Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web

Marco Squarcina (TU Wien)
30th USENIX Security Symposium
August 11-13, 2021

Joint work with M. Tempesta¹ // L. Veronese¹ // S. Calzavara² // M. Maffei¹
¹ TU Wien, ² Ca’ Foscari Venezia
The Related-Domain Attacker (RDA)

Both domains belong to the same site bank.com

www.bank.com

origin Cookies: Session Integrity for Web Applications

Andrew Bortz
Stanford University
abortz@cs.stanford.edu

Adam Barth
Google, Inc.
abarth@google.com

Alexei Czeskis
University of Washington
aczeskis@cs.washington.edu

Abstract

Virtually every web site on the Internet uses cookies to maintain session state between HTTP requests. Unfortunately, cookies have a serious design flaw which limits their security. In particular, cookies cannot provide session integrity against an attacker who can host content on a related domain. This type of attack is surprisingly common and problematic, yet existing proposals and best practices do not address this vulnerability. A lack of session integrity can result in session hijacking and session substitution that seriously compromise the security of web sites. In this paper, we demonstrate the possibility of achieving session integrity in existing browsers, but this requires the use of techniques that most existing web sites would have difficulty implementing. Therefore, we propose a lightweight extension to cookies that is secure against related-domain and network attackers, and illustrate how it facilitates session integrity.

However, there remains a significant design flaw in cookies, and consequently, secure session state: cookies stored by one site can be modified by another if the two sites happen to share a sufficiently long suffix [1, 2]. For example, two such sites are docs.google.com and www.google.com, having google.com as a suffix. While not all suffixes are considered long enough (e.g., com, co.uk), nearly every domain that can be purchased by individuals or corporations will be. We call two domains that share a sufficiently long suffix related domains, and attackers who control a related domain to their target can manipulate their target’s cookies.

Even though an attacker who controls a related domain...
Same-Site Relation

- **eTLDs** (Effective Top Level Domains) are defined by the [Public Suffix List (PSL)](https://publicsuffix.org)
- **eTLDs+1** are also called **registrable domains**
- 2 domains belong to the same site if they share a **common registrable domain**

Examples:

- `https://www.tuwien.ac.at`
- `https://old-project.tuwien.ac.at`
- `http://test.tuwien.ac.at`
- `http://test.tuwien.ac.at:8080` (Red
- `https://lavish.github.io` (Wrong
- `https://wert310.github.io` (Right)
Same-Site Security Boundary

- **Site Isolation** in Chromium / **Fission** in Firefox
  "cross-origin attacks within a site are not mitigated"
  -- from the original Site Isolation paper (USENIX'19)

- **Same-Site cookies** are effective **against CSRF**
  ... but they **do not apply to same-site requests**!

- **Trust abuses** against site operators and web users
Contributions

- **Systematic characterization of the RDA threat model**
  Not all sites are vulnerable to RDAs: attack vectors?
  Are all the RDAs created equal?
  Mapping between attack vectors and RDA's capabilities

- **Identification of the main web security threats available to RDAs**
  Which web mechanisms are at harm?
  Which capabilities are required to exploit them?
  What is the improvement over a traditional web attacker?

- **Measurement platform for large-scale evaluation**
  Evaluation of Tranco Top 50k
  Analysis of the security implications on sites with subdomains vulnerable to takeover
Attack Vectors

- A wide range of attack vectors
- We focus on Dangling DNS records, DNS misconfigurations exploitable by attackers
A wide range of attack vectors

We focus on **Dangling DNS records**, DNS misconfigurations exploitable by attackers

- Expired Domains
- Discontinued Services
- Deprovisioned Cloud Instances

![Diagram](/content/diagram.png)
Attack Vectors

- A wide range of attack vectors
- We focus on **Dangling DNS records**, DNS misconfigurations exploitable by attackers

- Expired Domains
- Discontinued Services
- Deprovisioned Cloud Instances
**Attack Vectors**

- A *wide range of attack vectors*
- We focus on **Dangling DNS records**, DNS misconfigurations exploitable by attackers

<table>
<thead>
<tr>
<th>Expired Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discontinued Services</strong></td>
</tr>
<tr>
<td><strong>Deprovisioned Cloud Instances</strong></td>
</tr>
</tbody>
</table>

![Diagram showing DNS resolution and subdomain delegation](Image)
Attack Vectors

- A **wide range of attack vectors**
- We focus on **Dangling DNS records**, DNS misconfigurations exploitable by attackers

- **Expired Domains**
- **Discontinued Services**
- **Deprovisioned Cloud Instances**

Custom domain `www.shop ...`

- `www.shop.example.org`
- `shop.example.org`
- `*.shop.example.org`
Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web

Attack Vectors

- A **wide range of attack vectors**
- We focus on **Dangling DNS records**, DNS misconfigurations exploitable by attackers

- Analysed **26 services**
  - WordPress, Shopify, Tumblr, GitHub, ...
- **17 vulnerable services**
  - where attackers can claim a subdomain of an already mapped domain

Custom domain **www.shop ...**

![Diagram showing DNS configuration and attack vectors](image-url)
Threats to Web Application Security

- Practical **web application security vulnerabilities** by intersecting the capabilities on vulnerable domains with the web security threats found on their related-domains
- Analyzed **5 mechanisms** across up to **200 domains of each vulnerable site**

**Cookies**
Domain cookies are leaked to subdomains (**confidentiality**)
Cookies can be **shadowed from subdomains** (**integrity**)

**CSP**
Policies might have milder restrictions on related domains and allow for **content inclusion** or **framing**

**CORS**
Test deployment of server-side policies which might enable **SOP bypasses**

**postMessage**
Dynamic testing of the postMessage API to identify dangerous sinks (e.g., **code execution**) due to lax or missing origin checking

**Relaxation**
Testing the legacy API `document.domain` to **sidestep the SOP** if the target and the RD set its value to a common ancestor
Modeling Approach: Example on Cookies

- **RDAs** put the **confidentiality** of **domain cookies** at risk
  - No security attribute: `js OR headers`
  - HttpOnly attribute: `headers`
  - Secure attribute: `(js OR headers) AND https`
  - Both attributes: `headers AND https`

- When a site has a **vulnerable subdomain**
  - Identify the RDA's **capabilities** granted by the attack vector
  - Inspect the security attributes of (session) cookies on related domains
  - Draw conclusions!
Measuring Subdomain Takeovers

Public Datasources

Domain List

DNS Scanner

Amass
dig

DNS enumeration
Construction of resolving chains

DNS

RDScan

Subdomain takeover scanner
Vulnerability disclosure

HTTP

Web Analyzer

Web crawler
Web vulnerability scanner

Crawler
PMForce
CORS checker...

Network

HTTP

Vulnerable
(sub)domains
Measuring Subdomain Takeovers

Public Datasources

Domain List

DNS Scanner

Amass dig
dig

26M subdomains

DNS enumeration
Construction of resolving chains

RDSScan

Vulnerable (sub)domains

Vulnerable (sub)domains

DNS | HTTP

Web Analyzer

HTTP

Crawler

top-50K sites

1520 vulnerable subdomains

887 vulnerable sites

Major websites affected
cnn.com, nih.gov, cisco.com,
f-secure.com, harvard.edu,
lenovo.com, ...
7.3% of .edu sites are vulnerable
Measuring Web Application (in)Security

- Public Datasources
- Domain List
- Amass
- DNS Scanner
- DNS enumeration
- Construction of resolving chains
- DNS
- HTTP
- RDSCan
- Subdomain takeover scanner
- Vulnerability disclosure
- Web analysis
- Vulnarable (sub)domains
- CSP
  - Most policies are broken
  - Gain +138 related domains
- CORS
  - >2K affected related domains
  - Gain +11%
- COOKIES
  - 23K affected related domains
  - 81% conf. issues
  - 99% int. issues
- relaxation
  - 57 affected related domains

Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web
Vulnerability Disclosure

- With **great power** comes **great responsibility**
- Developed a methodology to maximise the chances of identifying the **correct security point of contact** of a website

Vulnerability disclosure programs

- `.well-known/security.txt`
- $ whois

After 6 months

- 34% visited the full advisory on our web portal
- 31% fix rate
Vulnerability Disclosure

- With great power comes great responsibility
- Developed a methodology to maximise the chances of identifying the correct security point of contact of a website

After 6 months
- 34% visited the full advisory on our web portal
- 31% fix rate
- Could not identify a point of contact for the 62% of the sites
- 10% fix rate
Conclusions

- **Subdomain takeover** is still a **prevalent threat** that affects high profile websites.
- **Third-party services** are often the cause. Weaknesses in the **(sub)domain ownership verification mechanisms** are pervasive: site operators are not always to be blamed!
- RDAs are a **concrete and dangerous threat** against sensitive targets. Considerable gain wrt traditional web attacker, taking over a subdomain to **escalate privileges** is practical and convenient.
- **Low remediation rate** (15% of the sites after 6 months): 1 vulnerable subdomain can void the security of the whole site.
Find out more at
https://canitakeyoursubdomain.name