**Qué es un 'relay attack' y cómo puede afectar al voto electrónico de Salta?**

**Escrito por**[**Iruya.com**](http://iruya.com/)

Publicado el Lunes 13 de Abril de 2015 - 05:41:46 h

El sistema de voto electrónico implantado en Salta, que reemplaza al tradicional voto de papel por la así llamada boleta única electrónica, que lleva incorporado un *contactless smart chip*(chip inteligente sin contacto), está diseñado alrededor de la tecnología RFID (*Radio-frequency identification*).

La elección de esta tecnología está relacionada con la mayor facilidad de uso de los terminales de votación, con el ahorro de costes y con la menor incidencia de fallos mecánicos que proporcionan estos sistemas en comparación con otros.

No obstante, los sistemas basados en comunicaciones RFID se hallan expuestos a **una poderosa clase de ataques**, basados en hardware, conocidos en criptografía como *«relay attacks»*, que son capaces de extender el rango de interrogación de los HF RFID o los UHF RFID mucho más allá del rango nominal de 5 centímetros.

Un *relay attack* es una técnica de *hacking*relacionada con los ataques conocidos como MitM (*man-in-the-middle* o "intermediario" en español). Este tipo de ataques permite a quienes en criptografía se llaman *adversarios* interceptar y manipular las comunicaciones entre dos partes, proporcionando la capacidad de leer, insertar y modificar a voluntad los mensajes entre esas dos partes sin que ninguna de ellas sepa que el enlace ha sido violado.

El rango nominal operativo de 5 centímetros (ISO/IEC 14443) conduce a la errónea suposición de que cada vez que un lector se comunica con una etiqueta *(tag)* es solamente porque ésta se encuentra físicamente muy cerca del lector. Los *relay attacks* cuestionan precisamente esta suposición subyacente, ya que **permiten una distancia casi ilimitada** entre la etiqueta y el lector. El atacante logra esta capacidad mediante la colocación de un *«relay»*, que consiste en una etiqueta de diseño personalizado y el hardware lector, conectados por un enlace de comunicación de alto rango y alta velocidad.

Como consecuencia de ello, cualquier dato intercambiado entre la etiqueta de la víctima y el lector puede ser desviado al canal *relay* (y consecuentemente manipulado antes de devolverlo al lector), aun cuando la información estuviera fuertemente encriptada y autenticada.

Esquemáticamente, el voto electrónico salteño consiste en un dispositivo (una pantalla táctil) en la que el elector compone su voto a partir de diferentes opciones, graba su elección en un chip RFID (a la vez que imprime un comprobante para cotejo) y verifica que lo grabado en el chip (y lo impreso en la tarjeta) concuerde con su elección. La tarjeta con el chip se introduce entonces en un sobre que es depositado en la urna. Cuando termina la votación y se inicia el recuento, los chips son leídos acercando simplemente los sobres a un lector, que finalmente totaliza los resultados de la mesa y los envía a un centro de cómputos.

De acuerdo con este esquema, se producen al menos tres comunicaciones importantes del chip RFID: la primera, de escritura (cuando al finalizar la selección en pantalla el elector decide grabar su voto); la segunda de lectura (cuando el propio elector procede a verificar la coincidencia de su voto con los datos grabados en el chip) y la tercera, también de lectura, cuando, concluida la votación, las autoridades de mesa acercan los chips a un lector para contabilizar el voto.

**Escenarios posibles**

Las siguientes secciones describen varios *relay attacks* que se podrían ejecutar contra un sistema de voto electrónico basado en *smartcards* RFID, como el salteño, aunque no necesariamente sobre éste, teniendo en cuenta sus particularidades. Los escenarios descritos están ordenados inversamente por su potencial gravedad.

**1) Ataque de *sniffing***
Permite al atacante conocer el contenido completo de todos los votos introducidos en la urna. Para ejecutar este ataque es necesario colocar un *relay* entre los votos que se hallan dentro de la urna y el terminal de verificación, que normalmente se encuentra en la propia máquina. A continuación el atacante activa repetidamente el terminal de verificación, cada vez con una boleta diferente. Desde el momento en que el terminal de verficación está emparejado con los votos depositados en la urna, el atacante puede contar los votos y mostrar el contenido grabado en los chips. Este proceso se puede realizar de forma fiable y eficiente, aun cuando haya muchos votos en la urna, debido a que el componente *leech* del *relay* utiliza protocolos anticolisión RFID.

Un ataque de *sniffing* **permite al atacante conocer los resultados parciales de la votación antes de que cierren las urnas**. Si los votos reales emitidos no se ajustan al resultado esperado, el atacante puede utilizar alguno de los métodos descritos más abajo para manipular los datos de la mesa. Si este tipo de ataque es ejecutado dos veces en un mismo día, sobre la misma urna, la interceptación de los datos puede ser utilizada para revelar el sentido del voto, violando su secreto y permitiendo la coacción sobre los electores.

**2) Ataque de desvío al voto disidente único**

Para llevar a cabo este ataque, el atacante debe estar físicamente presente cerca del terminal de votación mientras otro elector está ejerciendo su derecho. Es condición necesaria que el atacante coloque un *relay* entre los terminales de votación y verificación y un voto individual previamente depositado en la urna, llamado *«voto del disidente individual»*. El *relay* puede ser activado y desactivado una y otra vez por el atacante. Este elige a un cierto grupo de electores cuyo voto desea invalidar y, cuando el *relay* está activo, todas las acciones del votante disidente que se encuentra en la cabina (selección del voto, verificación, etc.) no se ejecutan contra la boleta en blanco que tiene en sus manos sino que son derivadas y referidas al voto del *«disidente único»*que se halla ya depositado en la urna.

Debido a que este voto disidente único se encuentra debidamente autenticado, tanto el terminal de votación como el de verificación registrarán alegremente el voto del nuevo votante y mostrarán los valores correctos. Así, el votante no tendrá idea de que el ataque está teniendo lugar, pero su boleta personal permanecerá en blanco. Luego de que el votante abandone la cabina, depositará en la urna un voto en blanco, que será, obviamente, ignorado.

Si el atacante acierta a adivinar la verdadera disposición de los votantes, el ataque asegurará de que la urna **no contenga más de un voto disidente** para cada partido indeseable, ya que todos los votos de los demás disidentes serán registrados como blancos o inválidos y no tendrán efecto alguno en el resultado de las elecciones.

Debido a que los votos que se hallan dentro de la urna guardan una relación directa con los valores escritos en el chip por el terminal de votación, el recuento al final de la jornada no mostrará discrepancias entre los dos.

Aunque este tipo de ataque parece al principio difícil de configurar y llevar a cabo, tiene la ventaja de ser virtualmente indetectable. Si uno de los votantes disidentes llegara a sospechar e intentara buscar huellas del ataque, no las encontraría. Incluso un examen manual de los votos de la urna sería incapaz de revelar el subterfugio, ya que al haber siempre un solo voto disidente en la urna, el votante creerá siempre que ese voto es el de él y, aunque le pueda parecer extraño, pensará que sus compañeros de partido cambiaron de parecer a último momento.

**3) Ataque de llenado de urna**

Esta técnica proporciona al atacante un **completo control** sobre los votos previamente emitidos. El *relay attack* se utiliza en este caso para reescribir los votos y sustituirlos por los del candidato que el atacante elija.

Para llevar a cabo esta maniobra es necesario colocar un *relay* entre la urna y un terminal de votación. El atacante utiliza un terminal para votar repetidas veces por el candidato de su elección, utilizando para ello, cada vez, un voto diferente de los depositados en la urna. Como los terminales de votación están emparejados con los votos previamente emitidos, no hay razón alguna para evitar que los votos sean modificados. Se ha de tener en cuenta, además, que el ataque se realiza desde el propio terminal de votación, que constantemente actualiza el conteo de los votos en curso y permanece perfectamente sincronizado con los votos emitidos que ya se encuentran dentro de la urna. Esto significa que el ataque no provocará discrepancias que puedan ser detectadas durante el recuento. El protocolo anticolisión RFID permitirá que este proceso sea ejecutado de forma fiable y eficiente, incluso cuando la urna contiene ya muchos votos.

**4) Ataque *zapper***

Se trata de un ataque **no-relay** que requiere el empleo de tecnología menos sofisticada, si bien proporciona al atacante un control menor sobre los resultados de la elección.

El atacante puede utilizar un dispositivo RFID *zapper* de bajo costo, que consiste en una fuente de energía de impulsos (por ejemplo el circuito de flash de una cámara desechable) conectado a una antena del lector con la forma adecuada. Cuando la fuente de potencia de impulsos está activada, un pulso electromagnético de gran alcance fluye a través de la antena y destruye cualquier etiqueta RFID através de una poderosa oleada de corriente que abruma sus circuitos de entrada y generalmente los vuelve inutilizables.

**Breve conclusión**

La experiencia demuestra que con conocimientos técnicos no demasiado avanzados y con un pequeño presupuesto se puede llevar a efecto devastadores *«relay attacks»* sobre los sistemas que utilizan RFID.

Si bien estos sistemas se utilizan también para otras aplicaciones sensibles como las tarjetas de crédito, los pasaportes electrónicos y los sistemas de acceso seguros a edificios y medios de transporte, en todos estos casos se dispone de medidas de seguridad adicionales (como por ejemplo, las auditorías, los seguros, los extractos de tarjeta, el control humano o la vídeovigilancia) que **resultan inaplicables al voto electrónico**. No se debe olvidar que, por imperativo constitucional, prima en todo momento la privacidad del votante y el secreto de su decisión.

Las medidas de seguridad implementadas en Salta, como por ejemplo la impresión física de la opción de voto, no garantizan por sí solas que el recuento automático mediante una conexión RFID esté exento de cualquier manipulación y de que un *relay attack* coordinado pueda distorsionar gravemente los resultados del escrutinio provisional.