Ataque de canal lateral

En seguridad informática, un ataque de canal lateral es un ataque basado en información obtenida gracias a la propia implementación física de un sistema informático, en lugar de basarse en puntos débiles del algoritmo implementado como sería el caso de recurrir a criptoanálisis o explotar errores en el software.

Por ejemplo, la sincronización de información, el consumo de energía, fugas electromagnéticas o incluso sonidos pueden ser una fuente adicional de información que puede explotarse para romper el sistema. Algunos ataques de canal lateral requieren conocimientos técnicos sobre el funcionamiento interno del sistema, aunque otros como es el caso del análisis de diferencias de consumo energético resultan eficaces como ataques de caja negra. Muchos ataques de canal lateral poderosos están basados en los métodos estadísticos con los que Paul Kocher fue pionero.