Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Mingming Zhang [1] Xiaofeng Zheng [1,2,✉] Kaiwen Shen [1] Ziqiao Kong [2] Chaoyi Lu [1] Yu Wang [1] Haixin Duan [1,2,✉] Shuang Hao [3] Baojun Liu [1] Min Yang [4]

[1]Tsinghua University [2]QI-ANXIN Group [3]University of Texas at Dallas [4]Fudan University

{zmm18,zxf19}@mails.tsinghua.edu.cn duanhx@tsinghua.edu.cn

Introduction

While several man-in-the-middle attacks (e.g., SSL Stripping) are available to break the secured connections, state-of-the-art security policies, such as the HSTS policy declared by websites and the security indicators shown in web browsers, have significantly increased the cost of successful attacks. However, the TLS certificates shared by multiple domains make HTTPS hijacking attacks possible again. In this paper, we term the HTTPS MITM attacks based on the shared TLS certificates as ***HTTPS Context Confusion Attack (SCC Attack)***.

Threat Analysis

HTTPS Context Confusion Attack (SCC Attack)

SCC attacks rely on the design that **multiple domains can share TLS certificates**. However, the **domains in the shared certificates do not always enforce the same security practices**, some of which are misconfigured, especially in HTTP security headers. By rerouting HTTPS requests to the flawed servers, adversaries can invite their weak policies to the secure origins, and bypass the security policies of the secure servers.

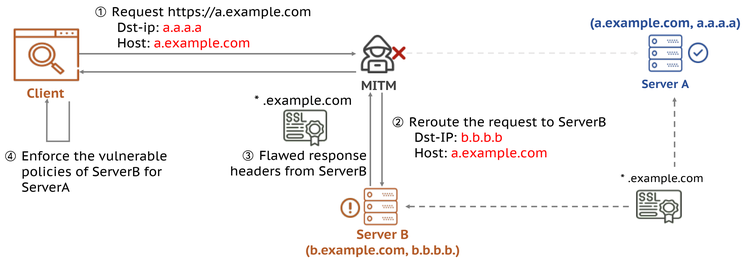


Figure 1: Attack Model

SCC Attack: an HTTPS MITM attacks leveraging shared TLS certificates

- **Goal**: Exploit flawed configurations of Server B to intercept an HTTPS connection between the client and a well-configured Server A.
- **MITM attacker**
  - Sniffer in local Wi-Fi or ethernet;
  - Locate in the open Wi-Fi network without strong security protection (e.g., WPA2);
  - Malicious middleboxes (e.g., gateway, proxies) , and so on.
- **Looking from client-side**
  - Client is actually talking with Server B (not Server A)
  - Can not be detected by browsers
  - Secure browsing context confusion for programs and users

SCC Attack in the Real World

Types of SCC Attack

To achieve the SCC attack goal, attackers can exploit the flowed HTTP headers of Server B. We have found two types of SCC Attacks, which have five subtypes in total.

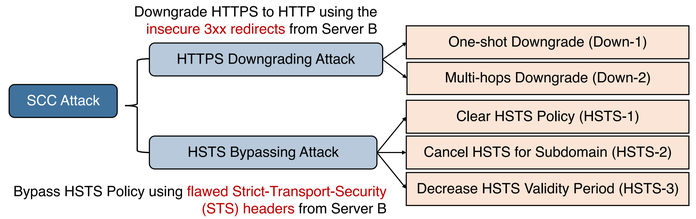
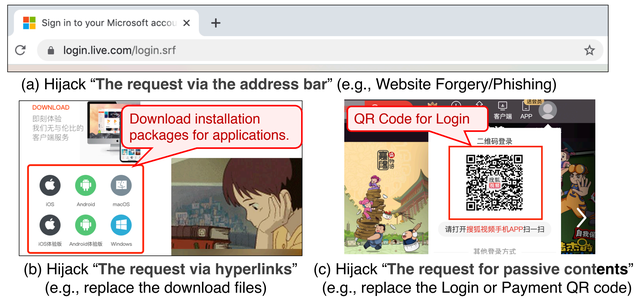


Figure 2: Attack Types

Attack Scenarios

1. Downgrade a new HTTPS connection (one request per connection).



(a) Hijack "**The request via the address bar**" (e.g., Website Forgery/Phishing)

(b) Hijack "**The request via hyperlinks**" (e.g., replace the download files)

(c) Hijack "**The request for passive contents**" (e.g., replace the Login or Payment QR code)

Figure 3: Three Types of Hijackable New HTTPS Connection

2. Downgrade an already-established HTTPS connection (multiple requests per connection).

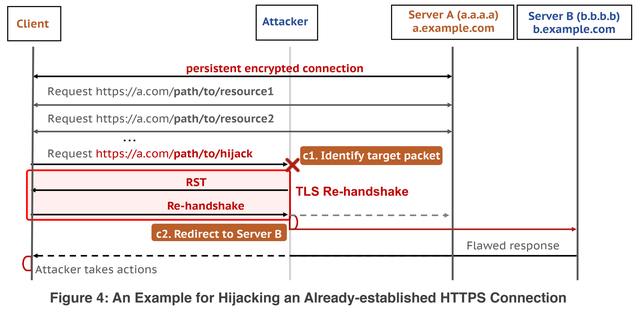


Figure 4: An Example for Hijacking an Already-established HTTPS Connection

TLS Re-handshake

- The process that browsers immediately start a new TLS handshake to resume the connection, to finish the incomplete requests.
- **Triggering conditions**: TCP Reset or Connection Timeout
- Mainstream browsers (e.g., Chrome, Firefox) will start the re-handshake process after receiving a Reset signal, instead of terminating the connection directly.

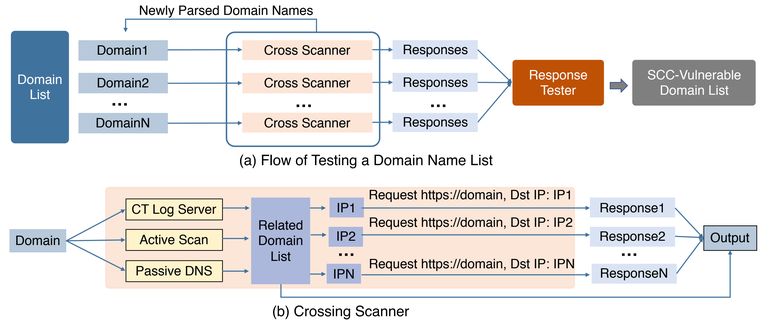
Trigger Method	Browser Vendor	Windows	MacOS	Linux	Trigger Method	Browser Vendor	Windows	MacOS	Linux
RST	Chrome	✓	✓	✓	Timeout	Chrome	✓		
	Firefox	✓	✓	✓		Firefox	✓		
	Edge	✓	-	-		Edge		-	-
	Safari	-	✓	-		Safari	-		-

The cases with ✓ can be exploited by attackers to trigger re-handshakes successfully.

Figure 5: Browser Re-handshake Behaviors

Vulnerable Servers in the Wild

Measurement Methodology



(a) Flow of Testing a Domain Name List

(b) Crossing Scanner

Figure 6: Methodology of Discovering SCC-Vulnerable Servers

Findings

Measurement on Alexa Top 500 Domains and All Their Subdomains

- 2,918 (8.50%) subdomains under 126 (25.2%) Alexa Top 500 base domains are vulnerable to SCC attacks.

Dataset		Affected Apex Domain Names		
Category	Count	Attack Type	Count	Total
Alexa Top Apex Domain	500	HTTPS Downgrade / Down-1	114 (22.8%)	126 (25.2%)
Multi-domain Certificates	8,892	HTTPS Downgrade / Down-2	24 (5.4%)	
All Extended FQDNs	292,227	HSTS Bypass / HSTS-1	5 (1%)	
All FQDNs with HTTPS	34,317	HSTS Bypass / HSTS-2	21 (4.2%)	
		HSTS Bypass / HSTS-3	31 (6.2%)	

- Popular applications could be affected by SCC attacks.

Possible Attacks

- Online Payment Hijacking
- Download Hijacking
- Website Phishing

- Certificate Sharing is prevalent, which could be vulnerable due to security dependencies between domains.

If the domains at the convergent nodes are vulnerable, there will be potential security threats for those around them.

Over 900 FQDNs depend on pages.ebay.com.