Domain Registration Policy Strategies and the Fight against Online Crime

Janos Szurdi and Nicolas Christin

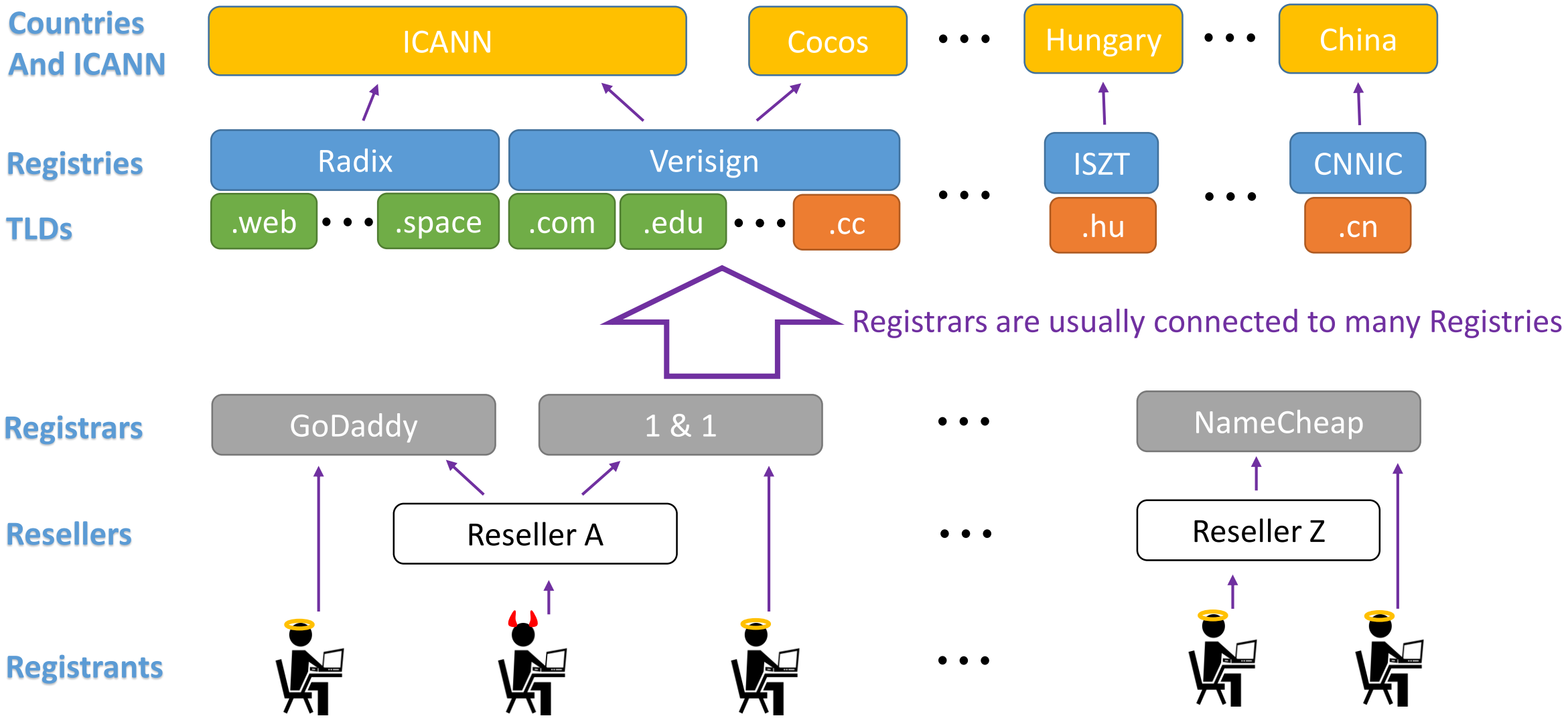
Carnegie Mellon University

CyLab
Security and Privacy Institute

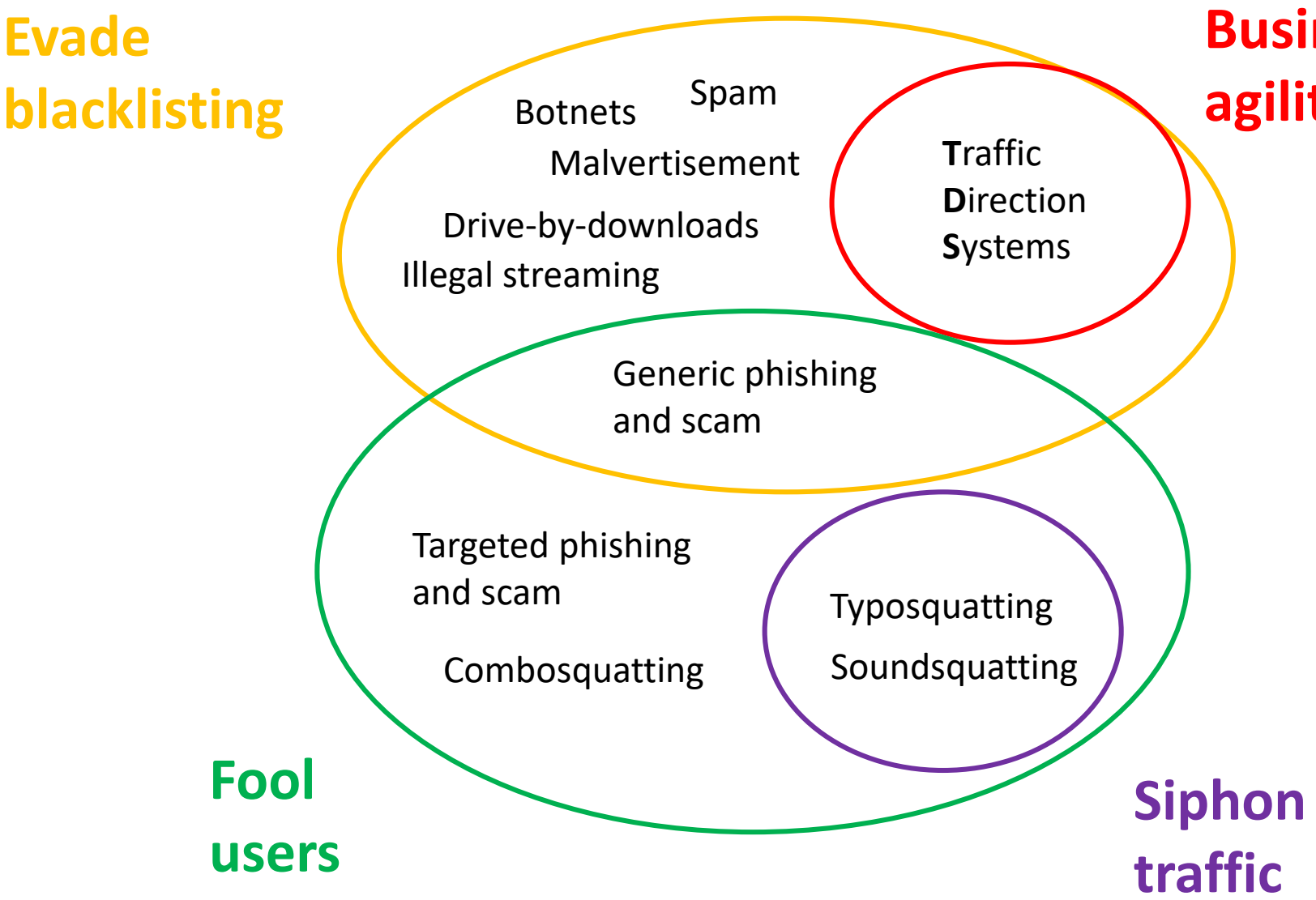
Which domain registration policies could be useful in the fight against online crime?

1. Background, motivation and related work
2. Policy analysis and promising proposals
3. Game theoretic analysis of one policy proposal

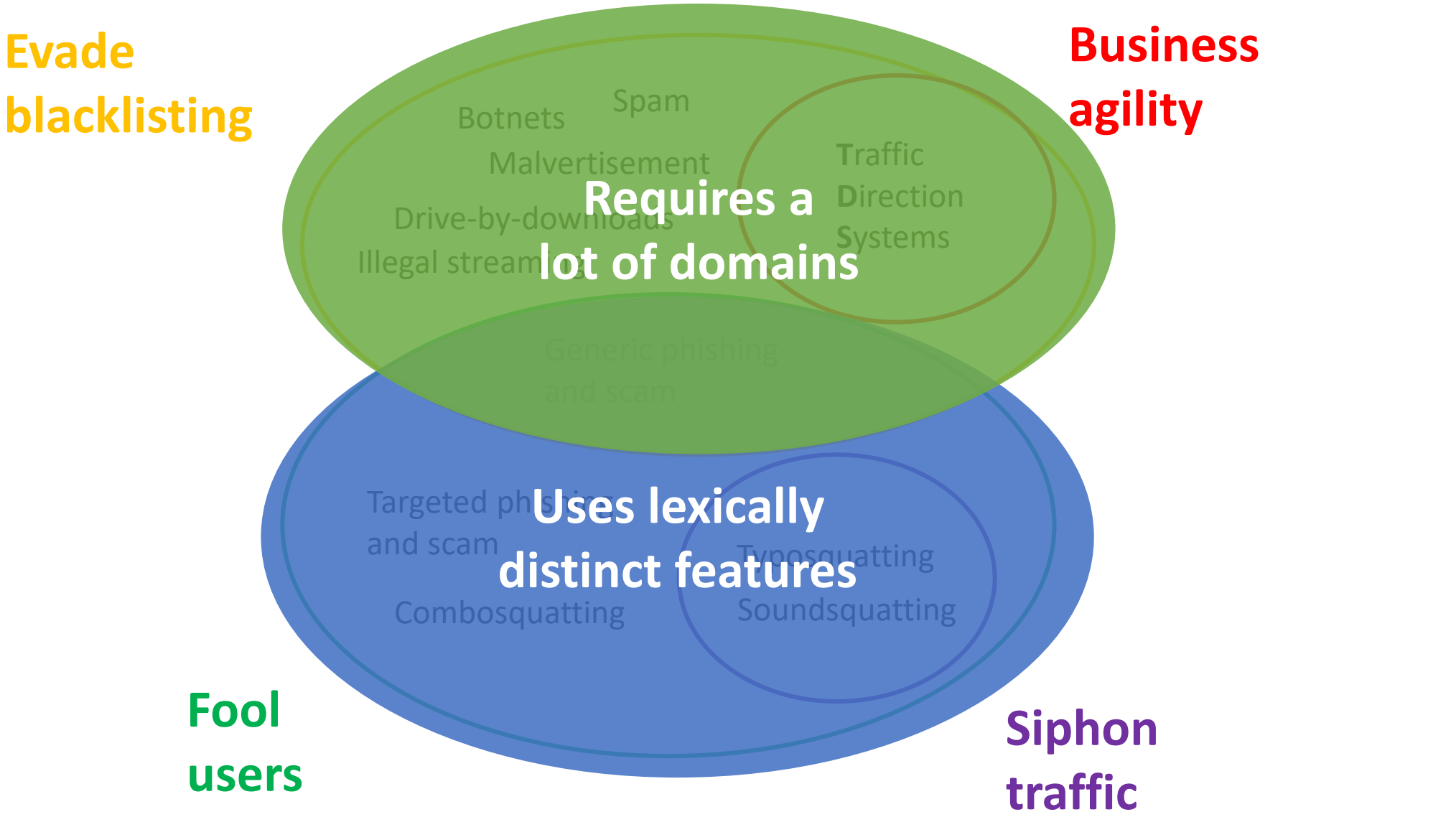
Ecosystem


Countries And ICANN
ICANN
Cocos
Hungary
China
Registries
Radix
Verisign
ISZT
CNNIC
TLDs
.web
.space
.com
.edu
.cc
.hu
.cn
Registrars are usually connected to many Registries
Registrars
GoDaddy
1 & 1
NameCheap
Resellers
Reseller A
Reseller Z
Registrants

Motivation: Malicious Registrations



Motivation: Malicious Registrations



Related Work

Detection and Blacklisting

- Reputation Antonakakis et al. 2010
- Detection Szurdi et al. 2014
- Prediction Hao et al. 2016

Studies Related to Policies

- Registrar-level intervention Liu et al. 2011
- Spam economics Chachra et al. 2014
- Security metrics for TLDs Korczynski et al. 2017

Related Work

Detection and Blacklisting

- Reputation Antonakakis et al. 2010
- Detection Szurdi et al. 2014
- Prediction Hao et al. 2016

Detection depends on registration policies and vice versa

Studies Related to Policies

- Registrar-level intervention Liu et al. 2011
- Spam economics Chachra et al. 2014
- Security metrics Stone-Gross et al. 2013

Systematic high-level analysis of multiple policies

The WHOIS Debate

2001 **First congressional hearing on WHOIS**

2005 **Operational Point Of Contact**

2015 **Registration Directory Service** (Whois 2)

2018 **General Data Protection Regulation**

Security	**Privacy**
Intellectual Property - Copyright & Trademark	Spam, Phishing and Scam
Law enforcement - Online crime	Registrant Privacy
Security researchers - Domain ownership - Notify domain owners	Freedom of speech
Regular Users - Look up domain owner	

The WHOIS Debate

2001 **First congressional hearing on WHOIS**

2005 **Operational Point Of Contact**

2015 **Registration Directory Service** (Whois 2)

2018 **General Data Protection Regulation**

Security	Privacy
Intellectual Property - Copyright & Trademark	Spam, Phishing and Scam
Law enforcement - Online crime	Registrant Privacy
Security researchers - Domain ownership	Freedom of speech
Regular Users - Look up domain owner	

High-level analysis of which policy proposals are potentially effective against malicious registrations

Policy Framework

- Effect on the number of malicious registrations
  - Effect on the profitability of the illegal activity itself
- Cost to benign registrants
  - Sensitive Registrants!
- Effect on the income of ICANN, registries, and registrars
  - And how they are motivated to adopt
- Effectiveness of policy depending on the rate of adoption

Policy 1: Anti-squatting

- Lexically distinctive features
- Remove known squatting domains
- Harden new squatting registrations
  - What the purpose of the domain name will be?
  - Stricter identity verification
  - Security Deposit
  - Monitor these domains
- Minimal effect on benign registrants
  - Low false positive rate classifiers exist
- Useful even if only one registry adopts it

Policy 2: Incentivizing Registries and Registrars

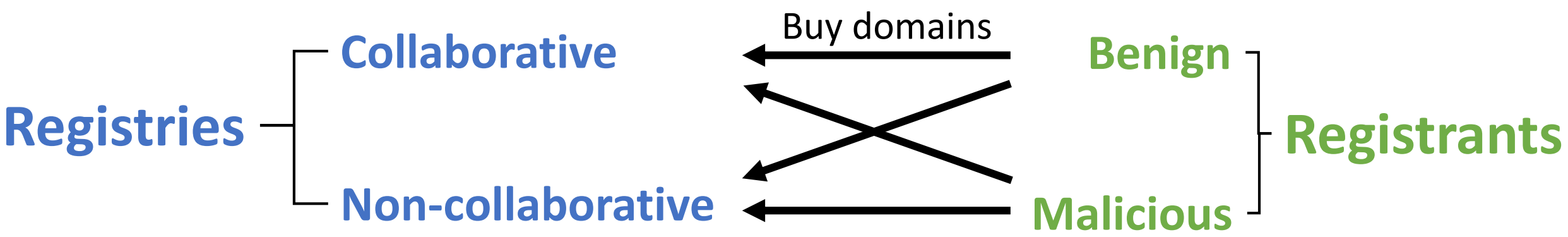
- Increase fee for registries and registrars with high abuse ratio
- Decrease fee for low abuse ratio
- Only affects bad registrars and malicious registrants
- DNSSEC example: registrars get discount if domains are signed

Policy 3: Anti-bulk Registration

- Malicious registrants need a lot of domain names
- Most benign registrants do not need a lot of domains, except
  - Speculative registrations
  - Defensive registrations
  - Hosting providers/website developers
- Currently bulk registration is rewarded
  - Instead we want to penalize it
- Increasing pricing per domain owned
- Stricter identity verification against Sybil attacks
  - Unusual combination of document + correct validation

A Game Theoretic Model

Players



Strategies

- Set Pricing Function
- Set Identity Validation Method

- Select number of domains to buy
- Select number of fraudulent identities to use

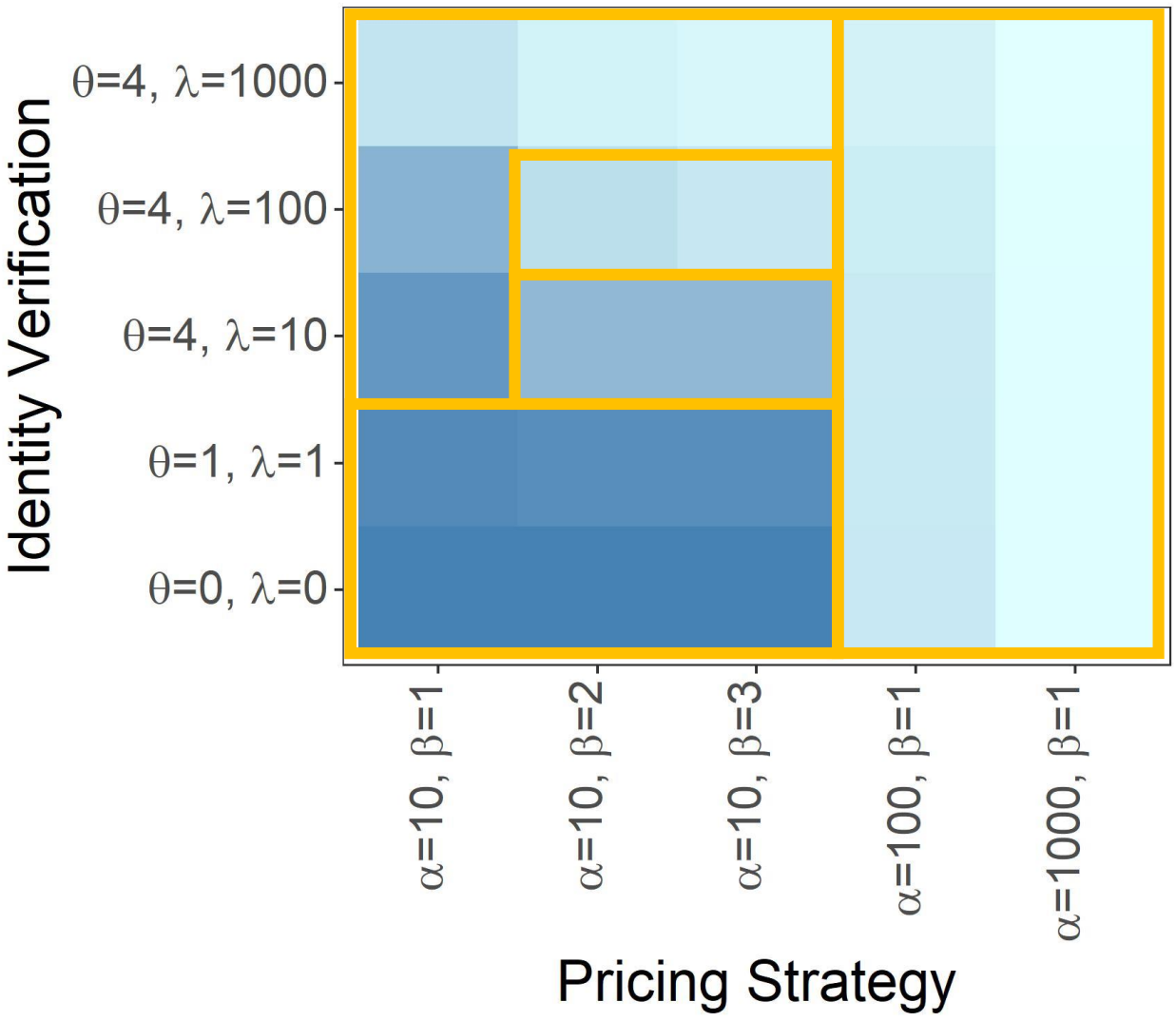
Utility Functions

$$Registry\ utility = registration\ fees - \rho * cost\ of\ online\ crime$$

$$Registrant\ utility = value\ of\ domains - registration\ fees - cost\ of\ id.verification - cost\ of\ fraudulent\ identities$$

ρ - how much a registry is affected by online crime

Effects on Typosquatting



$Price = \alpha n^{\beta}$

α: Base price

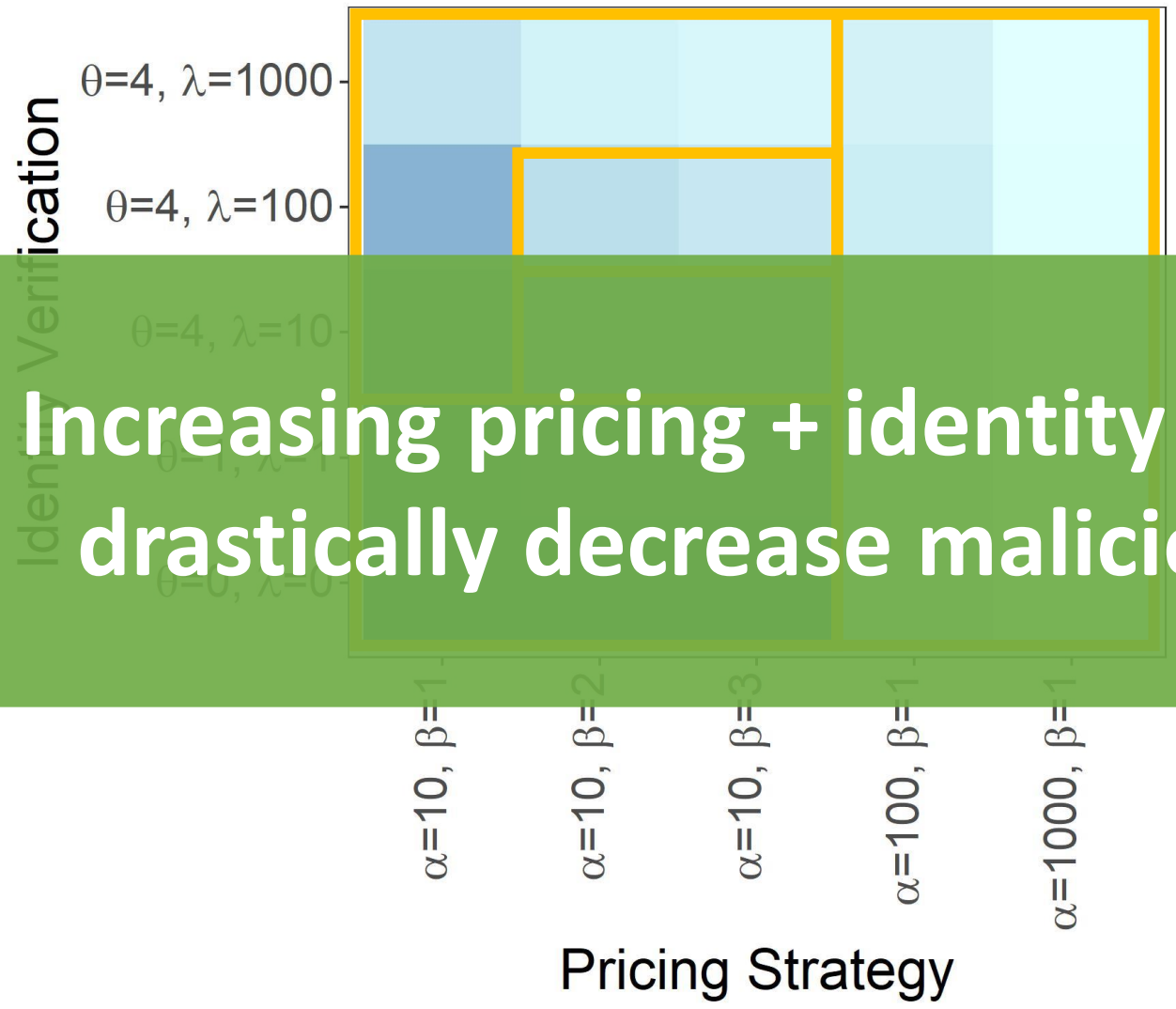
n: Number of domains registered

β: Exponential pricing

Θ: Cost of identification

λ: Cost of fraudulent identities

Effects on Typosquatting

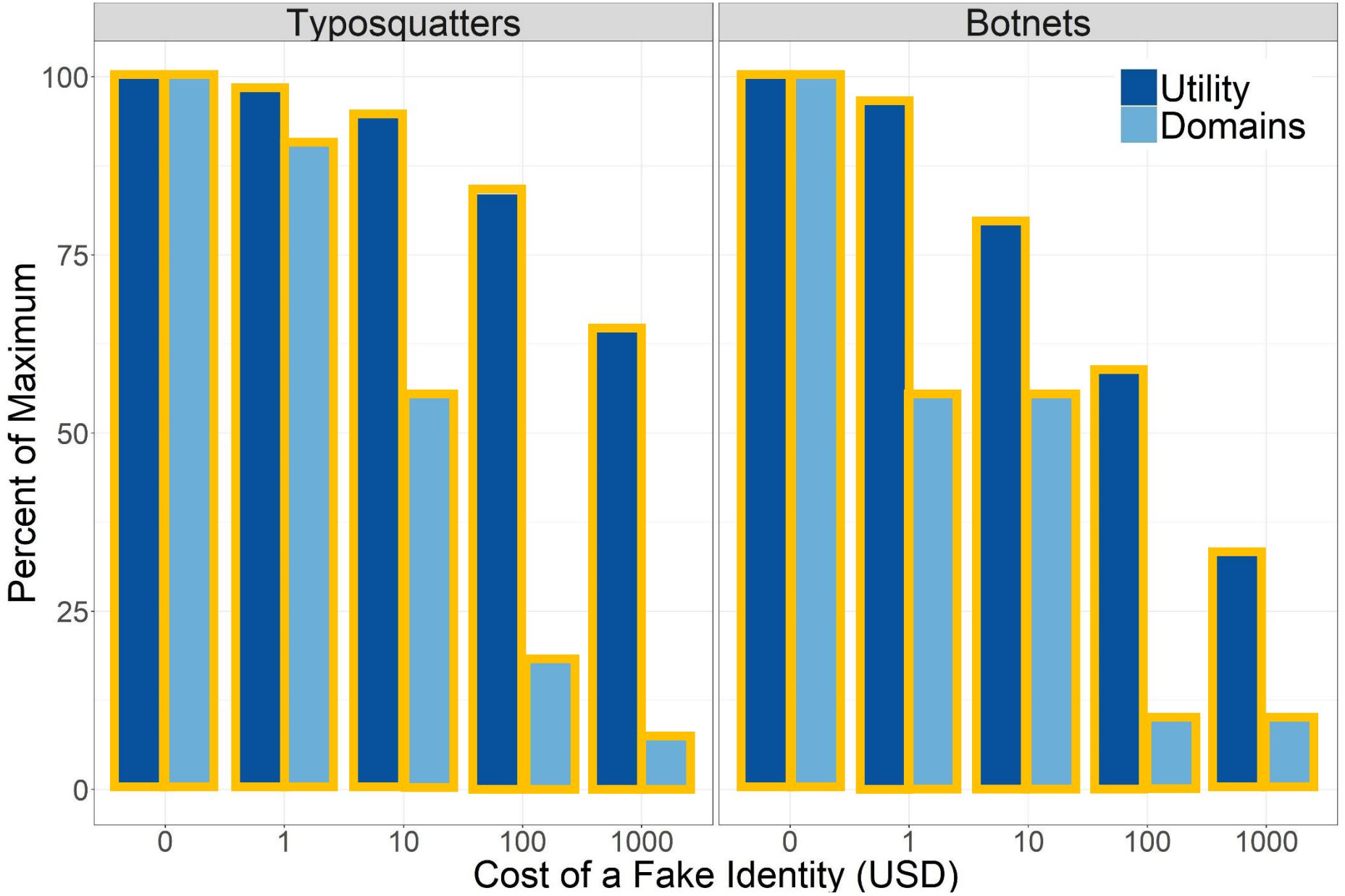


Increasing pricing + identity verification could drastically decrease malicious registrations

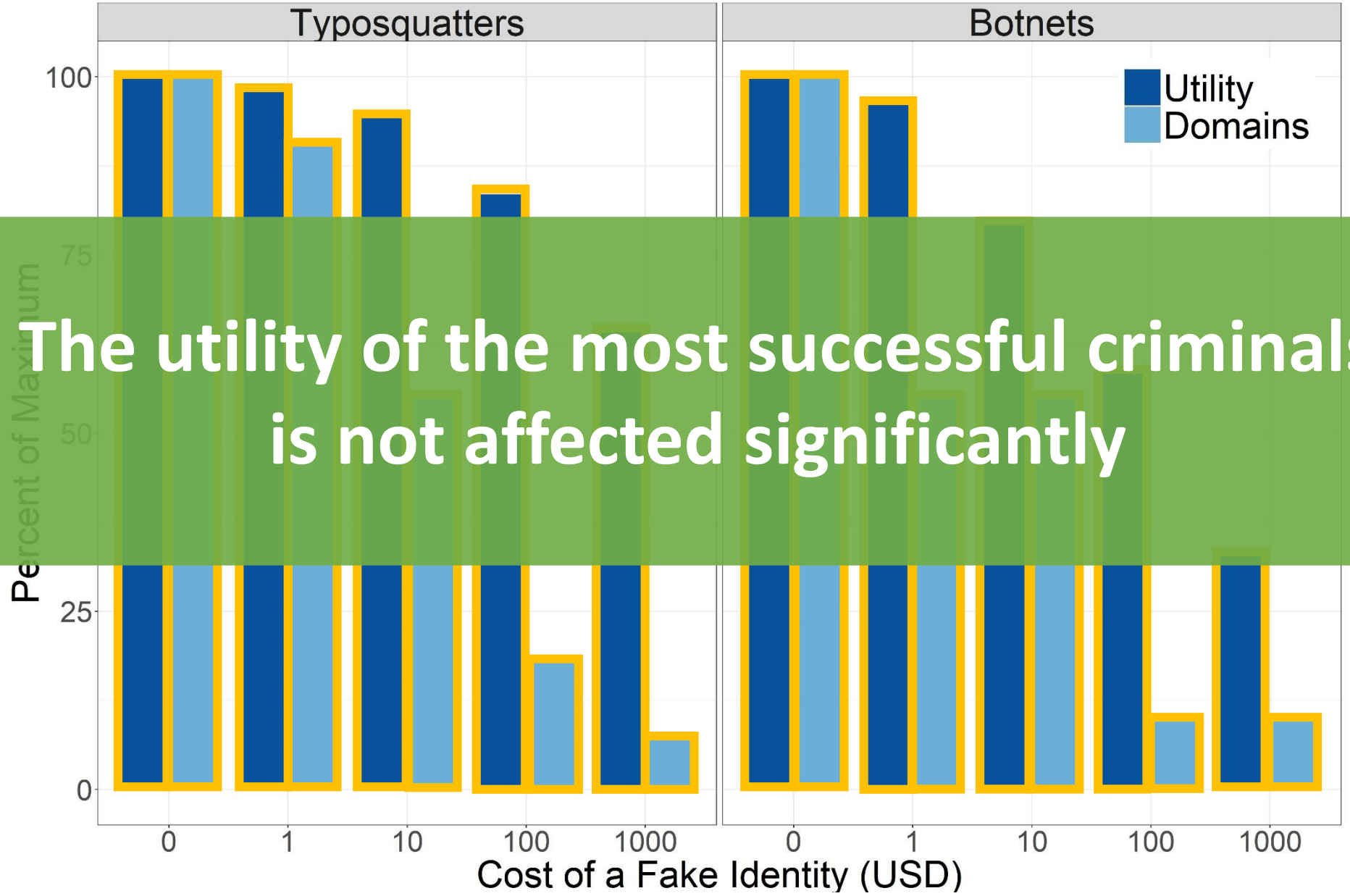
$$Price = \alpha n^{\beta}$$

α: Base price
n: Number of domains registered
β: Exponential pricing
Θ: Cost of identification
λ: Cost of fraudulent identities

Effects of Fraudulent Identity Costs



Effects of Fraudulent Identity Costs



The utility of the most successful criminals is not affected significantly

Game Summary

- Policy: exponential pricing + strict identity verification
- Most malicious registrations could become economically non-viable
- Synergy between detection and registration policies is important

Conclusions

- Developed a framework to analyze policies
- Found three promising policies
- Policies + detection -> drastically decreased malicious registrations

jszurdi@andrew.cmu.edu