Domain Shadowing: Leveraging Content Delivery Networks for Robust Blocking-Resistant Communications

Mingkui Wei
Assistant Professor
Cybersecurity Engineering Department
George Mason University

Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Domain Shadowing

- A censorship evasion technique using content delivery networks (CDNs)

- Similar to, but different from, *domain fronting*:
  - Can use one CDN to visit any websites, no matter they are on the same CDN or even using a CDN
  - Exploits a legitimate CDN feature that is harder to be disabled

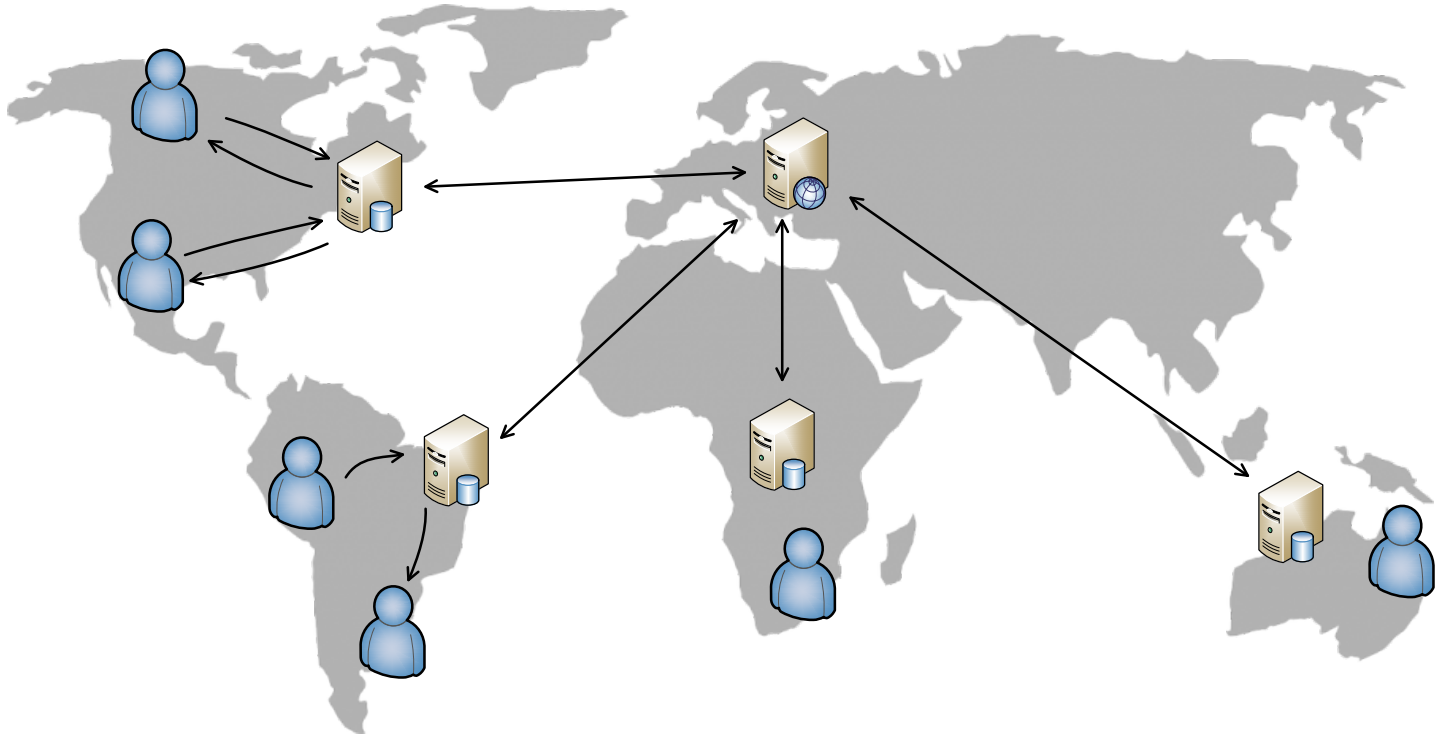
MASON

Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

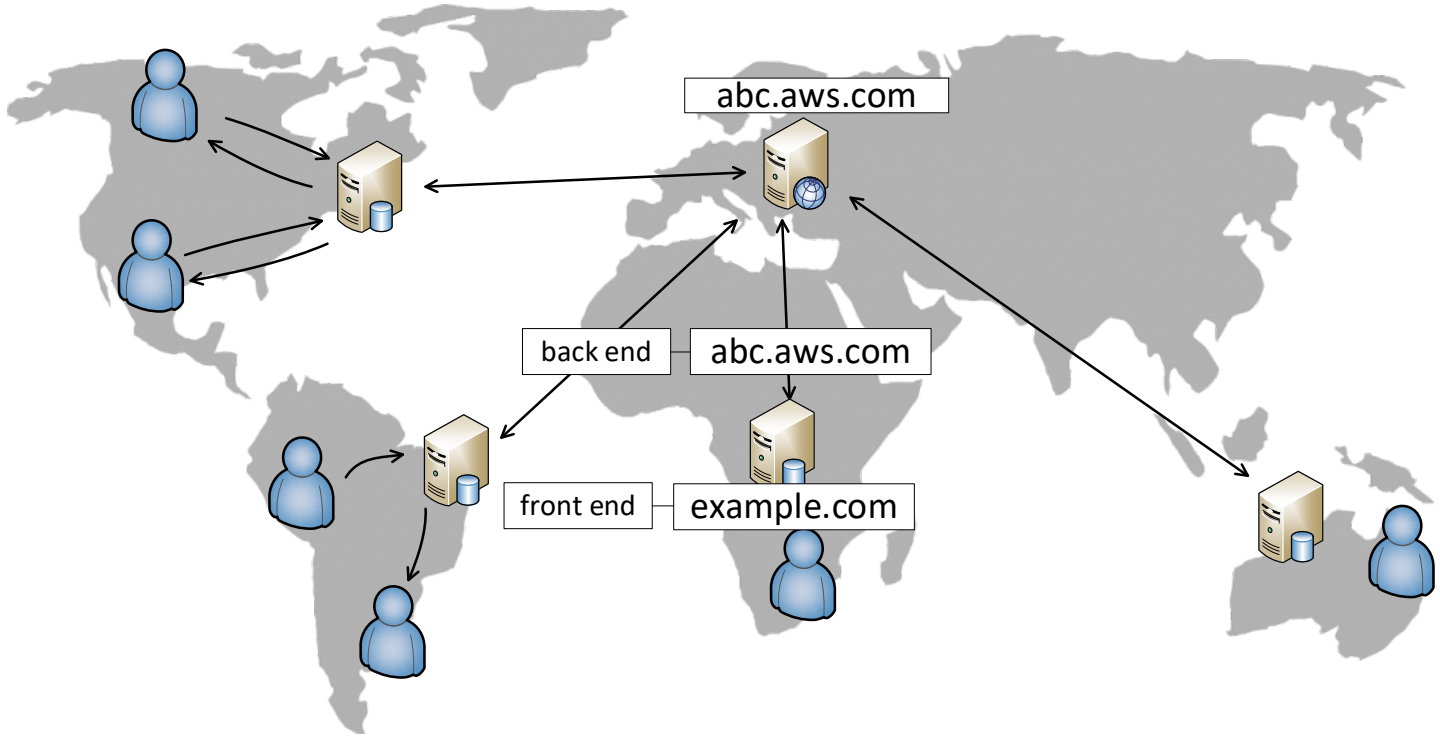
Content Delivery Networks

- Basically, a CDN is a shared web cache



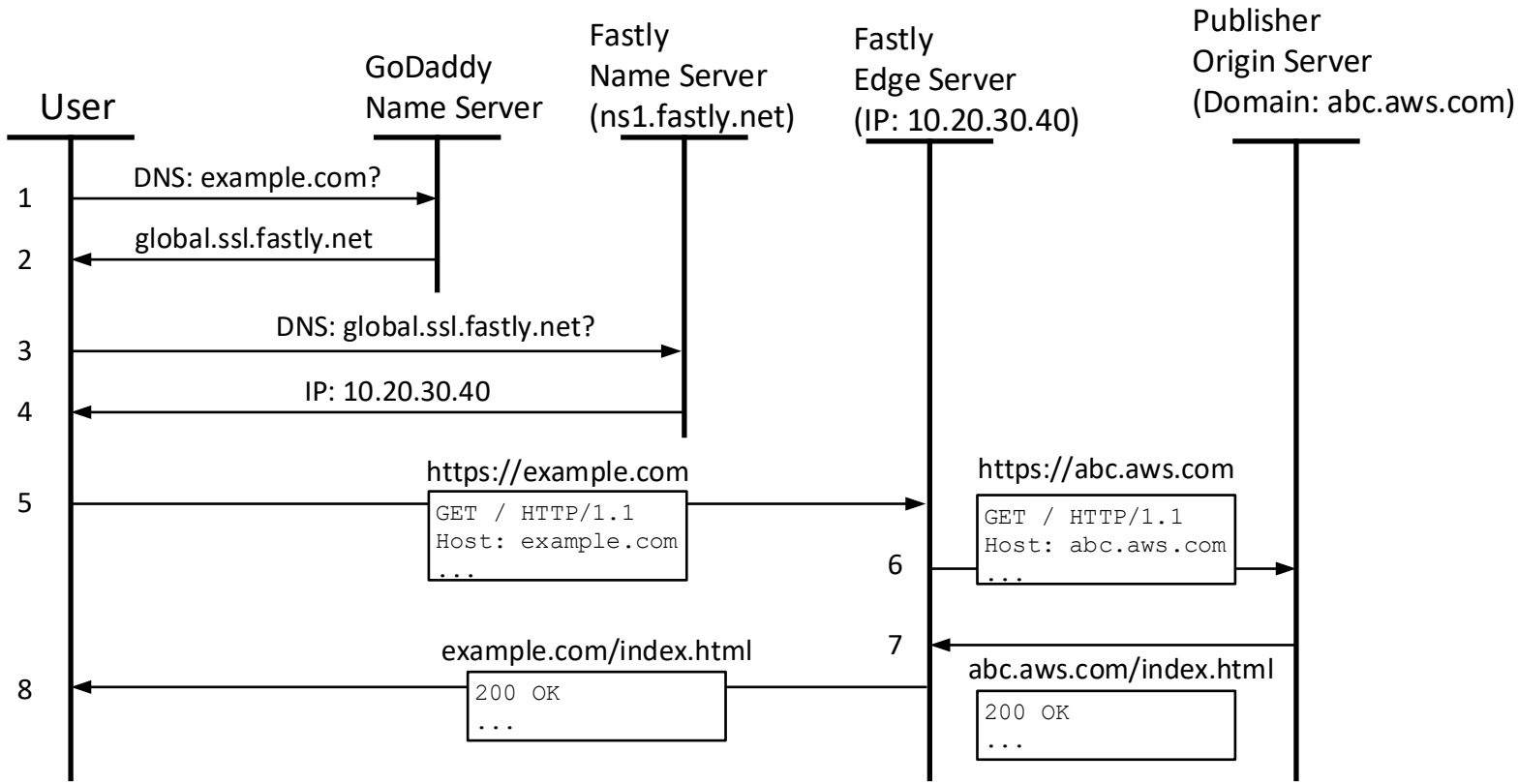
Content Delivery Networks

- But it also handles domain name transformation



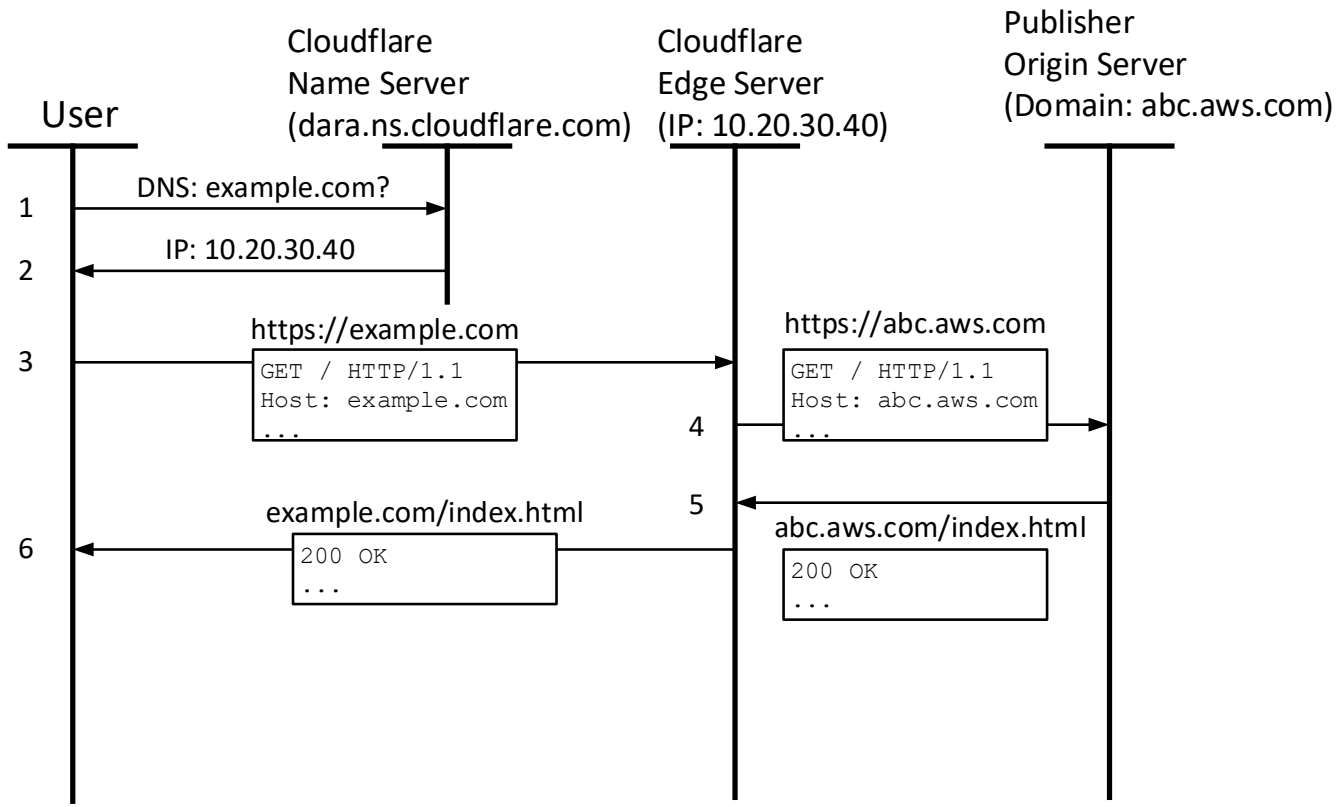
Domain Name Transformation

- The Fastly version (abc.aws.com → example.com)



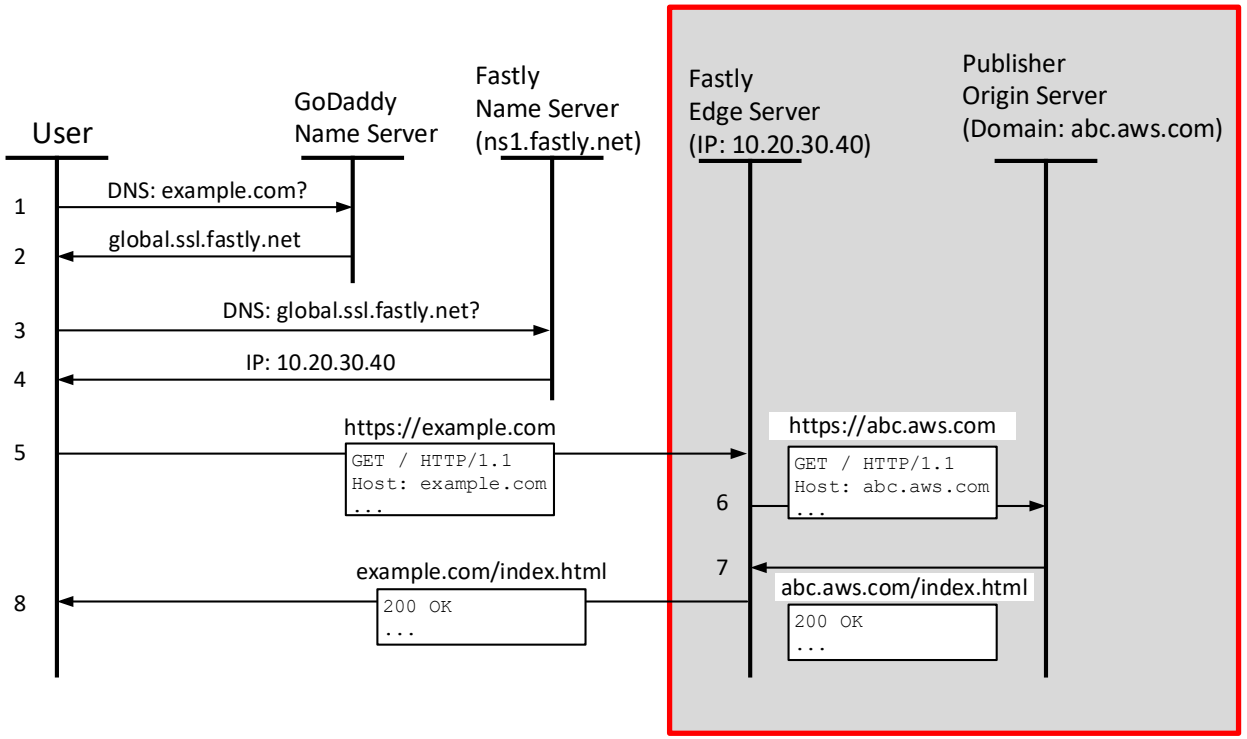
Domain Name Transformation

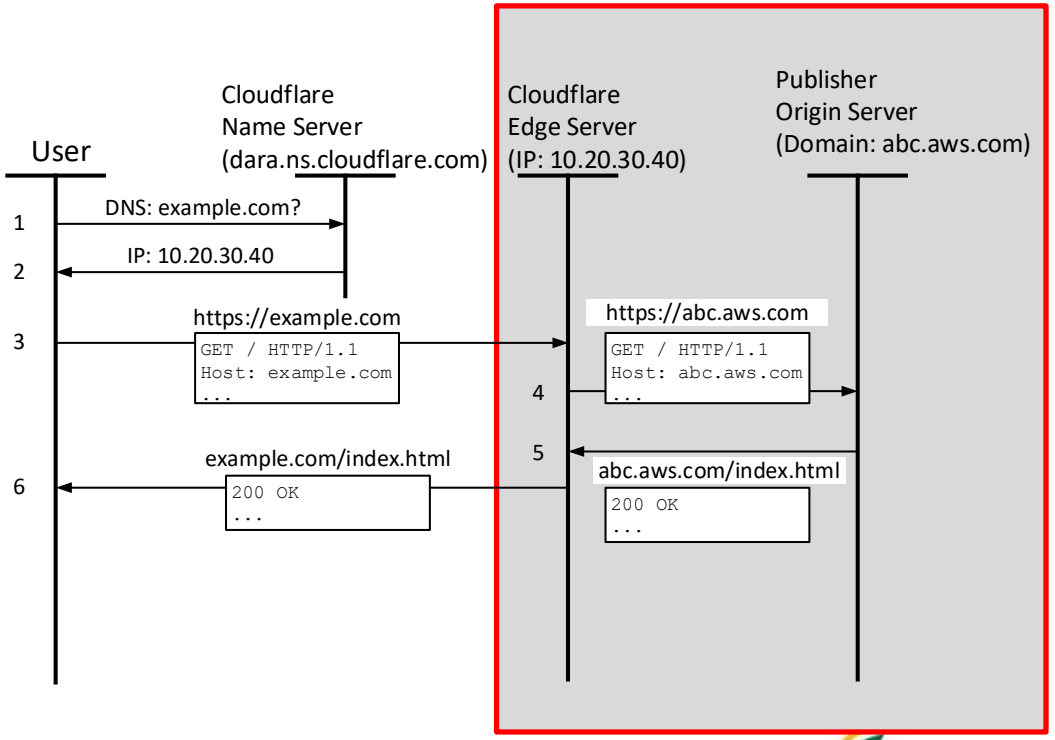
- The Cloudflare version (abc.aws.com → example.com)



Domain Name Transformation inside a CDN

- No one (either a user or the censor) knows the domain transformation but the domain owner





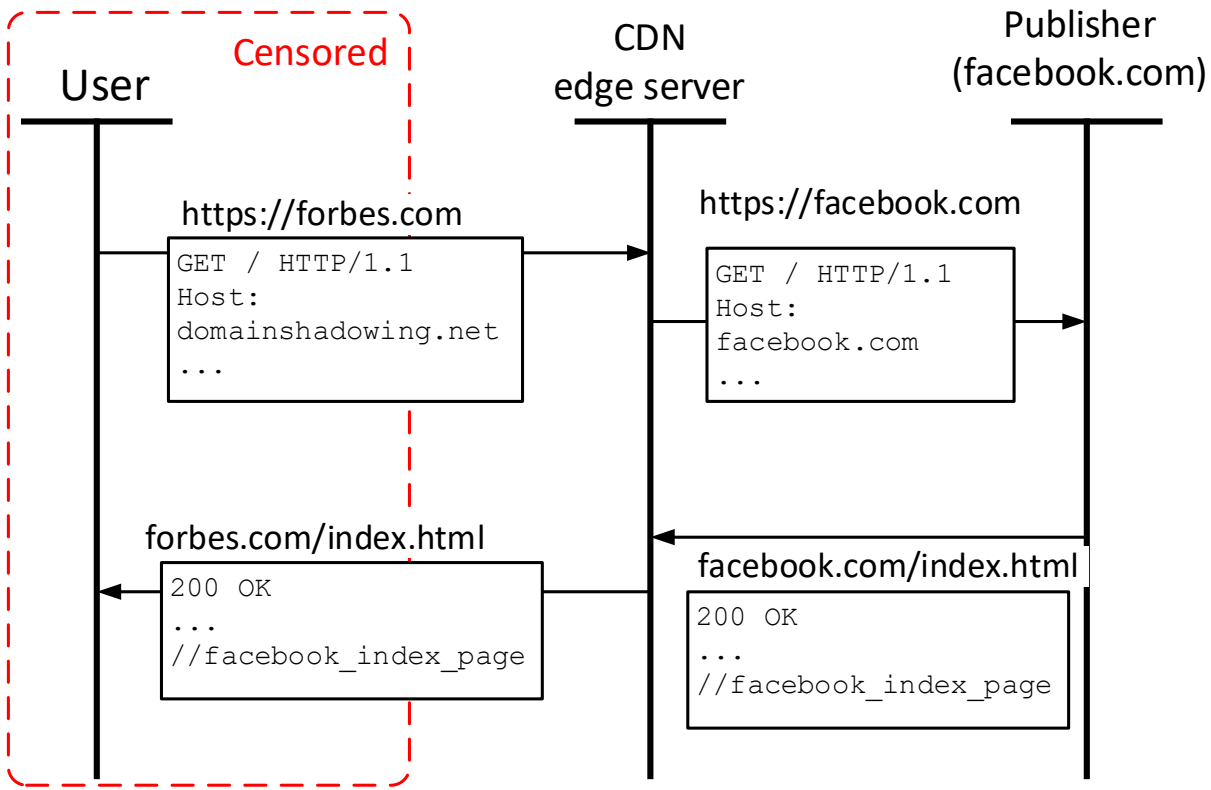
Evade Censorship using a CDN

1. The user registers a new domain, say, `shadow.com` (assume new domain is not blocked by the censor).
2. The user subscribes to a CDN service that is not censored.
3. In the CDN, the user sets `shadow.com` as the front-end and `blocked.com` as the back-end.
4. After all set, the user can visit the blocked (censored) domain by visiting the shadow domain.
5. All above configuration steps can be handled by a browser extension, which we have developed for Firefox.
6. More details of the configuration can be found in the paper.

MASON

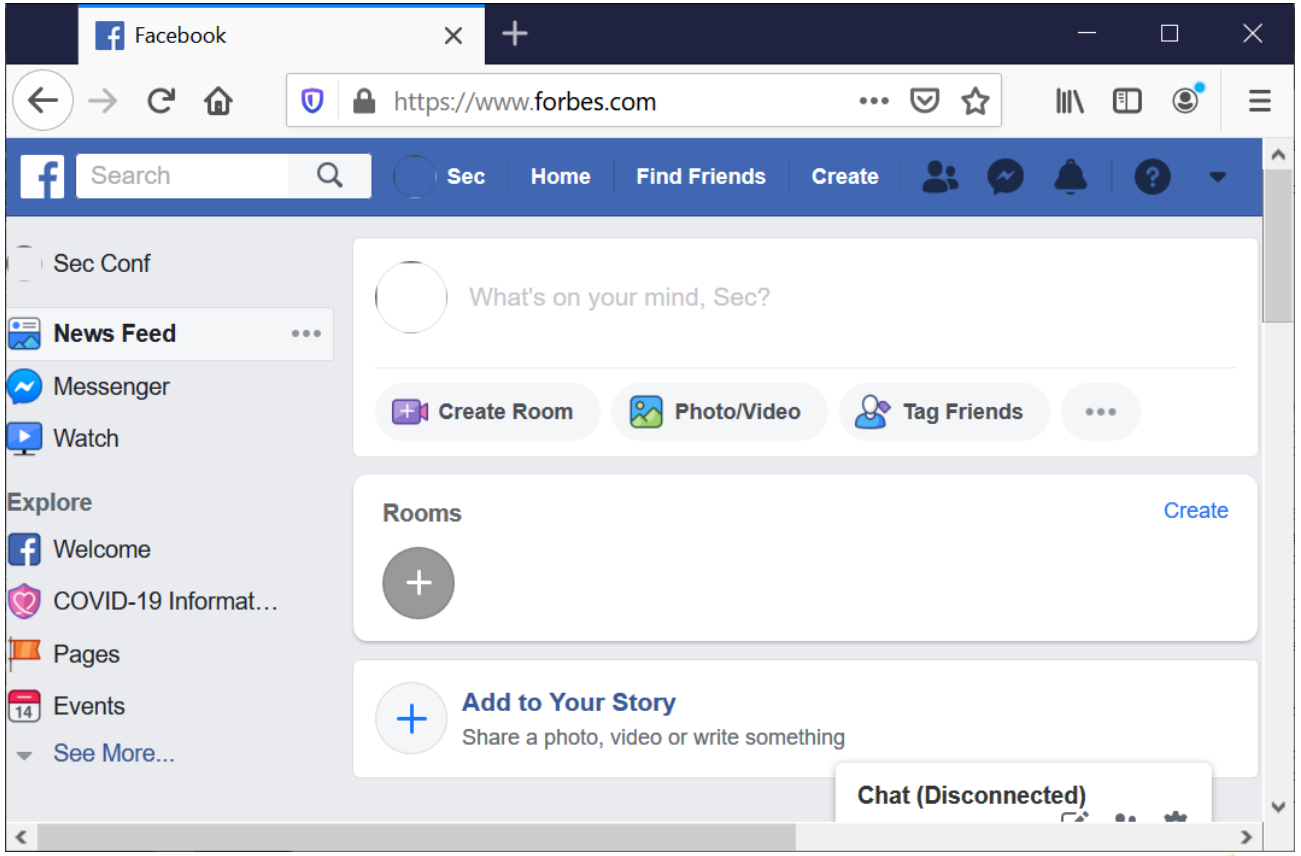
Result

- we registered `domainshadowing.net` and linked it to Facebook from within a censored country.
- Also used `forbes.com` as the front domain (as in domain fronting).



Result

- we registered `domainshadowing.net` and linked it to Facebook from within a censored country.
- Also used `forbes.com` as the front domain (as in domain fronting).

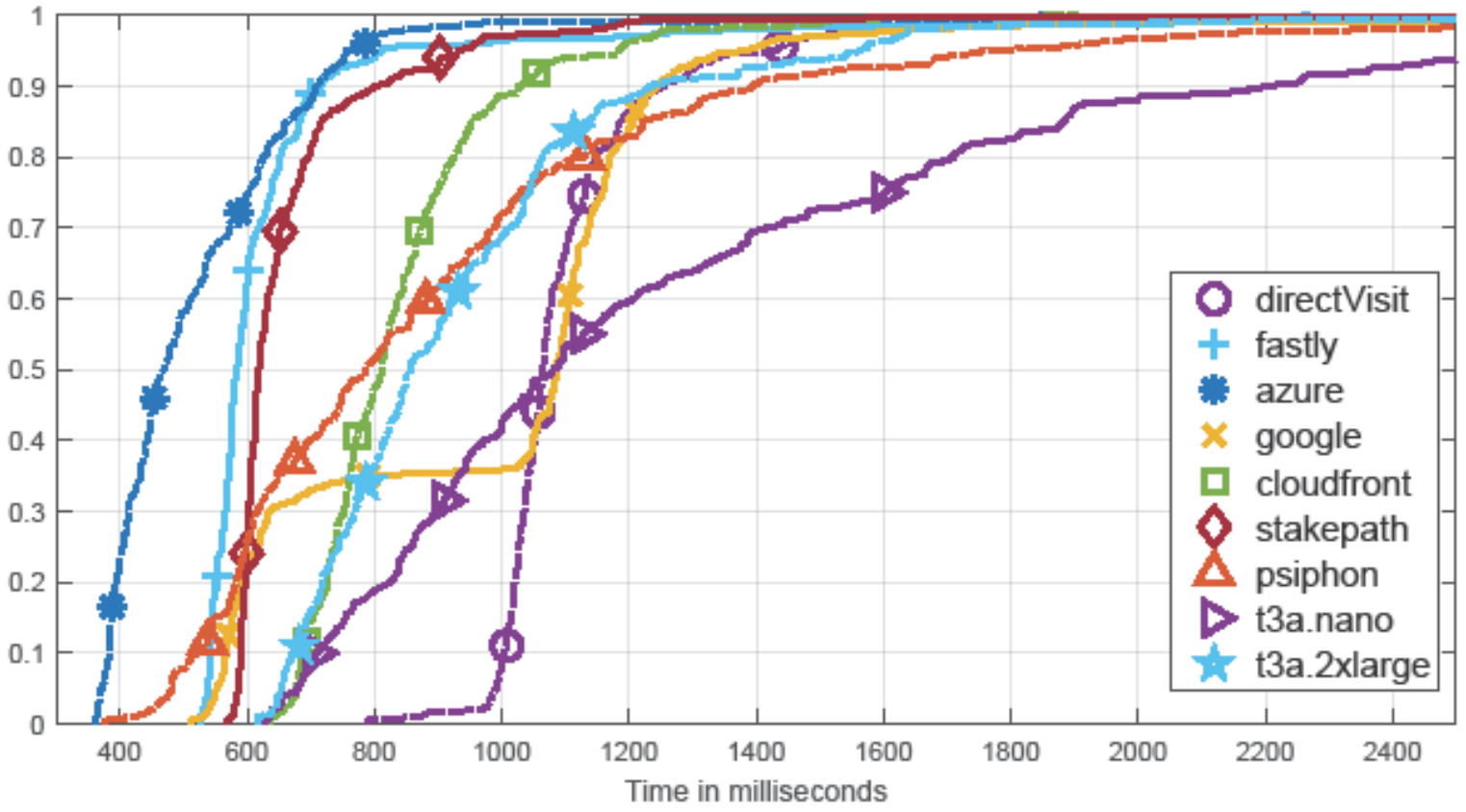


Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Performance

- Delay performance beats most virtual private server (VPS) based approaches. It is even faster than directly fetching web pages from the origin server.



Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Security Concerns

- Root cause: the domain name transformation confuses the browser, which may allows cross-domain attacks.
  - Cross-site scripting
  - Same origin policy
  - Cookies and sessions
- Solutions
  - Integrate into browser extension
  - User education
  - Ultimate solution: deeply modified browser (e.g., the Tor browser)

Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Blocking Resistance

- Domain shadowing is made possible because the CDN allows a user to set *any* domains as the backend.
  - The CDN cannot easily disallow it because it has legitimate use.
- The censor can see nothing but normal communication between the user and `shadow.com`, as long as HTTPS is used.
  - Traffic analysis, website fingerprinting, etc., are not impossible to circumvent.
- The CDN can identify the use of domain shadowing but the identification can be laborious.
  - Essentially an arms race, counter-counter-…-measures are not impossible.

MASON

Layout

1. What is domain shadowing
2. How domain shadowing works
3. Performance evaluation
4. Security considerations
5. Blocking resistance
6. Conclusion

Conclusion

- A single-user censorship evasion solution. The user handles everything, and does not need support from any dedicated third-party, nor collaboration from the censored website.
- Light-weight, only reply on a simple browser extension to work; and better performance, faster than VPS-based or even direct-access.
- Harder to block. Utilized a legitimate feature of the CDN, without which the CDN won’t work (or at least will sacrifice a lot).
- More details can be found in the paper.

MASON

Thanks!

Thanks for watching!

Please direct any questions to mwei2@gmu.edu.