

Binding Identity to Domains: An Analysis of Security Risks and Synchronization Failures



Anupam Khargharia '26

Dr. Ewa Syta, Department of Computer Science, Trinity College

DNS-based identity verification (DNS integration) often fails to stay in sync in practice, leaving outdated “verified” identities that can be exploited when the underlying domain state changes. We conduct a large-scale measurement study to quantify this risk and build tools to detect stale bindings and protect users and organizations.

Introduction

- Platforms verify organizations by asking them to prove control of domain via DNS.
- Once verified, the domain is shown as a trusted badge.
- If the domain’s state changes, the app should update the badge.
- In practice, DNS is not re-checked frequently → outdated badges and misplaced trust.

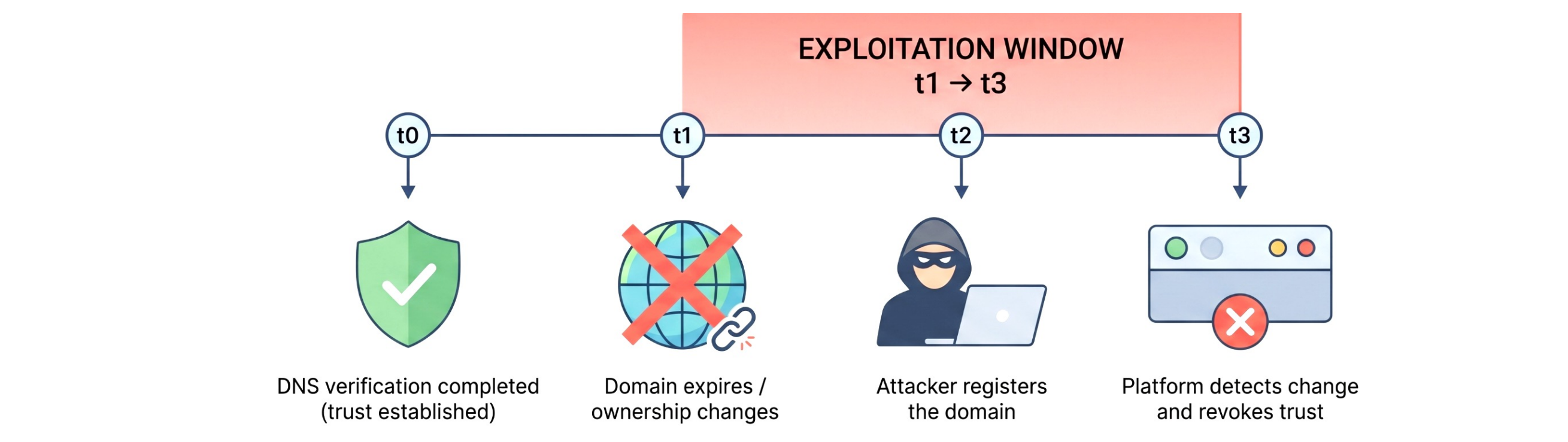
Research Questions – Part 1

- How fast does DNS update across resolvers?
- How long do apps keep the trusted badge after domain state changes?

Results – Part 1

- DNS updates in < 1 minute → resolvers are not the bottleneck.
- GitHub and Bluesky: no revocation observed.
- Keybase: revokes within 24 hours.
- Repeated across multiple trials over 8 weeks for consistent results.

Accurate DNS integration application badge Stale DNS integration application badge



Organization service

Scan Summary
An overview of your domain's monitoring status and detected integrations.

MONITORED TARGET
bskyakhargha1.help
kharghariaanupam07@gmail.com

LAST SCAN
Apr 28, 12:22 AM
Next: Apr 29, 12:22 AM

INTEGRATIONS
1/3 Active
3 total tracked

ALERT STATE
1 BROKEN
Check timeline for details

User extension

GoDaddy
Proof not present
Verified
222 followers

Unverified
One or more domains are missing the required proof for being linked to this organization.
godaddy.com - Unverified
Checked: _gh-godaddy-o.godaddy.com

GitHub Organization
broken

Shared live domain status

FIRST DISCOVERED
Apr 13, 2026, 12:22 AM

LAST VALID CHECK
Apr 27, 2026, 12:22 AM

PROOF BROKEN AT
Apr 28, 2026, 12:22 AM

Research Questions – Part 2

- Given that stale DNS integrations exist, what is their scale, and how many are exploitable today and at what cost?
- What should robust DNS verification behavior look like?

Scale of stale DNS integrations

Platform	Total organizations	Stale organizations	Cost to hijack (USD)
GitHub	10,125,663	10,337 (0.1%)	714,287 (\$70 avg.)
Bluesky	257,277	3,352 (1.3%)	136,152 (\$40 avg.)

Results – Part 2

- Identified stale badges tied to expired domains via large-scale study.
- Built a monitoring service to detect and alert organizations to stale DNS integrations.
- Built a browser extension that shows real DNS state to end users.

Acknowledgment

- Prof. Ewa Syta for her guidance and support
- The Trinity College Computer Science Department