GAME OF MISSUGGESTIONS
Semantic Analysis of Search-Autocomplete Manipulations

Peng Wang¹, Xianghang Mi¹, Xiaojing Liao², XiaoFeng Wang¹, Kan Yuan¹, Feng Qian¹, Raheem Beyah³

Indiana University Bloomington¹
William and Mary²
Georgia Institute of Technology³

NDSS 2018, San Diego
Autocomplete
Autocomplete

How predictions are made
https://support.google.com/websearch/answer/106230
Winter is here
Winter is here

promotion target
Autocomplete Manipulation

pollute search logs

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Country</th>
<th>Supported Platforms</th>
<th>Cost</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affordable Reputation Management</td>
<td>USA</td>
<td>Google, Bing, Yahoo!, Amazon etc.</td>
<td>$370 / m</td>
<td>1 - 3 months</td>
</tr>
<tr>
<td>Search Reputation</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$1,200 / m</td>
<td>3 months</td>
</tr>
<tr>
<td>Google Autocomplete Changer</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$2,500 (fixed)</td>
<td>3 months</td>
</tr>
<tr>
<td>Seopmb</td>
<td>China</td>
<td>Baidu, Sogou, 360</td>
<td>$1 ~$20 / d</td>
<td>1 month</td>
</tr>
<tr>
<td>iXiala</td>
<td>China</td>
<td>Baidu, Sogou, 360, Taobao etc.</td>
<td>$2 ~$12 / d</td>
<td>3 - 15 days</td>
</tr>
</tbody>
</table>
Autocomplete Manipulation

pollute search logs

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Country</th>
<th>Supported Platforms</th>
<th>Cost</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affordable Reputation Management</td>
<td>USA</td>
<td>Google, Bing, Yahoo!, Amazon etc.</td>
<td>$370 / m</td>
<td>1 - 3 months</td>
</tr>
<tr>
<td>Search Reputation</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$1,200 / m</td>
<td>3 months</td>
</tr>
<tr>
<td>Google Autocomplete Changer</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$2,500 (fixed)</td>
<td>3 months</td>
</tr>
<tr>
<td>Seopmb</td>
<td>China</td>
<td>Baidu, Sogou, 360</td>
<td>$1 ~$20 / d</td>
<td>1 month</td>
</tr>
<tr>
<td>iXiala</td>
<td>China</td>
<td>Baidu, Sogou, 360, Taobao etc.</td>
<td>$2 ~$12 / d</td>
<td>3 - 15 days</td>
</tr>
</tbody>
</table>

NDSS 2018, San Diego
Autocomplete Manipulation

- pollute search logs

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Country</th>
<th>Supported Platforms</th>
<th>Cost</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affordable Reputation Management</td>
<td>USA</td>
<td>Google, Bing, Yahoo!, Amazon etc.</td>
<td>$370 / m</td>
<td>1 - 3 months</td>
</tr>
<tr>
<td>Search Reputation</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$1,200 / m</td>
<td>3 months</td>
</tr>
<tr>
<td>Google Autocomplete Changer</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$2,500 (fixed)</td>
<td>3 months</td>
</tr>
<tr>
<td>Seopmb</td>
<td>China</td>
<td>Baidu, Sogou, 360</td>
<td>$1 ~ $20 / d</td>
<td>1 month</td>
</tr>
<tr>
<td>iXiala</td>
<td>China</td>
<td>Baidu, Sogou, 360, Taobao etc.</td>
<td>$2 ~ $12 / d</td>
<td>3 - 15 days</td>
</tr>
</tbody>
</table>

- pollute web content
- compromised websites
- spam hosting webpages

NDSS 2018, San Diego
Autocomplete Manipulation

🔍 pollute search logs

🔍 pollute web content

compromised websites

spam hosting webpages

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Country</th>
<th>Supported Platforms</th>
<th>Cost</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affordable Reputation Management</td>
<td>USA</td>
<td>Google, Bing, Yahoo!, Amazon etc.</td>
<td>$370 / m</td>
<td>1 - 3 months</td>
</tr>
<tr>
<td>Search Reputation</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$1,200 / m</td>
<td>3 months</td>
</tr>
<tr>
<td>Google Autocomplete Changer</td>
<td>USA</td>
<td>Google, Bing, Yahoo!</td>
<td>$2,500 (fixed)</td>
<td>3 months</td>
</tr>
<tr>
<td>Seopmb</td>
<td>China</td>
<td>Baidu, Sogou, 360</td>
<td>$1 ~ $20 / d</td>
<td>1 month</td>
</tr>
<tr>
<td>iXiala</td>
<td>China</td>
<td>Baidu, Sogou, 360, Taobao etc.</td>
<td>$2 ~ $12 / d</td>
<td>3 - 15 days</td>
</tr>
</tbody>
</table>

NDSS 2018, San Diego
Challenges

• Search log analysis
  can only be done by search providers

• Web content analysis
  a thorough study is non-trivial on massive data

Little understanding about the real-world impacts of illicit promotions
Sacabuche

**Search AutoComplete Abuse Checking**

- *first* detection system *without* accessing to search logs
- *novel NLP techniques* achieves highly efficient, accurate and scalable
- *first large-scale analysis* of autocomplete missuggestions
- *first step* to understand the ecosystem of this underground business
Observation

• Semantic inconsistency
  
  trigger: online backup free download
  
  legitimate: ✓ online backup software free download
  
  manipulated: ✗ strongvault online backup free download
Observation

• Semantic inconsistency
  trigger:     online backup free download
  legitimate: ✓ online backup software free download
  manipulated: X strongvault online backup free download

\[ \text{semSim} = 0.96 \]
Observation

• Semantic inconsistency
  trigger: online backup free download
  legitimate: ✓ online backup software free download
  manipulated: X strongvault online backup free download

semSim = 0.96
semSim = 0.43
Sentence Similarity

• Semantic inconsistency
  trigger:
  legitimate:
  manipulated:

- legiti\m overal\m manipul\ed:

\[ \text{semSim}^{=} 0.96 \]
\[ \text{semSim}^{=} 0.43 \]

\[ \text{Sim}^{=} 0.96 \]
\[ \text{semSim}^{=} 0.43 \]

NDSS 2018, San Diego
Observation

• Semantic inconsistency

  trigger: online backup free download

  legitimate: ✓ online backup software free download

  manipulated: X strongvault online backup free download

  legitimate: ✓ norton online backup free download
Observation

• Semantic inconsistency

trigger: online backup free download

legitimate: ✓ online backup software free download

manipulated: ✗ strongvault online backup free download

legitimate: ✓ norton online backup free download
Observation

• Search results inconsistency

missuggestion: **strongvault** online backup free download

trigger: online backup free download

suggestion: **norton** online backup free download
Observation

• Search results inconsistency

missuggestion: stongvault online backup free download

trigger: online backup free download

suggestion: norton online backup free download
Search Results Similarity

- Search results inconsistency

![Graph showing search result similarity]

- Trigger: online backup
- Suggestion: StrongVault online backup free download
- Missuggestion: Norton online backup free download

NDSS 2018, San Diego
Architecture

Game of Missuggestions

NDSS 2018, San Diego
Prediction Finder

GAME OF MISSUGGESTIONS

NDSS 2018, San Diego
Search Term Analyzer

NDSS 2018, San Diego
Semantic Feature example

online backup free download -> **strongvault** online backup free download

• Sentence level similarity

*strongvault* online backup free download VS. online backup free download
Semantic Feature example

online backup free download -> **strongvault** online backup free download

• Sentence level similarity
Semantic Feature example

online backup free download -> **strongvault** online backup free download

• Sentence level similarity

**strongvault** online backup free download VS. online backup free download

phrases
- strongvault online
- online backup
- backup free
- free download

words
- strongvault
- online
- backup
- free
- download
Semantic Feature example

online backup free download -> **strongvault** online backup free download

• Sentence level similarity
Semantic Feature example

online backup free download -> **strongvault** online backup free download

• Sentence level similarity
Semantic Features

• Sentence similarity
\[ F_{ss}(s^a, s^t) = \frac{SK(s^a, s^t)}{\sqrt{SK(s^a, s^a)SK(s^t, s^t)}}, \quad SK(s^a, s^t) = \sum \lambda^2 PK(p^a, p^t) \]
\[ PK(p^a, p^t) = \prod_{i=1}^{\text{len}} WK(w^a_i, w^t_i), \quad WK(w^i, w^j) = \left[ \frac{1}{2} (1 + \cos Sim(w^i, w^j)) \right]^\alpha \]

• Word similarity
\[ F_{ws}(w^a, w^t) = \text{MAX}(\text{AVG}_j(WK(w^a_i, W^i_j))) \]

• Infrequency
\[ F_{if}(w^a, w^t) = \frac{\text{MAX}_j(9 - \log_{10} \text{Freq}(w^t_j))}{\text{MAX}_i(9 - \log_{10} \text{Freq}(w^a_i))} \]
Search Result Analyzer

Game of Missuggestions

Search Result Analyzer
- Manipulation Classifier
- Search Result Feature Extraction

Search Term Analyzer
- Semantic Consistency Classifier
- Semantic Consistency Feature Extraction

Prediction Finder
- Pre-processing
- Suggestion Discovery

NDSS 2018, San Diego
Search Result Features

• Result similarity
  
  \[ F_{rs}(D^a, D^t) = (1 - p) \sum_{d=1}^{\infty} p^{d-1} A(D^t, D^a)^d \]

• Content impact
  
  \[ F_{ci}(w^a, H^a, H^t) = \text{MIN}_i(R(w^a, H^a, H^t)) \]

• Result popularity
  
  \[ F_{rp}(D^a, D^t) = \text{ROB}(AP^a(D^a), AP^t(D^t)) \]

• Result size
  
  \[ F_{rs}(N^a, N^t) = \frac{N^a - N^t}{N^t} \]
Evaluation

• Datasets
  • Badset: 150 missuggestions, 296 result pages
  • Goodset: 300 legitimate suggestions, 593 result pages
  • Unknown set: 114 millions trigger-suggestion pairs, 1.6 millions result pages

• Accuracy and coverage
  • Ground truth: precision 96.23%, recall 95.63%
  • Unknown set: precision 95.4% on 1K suspicious trigger-suggestion pairs

• Performance
  • 1.5s / trigger-suggestion pair
Scope and magnitude

Number of missuggestions on each platform
(G: 0.48%, B: 0.37%, Y: 0.2%)

Categories of the polluted triggers
Scope and magnitude

Number of missuggestions on each platform
(G: 0.48%, B: 0.37%, Y: 0.2%)

Categories of the polluted triggers

<table>
<thead>
<tr>
<th>Trigger Category</th>
<th># of terms</th>
<th># of manipulations</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lending Products</td>
<td>1389</td>
<td>1580/34629</td>
<td>4.13%</td>
</tr>
<tr>
<td>Home Services</td>
<td>17059</td>
<td>16712/413836</td>
<td>2.47%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>3715</td>
<td>3876/93929</td>
<td>2.09%</td>
</tr>
<tr>
<td>Auto Services</td>
<td>3477</td>
<td>3916/92220</td>
<td>1.08%</td>
</tr>
<tr>
<td>Technology</td>
<td>29115</td>
<td>32696/762548</td>
<td>0.91%</td>
</tr>
<tr>
<td>Education</td>
<td>17311</td>
<td>17628/423352</td>
<td>0.81%</td>
</tr>
<tr>
<td>Shopping</td>
<td>30465</td>
<td>32986/773087</td>
<td>0.72%</td>
</tr>
<tr>
<td>Gambling</td>
<td>413</td>
<td>454/10314</td>
<td>0.68%</td>
</tr>
<tr>
<td>Travel</td>
<td>6434</td>
<td>6554/153842</td>
<td>0.48%</td>
</tr>
<tr>
<td>Legal Services</td>
<td>14064</td>
<td>14084/348548</td>
<td>0.55%</td>
</tr>
</tbody>
</table>
Scope and magnitude

Number of missuggestions on each platform

(G: 0.48%, B: 0.37%, Y: 0.2%)

Categories of the polluted triggers

257K polluted triggers

383K missuggestions

<table>
<thead>
<tr>
<th>Trigger Category</th>
<th># of terms</th>
<th># of manipulations</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lending Products</td>
<td>1389</td>
<td>1580/34629</td>
<td>4.13%</td>
</tr>
<tr>
<td>Home Services</td>
<td>17059</td>
<td>16712/413836</td>
<td>2.47%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>3715</td>
<td>3876/93929</td>
<td>2.09%</td>
</tr>
<tr>
<td>Auto Services</td>
<td>3477</td>
<td>3916/92220</td>
<td>1.08%</td>
</tr>
<tr>
<td>Technology</td>
<td>29115</td>
<td>32696/762548</td>
<td>0.91%</td>
</tr>
<tr>
<td>Education</td>
<td>17311</td>
<td>17628/423352</td>
<td>0.81%</td>
</tr>
<tr>
<td>Shopping</td>
<td>30465</td>
<td>32986/773087</td>
<td>0.72%</td>
</tr>
<tr>
<td>Gambling</td>
<td>413</td>
<td>454/10314</td>
<td>0.68%</td>
</tr>
<tr>
<td>Travel</td>
<td>6434</td>
<td>6554/153842</td>
<td>0.48%</td>
</tr>
<tr>
<td>Legal Services</td>
<td>14064</td>
<td>14084/348548</td>
<td>0.55%</td>
</tr>
</tbody>
</table>
Evolution and lifetime

- **71.3%** of newly-appeared missuggestions related to newly-appeared polluted triggers
- **1.9%** of triggers were polluted on average

**Lifetime distribution of missuggestions**
- **39.3%** of missuggestions stay > 30 days
- **34** days vs. **63** days (missuggestion vs. legit.)
Evolution and lifetime

Number of missuggestions over time
- 71.3% of newly-appeared missuggestions related to newly-appeared polluted triggers
- 1.9% of triggers were polluted on average

Lifetime distribution of missuggestions
- 39.3% of missuggestions stay > 30 days
- 34 days vs. 63 days (missuggestion vs. legit.)
Missuggestion content and pattern

• 20% missuggestions related to more than one trigger

“free web hosting and domain name registration services by doteasy.com” related to 123 triggers
Missuggestion content and pattern

- **20%** missuggestions related to more than one trigger

  "free web hosting and domain name registration services by doteasy.com" related to 123 triggers

- **missuggestion grammatical pattern**

<table>
<thead>
<tr>
<th>Pattern</th>
<th># of missuggestions</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>trigger relevant content+target</td>
<td>195,738</td>
<td>phoenix divorce attorney &lt;br&gt;sampair</td>
</tr>
<tr>
<td>target+trigger relevant content</td>
<td>188,238</td>
<td>strongvault online backup free download &lt;br&gt;bd&amp;j - los angeles personal injury lawyers</td>
</tr>
<tr>
<td>target+“ - ”+ trigger relevant content</td>
<td>2,278</td>
<td></td>
</tr>
<tr>
<td>trigger relevant content+by+URL</td>
<td>1,446</td>
<td>custom t shirt design software and application tool by panaceatek.com</td>
</tr>
<tr>
<td>trigger relevant content+from+URL</td>
<td>427</td>
<td>reliable web hosting from webhostinghub.com</td>
</tr>
</tbody>
</table>

Top 5 missuggestion patterns
Missuggestion content and pattern

- 20% missuggestions related to more than one trigger

  "free web hosting and domain name registration services by doteasy.com" related to 123 triggers

- Missuggestion grammatical pattern

<table>
<thead>
<tr>
<th>Pattern</th>
<th># of missuggestions</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>trigger relevant content+target</td>
<td>195,738</td>
<td>phoenix divorce attorney sampair</td>
</tr>
<tr>
<td>target+trigger relevant content</td>
<td>188,238</td>
<td>strongvault online backup free download</td>
</tr>
<tr>
<td>target+&quot; - &quot;+ trigger relevant content</td>
<td>2,278</td>
<td>bd&amp;j - los angeles personal injury lawyers</td>
</tr>
<tr>
<td>trigger relevant content+by+URL</td>
<td>1,446</td>
<td>custom t shirt design software and application tool by panaceatek.com</td>
</tr>
<tr>
<td>trigger relevant content+from+URL</td>
<td>427</td>
<td>reliable web hosting from webhostinghub.com</td>
</tr>
</tbody>
</table>

Top 5 missuggestion patterns
Missuggestion content and pattern

• 20% missuggestions related to more than one trigger

“free web hosting and domain name registration services by doteasy.com” related to 123 triggers

• missuggestion grammatical pattern

<table>
<thead>
<tr>
<th>Pattern</th>
<th># of missuggestions</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>trigger relevant content+target</td>
<td>195,738</td>
<td>phoenix divorce attorney sampa...</td>
</tr>
<tr>
<td>target+trigger relevant content</td>
<td>188,238</td>
<td>strongvault online backup free...</td>
</tr>
<tr>
<td>target+“ - ”+ trigger relevant content</td>
<td>2,278</td>
<td>bd&amp;j - los angeles personal injury lawyers</td>
</tr>
<tr>
<td>trigger relevant content+by+URL</td>
<td>1,446</td>
<td>custom t shirt design software and application tool by panaceatek.com</td>
</tr>
<tr>
<td>trigger relevant content+from+URL</td>
<td>427</td>
<td>reliable web hosting from webhostinghub.com</td>
</tr>
</tbody>
</table>

Top 5 missuggestion patterns
Revenue analysis

• Manipulation service provider
  iXiala
  10K sites request suggestion manipulation
  $54K/week commission earned by manipulation operators
  $515K/week for 465K manipulated suggestions
Discussion

• Limitations
  • adversary can make the manipulations mimic benign ones
  • lack of ground truth, manual efforts involved
Discussion

• Limitations
  • adversary can make the manipulations mimic benign ones
  • lack of ground truth, manual efforts involved

• Lesson learned
  • unpopular targets related to triggers
  • similar keyword patterns
Conclusion

• **first large-scale analysis** of autocomplete missuggestions, and make **first step** to understand the underground ecosystem

• **novel NLP techniques** to build up the first detection system **without accessing** to search logs
GAME OF MISSUGGESTIONS

QUESTIONS & ANSWERS

NDSS 2018, San Diego
Data collection

• Datasets

<table>
<thead>
<tr>
<th>Dataset</th>
<th># of suggestions</th>
<th># of triggers</th>
<th># of result pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badset</td>
<td>150</td>
<td>145</td>
<td>295</td>
</tr>
<tr>
<td>Goodset</td>
<td>300</td>
<td>298</td>
<td>593</td>
</tr>
<tr>
<td>Unknown set</td>
<td>114,275,000</td>
<td>1,000,900</td>
<td>1,607,951</td>
</tr>
</tbody>
</table>

• Validation criteria
  • missuggestion must promote a target whose own reputation cannot make itself stand out in the search results of the trigger
  • missuggestion and its search results conflict with the user’s original search intention
Semantic Consistency Classifier

- 100 missuggestions + 150 legitimate trigger-suggestion pairs
- SVM classification model with 5-folder cross validation
- Precision 94.59%, Recall 95.89%

<table>
<thead>
<tr>
<th>Label</th>
<th>Feature</th>
<th>F-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_{ss}(s^a, s^t)$</td>
<td>sentence similarity</td>
<td>0.597</td>
</tr>
<tr>
<td>$F_{ws}(w^a, w^t)$</td>
<td>word similarity</td>
<td>0.741</td>
</tr>
<tr>
<td>$F_{if}(w^a, w^t)$</td>
<td>infrequency</td>
<td>0.653</td>
</tr>
</tbody>
</table>
Missuggestion Classifier

- 150 missuggestions + 300 legitimate trigger-suggestion pairs
- SVM classification model with 5-folder cross validation
- Precision: 96.23%, Recall 95.63%

<table>
<thead>
<tr>
<th>Label</th>
<th>Feature</th>
<th>F-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_{rs}(D^a, D^t)$</td>
<td>result similarity</td>
<td>0.782</td>
</tr>
<tr>
<td>$F_{ci}(w^a, H^a, H^t)$</td>
<td>content impact</td>
<td>0.808</td>
</tr>
<tr>
<td>$F_{rp}(D^a, D^t)$</td>
<td>result popularity</td>
<td>0.632</td>
</tr>
<tr>
<td>$F_{rs}(N^a, N^t)$</td>
<td>result size</td>
<td>0.745</td>
</tr>
</tbody>
</table>
Evaluation

• Accuracy and coverage
  • Tow-step analysis: precision 96.23%, recall 95.63% on ground truth
  • One-step analysis: precision 97.68%, recall 95.59% on ground truth

• Performance
  • Tow-step analysis: 0.016s/pair (94X faster)
  • One-step analysis: 1.5s/pair