A Domain-Agnostic Approach to Spam-URL Detection via Redirects

Heeyoung Kwon

Mirza Basim Baig

Leman Akoglu

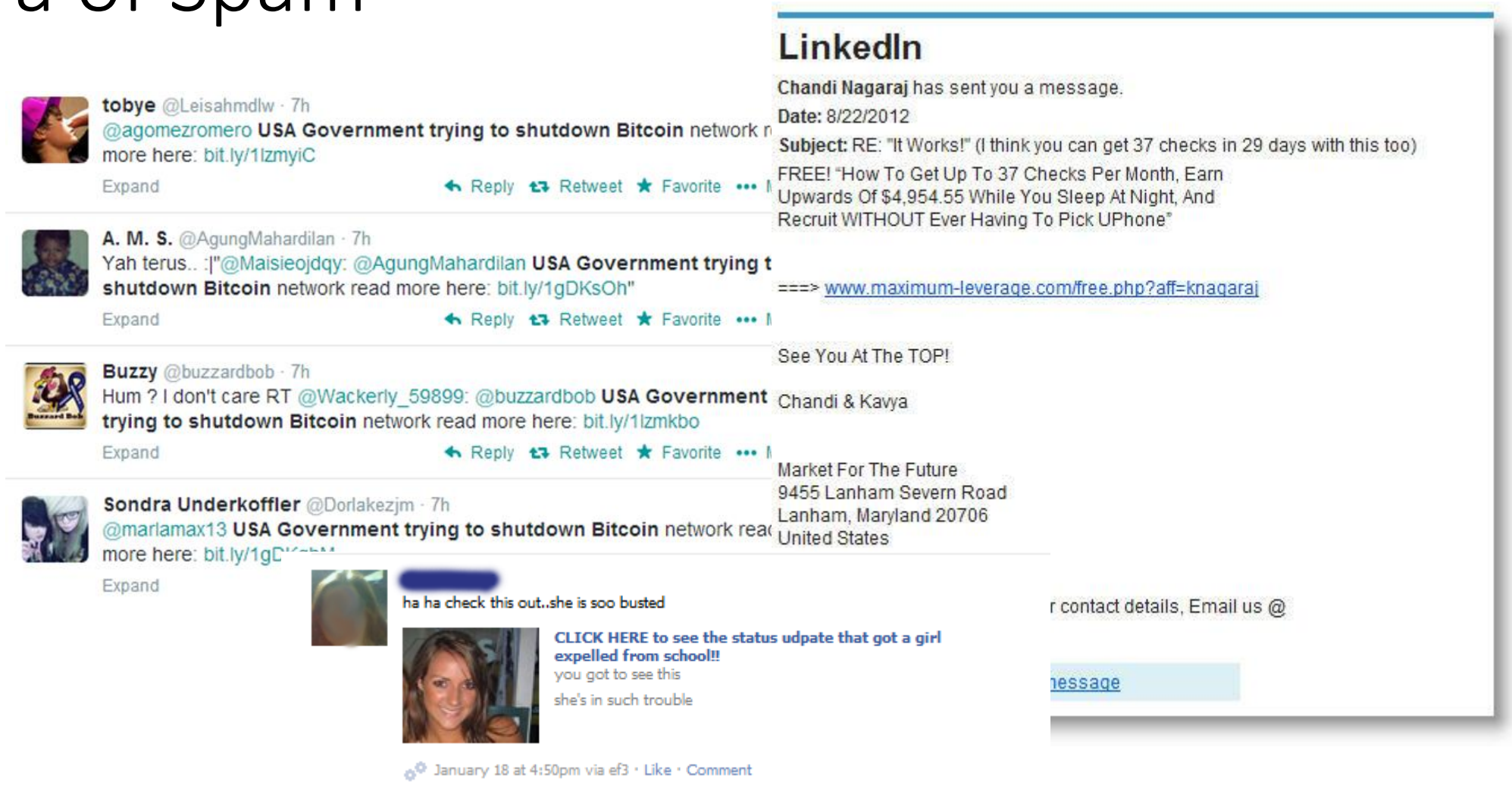
Stony Brook University

Carnegie Mellon University

Stony Brook University

Carnegie Mellon University

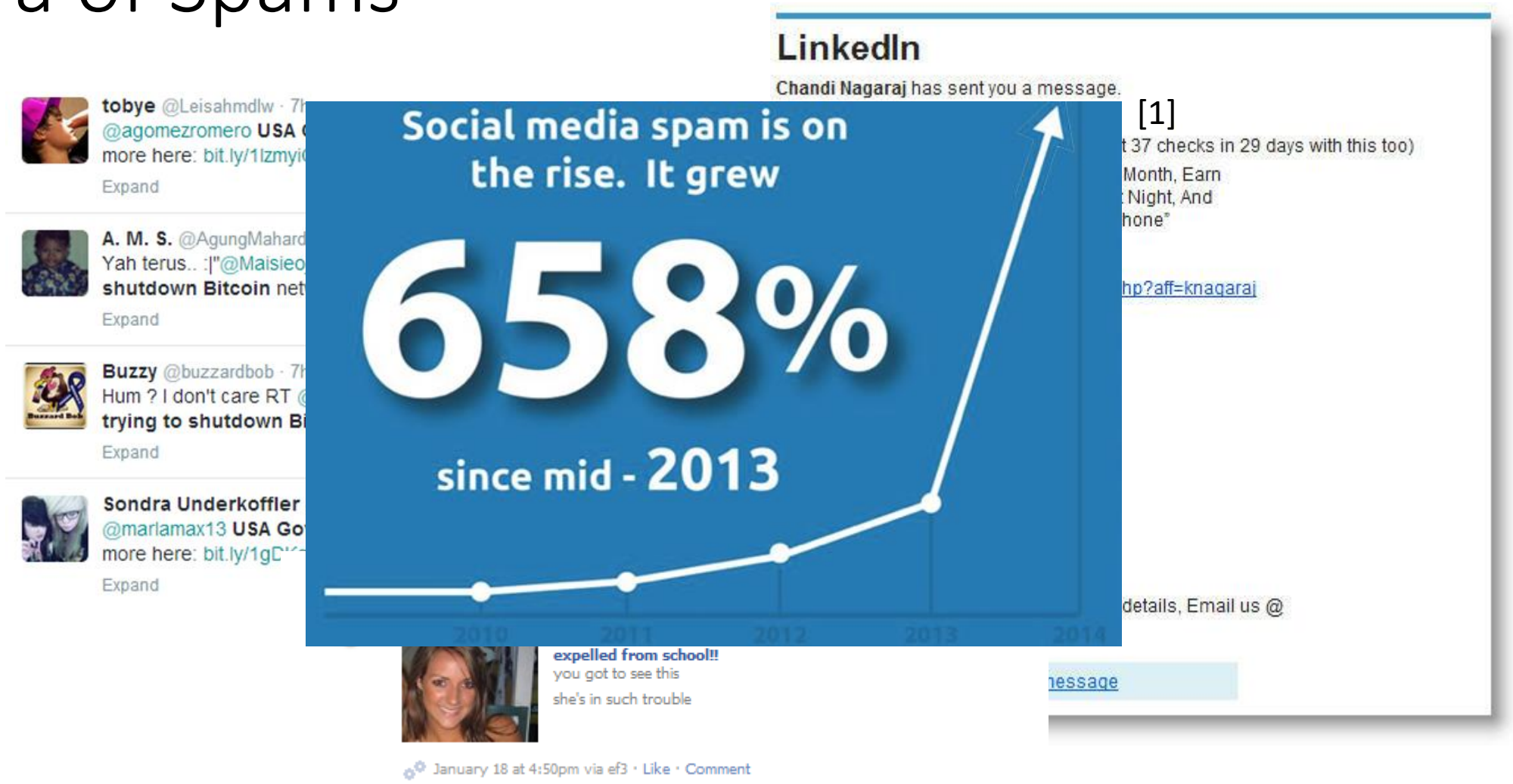
Era of Spam



Stony Brook University

Carnegie Mellon University

Era of Spams



[1] Social Media Spamming Grew By 658% Between 2013 And 2014: Entertainment, Financial And News Categories Main Target, https://dazeinfo.com/2014/12/15/social-media-spamming-growth-2014-facebook-twitter-entertainment/

Stony Brook University
Carnegie Mellon University

Popular Solutions

- IP blacklisting
  - Popular for social media and URL shortening services
  - False negative rates between 40.2 to 98.1%
  - Slow and unscalable

- Account based approach
  - Limited ability to detect compromised accounts
  - Require a history of malicious behavior
  - Not generalizable to different services

Stony Brook University
Carnegie Mellon University

Popular Solutions

- IP blacklisting

URL-level decisions are required
- able to filter individual post
- more generalizable

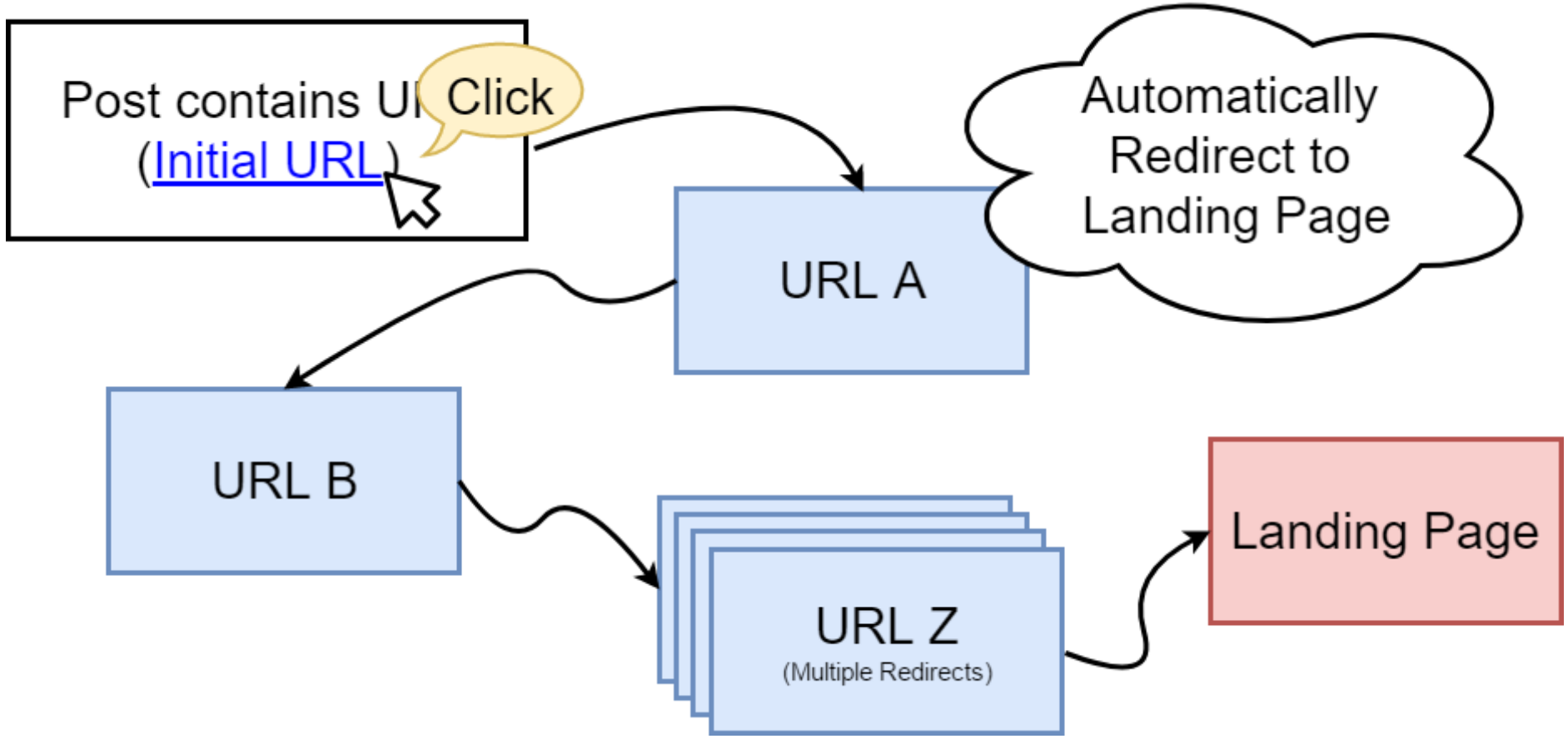
- A
  - Require a history of malicious behavior

Stony Brook University
Carnegie Mellon University

Domain-Agnostic Approach

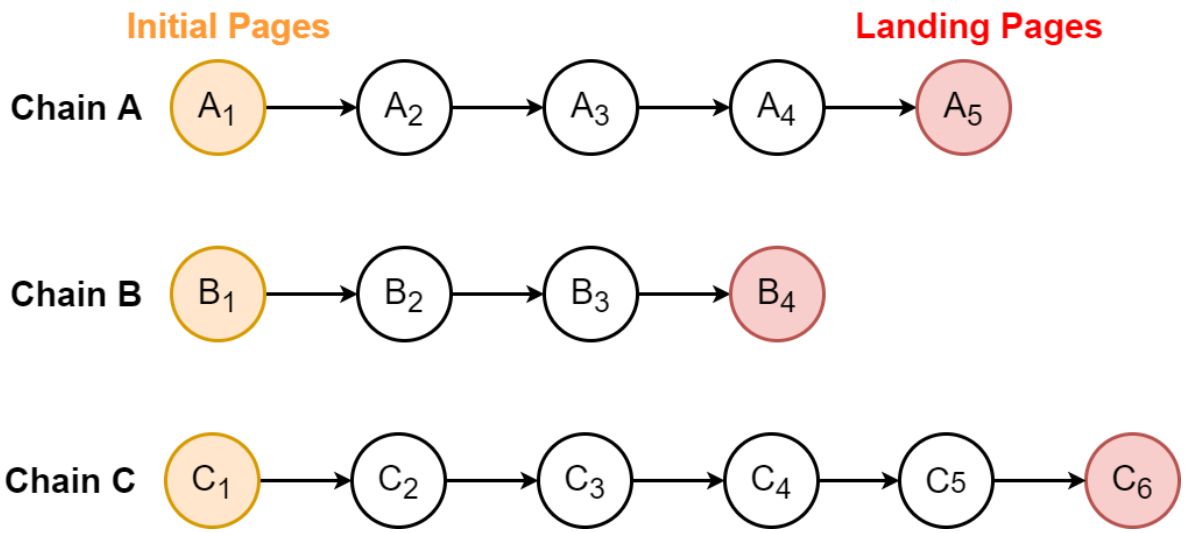
- Leverages widespread of redirect chains by spammers
- Extracts robust features to capture the nature of spammers' behavior
- Can be applied into different domains

Redirect Chain



Stony Brook University
Carnegie Mellon University

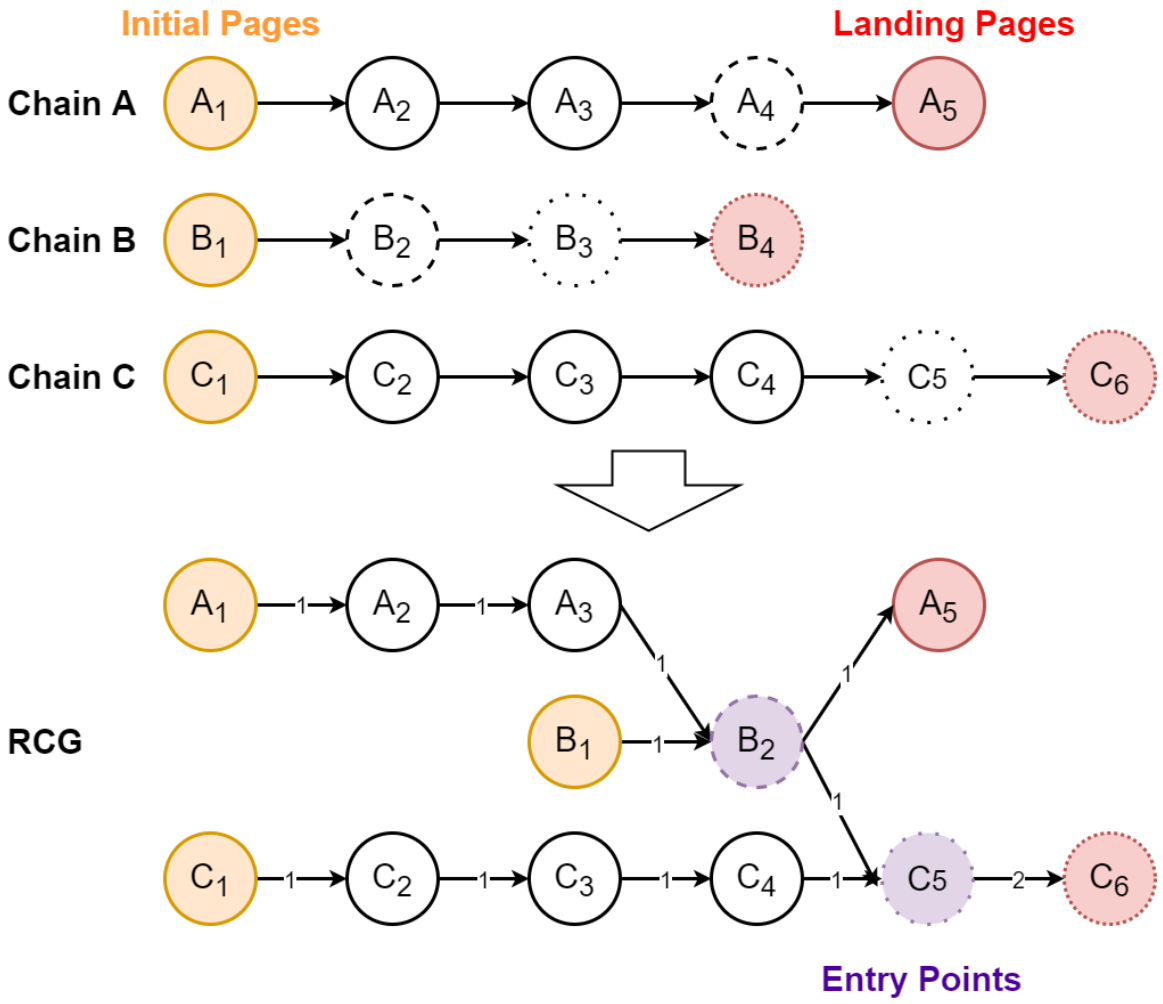
Redirect Chain



- Initial Pages
  - URL displayed to users
- Landing Pages
  - Where the user ends up

Stony Brook University
Carnegie Mellon University

Redirect Chain Graph



- Identify same URLs
- Aggregate chains
- Find Entry points
  - Largest in-weight node in each chain

Stony Brook University
Carnegie Mellon University

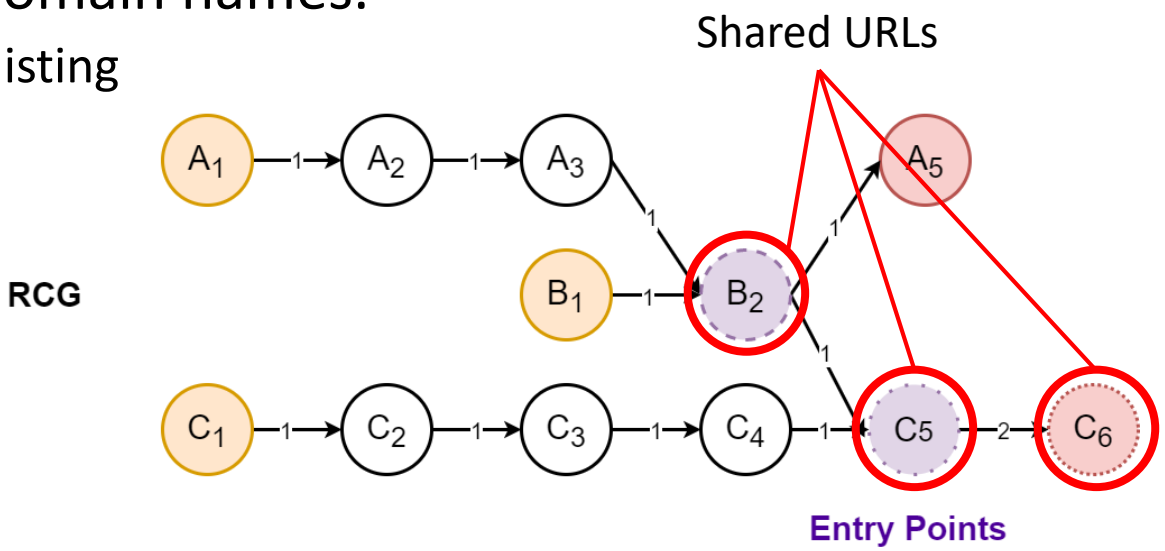
Feature Design

- Three groups of Features that characterize spammers' behavior
  - Shared resources
  - Heterogeneity
  - Flexibility

Stony Brook University
Carnegie Mellon University

Features – Shared Resources

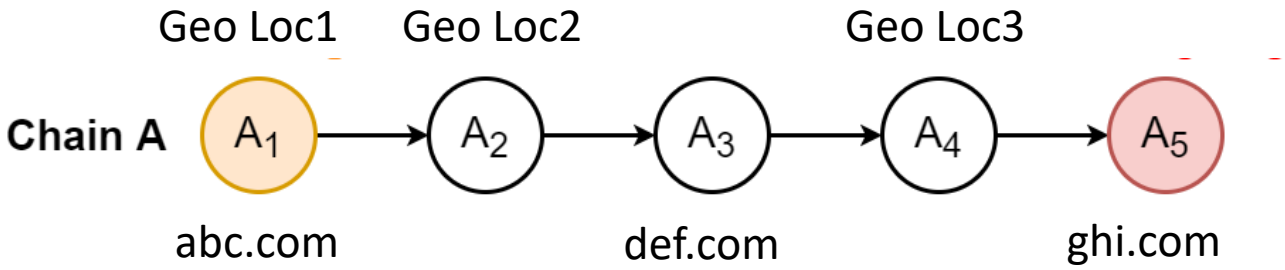
- To reduce costs, sharing resources is inevitable
  - Reuse of URLs
  - Same servers hosting many different domain names.
    - To evade and stay ahead of domain blacklisting
- Total 17 features



Stony Brook University
Carnegie Mellon University

Features – Heterogeneity

- “Don't put all your eggs in one basket”
  - Place servers to different geo-locations
  - Use of compromised servers and bot machines
- Total 12 features

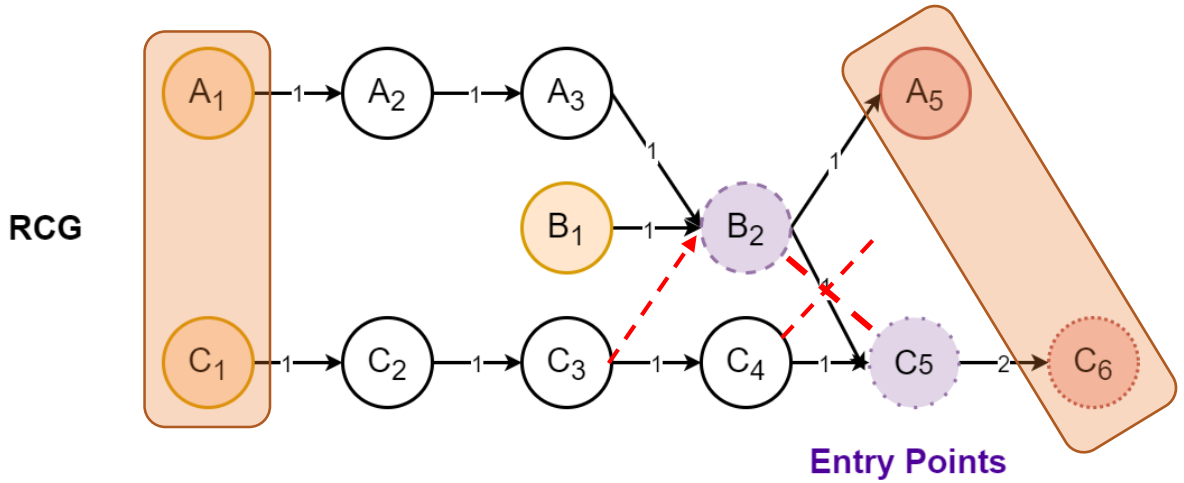


Stony Brook University

Carnegie Mellon University

Features – Flexibility

- Two types of flexibility:
  - For luring more users
    - Multiple different initial URLs
  - For evading detection
    - Using multiple landing URLs with redundant content
    - Same URLs with different IPs
    - Dynamicity and selectivity using long redirect chains
- Total 10 features



Stony Brook University
Carnegie Mellon University

Dataset

- Tweets
  - 3,764,395 tweets have URLs
    - 3,871,911 initial URLs are identified
- Redirect Chain
  - Chain lengths are vary from 1 to 46
  - 99% of chains are less than length 6
- Redirect Chain Graph
  - 4,874,256 nodes
  - 3,839,633 edges

Stony Brook University
Carnegie Mellon University

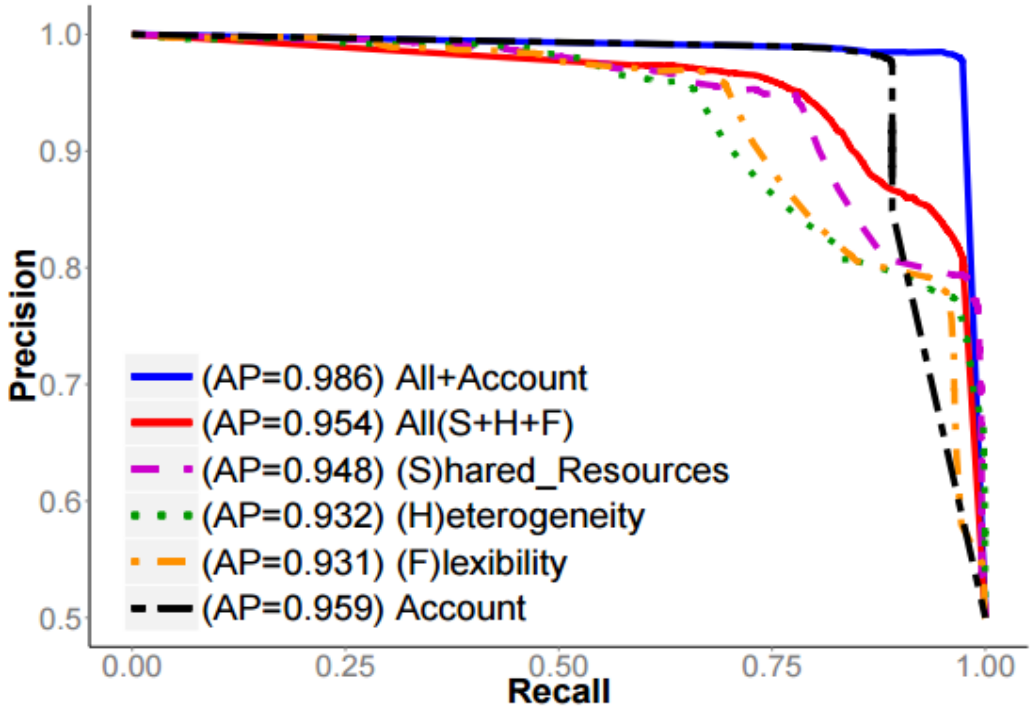
Experiment

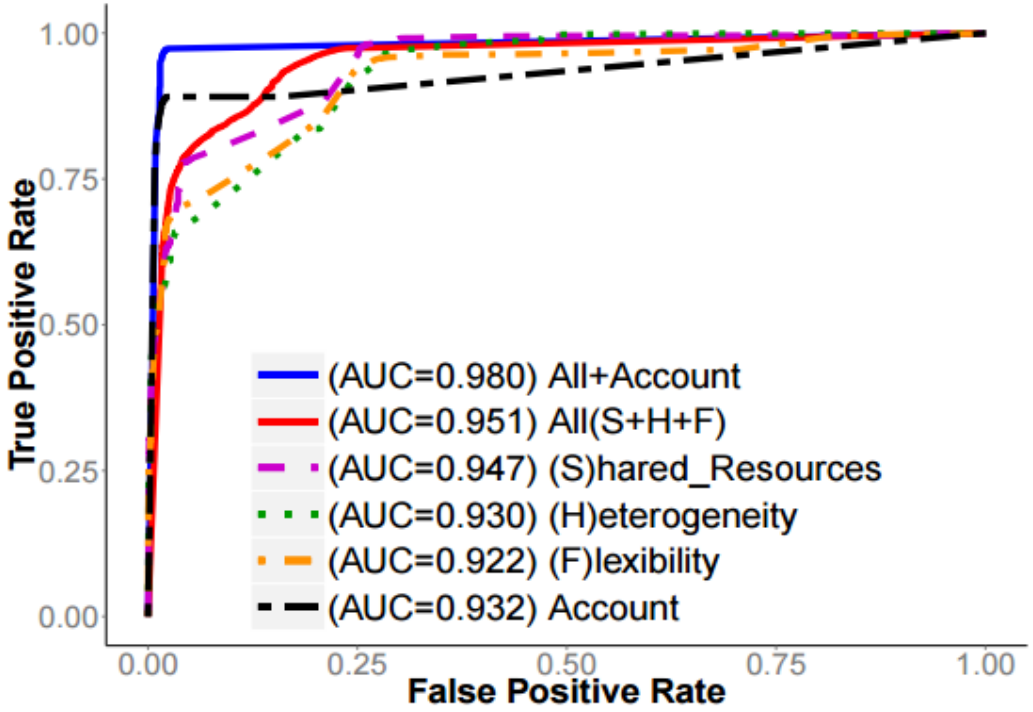
- Supervised Detection
  - Compare between context-free and context-aware detection

- Semi-supervised Detection
  - Small fraction of labels are revealed (1% or 5%)
  - Loopy belief propagation (LBP) through user-URL bipartite graph

Stony Brook University
Carnegie Mellon University

Result – Supervised methods

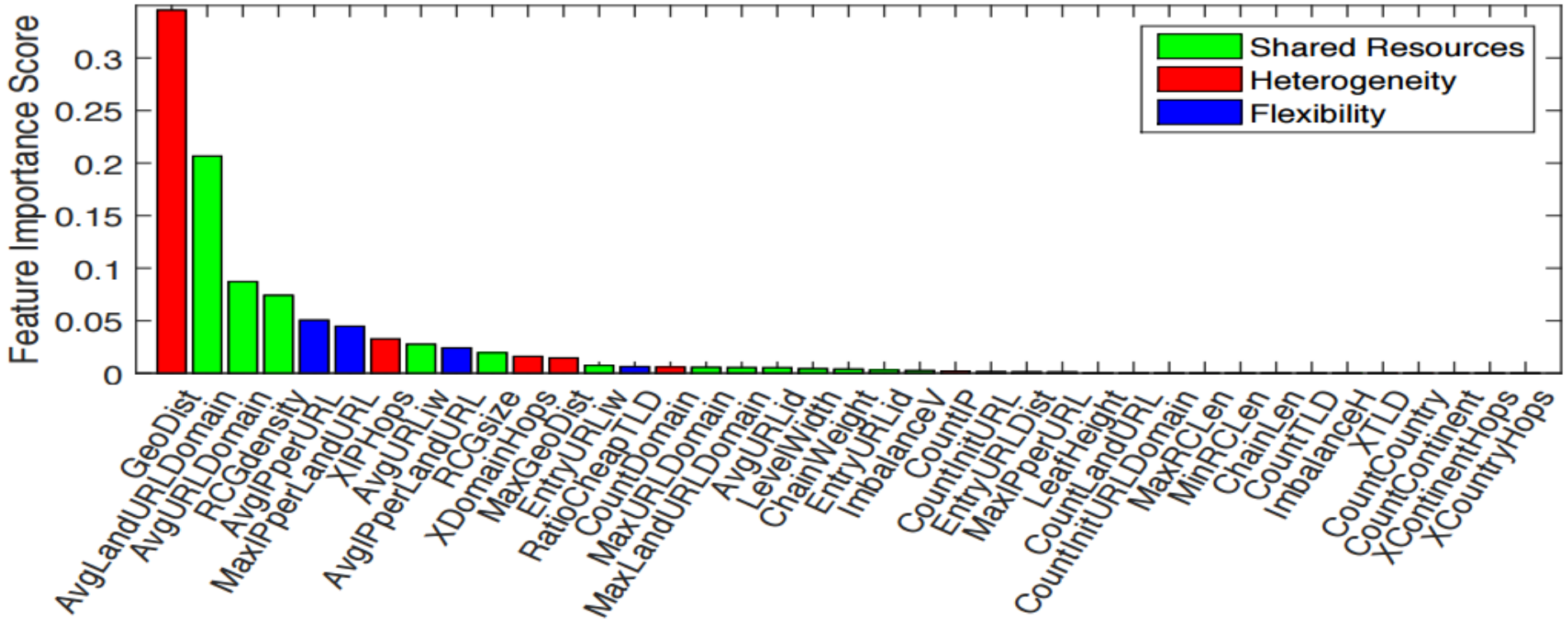




- Context-free features achieve competitive performance

Stony Brook University
Carnegie Mellon University

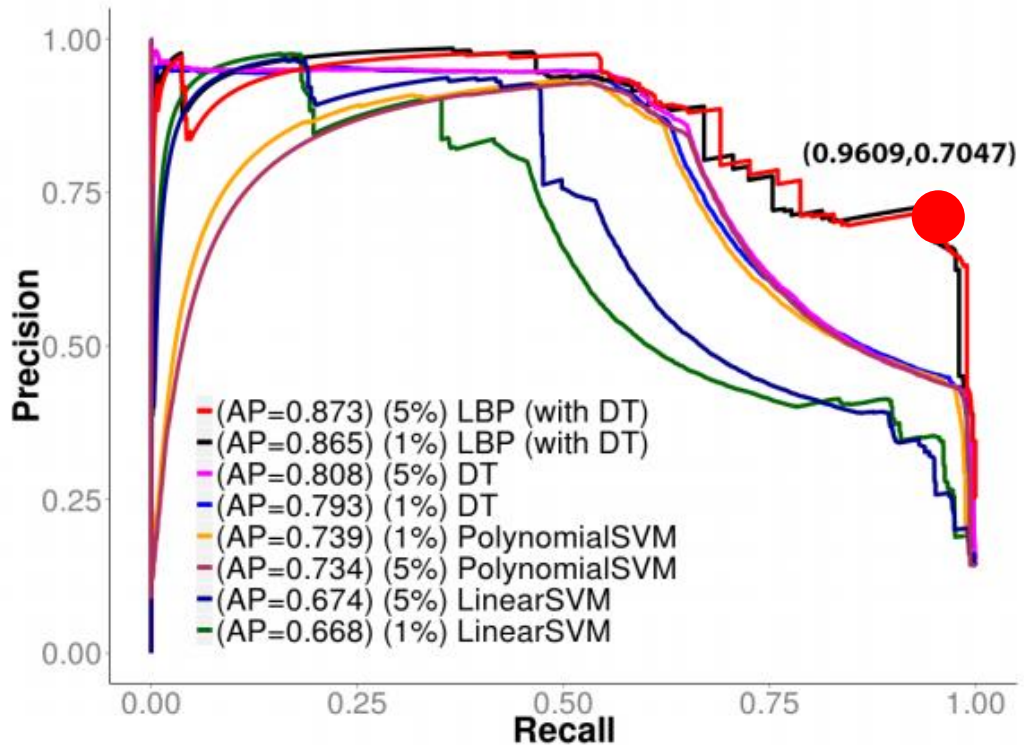
Result – Feature importance score

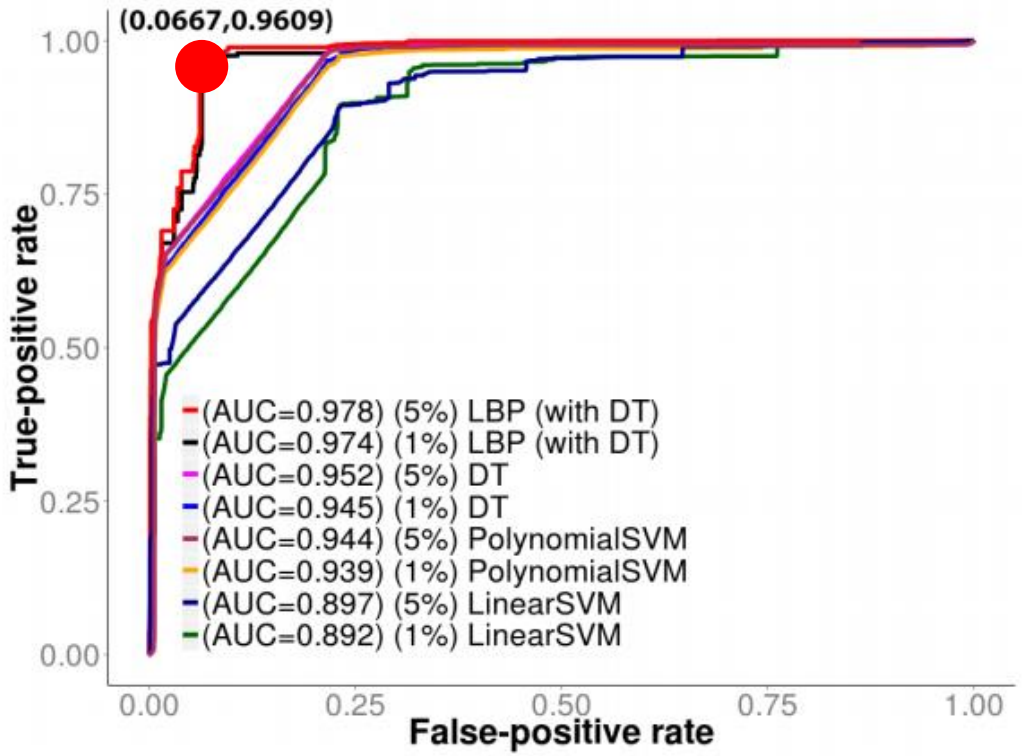


- Top features evenly come from all three categories

Stony Brook University
Carnegie Mellon University

Result – Semi-supervised methods





- Red dots show the performance at threshold 0.5

Stony Brook University
Carnegie Mellon University

Conclusion

- Alternative approach to detect spam URL using Redirect Chain Graph
  - Context-free
  - Adversarially robust
  - Semi-supervised

data available at: http://cs.stonybrook.edu/~heekwon

Stony Brook University

Carnegie Mellon University

Thank you!