[PAN] Ataques de reconstrucción de bases de datos (Resumen)

Adversary Quering

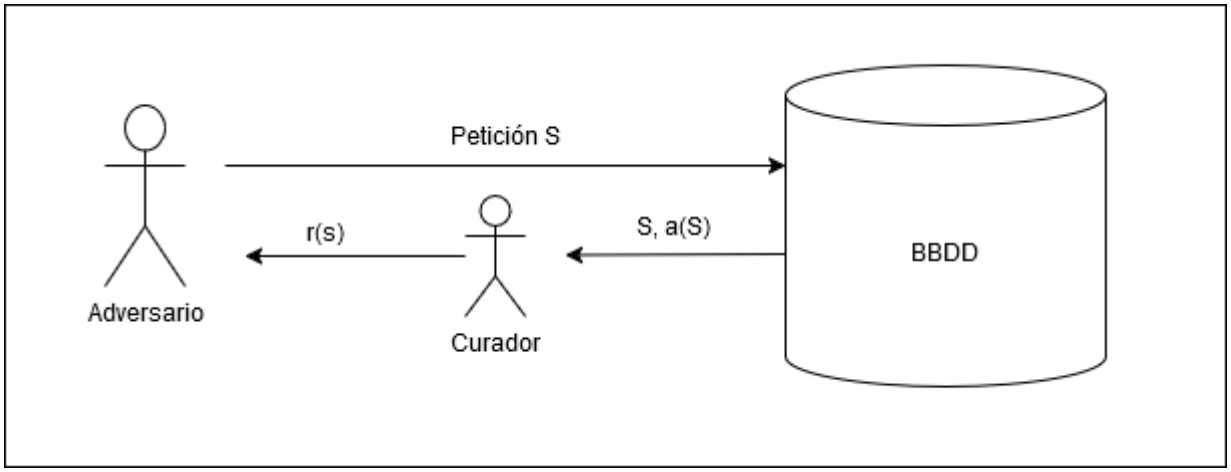
Adeversary Quering o “Consulta Contradictoria” puede parecer un tipo de ataque bastante inocente, pero puede incurrir en riesgos de privadidad mediante el uso de inferencia. Para prevenir este tipo de ataques se recomienda rechazar las consultas que se puedan considerar peligrosas. El problema de esto es que los rechazos también pueden filtrar información. Por ejemplo, si tenemos una base de datos de salarios, se rechaza una consulta que pueda revelar el salario de un usuario en particular, pero si el atacante hace una consulta para saber cual es el máximo de los salarios de todos los empleados y después realiza una consulta para saber cual es el salario más alto de todos los usuarios menos el que se ha especificado y resulta ser este el más alto, la nueva respuesta a la consulta devolverá una cifra diferente, indicando al atacante cual era el sueldo del empleado en cuestión.

Ataques de reconstrucción de base de datos

Este tipo de ataques están orientados a bases de datos “Curadas”. Que una base de datos esté curada significa que cuando se realiza una consulta, los datos pasan por un “Curador” antes de ser publicadas para anonimizar los datos que se consideren críticos. Generalmente para curar una base de datos se recomienda evitar mostrar datos que sean demasiado detallados. Si no se cura correctamente una base de datos es posible reconstruir esta y obtener los datos anonimizados mediante el uso de estadística. En 2010 el ceso de estados unidos realizó un ataque de reconstrucción contra su propia base de datos, con este ataque se logró desanonimizar un 46% de la población y un 71% si se tolera un margen de error de 1 año en la edad. Enlazando estos datos con bases de datos comerciales fue posible reidentificar a 50 millones de personas. Para mitigar esto a partir de 2020 se comenzó a usar privacidad diferencial en el censo.

Curando las bases de datos

Responder a una petición S con la verdad a(S) viola la privacidad, si el adversario quiere descubrir el secreto de una fila en especial, simplemente debe construir un vector de petición con 1 en la fila y 0 en el resto. Es por ello que la respuesta debe ser r(S), una versión ofuscada de a(S). Para poder preservar cierta utilidad de la base de datos se debe imponer ciertos límites a la ofuscación.



Ataque de reconstrucción linear

Si el adversario puede realizar 2^n consultas y el curador añade ruido con un límite E, luego, basándose en los resultados, el adversario puede reconstruir la base de datos entera salvo 4E posiciones. Este ataque se debe realizar de la siguiente forma:

- Fase 1: Realizar todas las consultas posibles, almacenando las respuestas
- Fase 2: Encontrar candidatos válidos

A menos que hay un límite en las peticiones que se pueden realizar a la base de datos, una reconstrucción casi perfecta de la base de datos puede ser lograda en 4E de las entradas.