

CAREER: Tools and Techniques for Preserving Integrity on the Web

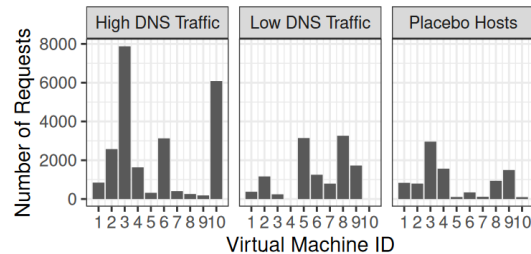
Problem:

- Attackers can compromise users and websites through a seemingly inexhaustible collection of web attacks
 - Domain hijacking
 - Search-engine poisoning
 - Re-registering expired domains
 - Malvertising

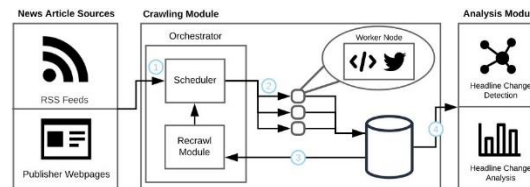
Our approach:

- **We identify "stateless linking" as the core problem that enables these attacks.** There are no guarantees that what was linked yesterday is the same as what is being accessed today.
- **Measure the magnitude of this effect in the wild.** How many critical domains expire each day? How many are trusted in the context of remote APIs, JavaScript libraries etc?
- **Develop countermeasures to preserve integrity.** Signature-based and anomaly-based systems that can handle the dynamicity of the web while stopping abuse.

Once popular domain names continue to be trusted by Internet Infrastructure post expiration



Tracking post-publication title changes by popular media outlets



Challenges:

- Web is highly dynamic, by design. Integrity-preserving systems must account for that.
- Our proposed systems must be able to work for both popular and unpopular web applications

Scientific Impact:

- First work that identifies stateless linking and lack of content integrity as a fundamental issue enabling multiple different attacks.
- Proposed link-discovery and link-management systems capture implicit and explicit expectations of web developers.
- Content integrity has implications outside of traditional security and privacy, namely, integrity of online content and misinformation.

Broader Impact:

- Increase the security of all websites and user trust of the web platform
- Educational opportunities for underrepresented groups through SBU's WISE program

Award Number: 1941617 (2020 – 2025)
Institution: Stony Brook University
Nick Nikiforakis (nick@cs.stonybrook.edu)