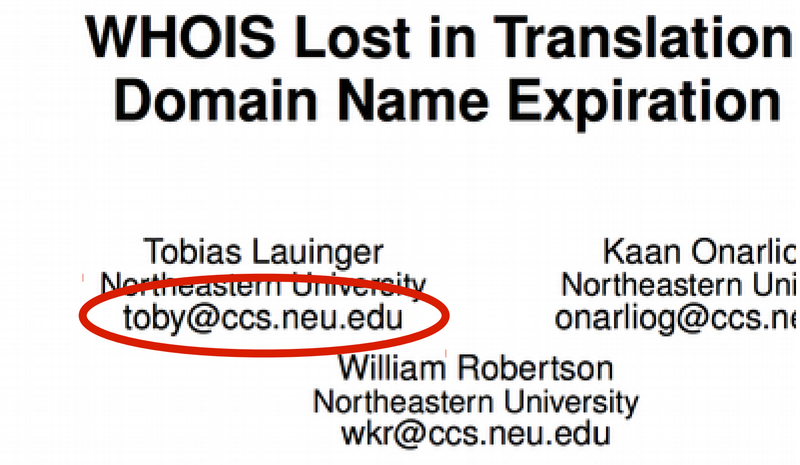
Toby Lauinger, Abdelberi Chaabane, Ahmet S. Buyukkayhan,
Kaan Onarlioglu, William Robertson

Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Usenix Security 2017

Internet Domain Names

- Used in many, often security-critical ways

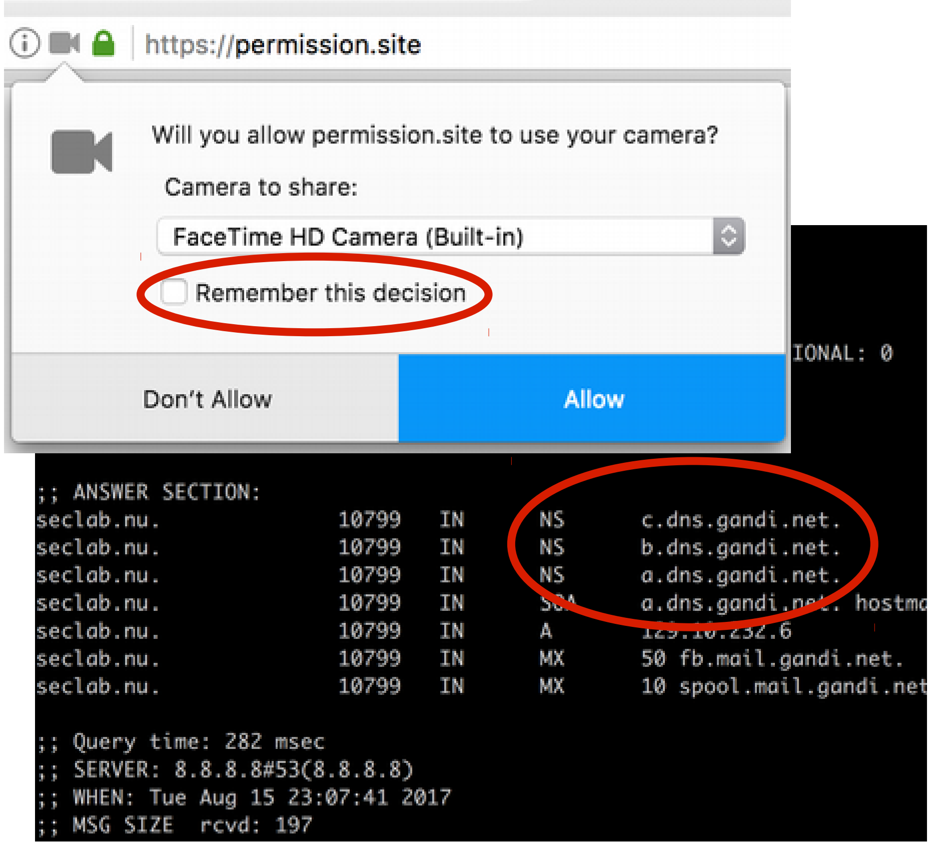


WHOIS Lost in Translation
Domain Name Expiration

Tobias Lauinger
Northeastern University
toby@ccs.neu.edu

Kaan Onarlic
Northeastern Uni
onarliog@ccs.ne

William Robertson
Northeastern University
wkr@ccs.neu.edu



https://permission.site

Will you allow permission.site to use your camera?

Camera to share: FaceTime HD Camera (Built-in)

☐ Remember this decision

```
                                                                   IONAL: 0

;; ANSWER SECTION:
seclab.nu.              10799   IN      NS      c.dns.gandi.net.
seclab.nu.              10799   IN      NS      b.dns.gandi.net.
seclab.nu.              10799   IN      NS      a.dns.gandi.net.
seclab.nu.              10799   IN      SOA     a.dns.gandi.net. hostma
seclab.nu.              10799   IN      A       129.10.232.6
seclab.nu.              10799   IN      MX      50 fb.mail.gandi.net.
seclab.nu.              10799   IN      MX      10 spool.mail.gandi.net

;; Query time: 282 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Aug 15 23:07:41 2017
;; MSG SIZE  rcvd: 197
```

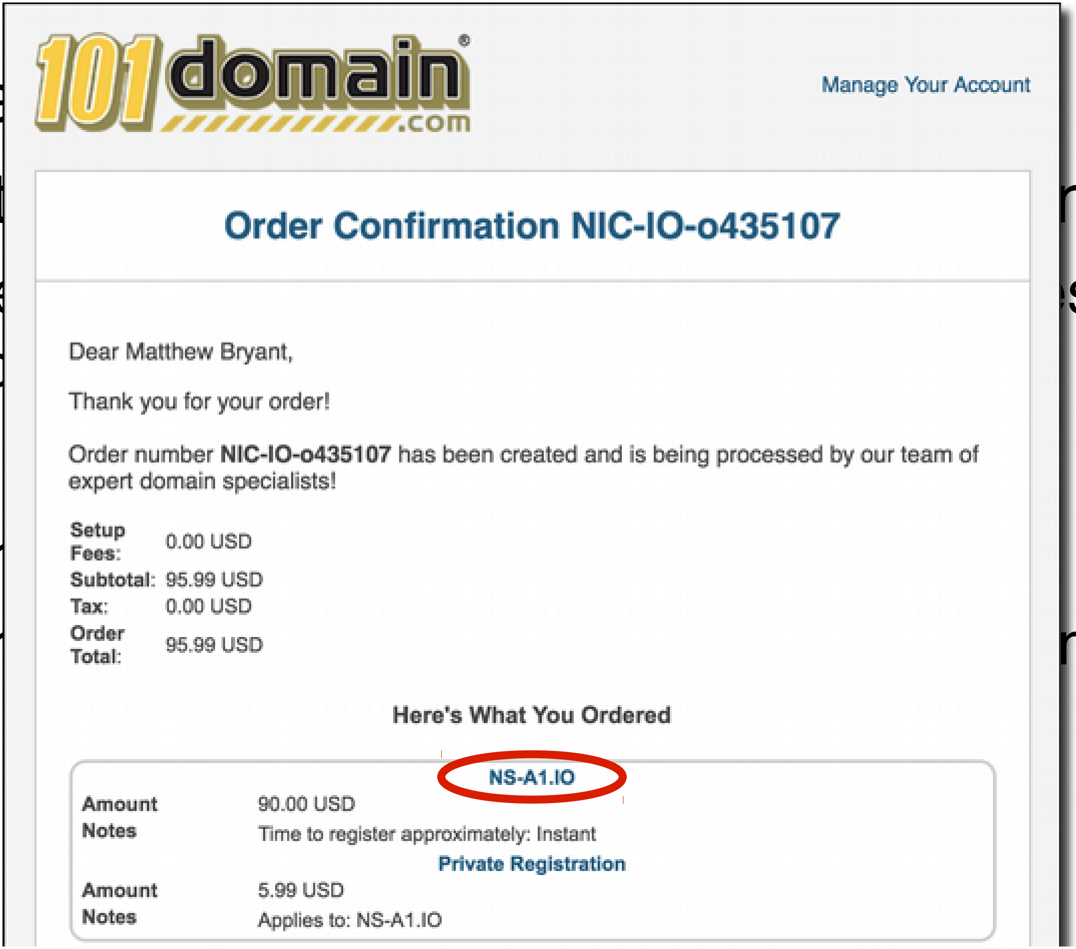
- Typically, assumption of constant ownership
- However, hundreds of thousands of domains expire *every day*

Attacks Involving Expired Domains

- Abuse of residual trust
- Schlamp et al., “The Abandoned Side of the Internet” (2014)
  - Re-register domains to take over email addresses used to manage critical resources (e.g., IP prefix or AS)
- Lever et al., “Domain-Z” (2016)
  - Take over software update/repository servers
  - Take over name servers used by non-expired domains

Attacks Involving Expired Domains

- Abuse of re
- Schlamp et ... nternet" (2014)
  - Re-registe ... s used to manage c
- Lever et al.
  - Take over
  - Take over ... mains



Manage Your Account

Order Confirmation NIC-IO-o435107

Dear Matthew Bryant,

Thank you for your order!

Order number **NIC-IO-o435107** has been created and is being processed by our team of expert domain specialists!

Setup Fees:	0.00 USD
Subtotal:	95.99 USD
Tax:	0.00 USD
Order Total:	95.99 USD

Here's What You Ordered

NS-A1.IO

Amount	90.00 USD
Notes	Time to register approximately: Instant

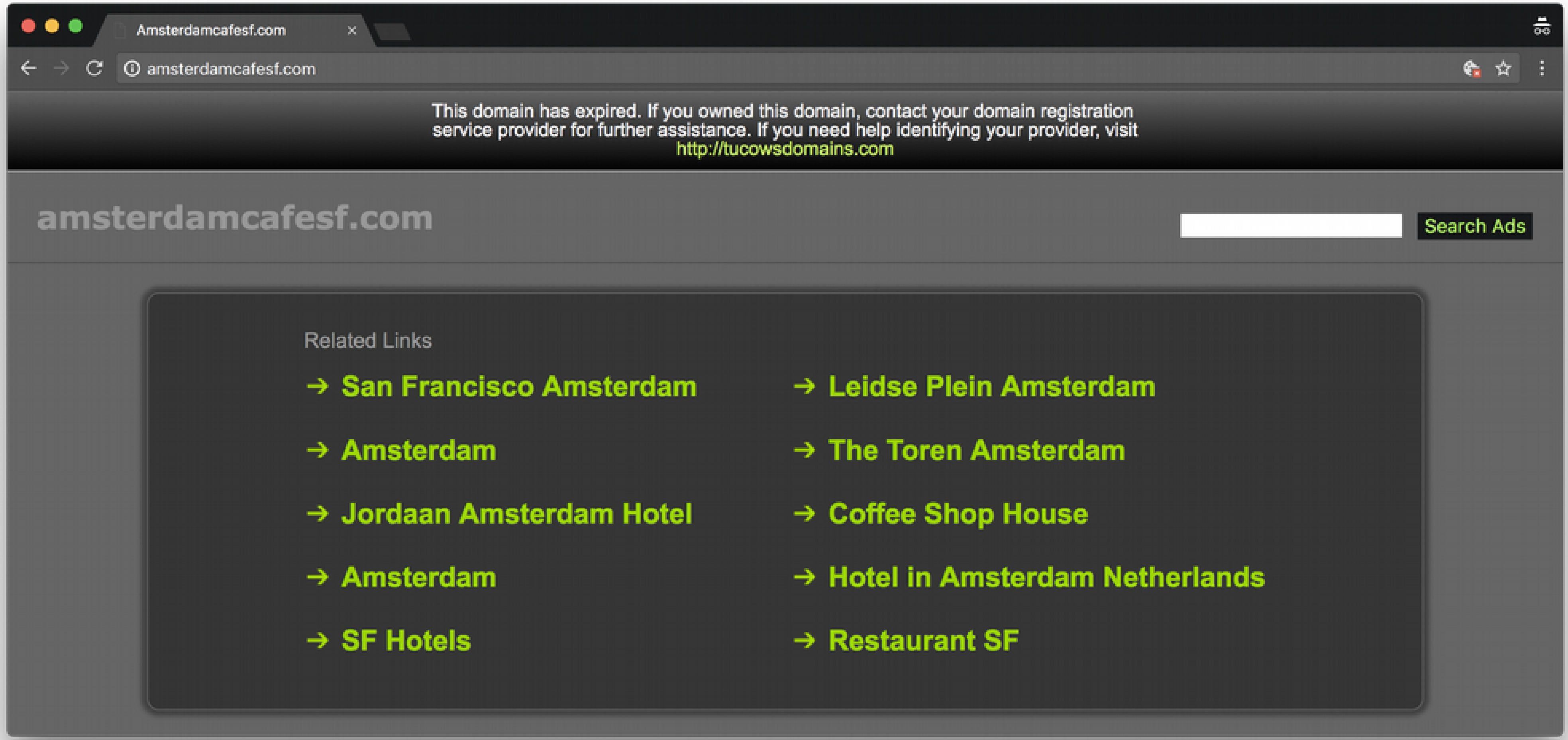
Private Registration

Amount	5.99 USD
Notes	Applies to: NS-A1.IO

Also, Undesirable Behaviour

- When re-registered, domains often not what visitors expect
  - E.g., formerly useful website turned into spam page
- ICANN:
  - "(…) websites featuring nothing but advertisements, thus leading to a form of **Internet graffiti**."
  - "(…) **profit-making abuse** of the domain name system"
  - https://www.icann.org/news/announcement-2009-08-12-en

Also, Undesirable Behaviour



This domain has expired. If you owned this domain, contact your domain registration service provider for further assistance. If you need help identifying your provider, visit http://tucowsdomains.com

amsterdamcafesf.com

Related Links

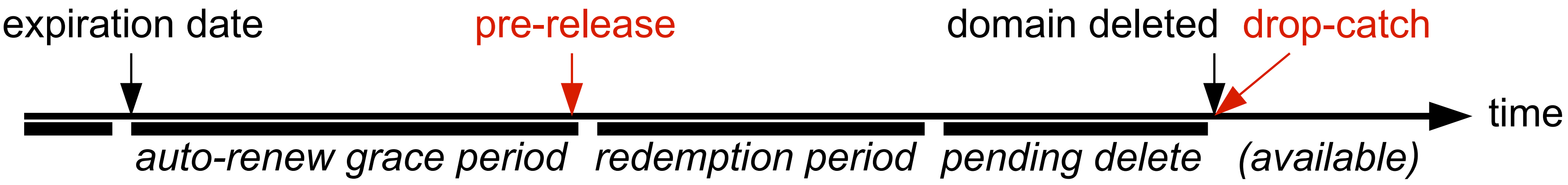
- → San Francisco Amsterdam
- → Amsterdam
- → Jordaan Amsterdam Hotel
- → Amsterdam
- → SF Hotels
- → Leidse Plein Amsterdam
- → The Toren Amsterdam
- → Coffee Shop House
- → Hotel in Amsterdam Netherlands
- → Restaurant SF

Contribution: The Big Picture

- Attack potential known, but how many opportunities?
- Quantification of domain name “recycling”; two scenarios:
  - Drop-catch: Re-registered instants after general availability
  - Pre-release: Sold by registrar before general availability

- Frequent and *competitive* domain takeovers
- Impact of this practice on domain registration ecosystem

Domain Expiration & Takeover Opportunities



- After expiration, two grace periods allow recovery before deletion
- See “Whois Lost in Translation” (IMC 2016) for the details of domain expiration states
- Re-register immediately when deleted (drop-catch)
- Old registrar: sell before deletion (pre-release)

Data Collection Overview

- Drop-catch services and pre-release platforms promote lists of available domains → use as seed for measurement
- Whois lookups every 14 days to detect status changes
- All listed domains during 4 weeks in July/August 2016

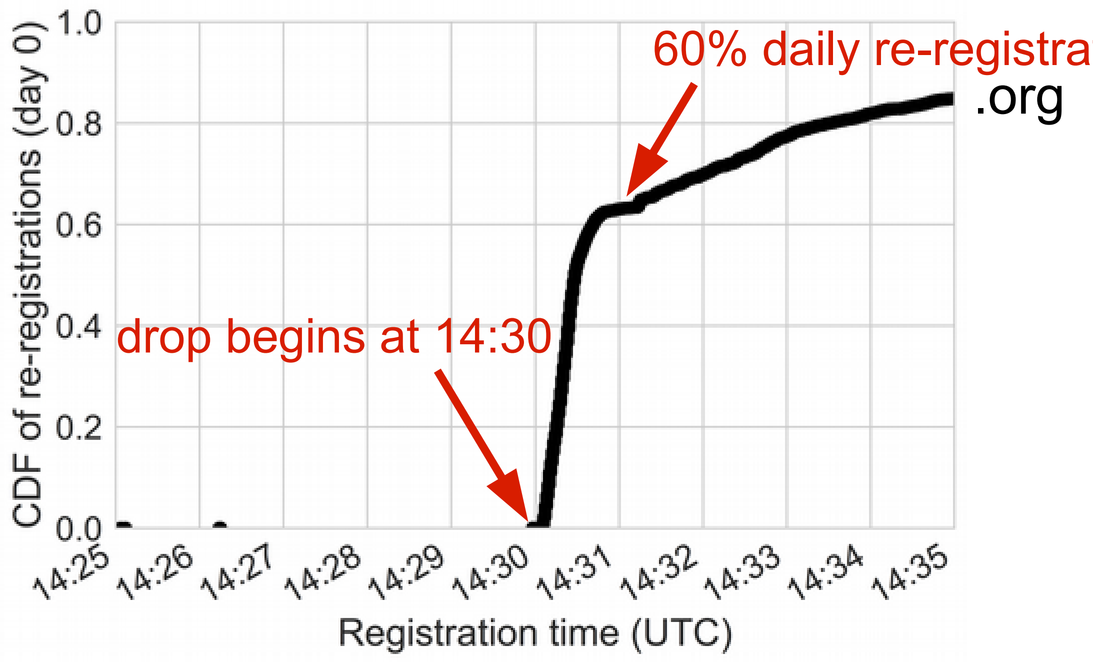
	com	net	org	biz	name
Pre-release total	1.2M	135k	116k	21k	182
Median/day	43.5k	4.9k	4k	710	7

	com	net	org	biz
Pending delete total	2.1M	255k	169k	51k
Median/day	76.4k	9.2k	6.1k	1.7k

Expiration, Pre-Release and Drop-Catch

- August 2016:
  - 131M .com domains registered
  - 2.2M .com domains deleted after expiration (1.7% of zone)
  - 2.6M .com domains created (new & re-registrations)
- Measurement (28 days):
  - 1.2M .com domains available *pre-release*; 71k sold
  - 10.1% of deleted .com domains re-registered as *drop-catch*
- *Domain reuse is a frequent phenomenon*

Re-Registrations During the Drop



60% daily re-registrations done by 14:31

drop begins at 14:30

- The “drop”: Domains deleted (and re-registered) during same daily time span
- *Re-registration as early as possible hints at significant competition*

Drop-Catch Registrars

- Registries impose rate limits on each registrar
- Drop-catch services use multiple registrars to increase success rates
  - “DropCatch.com *n* LLC”
  - “Charlemagne 888, LLC”, “George Washington 888, LLC”, “Napoleon Bonaparte, LLC”, ...

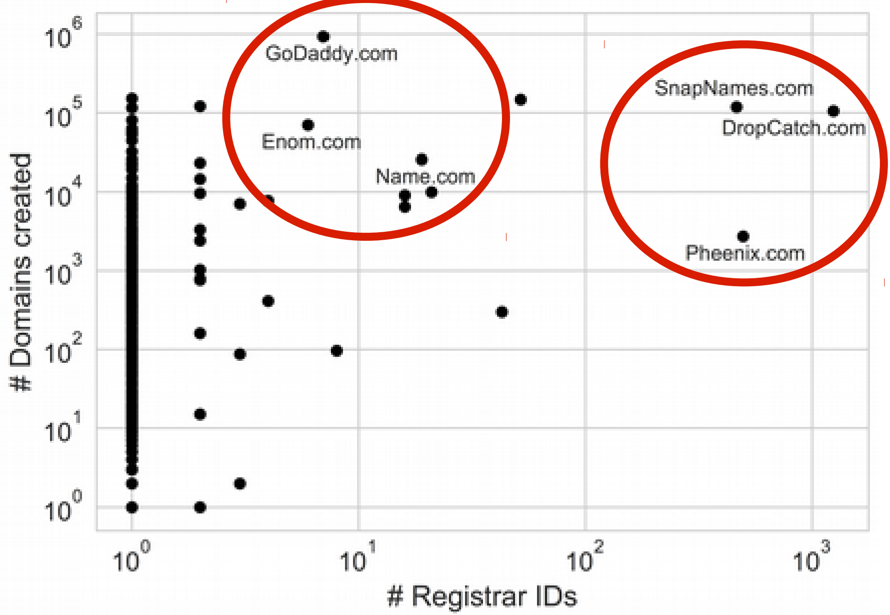
Registrar Clustering

Name	Cluster Size	%
DropCatch.com	1252	42.6%
Pheenix.com	498	16.9%
SnapNames.com	466	15.8%
LogicBoxes.com	53	1.8%
MyDomain.com	43	1.5%

February 2017

- Top 3 clusters are well-known drop-catch services
- They account for over 75% of all accredited registrars (but only 8% of monthly domain creations)
- These clusters have been growing in size
- *Significant resources are deployed to compete in the drop*

Cluster Size ⇎ Domain Registrations



February 2017

- Large cluster not necessary to create many domains
- 99.9% of domain creation attempts fail; drop-catch responsible for at least 80%
- *Drop-catch has large impact on domain registration ecosystem*

Discussion & Recommendations

- Results show frequent, professionally organised “recycling” of domains, expending significant resources
- Security consequences of domain “recycling”:
  - Attacks related to residual trust abuse
  - Annoyance (“Internet graffiti”)
  - Pre-release risks (potential to evade registration-time detection)
- Recommendation: “Domain Transparency”

Conclusion

- Take-away points:
  - *Domain-based trust mechanisms should anticipate ownership changes as a common, expected event.*
  - *Anti-abuse tools may need improved detection of ownership changes that are not re-registrations.*

- Paper-exclusive material:
  - Drop-catch domain tasting, auctions and prices, age and traffic
  - More on pre-release, drop-catch registrar characteristics & arms race...

Northeastern

Secure Systems Lab

https://seclab.ccs.neu.edu/