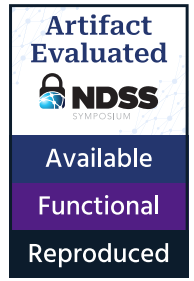


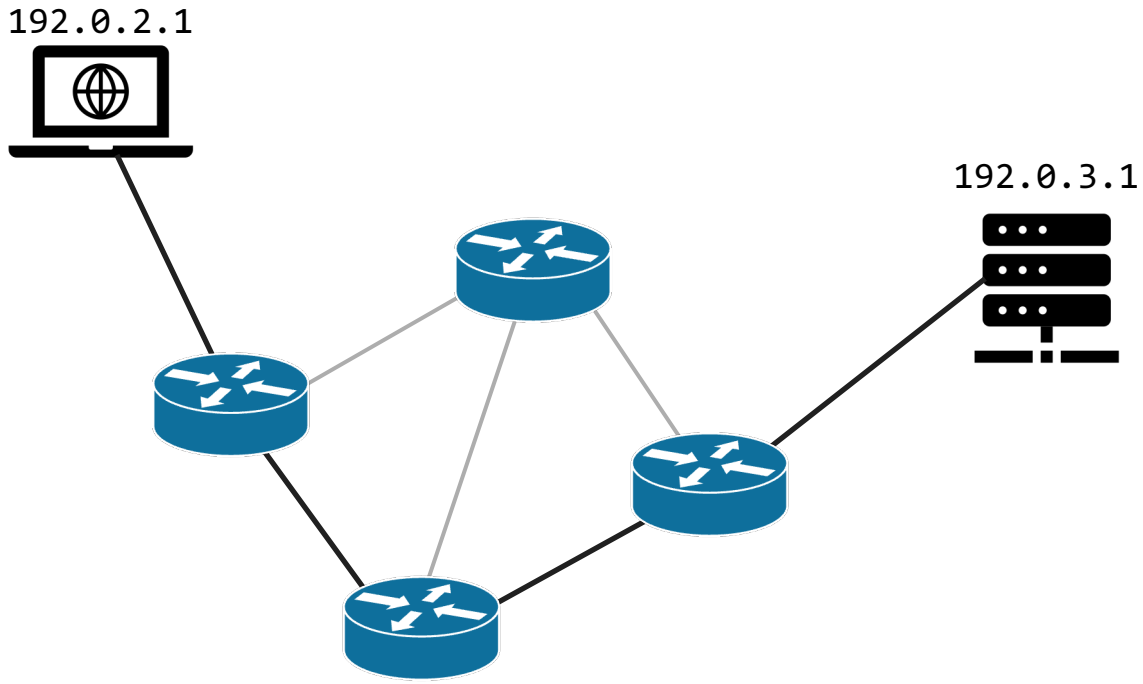
Secure IP Address Allocation at Cloud Scale

Eric Pauley, Kyle Domico, Blaine Hoak , Ryan Sheatsley,
Quinn Burke, Yohan Beugin, Engin Kirda, Patrick McDaniel

What's in an IP(v4) Address?

Intended use: routing traffic between network endpoints

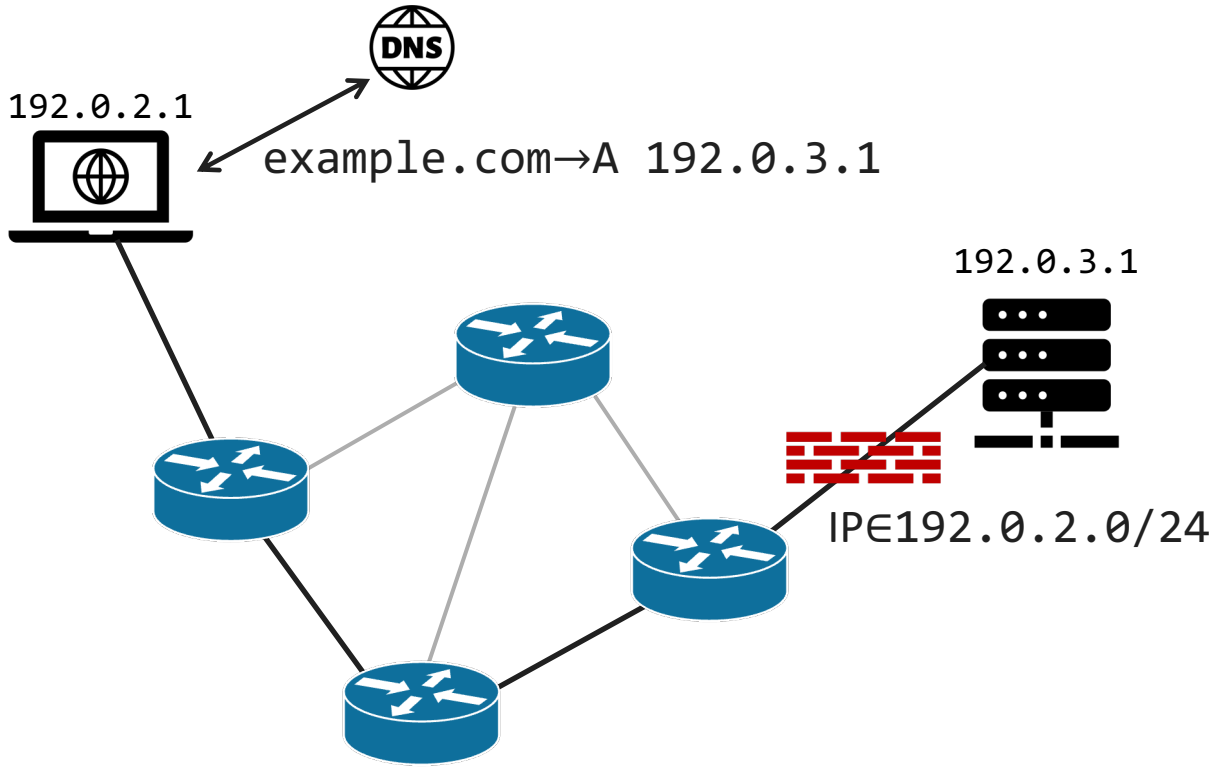
- Map to physical infrastructure
- Owned by organizations
- Long-lived associations



What's in an IP(v4) Address?

In Practice: Security Enforcement

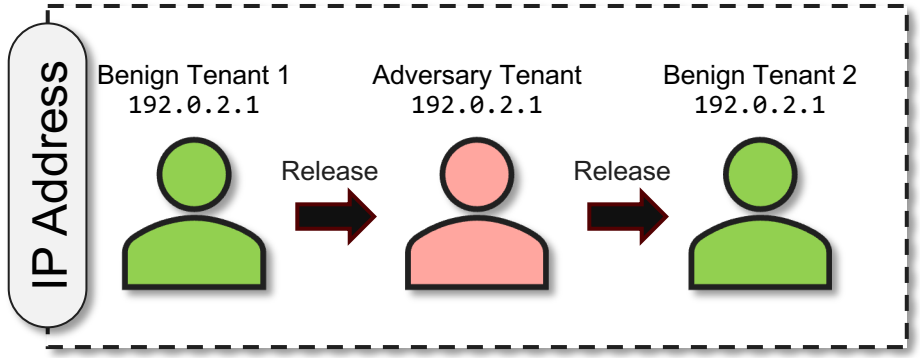
- Firewall rules
- Routing sensitive data
- TLS certificate issuance
  (E.g., LetsEncrypt)
- Email server reputation
- …



Result IPs as *security principals*

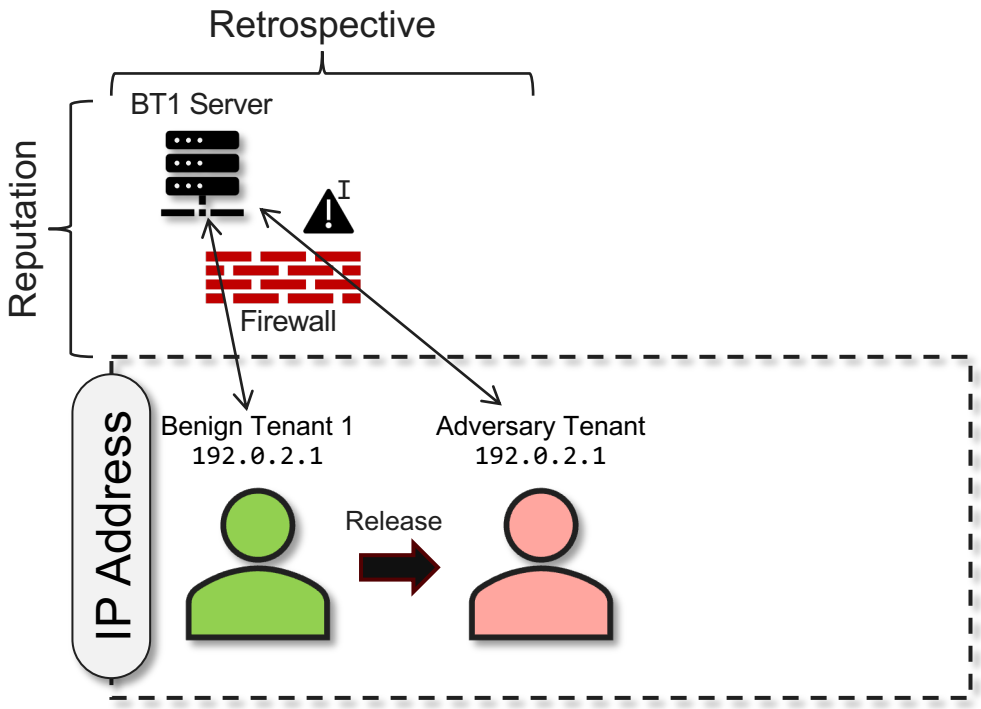
Public Clouds Challenge IP Address Assumptions

- Address control is short-lived
- Elasticity enables attackers to control many addresses
- Benign tenant has *temporal locality* with adversary
  - Next tenant could be adversarial
  - Attacker controlled address previously



Threat: IP Address Reuse in the Cloud Setting

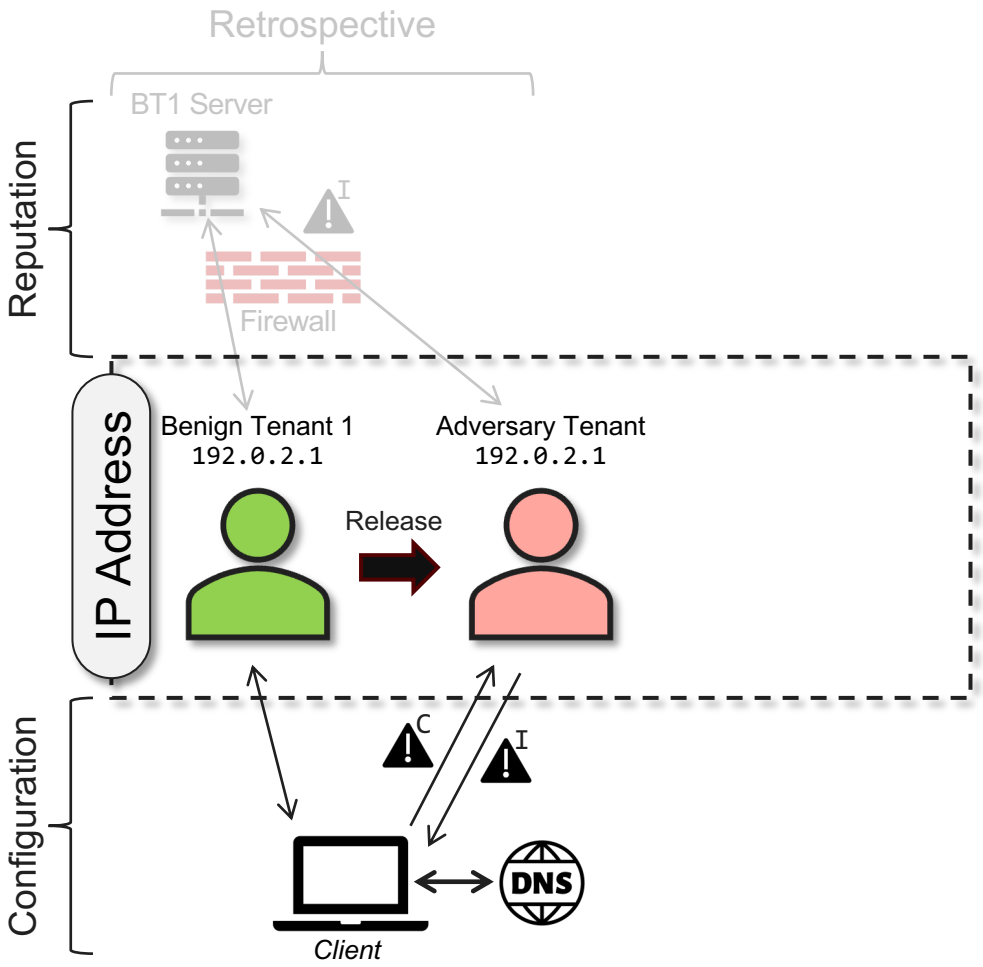
- **Problem 1**: Cloud tenants use IP addresses as a *security principal*
  - Explicitly (security groups) or…



Threat: IP Address Reuse in the Cloud Setting

- **Problem 1**: Cloud tenants use IP addresses as a *security principal*
  - Explicitly (security groups) or…
  - Implicitly (DNS records)

    Result: exploitation by next tenant

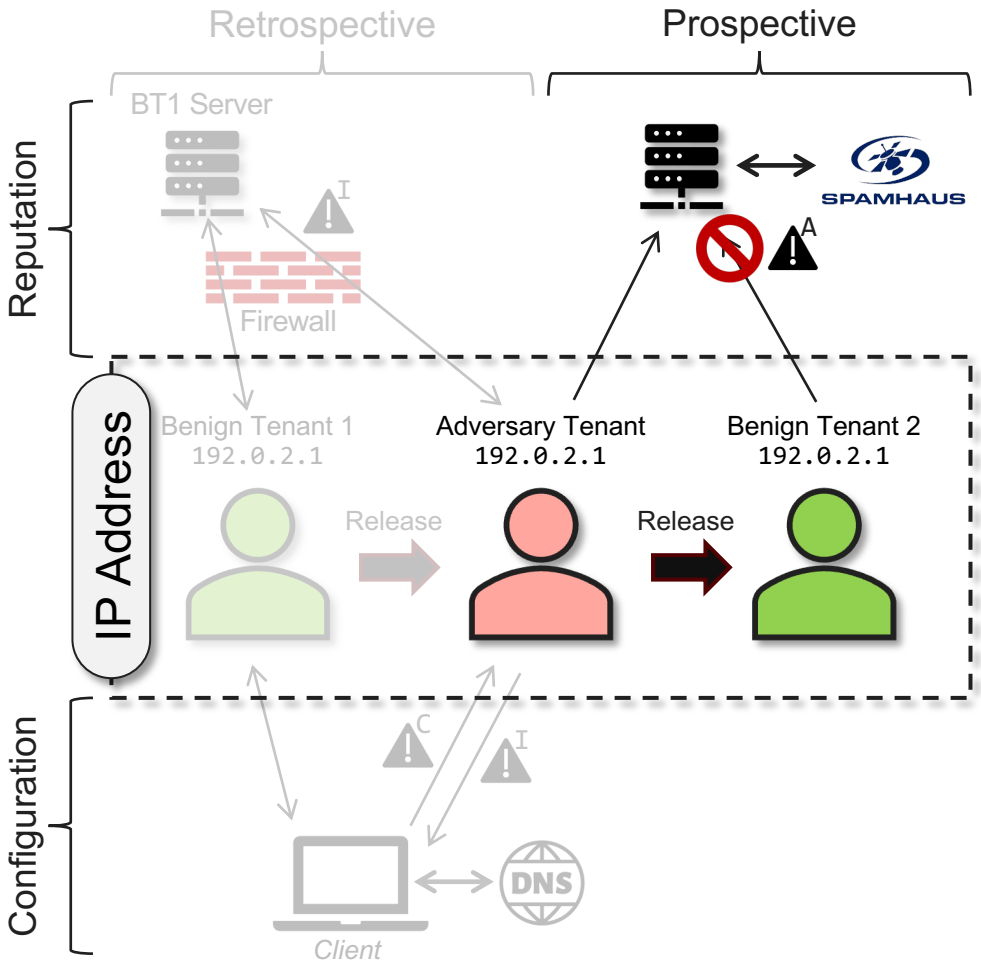


Threat: IP Address Reuse in the Cloud Setting

- **Problem 1**: Cloud tenants use IP addresses as a *security principal*
  - Explicitly (security groups) or…
  - Implicitly (DNS records)

  Result: exploitation by next tenant

- **Problem 2**: Cloud tenants are harmed by previous IP owners
  - Poor address reputation or…



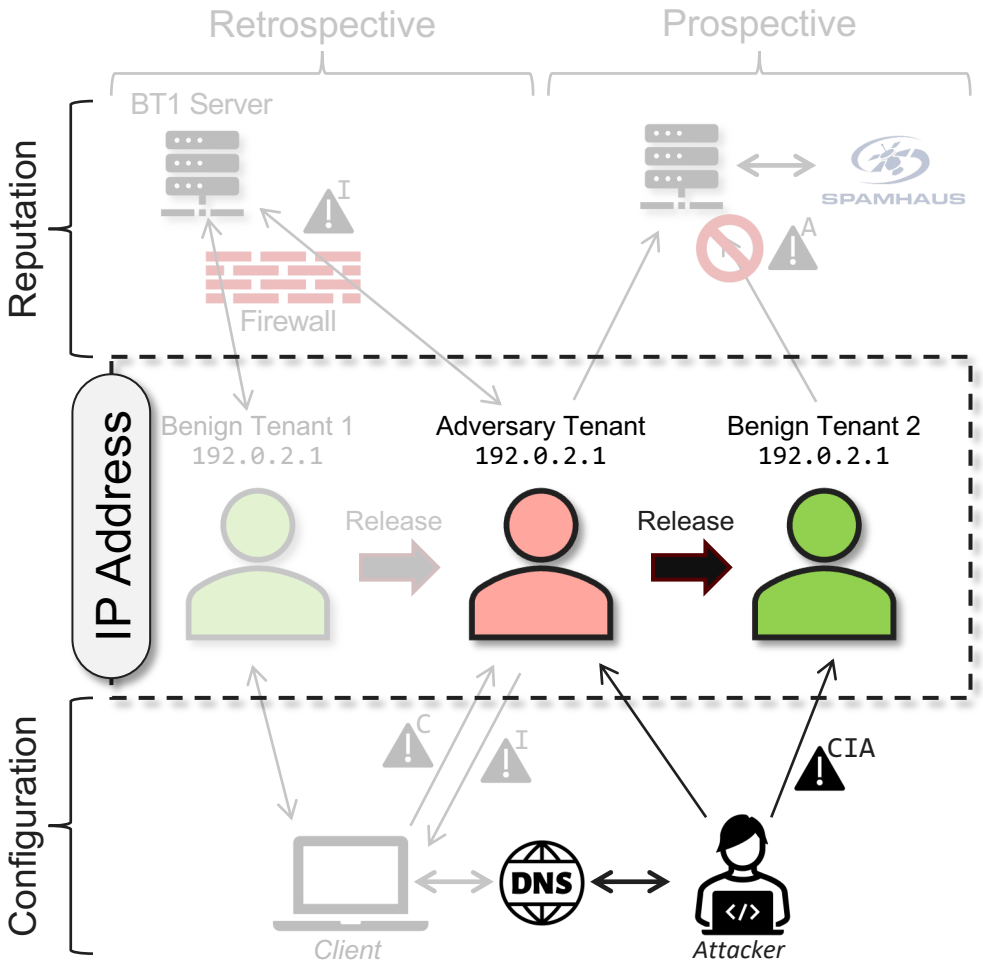
Threat: IP Address Reuse in the Cloud Setting

- **Problem 1**: Cloud tenants use IP addresses as a *security principal*
  - Explicitly (security groups) or…
  - Implicitly (DNS records)

  Result: exploitation by next tenant

- **Problem 2**: Cloud tenants are harmed by previous IP owners
  - Poor address reputation or…
  - Unwanted/attack traffic

    Result: harmed by previous tenant



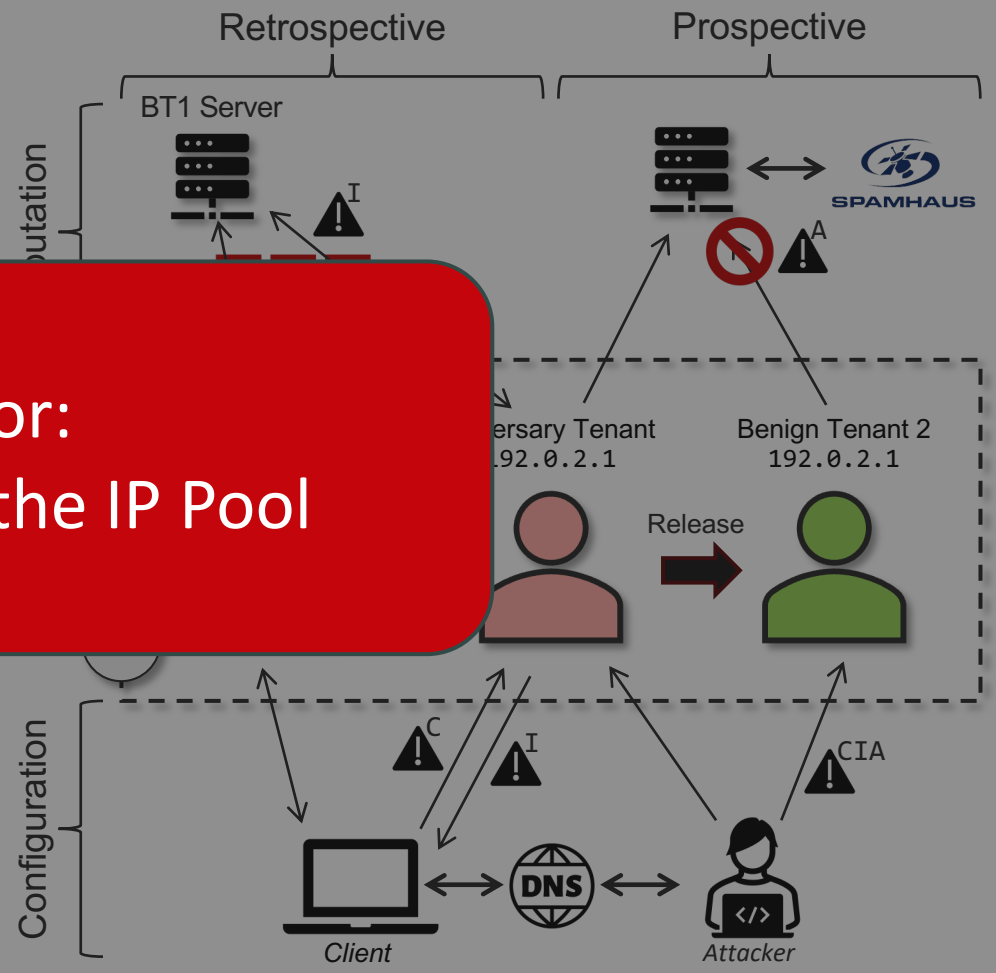
Threat: IP Address Reuse in the Cloud Setting

- **Problem 1**: Cloud tenants use IP addresses as a *security principal*
  - Explicitly (security groups) or…
  - Implicitly (DNS records)

    Result: exp

- **Problem 2**: C
  harmed by previous IP owners
  - Poor address reputation or…
  - Unwanted/attack traffic

    Result: harmed by previous tenant



Common Factor:
Adversaries Scanning the IP Pool

Attackers can enumerate the IP pool (Pauley et al., S&P'22)

Zone	Servers	Unique IPs	Estimated IPs	Capture Rate
us-east-1a	581 k	383 k	789 k	49 %
us-east-1b	607 k	389 k	762 k	51 %
us-east-1c	630 k	236 k	313 k	76 %
us-east-1d	573 k	360 k	700 k	51 %
us-east-1f	647 k	171 k	198 k	87 %
Total	3039 k	1540 k	2762 k	56 %

Random IP address allocation makes pool scanning trivial.

Can we allocate IP addresses securely?

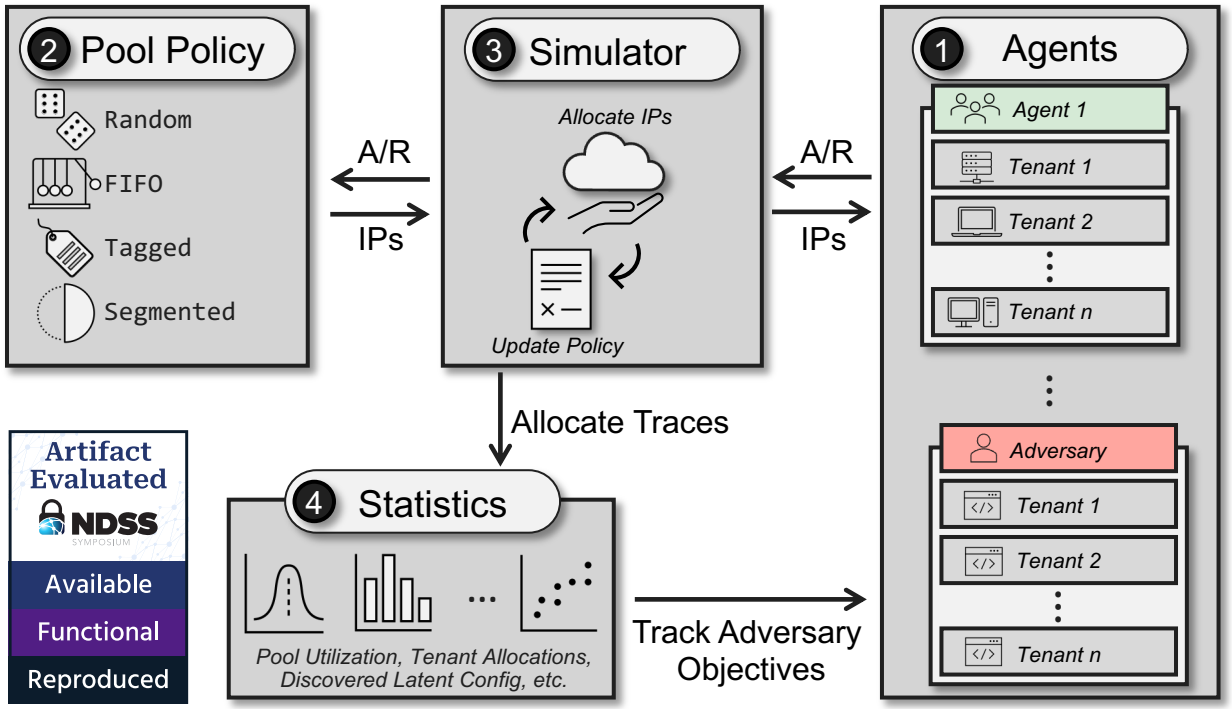
- Goal: Design new allocation *policies* that:
  1. Prevent adversaries from allocating many IPs
  2. Separate adversaries *spatially* and *temporally*

- Challenges:
  1. Adversaries are unknown (must infer from behavior)
  2. Policies cannot harm benign tenants

EIPSIM: Modeling Secure Cloud IP Allocation

Key EIPSIM Features:

- Modular Allocation Policies
- Real & Simulated Traces
- Fine-grained Metrics
- Adversarial Simulation



Existing “smart” policy: IP Tagging (Pauley et al., S&P’22)

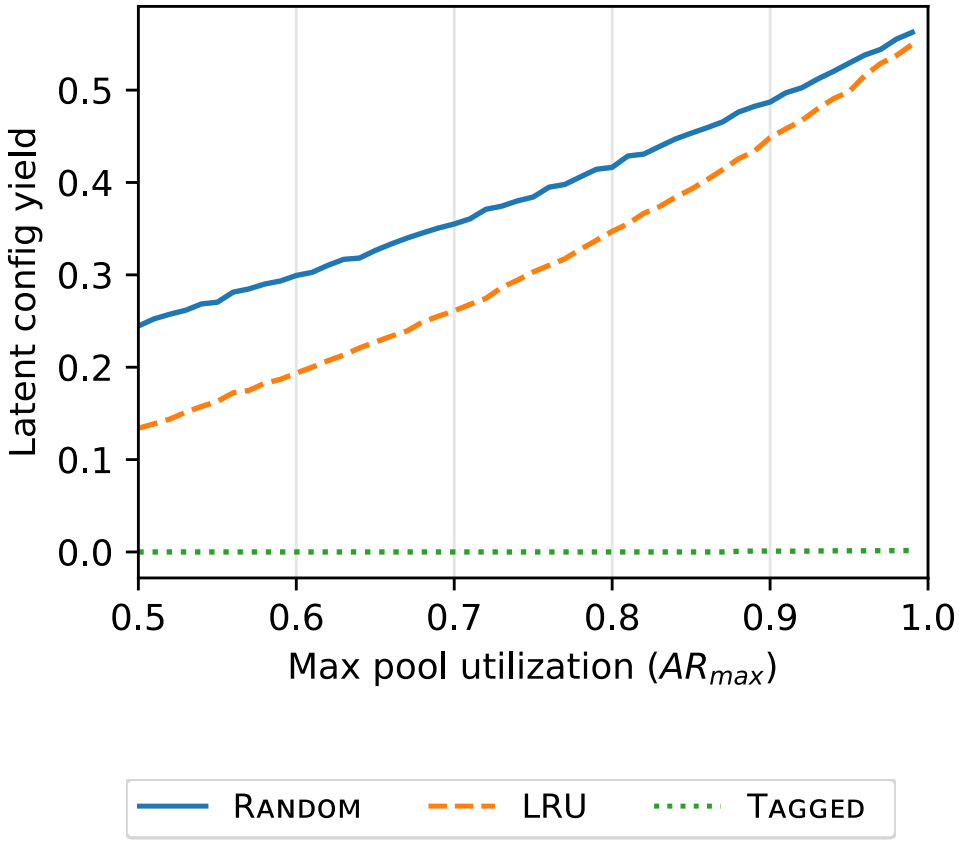
Idea: released IPs are tagged with the tenant’s account ID

- Allocations prefer available IPs tagged to that tenant
- Otherwise: LRU allocation

Existing “smart” policy: IP Tagging (Pauley et al., S&P’22)

Idea: released IPs are tagged with the tenant’s account ID

- Allocations prefer available IPs tagged to that tenant
- Otherwise: LRU allocation

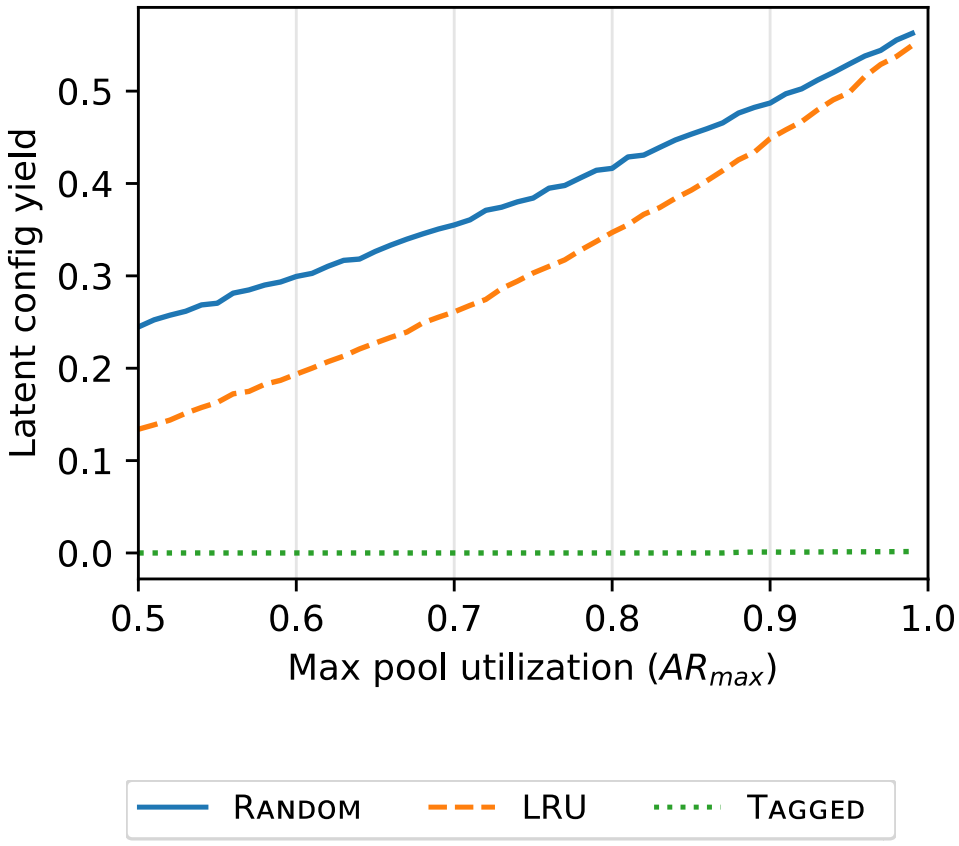


Existing “smart” policy: IP Tagging (Pauley et al., S&P’22)

Idea: released IPs are tagged with the tenant’s account ID

- Allocations prefer available IPs tagged to that tenant
- Otherwise: LRU allocation

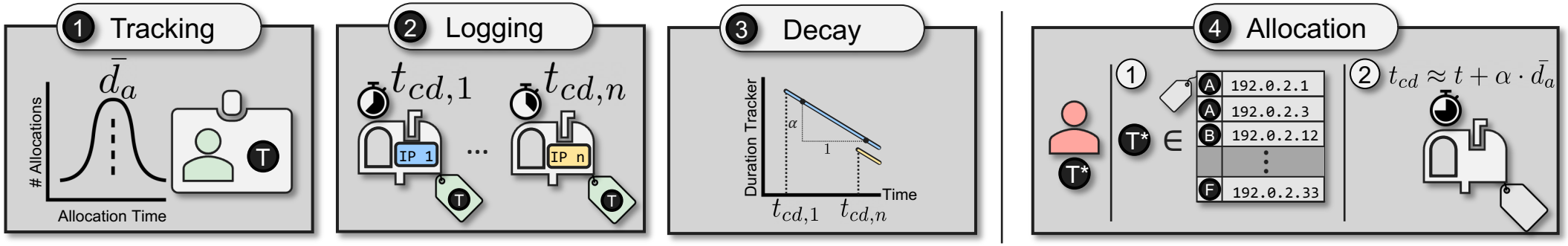
Problem: Relies on adversaries using one cloud account



IP Scan Segmentation: A Robust Defense for IP Pools

Idea: Identify behavior associated with IP pool scanning

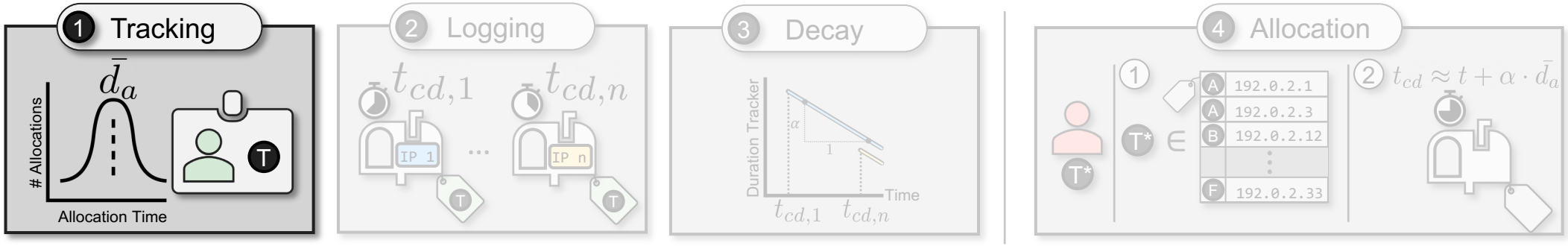
- Prefer allocating the same IPs to these tenants
- Based on allocation duration (shorter is adversarial)



IP Scan Segmentation: A Robust Defense for IP Pools

Idea: Identify behavior associated with IP pool scanning

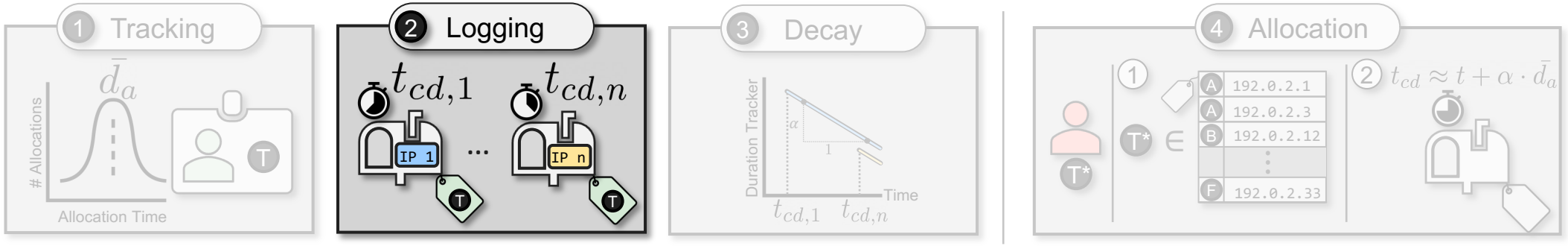
- Prefer allocating the same IPs to these tenants
- Based on allocation duration (shorter is adversarial)



IP Scan Segmentation: A Robust Defense for IP Pools

Idea: Identify behavior associated with IP pool scanning

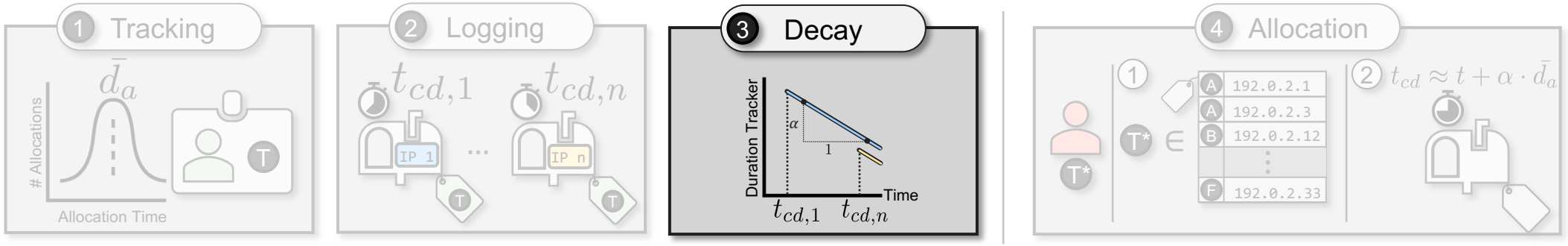
- Prefer allocating the same IPs to these tenants
- Based on allocation duration (shorter is adversarial)



IP Scan Segmentation: A Robust Defense for IP Pools

Idea: Identify behavior associated with IP pool scanning

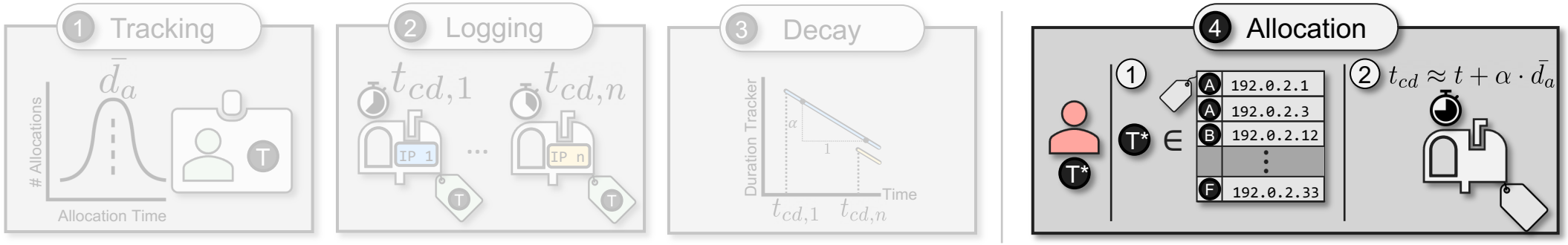
- Prefer allocating the same IPs to these tenants
- Based on allocation duration (shorter is adversarial)



IP Scan Segmentation: A Robust Defense for IP Pools

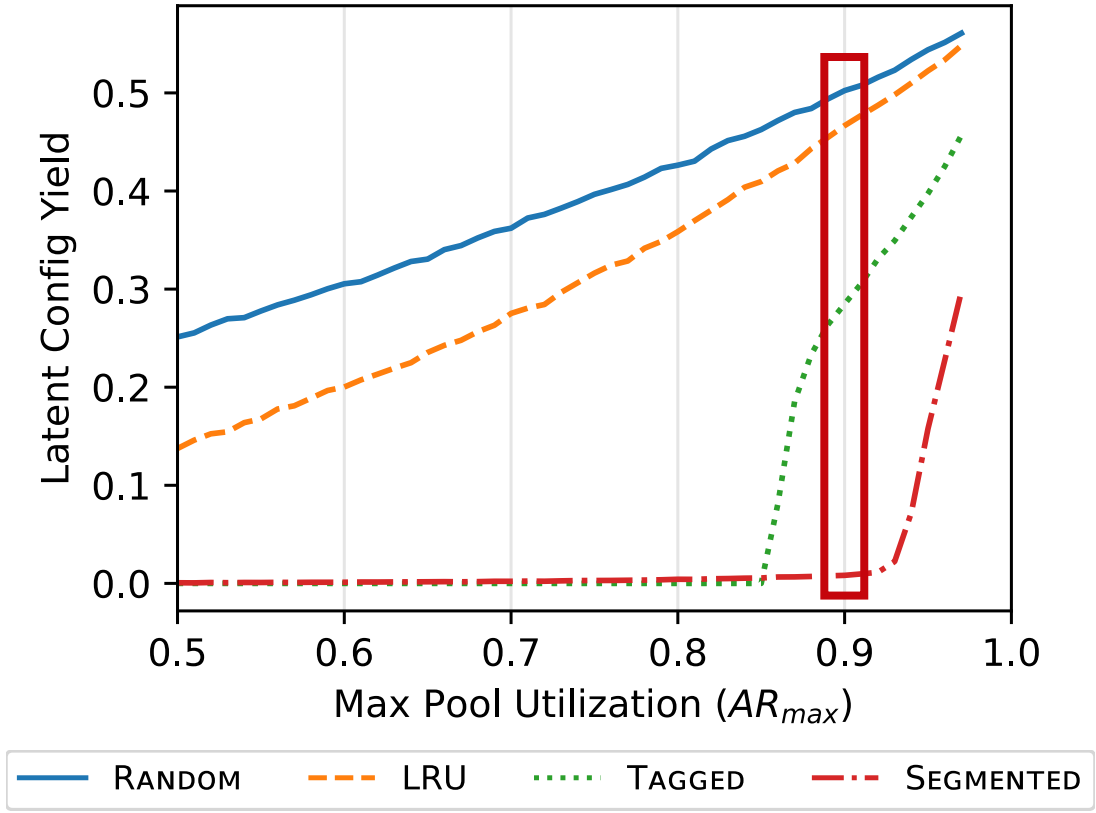
Idea: Identify behavior associated with IP pool scanning

- Prefer allocating the same IPs to these tenants
- Based on allocation duration (shorter is adversarial)



Result: Strong Protection Against IP Pool Scanning

84% reduction in adversary success (worst-case)

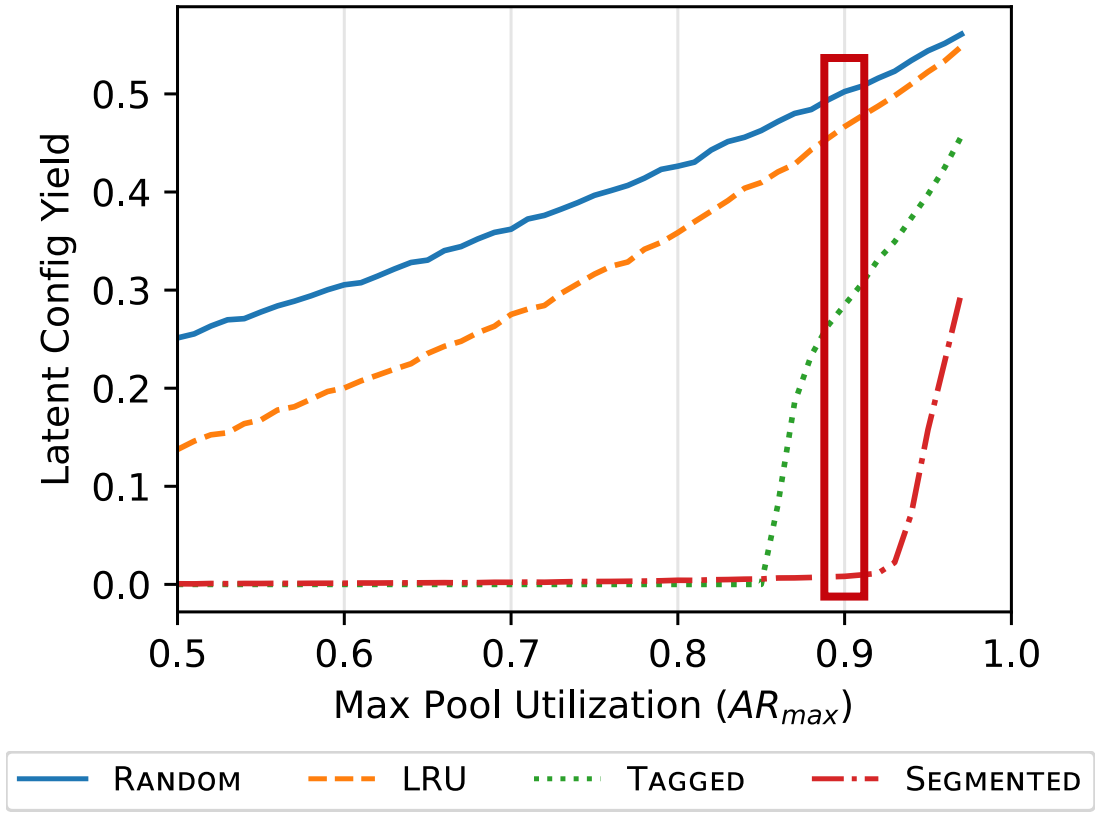


Result: Strong Protection Against IP Pool Scanning

84% reduction in adversary success (worst-case)

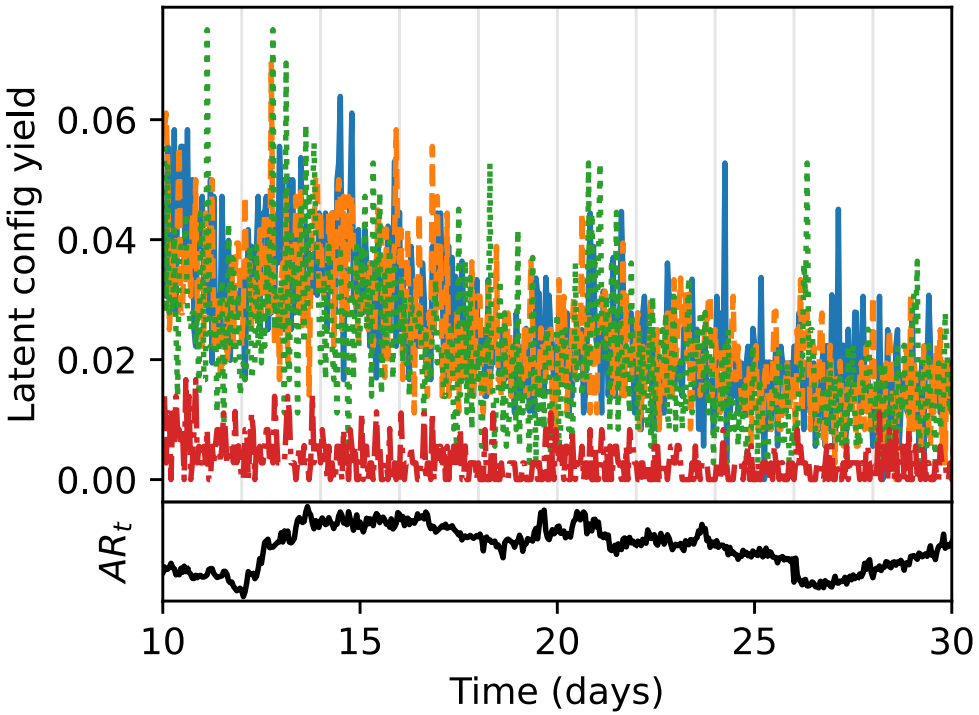
Scales to 10M+ Addresses (more than largest cloud AZ)

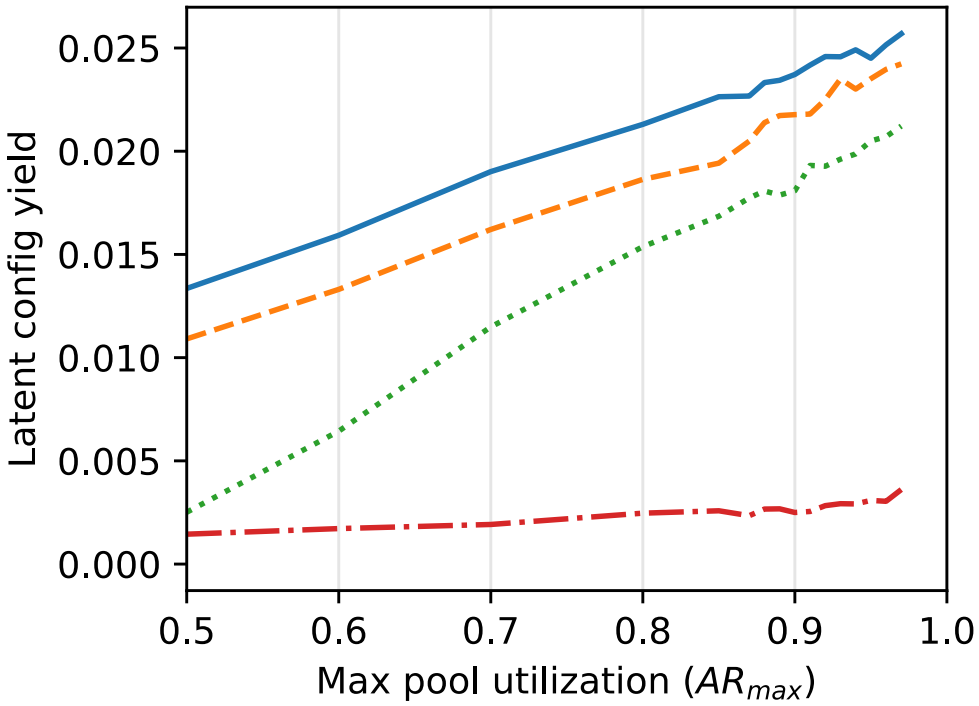
# IPs	Runtime	Speedup	Allocations	Allocs/s
100	500 ms	17 M	4.2 k	8.3 k
1 k	530 ms	16 M	26 k	48 k
10 k	2 s	4.3 M	220 k	110 k
100 k	14 s	630 k	2.2 M	160 k
1 M	187 s	46 k	22 M	120 k
10 M	2.3 ks	3.8 k	220 M	97 k



Validation on Real-World Traces

Real-world allocations via Google `clusterdata-2019` dataset





Now what?

Cloud Providers	→	Adopt new IP allocation policies to protect customers
Cloud Customers	→	Avoid public IP addresses for access control (use TLS, IAM, private networks)
Security Researchers	→	Embrace simulation using synthetic and real-world data for evaluation of secure systems
CS Departments	→	*Hire me!*

epauley@cs.wisc.edu

pauley.me/eipsim