Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosqatting

Mohammad Taha Khan*, Xiang Huo*, Zhou Li† & Chris Kanich*

University of Illinois at Chicago* & RSA Labs†

Goal of This Work

- Understand the harm caused by cybercrime
- Prior studies have focused on monetary losses and data breaches
- An additional dimension is the “loss of user time”

What is Typosquatting?

- Identification and registration of well-known typos for established websites
- Populate typo domains with: i. Competing content
  ii. Malware
  iii. Advertisements

Our Contributions

- Develop an intent based method to detect passive typosquatitng instances
- Present a harm metric based on user time lost as a result of typosquatting
- Quantify the harm caused by different characterizations of typosquatting

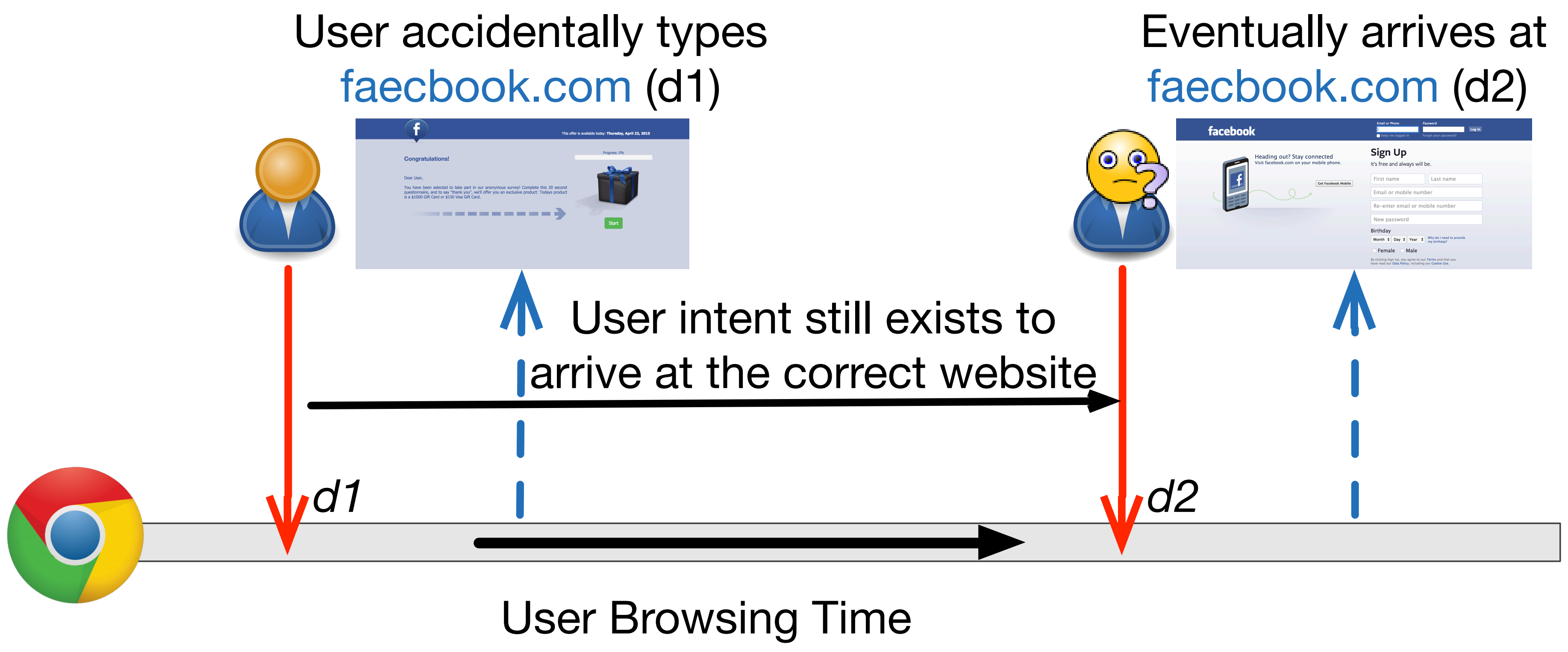
The Datasets

- University HTTP and DNS packet captures
- Enterprise HTTP proxy logs
- Active crawls of typosquatting domain names

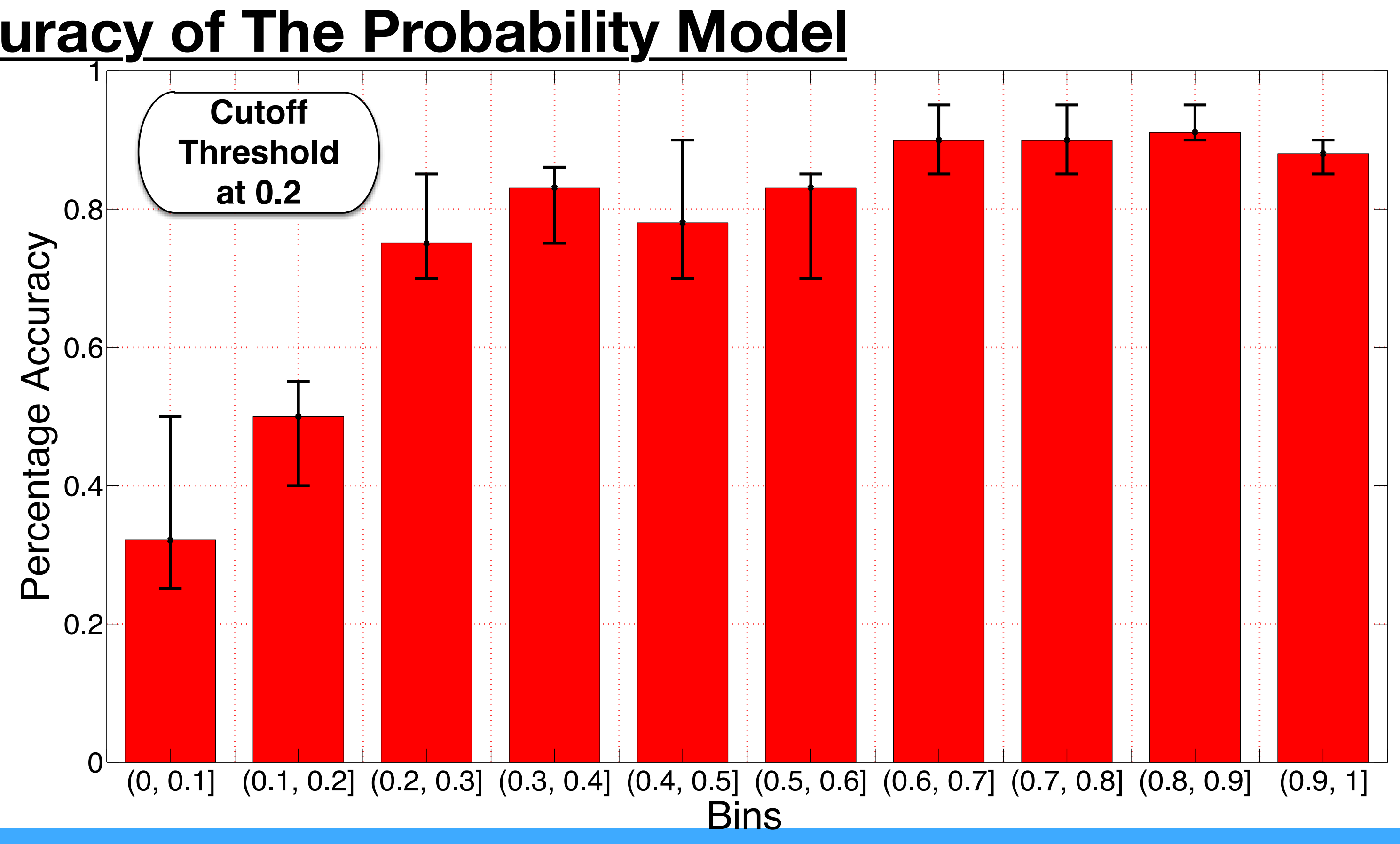
Detection of Tposquatting Instances

- To Identify a typo domain we evaluate the conditional probability of a typo website being followed by a request to a similar legitimate website

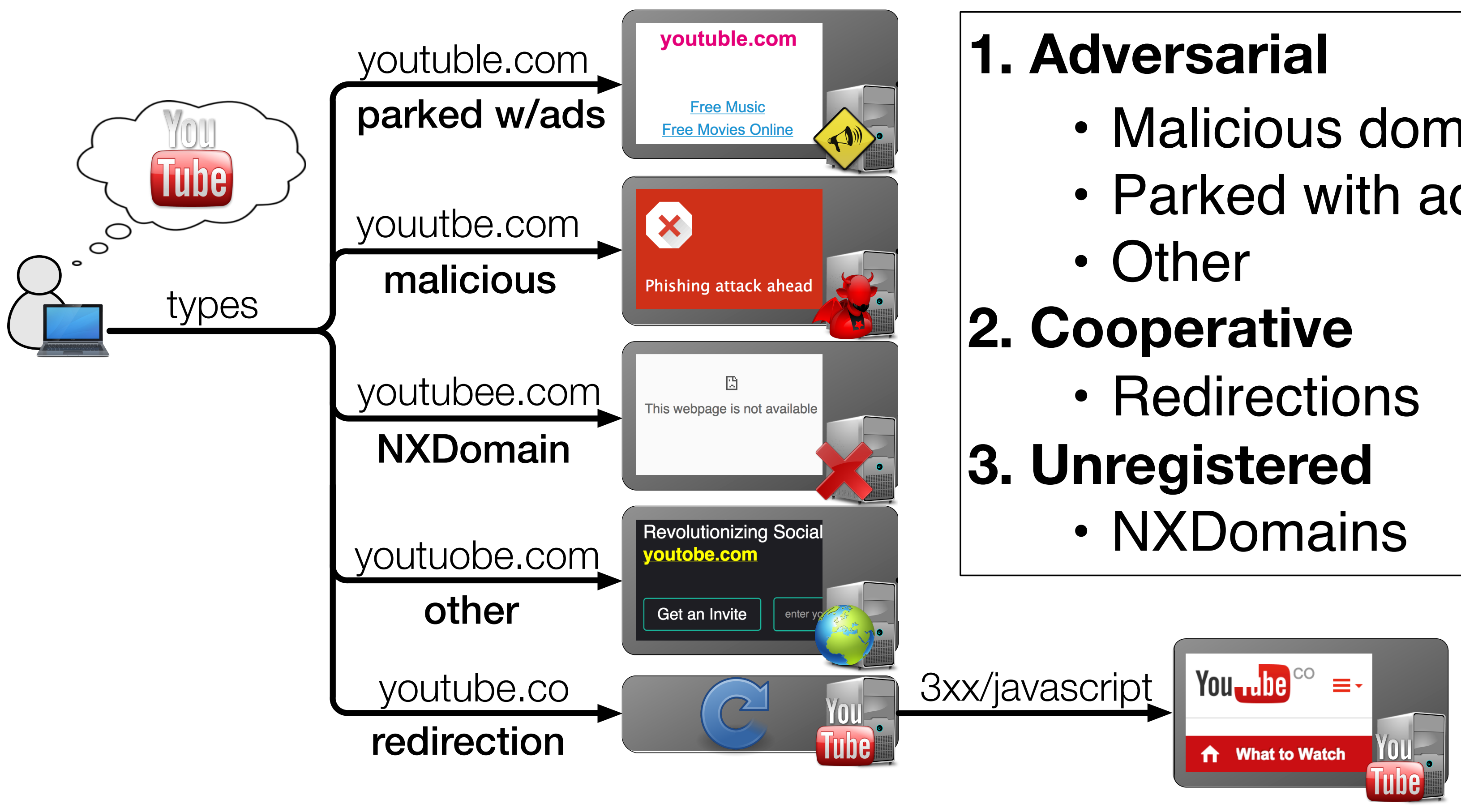
User Behavior on Encountering a Typo Domain



Accuracy of The Probability Model

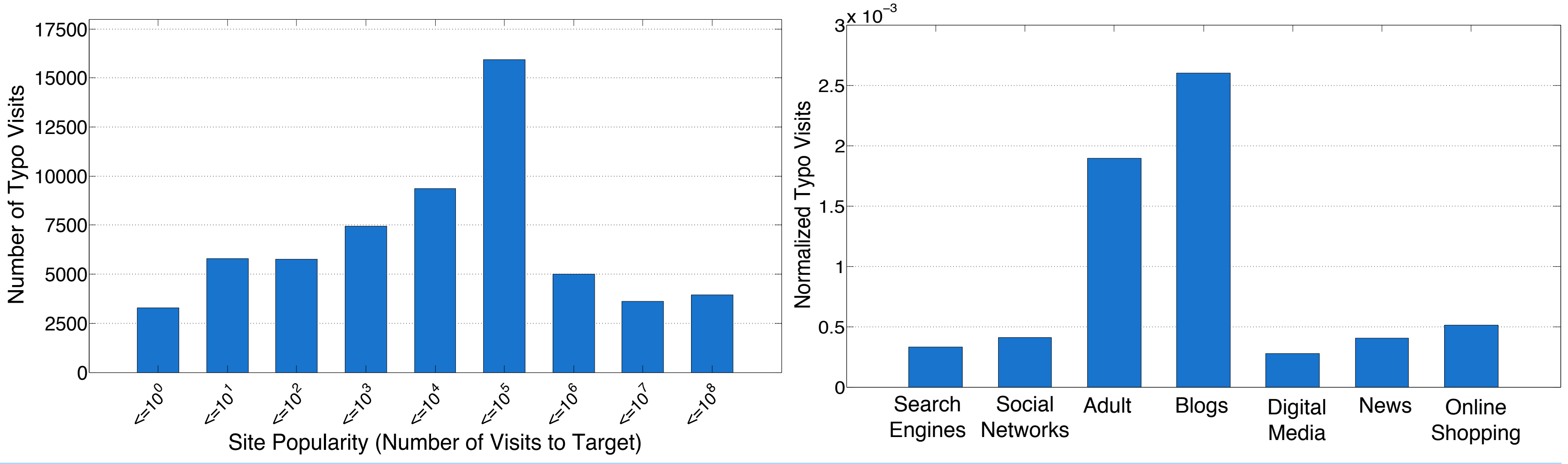


Typo Characterization



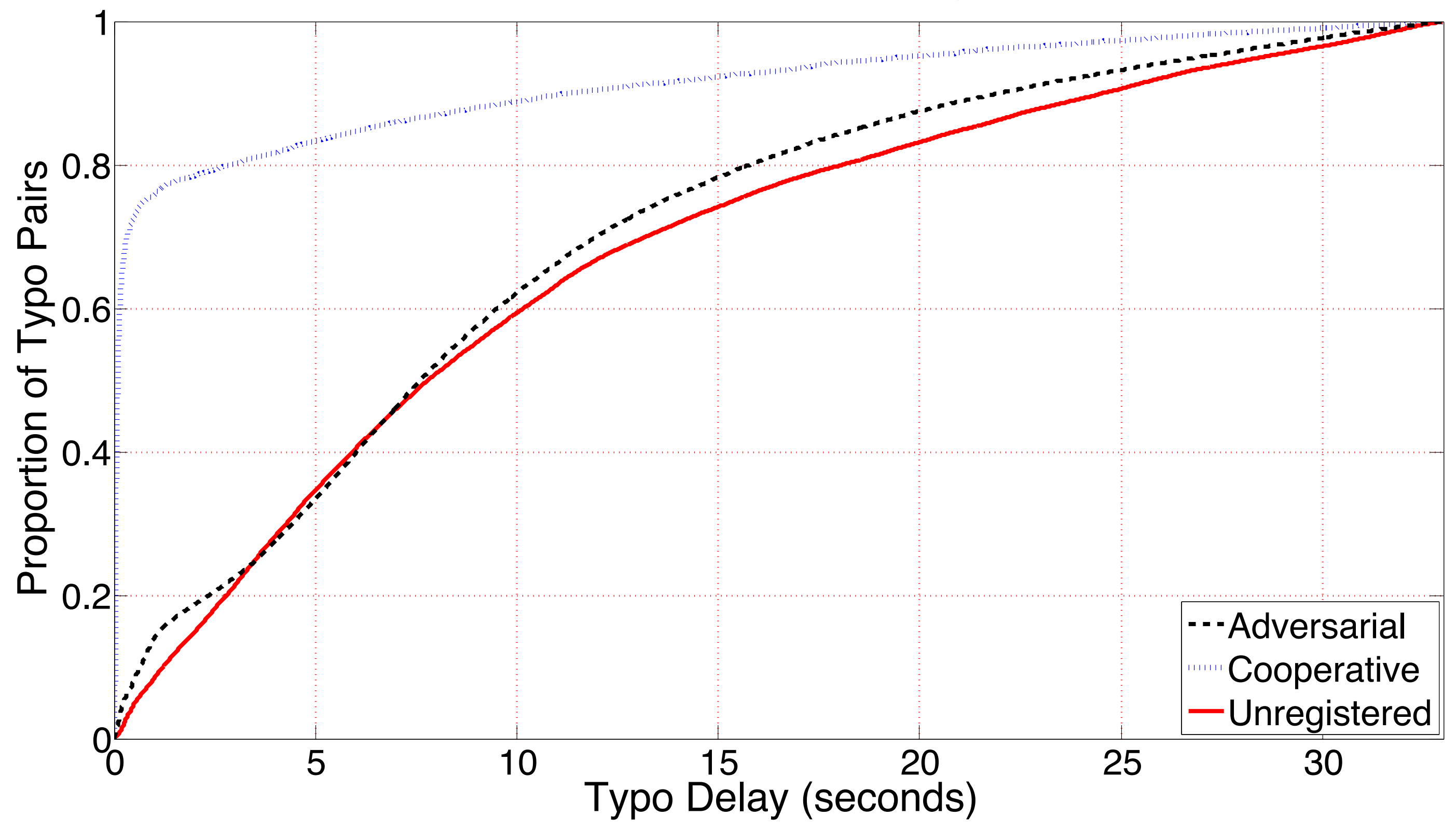
1. **Adversarial**
   - Malicious domains
   - Parked with ads
   - Other
2. **Cooperative**
   - Redirections
3. **Unregistered**
   - NXDomains

Typosqautting Domain Popularity



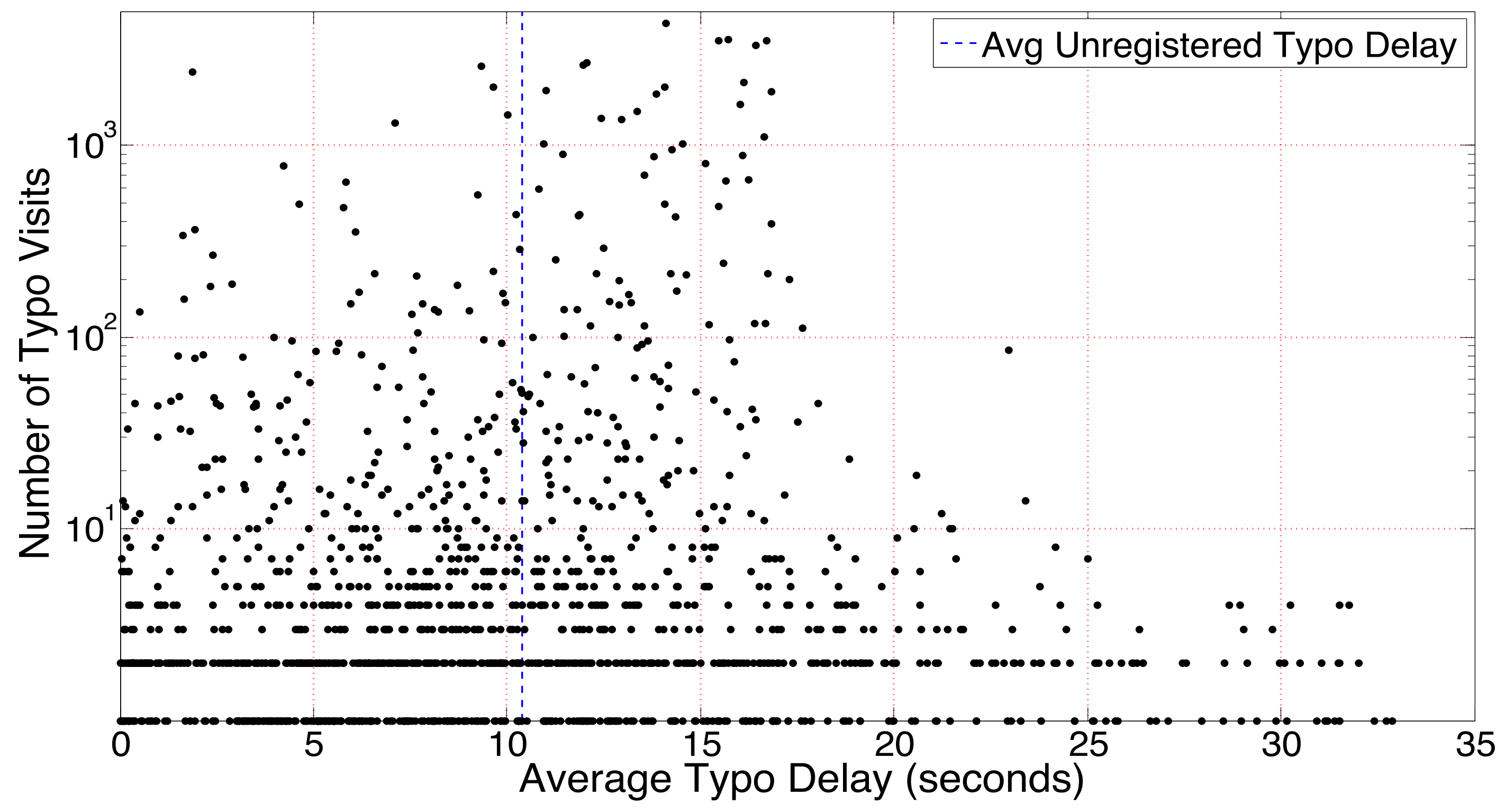
Quantifying Harm

Cumulative delays of each typo category



- Adversarial domains have a higher user loss rate, but approximately the same average delays

Delay clustering of adversarial domains by DNS provider



- Significant number of adversarial clusters have lower delays than unregistered domains

Conclusive Findings

- As a result of typosquatting, an individual loses on average, 64 seconds and $0.29 per capita income per year
- The harm is not the worth investing into defensive registrations

UIC UNIVERSITY OF ILLINOIS AT CHICAGO Bits Networked Systems Laboratory COLLEGE OF ENGINEERING

RSA