

SSL



SSL/TLS

HTTPS

PLC-BLASTER



PLC-Blaster

!PLC-BLASTER

معمولاً در این روش مهاجم می‌تواند داده‌های رمزنگاری شده را با استفاده از یک کانال جانبی (side channel) رمزگشایی کند. این کانال جانبی می‌تواند به صورت فیزیکی یا منطقی باشد. در این روش، مهاجم می‌تواند با اندازه‌گیری زمان اجرای عملیات رمزنگاری، داده‌های رمزگشایی شده را استخراج کند. این روش به عنوان «Man in the middle» شناخته می‌شود. در این روش، مهاجم می‌تواند با استفاده از یک کانال جانبی، داده‌های رمزنگاری شده را رمزگشایی کند. این روش به عنوان «BREACH» شناخته می‌شود. در این روش، مهاجم می‌تواند با استفاده از یک کانال جانبی، داده‌های رمزنگاری شده را رمزگشایی کند. این روش به عنوان «CRIME» شناخته می‌شود. در این روش، مهاجم می‌تواند با استفاده از یک کانال جانبی، داده‌های رمزنگاری شده را رمزگشایی کند. این روش به عنوان «Man in the middle» شناخته می‌شود. در این روش، مهاجم می‌تواند با استفاده از یک کانال جانبی، داده‌های رمزنگاری شده را رمزگشایی کند. این روش به عنوان «BREACH» شناخته می‌شود. در این روش، مهاجم می‌تواند با استفاده از یک کانال جانبی، داده‌های رمزنگاری شده را رمزگشایی کند. این روش به عنوان «CRIME» شناخته می‌شود.

:معمولاً
معمولاً
معمولاً

:معمولاً
13:46 - 25/05/1395

:معمولاً
معمولاً - ssl - TLS - HTTPS - HESIT - معمولاً - معمولاً

<https://www.shabakeh-mag.com/security/4089>:معمولاً معمولاً