Website Fingerprinting Attack Mitigation using Traffic Morphing

Eric Chan-Tin (Loyola University Chicago¹)
Taejoon Kim (Texas A&M University, Commerce)
Jinoh Kim (Texas A&M University, Commerce)

¹Previously at Oklahoma State University
To: Charlie
To: Charlie

To: Bob

From: Eric

To: Alice
To: Charlie
From: Bob

To: Bob
From: Alice

To: Alice
From: Eric
Tor

- Free, open-source
- 2002
- Anonymity network
- Onion routing
- 2,000,000+ users daily
- 7,000+ volunteers (relay nodes)
Website Fingerprinting Attack

Uses only number of packets, size of packets, and direction of packets
Accuracy

- 80+% accuracy
- Machine learning such as k-NN, SVM, RandomForest
• Padding
  • Every packet has same size
• Delay
  • Same delay
• Extra packets (noise)

• Make every website look similar using traffic morphing
But...

- Hard to make every website on the Internet look similar
Contribution

• Some websites already look "similar"
  • Number of packets
  • Size of packets
• Cluster "similar" websites and make all websites within a cluster indistinguishable
  • Easier to do within a cluster than for ALL websites on the Internet
  • Use traffic morphing
Dataset

- Panchenko et. al., “Website fingerprinting at Internet scale,” NDSS 2016
- 757 unique websites
  - 40 instances each
Proposed Algorithm

- Cluster websites
  - PCA (Principal Component Analysis)
  - 104 features
    - Total number of outgoing packets
    - Total number of incoming packets
    - Total size of all outgoing packets
    - Total size of all incoming packets
    - 100 samples of cumulative packet sizes
- Traffic morph each cluster to make all websites within that cluster indistinguishable
Clustering
Elbow Method
Traffic Morph Method

- **Biggest**
- Make the size of every packet in a cluster be the same size as the biggest packet in that cluster
Experiment Setup

- 50% of dataset for training, 50% for testing
- Repeat 10 times
# Accuracy

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>No defense (Tor)</td>
<td>91%</td>
</tr>
<tr>
<td>CS-BuFLO</td>
<td>22%</td>
</tr>
<tr>
<td>Tamaraw</td>
<td>10%</td>
</tr>
<tr>
<td>WTF-PAD</td>
<td>15%</td>
</tr>
<tr>
<td>Walkie-Talkie</td>
<td>19%</td>
</tr>
<tr>
<td>Our Algorithm</td>
<td>&lt; 1%</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Latency Overhead</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>No defense (Tor)</td>
<td>0%</td>
</tr>
<tr>
<td>CS-BuFLO</td>
<td>173%</td>
</tr>
<tr>
<td>Tamaraw</td>
<td>200%</td>
</tr>
<tr>
<td>WTF-PAD</td>
<td>0%</td>
</tr>
<tr>
<td>Walkie-Talkie</td>
<td>34%</td>
</tr>
<tr>
<td>Our Algorithm</td>
<td>0%</td>
</tr>
</tbody>
</table>
Summary

• Promising research
  • Clustering
  • Traffic morphing within each cluster
• Almost completely mitigates website fingerprinting attacks (<1% accuracy)
• Other methods such as average packet size, random packet size, and closest packet size
Thank you!

Questions?

Eric Chan-Tin, chantin@cs.luc.edu