

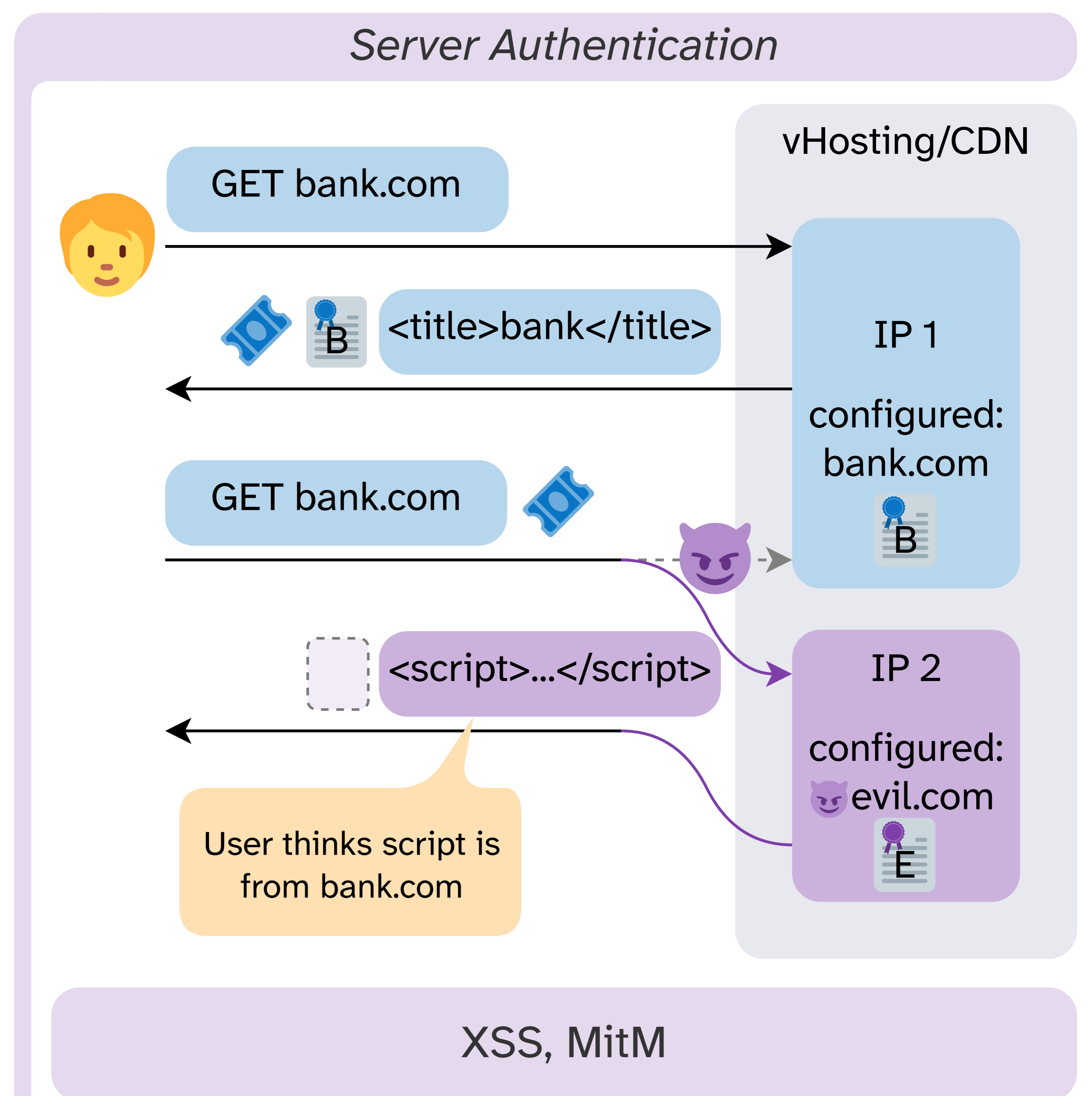
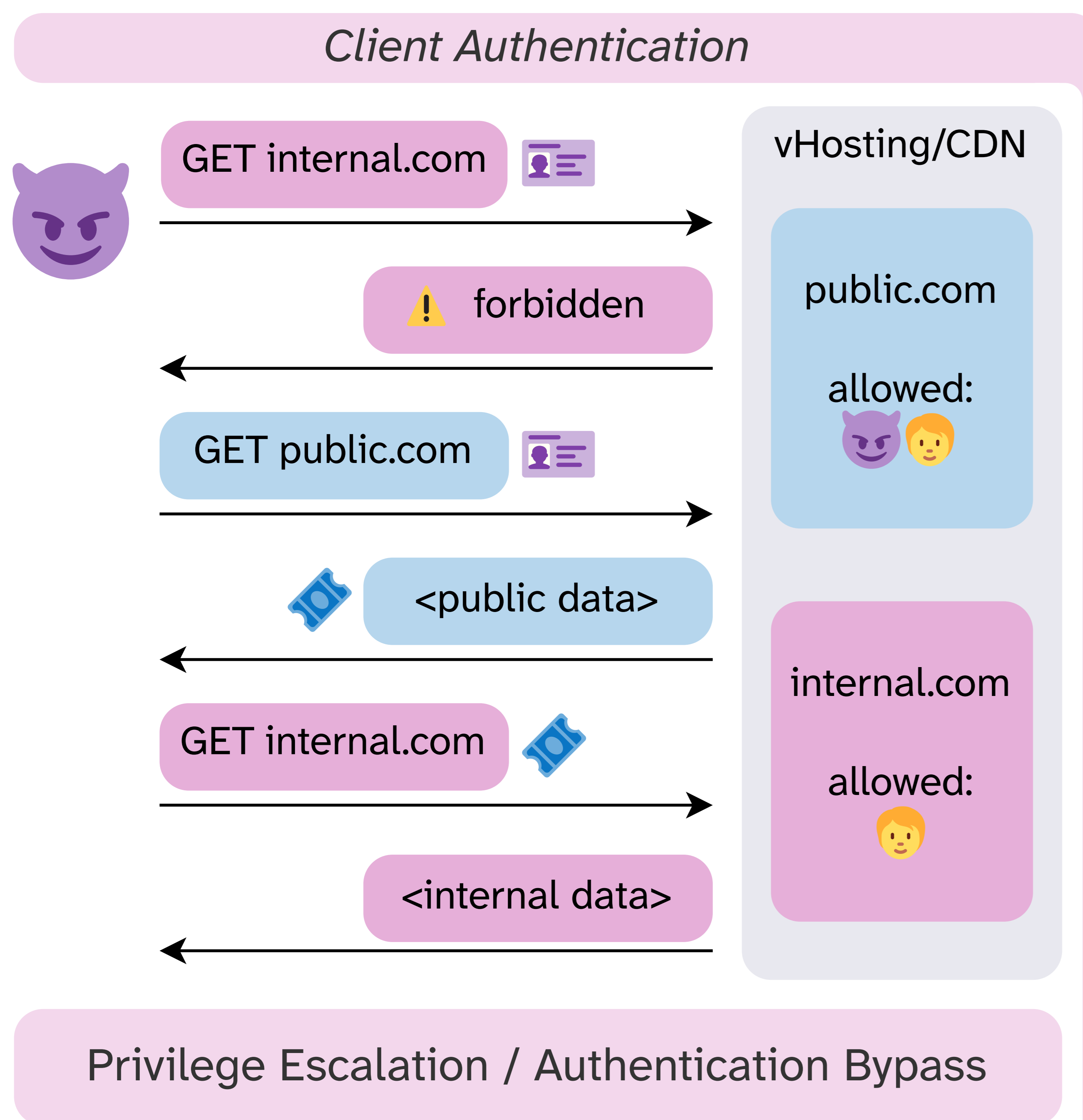
STEK Sharing is Not Caring: Bypassing TLS Authentication in Web Servers using Session Tickets

Sven Hebrok, Tim Leonhard Storm, Felix Matthias Cramer, Maximilian Radoy, Juraj Somorovsky

- TLS session tickets accelerate connections
- Skip costly authentication step in resumption

- Virtual hosting uses a single server for multiple domains

How do session tickets affect TLS authentication guarantees?



Do these vulnerabilities exist in the real-world?

	TLS SNI →	public		internal		omitted	
		public	internal	public	internal	public	internal
Apache	TLS 1.2						
	TLS 1.3	public	421	not resumed		public	internal
Apache (strict)	TLS 1.2						
	TLS 1.3	public	421	not resumed		403	403
Caddy	TLS 1.2						
	TLS 1.3	public	421	421	internal	not resumed	
nginx	TLS 1.2						
	TLS 1.3	public	421	public	421	public	internal
nginx (strict SNI)	TLS 1.2						
	TLS 1.3	public	421	421	internal	not resumed	
LiteSpeed	TLS 1.2						
	TLS 1.3	public	internal	not resumed		public	internal

Manually found affected provider: Cloudflare

Performed large-scale scan

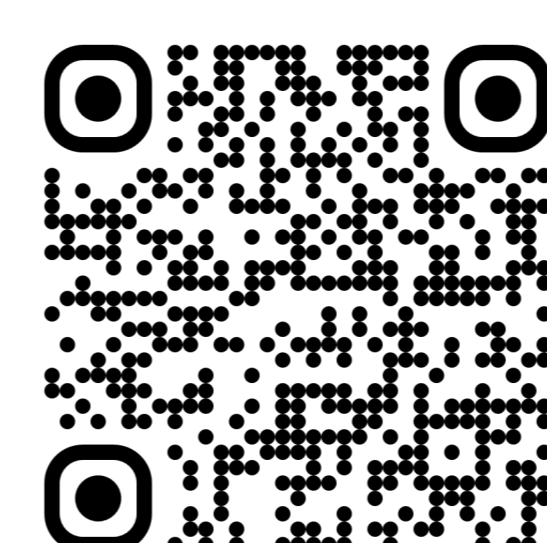
Found 3 affected CDNs/providers:

Fastly, DDoS-Guard, Variti

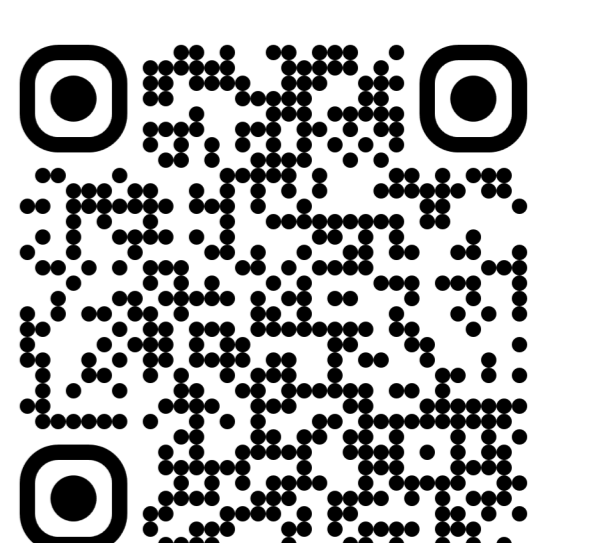
Discovered routing issue in Cloudflare allowing MitM

Reasons for these vulnerabilities:

- Easy to misuse APIs in TLS libraries
- Standards vague about interaction of
 - Session resumption
 - Virtual hosting (SNI, Host header)



Read the Paper



Contact us
sven.hebrok@upb.de

