跨站点泄露漏洞

George Tian（田正祺）

2022 年 7 月 7 日

1 引言

1.1 基础概念

来源（Origin）[1]: Web 内容的 URL 的方案 (协议)，主机 (域名) 和端口。两个对象是同源的当且仅当以上三个元素都相等。

旁道攻击（Side-channel attack）：通过观察系统运行过程中的物理属性从而获取信息，而非暴力破解或运用算法的理论弱点。

跨站点泄露漏洞（Cross-site leaks, XSLeaks）[2]：一类存在与浏览器中的旁道攻击，让一个站点获取另一个站点的某些信息。

例子：`evil.com` 想得知用户在 `google.com` 上的搜索的关键字。`evil.com` 可以发出请求 `https://google.com/search?q=a`, `https://google.com/search?q=b` ……并测量从发出请求和接受到响应之间的时间间隔。若请求中发出的关键字是用户被曾经访问过，响应时间与未访问过的关键字响应相比会较短，因为本地会缓存响应中一部分的数据。

1.2 形式化建模

1.2.1 基础模型[3]

跨站点泄露漏洞是输出一个比特 b' 的函数 xsl

$$b' = xsl(sdr, i, t)$$

其输入为：

- sdr：依赖于状态的资源（state-dependent resource），而它是二元组 $(url, (s, d))$，其中 $(s, d) \in \{(s_0, d_0), (s_1, d_1)\}$：
  - url：目标资源的 URL
  - $S = \{s_0, s_1\}$：网站的两个状态的集合
  - $D = \{d_0, d_1\}$：网站的行为的差异，依赖于 s_0 和 s_1
- $i \in I$：包合技术，即如何从攻击网站向 sdr 发出请求
- $t \in T$：泄露技术，即如何观察目标网站上的差异

在以上的例子中：

- $url =$ `https://google.com/search?q=[query]`
- $S =$ { `query` 未被查询, `query` 已被查询 }

- $D =$ { 时间间隔较长, 时间间隔较短 }
- i 可以使用多种方式，比如将 url 嵌入到攻击网站中的 `iframe`
- t 为计时攻击

1.2.2 扩展模型[4]

Goethem et al. 用 Knittel et al. 的模型为基础，作出了扩展：

1.3 COSI

跨源状态推断（Cross-Origin State Inference）攻击[5]：

- 考虑两个网站
  - 攻击网站：用于发出跨站点请求，是攻击者（部分）控制的网站
  - 目标网站：用户在此网站上有不同的状态，不被攻击者控制的网站
- 攻击网站中含有依赖于状态的网址（state-dependent URL, SD-URL），比如一个只有用户登录后才能访问的网页
- 被包含的 SD-URL 使用户的浏览器发出跨源请求，但同源策略防止攻击网站直接阅读响应
- 攻击者可以通过跨站点泄露漏洞间接地读取响应

参考文献

[1] MDN contributors. Origin[EB/OL]. (2022-07-03) [2022-07-07]. https://developer.mozilla.org/zh-CN/docs/Glossary/Origin.

[2] SOUSA M, Terjanq, CLAPIS R, et al. XS-Leaks Wiki[EB/OL]. (2020-10-03) [2022-07-07]. https://xsleaks.dev/.

[3] KNITTEL L, MAINKA C, NIEMIETZ M, et al. XSinator.com: From a Formal Model to the Automatic Evaluation of Cross-Site Leaks in Web Browsers[C/OL]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2021. https://doi.org/10.1145%2F3460120.3484739. DOI: 10.1145/3460120.3484739.

[4] GOETHEM T V, FRANKEN G, SANCHEZ-ROLA I, et al. SoK[C/OL]//Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. ACM, 2022. https://doi.org/10.1145%2F3488932.3517416. DOI: 10.1145/3488932.3517416.

[5] SUDHODANAN A, KHODAYARI S, CABALLERO J. Cross-Origin State Inference (COSI) Attacks: Leaking Web Site States through XS-Leaks[J/OL]., 2019. https://arxiv.org/abs/1908.02204. DOI: 10.48550/ARXIV.1908.02204.