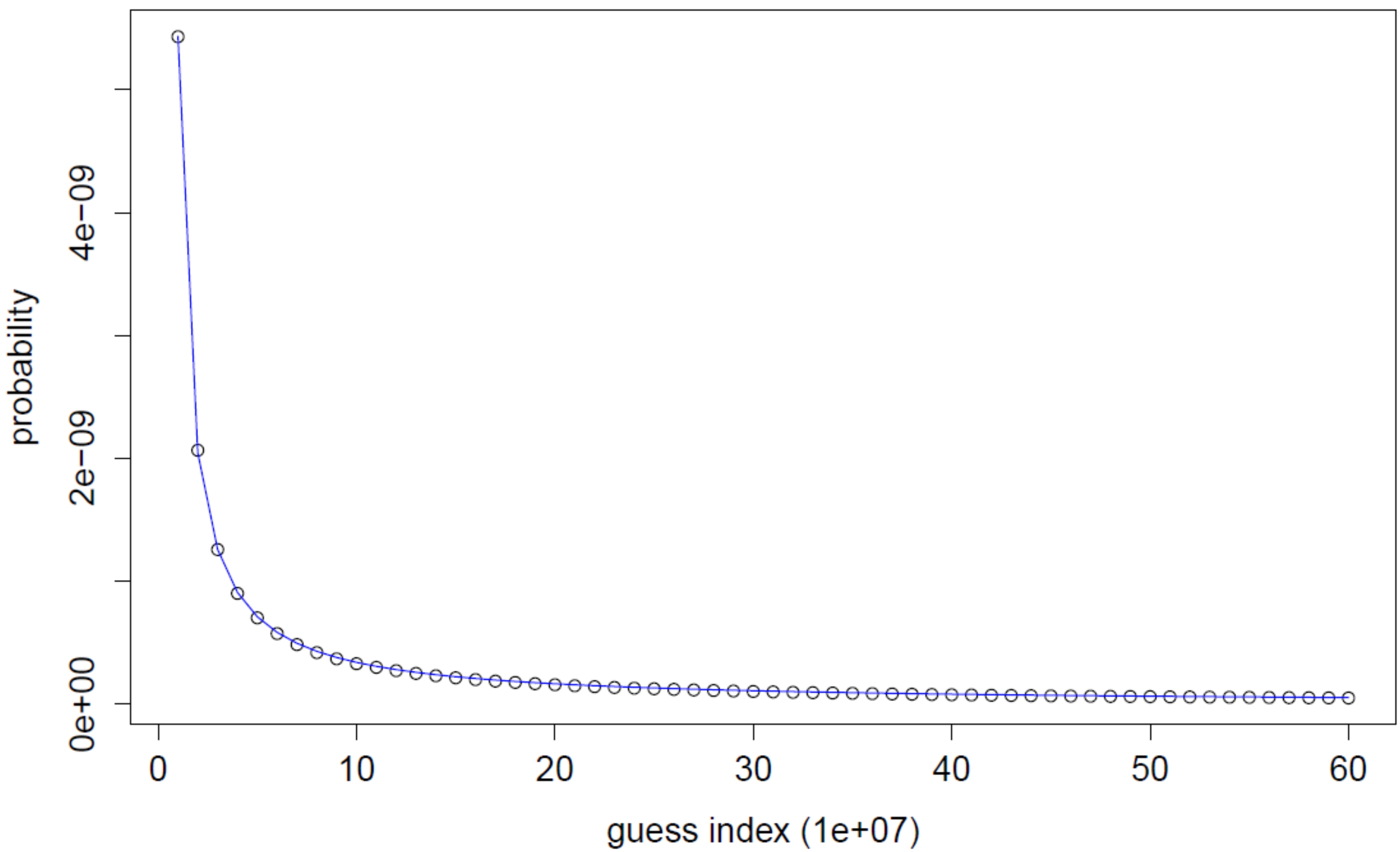


TABLE XII. COMPARISON BETWEEN GRAMMARS GENERATED BY THE SEMANTIC AND WEIR APPROACHES TRAINED WITH THE ROCKYOU LIST, AND A COMPARABLE BRUTE FORCE ATTACK. ⋆ SEE SECTION V-C FOR DESCRIPTION OF APPROXIMATION METHODS AND BRUTE FORCE COMPARISON.

| | | | | | MySpace attack | |
|---|---|---|---|---|---|---|
| Approach | Base structures | Non-terminals | Terminals | Terminal Struct. | Guessed passwords (%) | Approximate # of guesses ⋆ |
| Semantic | 1,861,821 | 12,410 | 4,045,458 | $1.3 \times 10^{86}$ | 91.76 | $4.8 \times 10^{11}$ |
| Weir | 78,126 | 166 | 3,554,133 | $1.8 \times 10^{73}$ | 60.83 | $8.2 \times 10^{9}$ |
| Brute force (until same percentage guessed as Semantic) | | | | | 91.76 | $3.2 \times 10^{43}$ |