Descubren punto débil en la autenticación RSA

La técnica de seguridad digital más comunmente utilizada para proteger los derechos de autor en medios y las comunicaciones en Internet tiene un punto débil importante, según descubrieron científicos de computación de la Universidad de Michigan (UM).

La autenticación RSA (siglas que obedecen a sus desarrolladores Ronald Rivest, Adi Shamir y Leonard Adelman) es un método popular de cifrado usado en reproductores digitales (audio y video), computadoras portátiles, teléfonos inteligentes, servidores y otros dispositivos; también los puntos de venta y bancos dependen de esto para asegurar la información de sus clientes en línea.

Los científicos descubrieron que se podría frustrar el sistema de seguridad variando el voltaje suministrado al poseedor de la "clave privada", el cual sería el dispositivo del consumidor en el caso de la protección contra copias y el punto de venta o el banco en el caso de comunicaciones por Internet. Es altamente improbable que el atacante pueda usar este enfoque en una gran institución, dicen los investigadores. Estos hallazgos afectan mayormente a las compañías de medios y fabricantes de dispositivos móviles, así como también quienes los usan.

Según Valeria Bertacco, una profesora asociada del Departamento de Ingeniería Eléctrica y Ciencias de Computación, "el algoritmo RSA brinda seguridad bajo el supuesto de que mientras la clave privada se mantenga en secreto, no podrá ser descifrada sino adivinándola. Hemos demostrado que no es cierto," dijo.

Usando su esquema de cambio de voltaje, los investigadores de la UM fueron capaces de extraer la clave privada en aproximadamente 100 horas. Manipularon cuidadosamente el voltaje con un dispositivo muy barato construido con este propósito. Variar la corriente eléctrica esencialmente

esfuerza a la computadora y provoca que cometa pequeños errores en su comunicación con otros clientes. Estas fallas revelan pequeñas partes de la clave privada. Una vez que los investigadores provocaron suficiente fallas, fueron capaces de reconstruir la clave desconectados.Este tipo de ataque no daña el dispositivo, de modo que no queda evidencia de la interferencia.

"La autenticación RSA es tan popular debido a que se pensaba que era tan segura," dijo Todd Austin, un profesor en el Departamento de Ingeniería Eléctrica y Ciencias de Computación. "Nuestro trabajo redefine los niveles de seguridad que ofrece. Disminuye la protección de la seguridad en un monto significativo."

Aunque el trabajo solo discute el problema, los profesores dicen que han identificado una solución. Es una técnica criptográfica común denominada “salar” (salting) que altera los dígitos de una forma cada vez que se solicita la clave.

"Hemos demostrado que es posible un ataque basado en fallas contra el algoritmo RSA," dijo Austin. "Con suerte, esto provocará que los fabricantes hagan pequeños cambios a sus implementaciones del algoritmo. RSA es un buen algoritmo y pienso, que a la larga, sobrevivirá este tipo de ataques."
El trabajo se llama "Ataque basado en fallas de la autenticación RSA" *("*Fault-based Attack of RSA Authentication*")*.

Fuente: http://blog.segu-info.com.ar/2010/03/descubren-punto-debil-en-la.html