BlockMeNot

Automatic Selection of Domain and URL Blocking Granularity to Minimize Collateral Damage and Evasion

Daud Ahmed · Srdjan Matic · Platon Kotzias · Emiliano Carlesi · Juan Caballero

USENIX Security Symposium · Baltimore, MD · August 14, 2026

Domain / URL Blocking

institute imdea software

A FUNDAMENTAL DEFENSE

PHISHING	MALWARE	PRIVACY	CONTENT FILTERING
credential theft	distribution & C2	trackers & ads	copyright, adult sites

SHARING ECOSYSTEM

URL BLOCKLISTS	DOMAIN BLOCKLISTS	THREAT EXCHANGES

PhishTank® OpenPhish

URLhaus by ABUSE.ch

CERT.PL

MALWARE WORLD

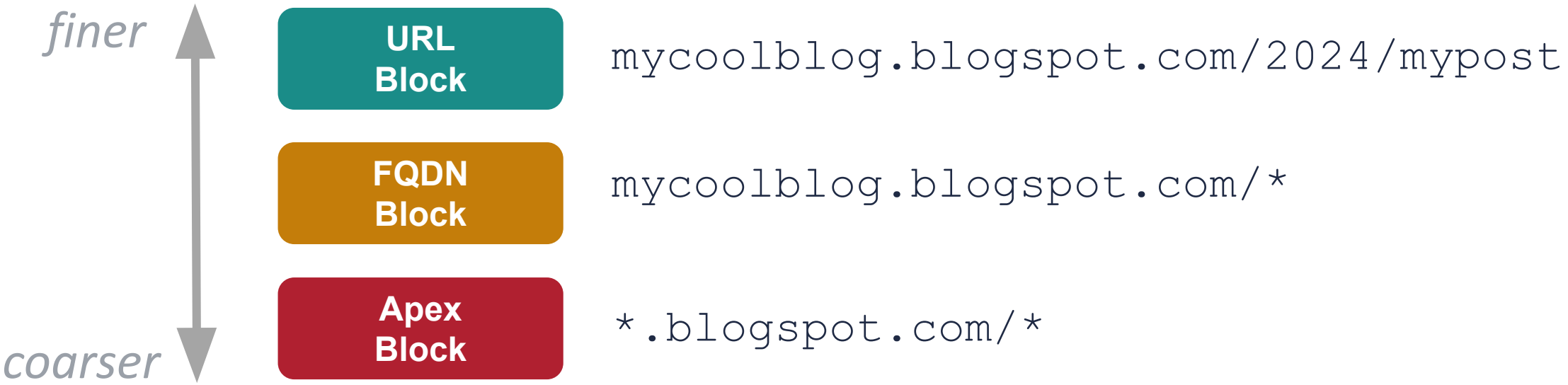
UNIVERSITÉ TOULOUSE CAPITOLE

APWG eCrimeX

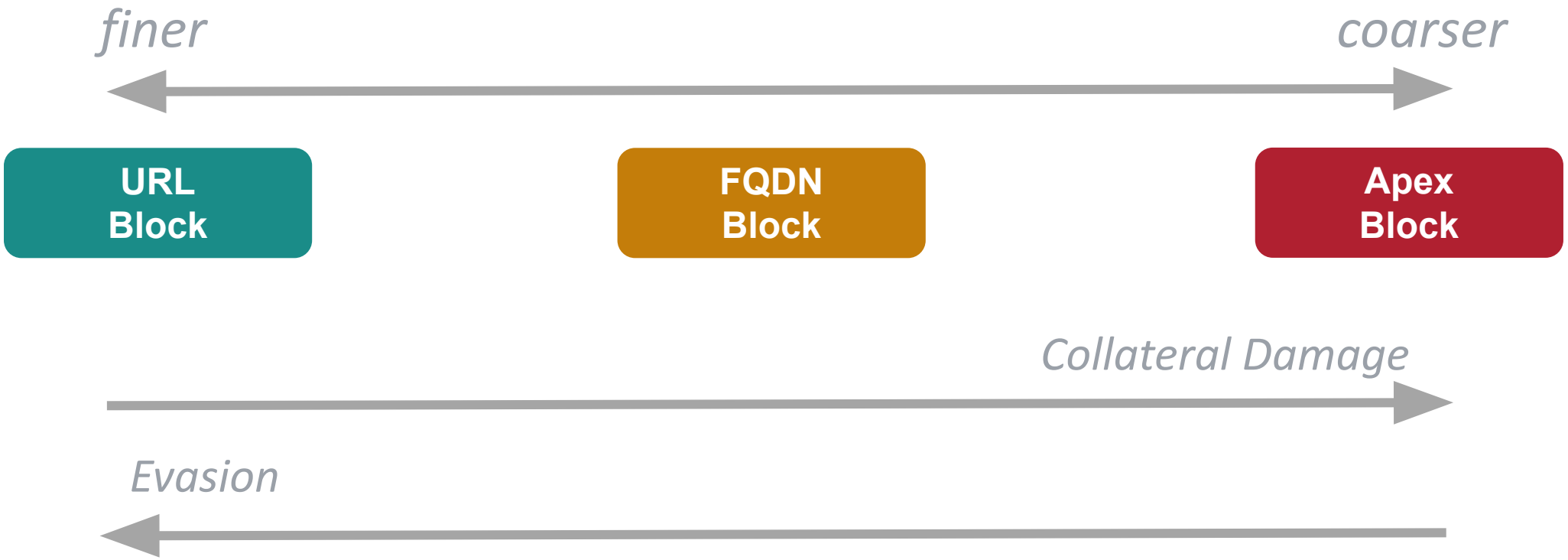
ALIEN VAULT

Blocking Granularity: An Open Challenge





Blocking Granularity Tradeoff



Too coarse-grained → **Overblocking** →Collateral Damage benign users affected

Too fine-grained → **Underblocking** → Trivial Evasion attacker moves content

Our Problem

Given a URL / Domain:

automatically select the optimal blocking granularity that minimizes collateral damage & evasion

Optimal Blocking Depends on Apex Type

institute IMDEA software

URL-LEASING

`github.com/alice/app`

hosts user content
under URLs

shorteners · code hosting
form builders · file sharing



URL Block

SUBDOMAIN-LEASING

`alice.blogspot.com`

users claim subdomains
under the apex

blog platforms · dynamic DNS
free web hosting



FQDN Block

PRIVATE

`evil-payments.com`

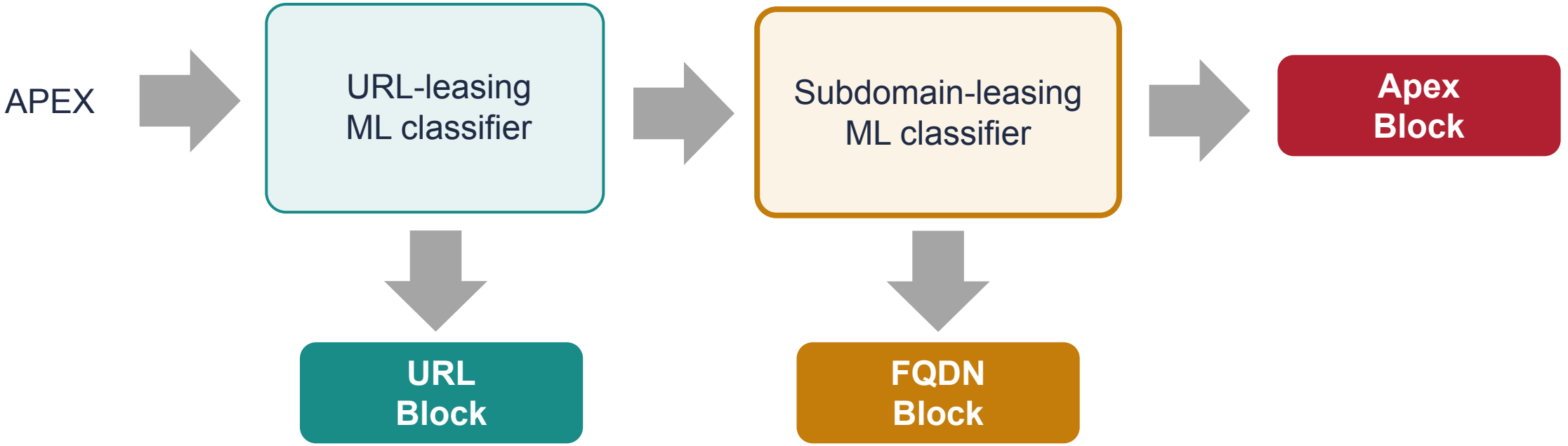
all resources belong
to same owner

attacker-registered
compromised sites

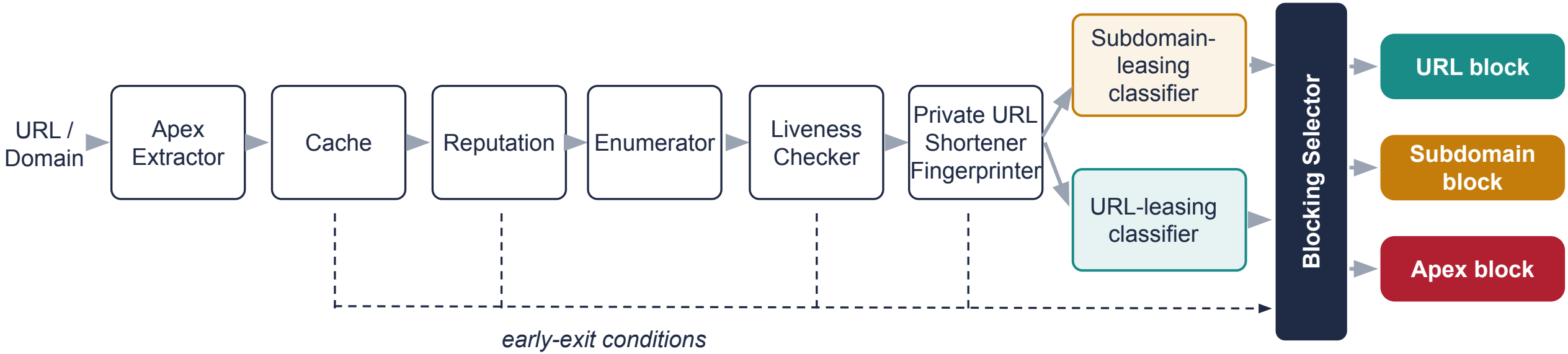


Apex Block

Determining the Apex Type



BlockMeNot: Architecture



Cheap checks first, ML last: ~90% of inputs early-exit, only ~10% reach the classifiers.

ML Classifiers

10,843

manually labeled apexes ground truth

- 6,637 subdomain-leasing
- 1,832 URL-leasing
- 2,394 private

Features: lifetime · volume · lexical · network

SUBDOMAIN-LEASING CLASSIFIER

Gradient Boosting
22 features

0.919

F1 score

precision 0.914 · recall 0.926

URL-LEASING CLASSIFIER

Random Forest
18 features

0.905

F1 score

precision 0.959 · recall 0.867

Evaluation: One Month in the Wild

225K
Entries (URLs / Domains)

75K
Apexes

8
Sources

1,976

leasing apexes identified

1,433 subdomain-leasing
517 URL-leasing
26 both

59%

not in our ground truth

1–10 new per day, even after 3 weeks

hard to keep up for static lists

2.6%

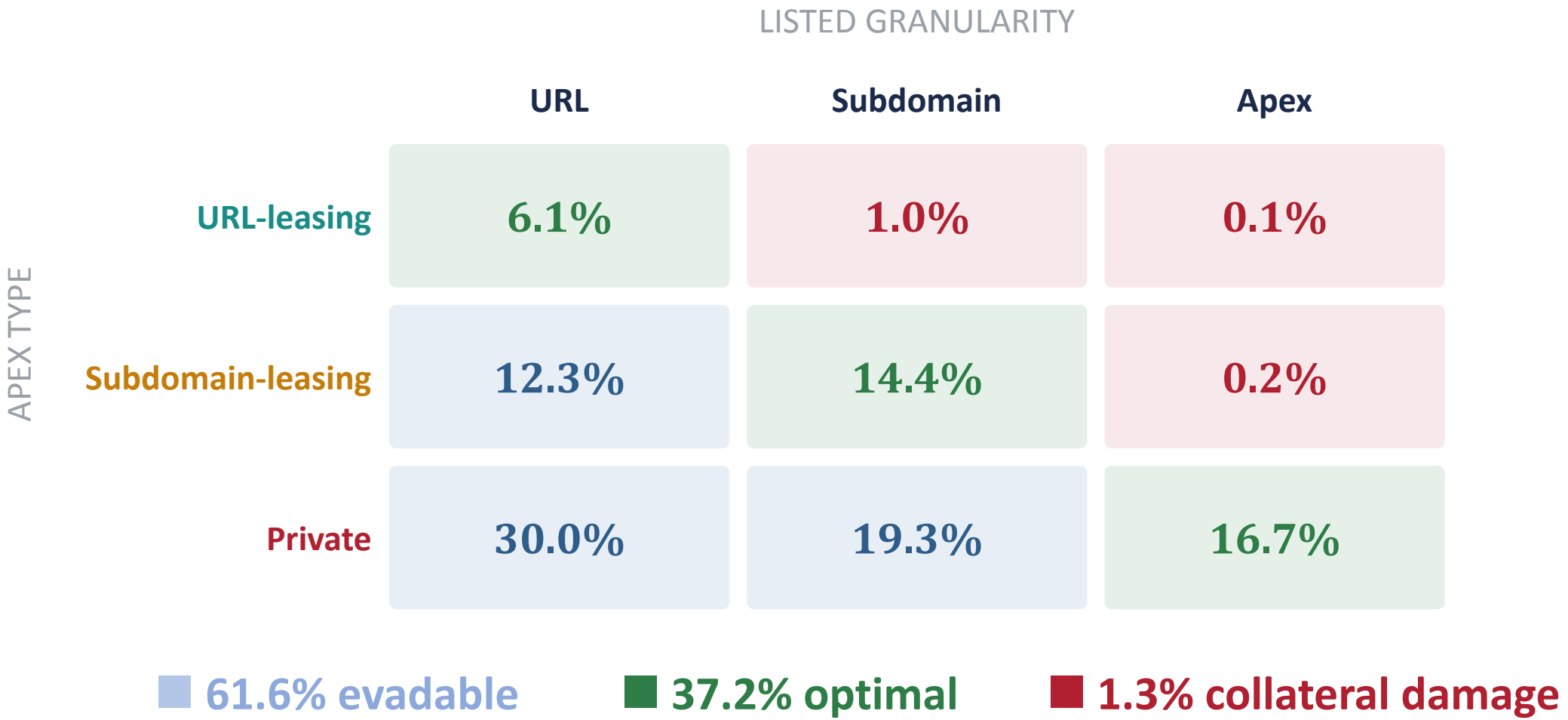
of apexes are leasers

yet they host

34.7%

of all listed entries

Only 37.2% of Listings at Right Granularity



Takeaways

1. First Approach for Automatic Selection of Optimal Blocking Granularity
2. Blocking granularity depends on apex (leasing) type
3. Know the apex type before you block
4. Today, only 1 in 3 listings are blocked at the right granularity

zenodo.org/records/20284621



daud.ahmed@imdea.org