Primeros pasos con LegionRSA

Al ejecutar el programa en Java LegionRSA, le aparecerá la siguiente pantalla.

Para diseñar un ataque en modo local, deberá ejecutar de forma independiente el programa Servidor y el programa Cliente. Si el ancho de su pantalla se lo permite, puede ajustar cada ventana (Servidor y Cliente) a la mitad de la misma como verá en una figura más adelante.

Recomendaciones para una primera ejecución de LegionRSA:

1. Arranque el Servidor y elija en Módulo N opción Asignar automáticamente 64 bits, para que la aplicación genere una clave RSA de ese valor.
2. Hecho esto, ejecute el Cliente y elija cuántos procesadores va a utilizar para el ataque. Seleccione ahora Unirse al ataque. Como aún no le ha indicado al Servidor comenzar el ataque, el Cliente le informará "Unido al ataque. Esperando órdenes del servidor".
3. Vuelva al Servidor y seleccione Iniciar ataque distribuido.
4. Observará cómo el Servidor va entregando trabajo a ese único cliente y el Cliente realizando cifrados. Mientras el ataque se ejecuta le indicará datos de interés del mismo.
5. Por ser 64 bits una clave de tamaño muy pequeño y que la tasa de cifrados del programa puede oscilar entre varias decenas hasta varias centenas de millones de cifrados por segundo, dependiendo de las características de su PC, este ataque debe prosperar a los pocos segundos, entre 10 y 30 segundos, entregando la clave privada buscada.
6. Por el principio de la paradoja del cumpleaños, el ataque terminará cuando se éste se encuentre entre el 75% y el 125% del porcentaje de cifrados probados sobre la estimación hecha por LegionRSA que es $3\sqrt{n}$.
7. Cada 10 minutos la aplicación guarda el estado del ataque (por favor mirar la ayuda).

Aunque el software es muy intuitivo, encontrará un fichero de ayuda en la misma aplicación.

Para realizar ataques en red (clientes en máquinas distintas con dirección IP) y poder comprobar así que se cumple el ataque distribuido y divide y vencerás, se recomienda leer el artículo "RSA cumple 36 años y se le ha caducado el carné joven" que encontrará en la siguiente dirección:

http://www.criptored.upm.es/descarga/articuloRSAcumple36.pdf

En los próximos meses cuando se publique la versión 5.0 del Asistente de Prácticas de Seguridad Informática, se incluirá una práctica completa con LegionRSA.

Madrid, 17 de marzo de 2014

Dr. Jorge Ramió Aguirre

Tutor del Trabajo Fin de Carrera LegionRSA de D. Roberto Ruiz Sánchez

La siguiente figura muestra un ataque en localhost, utilizando 4 de los 8 procesadores de la máquina, a una clave de 64 bits en 16 segundos.