Criptoanálisis del RFID de David-Prasad Protocolo de autenticación ultraligero

Julio César Hernández-Castro1, Pedro Peris-López2, Raphael C.-W. Phan3, y Juan ME Tapiador4

[1] Facultad de Informática, Universidad de Portsmouth
[2] Laboratorio de seguridad, Facultad de EEMCS, Universidad Tecnológica de Delft
[3] Departamento de Ingeniería Electrónica y Eléctrica, Universidad de Loughborough
[4] Departamento de Ciencias de la Computación, Universidad de York

Resumen. En septiembre de 2009, David y Prasad propusieron en Mo-biSec'09 un nuevo e interesante protocolo de autenticación mutua ultraligero para etiquetas RFID de bajo costo. En este artículo, presentamos un método bastante potente.
Ataque criptoanalítico contra su propuesta: comenzamos con una trazabilidad ataque, luego describa cómo se puede extender para filtrar información almacenada a largo plazo. secretos, y finalmente presentar un ataque de divulgación total (llamado ataque Tango) donde se muestran todos los secretos que el protocolo está diseñado para ocultar. ser recuperable, incluso por un atacante pasivo después de espiar solo una pequeña parte número de sesiones de autenticación. Estos resultados implican que es muy realista Los escenarios de ataque son completamente posibles. El ataque de Tango constituye una nueva, sencilla pero poderosa técnica de criptoanálisis que se basa sobre el cálculo y la explotación completa de múltiples aproximaciones a los valores secretos, utilizando distancias de Hamming y la representación de variables en un espacio n-dimensional.

1 Introducción

Los protocolos de autenticación para sistemas de identificación por radiofrecuencia (RFID) permiten que un lector RFID y una etiqueta se autentiquen mutuamente.
Recientemente se han propuesto protocolos en la literatura, y el campo es desafiante ya que las etiquetas RFID solo pueden funcionar en entornos muy confinados con escasa recursos, por lo que los protocolos deben garantizar que los cálculos subyacentes no sean Uso intensivo de recursos. En esta línea, se ha propuesto una clase de protocolos de autenticación ultraligeros, en particular [7,8,9]. Estos protocolos utilizan solo operaciones, por ejemplo, OR exclusivo (XOR), AND bit a bit, NOT bit a bit, que son muy Son ligeros pero, por otro lado, sólo ofrecen propiedades de difusión muy limitadas.

Uno de los requisitos críticos para los protocolos de autenticación RFID es que Deben ser imposibles de rastrear, es decir, no debe ser posible rastrear los movimientos de una etiqueta. para ser rastreado; esto es especialmente relevante cuando se considera que las etiquetas deben ser incrustado en objetos (por ejemplo, ropa) y, por lo tanto, inherentemente ubicuo.
A partir de los crecientes ataques de trazabilidad, se pueden realizar ataques más fuertes mediante ataques pasivos. adversarios, incluida la recuperación de todos los secretos a largo plazo almacenados en las etiquetas, lo que implica que la etiqueta no solo es rastreable sino también totalmente identificable y clonable. El anonimato quedaría así totalmente roto.

SB Ors Yalcin (Ed.): RFIDSec 2010, LNCS 6370, págs. 22–34, 2010.

En este artículo se presentan resultados criptoanalíticos tanto en términos de ataques de trazabilidad como de ataques que recuperan secretos almacenados a largo plazo, incluidas las claves y el identificador estático. Estos solo requieren que el adversario sea pasivo (es decir, que escuche a escondidas) y, por lo tanto, son ataques devastadores con enormes implicaciones de seguridad para el protocolo en cuestión.

Al montar estos ataques, demostramos todo el poder de los recientes desarrollos criptoanalíticos, en particular el ataque de trazabilidad basado en diferencias de tablas de verdad con respecto a un juego de impracticabilidad [10], y el criptoanálisis Tango, que se basa en el cálculo de múltiples aproximaciones y es una técnica novedosa introducida por primera vez en este artículo.

A continuación, aplicamos estas técnicas criptoanalíticas a un protocolo RFID reciente propuesto por David y Prasad en MobiSec '09 [2], y mostramos y analizamos los resultados con cierta profundidad.

2 El Protocolo David-Prasad

En septiembre de 2009, David y Prasad propusieron en MobiSec'09 un nuevo protocolo de autenticación ultraligero inspirado en enfoques anteriores como la familia de protocolos UMAP [7,8,9] y los esquemas SASI [1] y Gossamer [6].
Su propuesta tiene como objetivo proporcionar un mecanismo de autenticación fuerte y, al mismo tiempo, ofrecer una reducción significativa en la carga computacional de la etiqueta, sin comprometer la seguridad.

La etiqueta y el servidor (también llamado base de datos back-end) comparten cuatro valores: el antiguo y el posible nuevo seudónimo {PID, PID2}, respectivamente, y dos claves secretas {K1, K2}. Además, la etiqueta almacena un identificador estático ID que facilita su identificación inequívoca. Los autores suponen que el ID y todas las variables restantes tienen la misma longitud de bits (es decir, {PID, PID2, K1, K2,ID} Z96 2).
Se asume el modelo de comunicación común, por lo que las comunicaciones entre el lector y el servidor (ambos dispositivos, sin duda, potentes) se consideran seguras, ya que estas entidades pueden permitirse el lujo de utilizar soluciones de seguridad clásicas (por ejemplo, TLS o SSL).
Por otro lado, los canales de avance (de lector a etiqueta) y de retroceso (de etiqueta a lector) se consideran inseguros y abiertos a todo tipo de ataques.

A continuación, describimos el protocolo, que se divide en seis pasos. Los operandos { , } simbolizan el OR exclusivo bit a bit (XOR) y el AND bit a bit, respectivamente, mientras que x denota el NOT $\overline{\text{bit}}$ a bit de x.

Paso 1: El lector envía un mensaje de solicitud C al servidor. Si resulta ser un lector autorizado, el servidor envía un certificado de acceso de autorización de un día C. Si el lector ya tiene un certificado válido, salta directamente al paso 2.

Paso 2: El lector envía un mensaje de solicitud IDrequest a la etiqueta, que responde con su seudónimo PID2.

Paso 3: El lector envía la tupla {PID2, C} al servidor para obtener la información privada vinculada a la etiqueta. Si el certificado es válido y PID2 coincide con una de las entradas de la base de datos, el servidor envía {K1, K2} de vuelta.

al lector. De lo contrario, el servidor informa al lector que PID2 no corresponder a cualquier entrada en su base de datos. En ese caso, el lector repite el paso 2 para obtener acceso al antiguo PID del seudónimo de la etiqueta. Luego, Paso 3 se ejecuta con la tupla {PID, C}.

Paso 4: El lector genera dos números aleatorios n1 y n2. Luego, calcula los mensajes {A, B, D} de la siguiente manera y los envía a la etiqueta:

$$A = (PID2 \quad K1 \quad K2) \quad n1 \tag{1}$$

$$B = (\overline{PID2} \quad K2 \quad K1) \quad n2 \tag{2}$$

$$D = (K1 \quad n2) \quad (K2 \quad n1) \tag{3}$$

Paso 5: A partir de los mensajes {A, B}, la etiqueta puede inferir fácilmente el valor de los nonces {n1, n2} asociado a la sesión actual. Con estos valores, calcula su versión local del mensaje D (llamémoslo D) y verifica si es idéntico al valor recibido. Si coinciden, entonces el lector está autentificado. De lo contrario, El protocolo se cancela. Después de una autenticación de lector exitosa, la etiqueta calcula los mensajes {E,F} de la siguiente manera y los envía de vuelta al lector:

$$mi = (K1 \quad n1 \quad ID) \quad (K2 \quad n2) \tag{4}$$

$$F = (K1 \quad n1) \quad (K2 \quad n2) \tag{5}$$

Finalmente, la etiqueta actualiza sus valores de seudónimos utilizando los nonces de sesión:

$$PID = PID2 \tag{6}$$

$$PID2 = PID2 \quad n1 \quad n2 \tag{7}$$

Paso 6: Al recibir los mensajes E y F, el lector calcula una versión local, F , y comprueba si es idéntico al valor recibido. Si ambos coinciden, el La etiqueta se autentica y el lector puede obtener el identificador estático ID de la etiqueta utilizando el mensaje E y los valores ahora conocidos {K1, K2, n1, n2} (es decir, $ID = E \quad (K2 \quad n2) \quad K1 \quad n1$). A continuación, actualiza los seudónimos vinculados a la etiqueta de la misma manera:

$$PID = PID2 \tag{8}$$

$$PID2 = PID2 \quad n1 \quad n2 \tag{9}$$

Finalmente, el lector envía una versión actualizada del par {PID, PID2} y su certificado C al servidor. Si el certificado es válido, el servidor actualiza el información (seudónimos) asociada a la etiqueta.

3 Ataque de trazabilidad

La trazabilidad es una de las amenazas de seguridad más importantes en los entornos RFID. Sin embargo, numerosos protocolos RFID lo ponen en riesgo al diseñar esquemas donde Las etiquetas responden a las consultas de los lectores con valores estáticos, lo que dificulta los ataques de trazabilidad. No sólo es posible, sino trivial. Por estas y otras razones (en particular, la privacidad).

implicaciones debido a la movilidad de las etiquetas), el problema de la trazabilidad ha atraído recientemente una gran cantidad de investigaciones interesantes. En [4], Juels y Weis dieron una definición formal de trazabilidad, que luego fue reformulada, en un estilo más similar a utilizado para protocolos de seguridad, en [10]. Utilizamos el último enfoque para analizar la Protocolo David-Prasad. Para que sea completo y fácil de leer, primero presentaremos el modelo, y más adelante detallaremos nuestra propuesta de ataque.

En los esquemas RFID, las etiquetas (T) y los lectores (R) interactúan en sesiones de protocolo. En términos generales, el adversario (A) controla las comunicaciones entre todos los participantes e interactúa pasiva o activamente con ellos. En concreto, A puede Ejecute las siguientes consultas:

– Consulta Execute(R, T, i). Esto modela un atacante pasivo. Un espía espía canal y obtiene acceso de lectura a los mensajes intercambiados entre R y T en la sesión i de una ejecución de protocolo genuino.
– Consulta Test(i, T0, T1) . Esto no modela ninguna habilidad de A, pero es necesario definir la prueba de imposibilidad de rastrear. Cuando se invoca esta consulta para la sesión i, se genera un bit aleatorio b {0, 1}. Luego, se genera un seudónimo P Tb ID2(i) y un nuevo conjunto de mensajes intercambiados {ATb , DTb , ETb , F Tb } desde el PF T1 }}, Para 0 ID2(i)} y {{AT0, BT0 ET0 F T0 }, {AT1 , BT1 , DT1 ET1 establecen {P ID2(i), , respectivamente, y correspondientes a las etiquetas {T0, T1} se dan a A.

Una vez definidas las capacidades del adversario, el problema de la imposibilidad de rastrear puede ser: definido como un juego G dividido en tres fases:

Fase 1 (Aprendizaje): A puede realizar cualquier cantidad de consultas Execute, que facilitan la escucha de los mensajes intercambiados, modelando un ataque pasivo.
– a través del canal de radio inseguro.

Fase 2 (Desafío): A elige dos etiquetas actuales cuyos identificadores asociados son IDT0 e IDT1 . Luego envía una consulta Test(i, T0, T1) . Como resultado, A recibe un seudónimo P Tb. ID2(i) y un nuevo conjunto de mensajes intercambiados { ATb , , DTB , ETB , F Tb } del conjunto {P Para 0 ID2(i), P T1 ID2(i)} y {{AT0, BT0 , BTb, DT0, ET0, F T0 }, {AT1 , BT1 , DT1 , ET1 , F T1 }}, respectivamente, que dependen de una bit aleatorio elegido b {0, 1}.

Fase 3 (Adivinación): A finaliza el juego y genera un bit d (d {0, 1}) como su conjetura del valor de b.

El éxito de A en ganar G es equivalente al éxito de romper la propiedad de imposibilidad de rastreo que ofrece el protocolo. Por lo tanto, la ventaja de A en distinguir
A continuación se define si los mensajes corresponden a T0 o T1 , donde t es un parámetro de seguridad (por ejemplo, la longitud en bits de la clave compartida por la etiqueta y el lector). y r es el número de veces que A ejecuta una consulta Execute.

$$\mathrm{AdvUNT}_A(t, r) = |Pr[d = b] - |. \quad \frac{1}{2}$$

Entonces, un protocolo RFID ofrece resistencia a la trazabilidad, es decir, se dice que ser irrastreable (UNT), si AdvUNT A (t, r) < ε(t, r), donde ε(·, ·) simboliza algún función despreciable

En esencia, esta noción de imposibilidad de rastrear (UNT) es análoga a la noción convencional noción de indistinguibilidad de texto cifrado (IND) para el cifrado o indistinguibilidad de clave para protocolos de establecimiento de clave. En la misma línea, la noción UNT
Capta el hecho de que ningún adversario puede distinguir entre dos etiquetas incluso si él/ella pueden elegir lo que quieren ser. De hecho, si el adversario no puede hacer esto, entonces
Está claro que no puede rastrear los movimientos de una etiqueta.

A continuación demostraremos cómo el esquema David-Prasad no satisface la condición antes mencionada, poniendo en riesgo la privacidad de la ubicación de las etiquetas titulares. Más precisamente, un adversario A lleva a cabo el procedimiento que se describe a continuación:

Fase 1 (Aprendizaje): A realiza la consulta Execute(R, T0, i), y así obtiene el seudónimo P T0 ID2(i) y mensajes {A, B, D, E, F}. Al calcular el XOR entre E y F, obtenemos

$$E \oplus F = (K1 \oplus n1 \oplus ID) \oplus (K2 \oplus n2) \oplus (K1 \oplus n1) \oplus (K2 \oplus n2)$$
$$= (K1 \oplus n1 \oplus ID) \oplus (K1 \oplus n1)$$
$$= (K1 \oplus n1) \oplus (K1 \oplus n1) \oplus ID.$$

Si analizamos poco a poco las tablas de verdad que se proporcionan a continuación

a	b	a	b	a ∧ b	a ∧ b ⊕ b
0	0	0	0	0	0
1	1	1	1	0	0
1	1	1	1	0	0
					1

Es fácil ver que XOR y AND son complementos entre sí con probabilidad $\frac{3}{4}$. Por lo tanto, para cualquier posición de bit, el valor de bit de (K1 ⊕ n1) es el opuesto de (K1 ∧ n1) con probabilidad $\frac{3}{4}$. Entonces su XOR es 1. Por lo tanto F = ID para cada bit con probabilidad $\frac{3}{4}$.

Fase 2 (Desafío): A elige dos nuevas etiquetas cuyos identificadores asociados son IDT0 e IDT1 . Luego envía una consulta Test(i, T0, T1) . Como resultado, A Se le da un nuevo seudónimo P Tb ID2(i) y un nuevo conjunto de mensajes intercambiados { ATb , ETb , FTb } del conjunto {P Para 0 ID2(i), P T1 ID2(i)} y {{AT0, BT0 , DT0 , ET0 , F T0 }, {AT1 , BT1 , DT1 , ET1 , F T1 }}, respectivamente, que dependen de una bit aleatorio elegido b {0, 1}.

Fase 3 (Adivinación): A termina G y genera un bit d = lsb(E ⊕ F) lsb(ETb ⊕ F Tb) como su conjetura del valor b, donde lsb(·) denota el menor un poco significativo. Así que tenemos,

$$\mathrm{AdvUNT}_{A}(t, 1) = \left|Pr[d = b] - \frac{1}{2}\right| = \frac{5}{8} - \frac{1}{2} = \frac{1}{8} > \varepsilon.$$

Así, el protocolo David-Prasad en un sistema RFID (S= {Ri, T0, T1, ... }) en el que un adversario pasivo A sólo escucha a escondidas una única ejecución del protocolo (modelado por una consulta de ejecución en el juego G), es vulnerable a las más simples y un ataque de trazabilidad efectivo es concebible.

4. Fuga de secretos guardados

Además de los problemas de trazabilidad, el protocolo David-Prasad también filtra sus secretos almacenados a largo plazo, en particular el identificador estático ID y las claves secretas K1 y K2.

Generalizando nuestro análisis anterior, específicamente la Fase 1 del ataque de trazabilidad, si denotamos por k la longitud de bit[1] de ID, entonces el identificador estático completo ID se puede recuperar con probabilidad $\frac{1}{3}^{4}$ Esto filtra demasiados fragmentos de identificación. y amenaza seriamente el anonimato de la etiqueta.

Un ataque para filtrar información sobre las claves secretas almacenadas funciona de la siguiente manera. El adversario puede realizar las consultas Execute(R, T0, i − 1), Execute(R, T0, i) para dos sesiones consecutivas, para obtener los seudónimos Xi−1 = P T0 ID2(i − 1), Xi = P T0 ID2(i) y los mensajes {Ai−1, Bi−1, Di−1, Ei−1, Fi−1}, {Ai, Bi, Di, Ei, Fi}, respectivamente. De la ecuación (7), vemos que Xi−1, Xi nos permite calcular el XOR entre los dos nonces {n1, n2} de la i-ésima sesión:

$$Y = Xi-1 \quad Xi$$
$$= n1 \quad n2.$$

Además, el adversario puede calcular el XOR de Ai y Bi:

$$Z = Ai \quad Bi$$
$$= ((P\ ID2(i) \quad K1 \quad K2) \quad n1) \quad (\overline{(P\ ID2(i) \quad K2} \quad K1) \quad n2)$$
$$= (K1 \quad K2) \quad n1 \quad n2.$$

De esta manera, el adversario obtiene

$$Y \quad Z = K1 \quad K2$$

Tenga en cuenta que para aquellos bits donde K1 K2 es 1, esto implica que ambos bits de clave son 1. En consecuencia, en promedio, se recuperarán $\frac{a}{4}$ bits de ambas claves después de dos sesiones. Estas observaciones tienen grandes implicaciones de seguridad y se pueden explorar y refinar más para revelar aún más información, pero esto ya no es necesario en vista del siguiente ataque de divulgación completa.

5 Un criptoanálisis pasivo de Tango

En esta sección presentamos un nuevo ataque pasivo (es decir, completamente realista en el modelo de seguridad subyacente) y extremadamente eficiente para recuperar completamente tanto los valores de clave secreta {K1, K2} como el identificador estático de la etiqueta ID, que son de hecho toda la información secreta que el protocolo está diseñado para ocultar. El ataque se divide en dos fases principales: 1) Selección de buenas aproximaciones; y 2) Combinación de las buenas aproximaciones así obtenidas para revelar Ki o ID. Describimos cada una de estas fases a continuación.

[1] David y Prasard suponen que la longitud de bits de todas las variables se establece en 96.

Fase 1: El ataque explota la fuga de información secreta a través del canal de radio inseguro debido al hecho de que los mensajes intercambiados se derivan de valores secretos utilizando únicamente funciones triangulares [5]. Se sabe que las operaciones triangulares y su composición (que también es triangular) tienen propiedades de difusión muy pobres. Por eso, el atacante puede comprobar y tener éxito en el uso de múltiples combinaciones simples de los mensajes públicos intercambiados {A, B, D, E, F} como Buenas Aproximaciones (GA) para los secretos Ki o ID. Los mensajes públicos intercambiados no ocultan lo suficientemente bien estos valores secretos. De todo el conjunto de aproximaciones, el adversario está interesado en aquellas que están sistemáticamente más cerca (en promedio) del valor secreto objetivo X {K1, K2, ID}. Es decir, aquellos para los que la distancia de Hamming entre una aproximación Z y, por tanto, o bien hw(Z, X) < 48 el valor X se desvía del valor esperado o bien hw(Z,X) < 48.2 En el Apéndice A, enumeramos la distancia de Hamming combinaciones posibles de los mensajes intercambiados con $\frac{96}{2}$, media dist(X, ·) de todas las los secretos. Presentamos en la siguiente tabla las mejores aproximaciones para cada uno de los tres valores secretos que queremos recuperar, que son los que empleamos en nuestro ataque:

Objetivo	Buenas aproximaciones
K1	GA-K1 = {D, F,(A D),(A F),(B D),(B F), (A B D),(A B F)}
K2	GA-K2 = {D, F,(A D),(A F),(B D),(B F), (A B D),(A B F)}
ID	GA-ID = {(E F),(A B E),(A D E), (A E F),(B D E),(D E F),(A B D E), (A D E F),(B D E F)}

Fase 2: La idea básica en esta fase del ataque es combinar múltiples aproximaciones (es decir, Z {GA-K1, GA-K2, GA-ID}) obtenidas en diferentes sesiones, para construir una global que esté altamente correlacionada con los valores secretos (es decir, claves {K1, K2} e identificador estático ID). Esto se puede hacer de varias maneras y formas diferentes, pero en el caso del protocolo David-Prasad funciona bastante bien un enfoque muy simplista. La forma en que procedemos es la siguiente: para cada sesión de autenticación interceptada, calculamos una serie de buenas aproximaciones a los valores secretos y luego las almacenamos como filas de tres matrices diferentes (una para cada uno de K1, K2 e ID). Después de interceptar una cantidad dada de sesiones, calculamos los valores globales simplemente sumando repetidamente cada una de las columnas de las matrices y devolviendo un 0 si la cantidad total de unos en dicha columna está por debajo de un umbral dado γ, o un 1 en cualquier otro caso. En la Figura 1, proporcionamos un ejemplo numérico simple para describir mejor el ataque, donde la longitud de bits de las variables involucradas se ha establecido en solo 8 bits. El procedimiento para recuperar El adversario tiene que proporcionar una conjetura del identificador estático ID o la clave Ki después de la escucha de algunas sesiones. En cada una de ellas, múltiples

[2] Suponemos una longitud de bits de 96 para cada uno de Ki,ID [3].

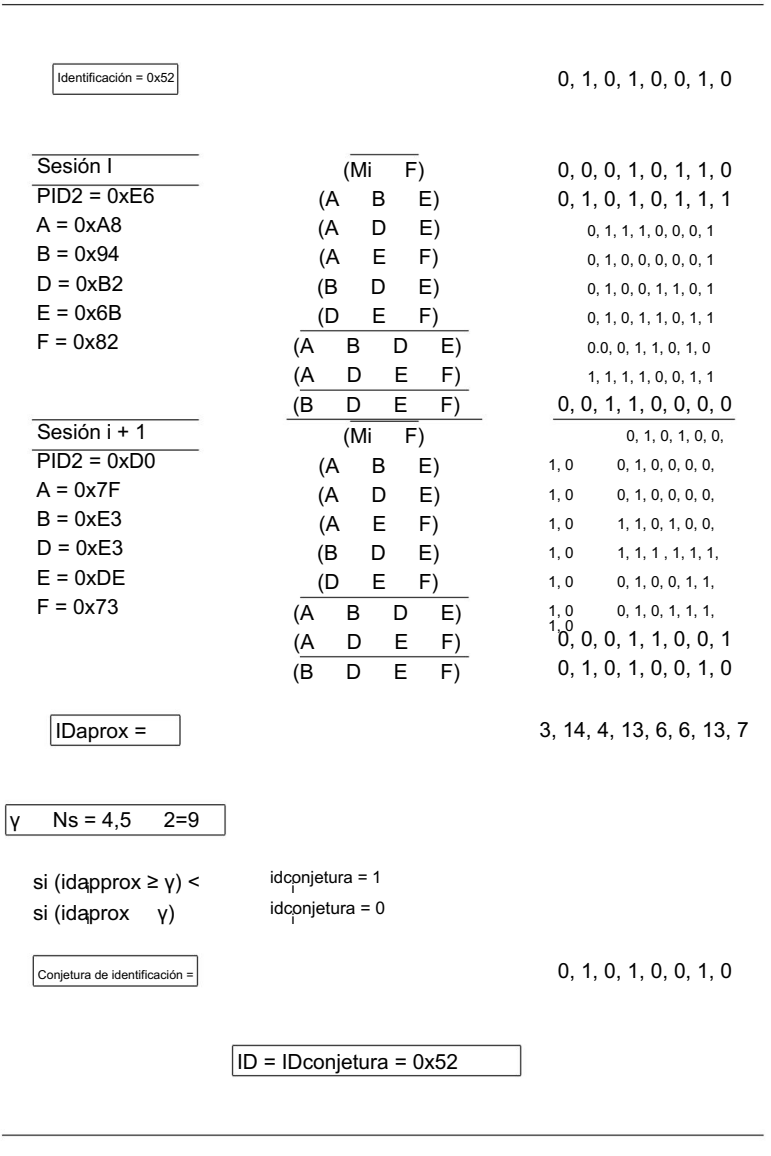


Fig. 1. Un ejemplo a escala reducida (que utiliza variables de 8 bits en lugar de 96 bits) de cómo funciona el criptoanálisis de Tango

Se obtienen aproximaciones del valor buscado – cada una de estas aproximaciones representa una fila en la matriz correspondiente. La forma más sencilla de obtener un valor final es seleccionar el valor mayoritario en cada columna de esta matriz. Podemos sumar rápidamente todas las filas para obtener un vector final. Entonces, si el valor en una columna de este vector es mayor que la mitad del número de aproximaciones NA por el número de sesiones interceptadas NS, conjeturamos un 1 en esa columna. De lo contrario, conjeturamos un 0. Podemos definir esto de una manera más formal: Sean X e Y dos vectores y xi e yi los valores en cada columna de estos vectores respectivamente. Si el vector X es la entrada de la función umbral th(X), el vector resultante se define por:

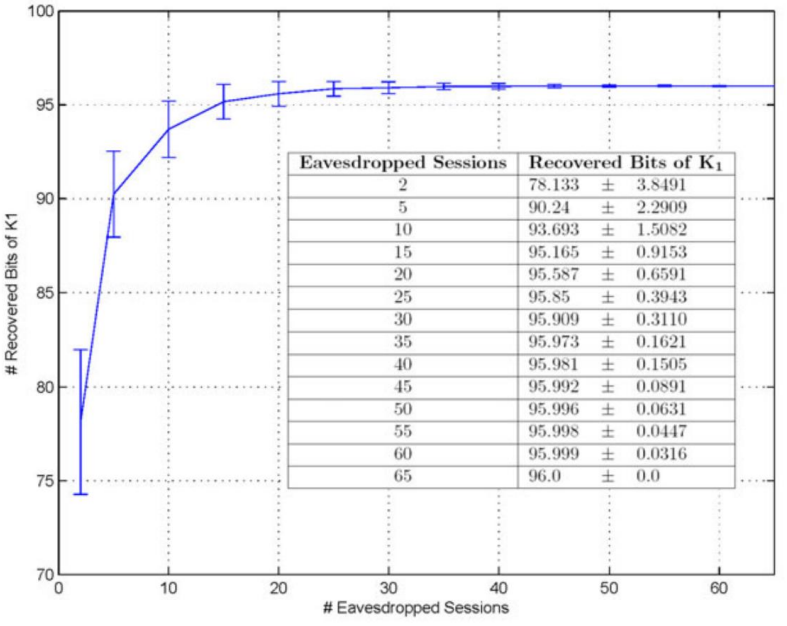
$$y(X) = \begin{matrix} \text{si } (Xi \geq \gamma) \text{ si} \\ (Xi < \gamma) \end{matrix} \quad \begin{matrix} Yi = 1 \\ Yi = 0 \end{matrix} \quad \text{donde } \gamma = 0{,}5 \quad NA \quad NS$$

Esta forma extremadamente fácil y eficiente de combinar aproximaciones funciona sorprendentemente bien para producir aproximaciones globales muy precisas para los tres valores secretos después de espiar una cantidad relativamente pequeña de sesiones de autenticación. Los resultados se presentan en las siguientes figuras.

Hemos simulado nuestro ataque para evaluar su viabilidad y eficacia. Primero, inicializamos aleatoriamente los valores secretos (es decir, {PID, PID2, K1, K2,ID}). Luego, simulamos NS sesiones legítimas del protocolo – el atacante escucha las sesiones NS – y ejecutamos la estrategia del adversario (Fase 2) para obtener una conjetura de las claves {K1, K2} y el identificador estático ID. Finalmente, comparamos el valor de conjetura global Xconjecture {K1conjecture , K2conjecture ,IDconjecture} con el valor real X {K1, K2,ID} para medir el éxito del adversario. La media y la desviación estándar del número de bits recuperados con éxito, para varios valores de sesiones interceptadas (NS), se resumen en las Figuras 2, 3 y 4. En nuestras simulaciones, la longitud de bits de las variables se establece en 96 y para cada valor de NS repetimos el experimento 10.000 veces. Para {K1conjecture , K2conjecture ,IDconjecture}, el umbral se establece en {0,5 8 NS, 0,5 8 NS, 0,5 9 NS} respectivamente, lo que significa que en todos los casos estamos adivinando el valor mayoritario entre los observados.

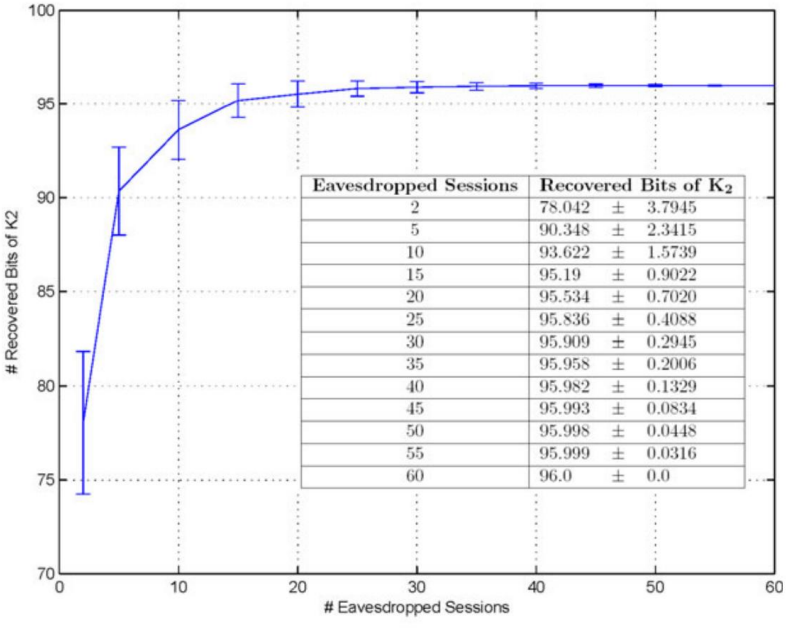
Como utilizamos el mismo número de aproximaciones (8 por cada sesión interceptada) para K1 y K2, y son igualmente potentes, los resultados obtenidos son bastante similares. En ambos casos, el número de sesiones interceptadas necesarias por un atacante para revelar la clave secreta completa Ki es menor o igual a 65.

La eficacia de este ataque para revelar el identificador estático ID es ligeramente superior en comparación, en parte debido al hecho de que en este caso se utilizan 9 aproximaciones, en lugar de 8. Para el ID, el adversario solo necesita alrededor de 50 sesiones para revelar por completo los 96 bits del identificador estático. Si bien estas cifras son más que suficientes para considerar que el protocolo está completamente roto, también observamos que un atacante más limitado no se ve obligado a evadir tal cantidad de sesiones para recuperar por completo los 96 bits: después de solo 5 o 10 sesiones, se adivinan correctamente más de 90 bits y los restantes se pueden identificar fácilmente mediante una búsqueda de fuerza bruta fuera de línea.



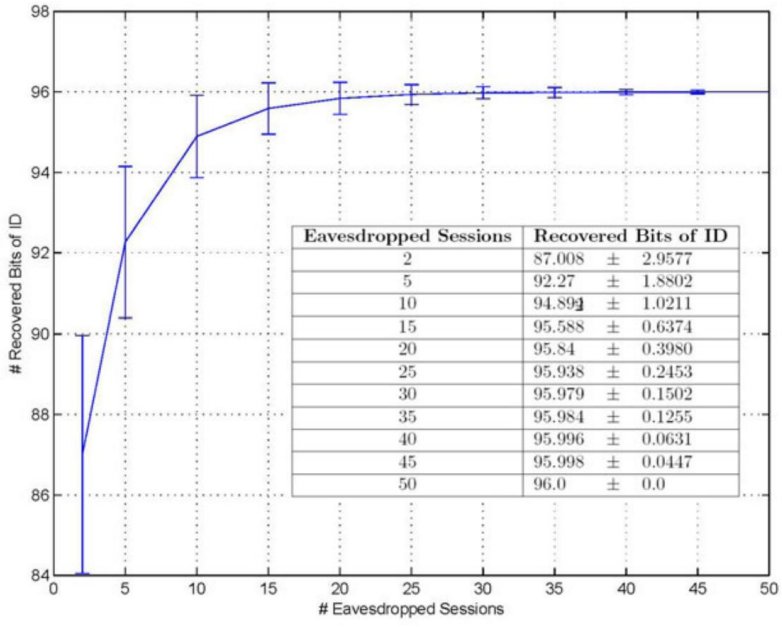
Eavesdropped Sessions	Recovered Bits of K_1
2	78.133 ± 3.8491
5	90.24 ± 2.2909
10	93.693 ± 1.5082
15	95.165 ± 0.9153
20	95.587 ± 0.6591
25	95.85 ± 0.3943
30	95.909 ± 0.3110
35	95.973 ± 0.1621
40	95.981 ± 0.1505
45	95.992 ± 0.0891
50	95.996 ± 0.0631
55	95.998 ± 0.0447
60	95.999 ± 0.0316
65	96.0 ± 0.0

Fig. 2. Recuperación del bit K1 , en función del número de sesiones interceptadas



Eavesdropped Sessions	Recovered Bits of K_2
2	78.042 ± 3.7945
5	90.348 ± 2.3415
10	93.622 ± 1.5739
15	95.19 ± 0.9022
20	95.534 ± 0.7020
25	95.836 ± 0.4088
30	95.909 ± 0.2945
35	95.958 ± 0.2006
40	95.982 ± 0.1329
45	95.993 ± 0.0834
50	95.998 ± 0.0448
55	95.999 ± 0.0316
60	96.0 ± 0.0

Fig. 3. Recuperación de bits de K2 , en función del número de sesiones interceptadas



Eavesdropped Sessions	Recovered Bits of ID
2	87.008 ± 2.9577
5	92.27 ± 1.8802
10	94.894 ± 1.0211
15	95.588 ± 0.6374
20	95.84 ± 0.3980
25	95.938 ± 0.2453
30	95.979 ± 0.1502
35	95.984 ± 0.1255
40	95.996 ± 0.0631
45	95.998 ± 0.0447
50	96.0 ± 0.0

Fig. 4. Recuperación del bit de identificación, en función del número de sesiones interceptadas

Los ataques que acabamos de presentar tienen graves consecuencias para la seguridad general del protocolo. De hecho, arruinan por completo todas las propiedades de seguridad que afirman sus autores. Después de realizar el ataque, el adversario puede recuperar toda la información secreta compartida entre la etiqueta y el servidor, por lo que puede eludir de forma trivial cualquier mecanismo de autenticación (es decir, la autenticación de la etiqueta y del lector) y suplantar la etiqueta en el futuro, o simplemente clonarla. La información confidencial se pone en riesgo y las respuestas de la etiqueta pueden rastrearse incluso aunque se utilicen dos números aleatorios en cada sesión en un intento fallido de evitar que esto suceda. Un ataque de desincronización contra la etiqueta (o el servidor) también es bastante sencillo, ya que el adversario puede generar cualquier mensaje de sincronización válido que de

6 Conclusiones

El diseño de protocolos de seguridad ultraligeros para etiquetas RFID de bajo coste es un desafío estimulante debido a las severas restricciones computacionales de estos dispositivos. Aunque recientemente se han publicado interesantes propuestas en este ámbito de investigación, el diseño de esquemas seguros sigue siendo una cuestión abierta. De hecho, la gran mayoría de los esquemas publicados ya están rotos.

Las funciones triangulares son muy atractivas porque se pueden implementar de manera eficiente en hardware, pero un criptoanalista puede aprovechar su uso debido a sus propiedades de difusión muy pobres. Por lo tanto, se pueden y probablemente se deban usar, pero no solas, ya que la composición de las funciones triangulares sigue siendo triangular.

Deberían combinarse con funciones no triangulares –como se propone en SASI [1]– para dificultar la tarea de romper el esquema. Las operaciones de rotación son una posibilidad bastante interesante ya que no son triangulares, permiten amplificar la difusión y también son muy eficientes para implementar en hardware. Si tuviéramos que señalar la principal razón para las debilidades encontradas en el protocolo David-Prasad, aparte del diseño de algunos mensajes, esta sería definitivamente la no inclusión de ningún tipo de rotaciones (basadas en Hamming o modulares) en el conjunto de operaciones utilizadas. La inclusión de nonces es muy probablemente una condición necesaria para garantizar el anonimato, pero por sí sola no asegura esta propiedad deseable, ni ninguna protección contra ataques de trazabilidad.

No afirmamos que los ataques y técnicas presentados aquí sean óptimos en ningún sentido y que se puedan diseñar ataques más sutiles y quizás un poco más potentes, pero creemos que a la luz de los resultados ofrecidos aquí no hay necesidad de ello. Sin embargo, posiblemente una combinación de la aproximación al ID obtenido en la Sección 4, combinada con las aproximaciones utilizadas en el ataque Tango podría conducir a un enfoque ligeramente más eficiente.

La técnica criptoanalítica presentada en este artículo, denominada ataque Tango, también podría considerarse una nueva herramienta para analizar protocolos ligeros y, por lo tanto, útil para el diseño de futuras propuestas más seguras. Creemos que resultará exitosa frente a otros protocolos y algoritmos ligeros porque, casi por definición, en muchos casos no tienen los recursos computacionales necesarios para permitir una mezcla adecuada (es decir, altamente no lineal) de los valores secretos internos para evitar la fuga de algunos bits en cada sesión.

Referencias

1. Chien, H.-Y.: SASI: Un nuevo protocolo de autenticación RFID ultraligero que proporciona una autenticación sólida y una integridad sólida. IEEE Trans. Dependable Secur. Computación 4(4), 337–340 (2007)
2. David, M., Prasad, NR: Proporcionar seguridad sólida y alta privacidad en redes RFID de bajo costo. En: Proc. of Security and Privacy in Mobile Information and Communication Systems, MobiSec 2009, págs. 172-179. Springer, Heidelberg (2009)
3. EPCglobal: Versión estándar del protocolo de interfaz aérea UHF de clase 1 generación 2 1.2.0: Generación 2. (2008), http://www.epcglobalinc.org/standards/
4. Juels, A., Weis, S.: Definición de privacidad sólida para RFID. En: Proc. of PerCom 2007, págs. 342–347. IEEE Computer Society Press, Los Alamitos (2007)
5. Klimov, A., Shamir, A.: Nuevas aplicaciones de funciones T en cifrados de bloques y funciones hash. En: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, págs. 18-31. Springer, Heidelberg (2005)
6. Peris-Lopez, P., Hernandez-Castro, JC, Estevez-Tapiador, JM, Ribagorda, A.: Avances en criptografía ultraligera para etiquetas RFID de bajo costo: protocolo Gossamer. En: Chung, K.-I., Sohn, K., Yung, M. (eds.) WISA 2008. LNCS, vol. 5379, págs. 56–68. Springer, Heidelberg (2009)
7. Peris-Lopez, P., Hernandez-Castro, JC, Estevez-Tapiador, J., Ribagorda, A.: LMAP: Un protocolo ligero de autenticación mutua real para etiquetas RFID de bajo coste. En: Hand. of RFIDSec (2006)

8. Peris-López, P., Hernández-Castro, JC, Estevez-Tapiador, J., Ribagorda, A.:
M2AP: un protocolo minimalista de autenticación mutua para etiquetas RFID de bajo coste.
En: Ma, J., Jin, H., Yang, LT, Tsai, JJ-P. (eds.) UIC 2006. LNCS, vol. 4159, págs.
912–923. Springer, Heidelberg (2006)
9. Peris-López, P., Hernández-Castro, JC, Estevez-Tapiador, JM, Ribagorda, A.:
EMAP: Un protocolo de autenticación mutua eficiente para etiquetas RFID de bajo costo. En:
Meersman, R., Tari, Z., Herrero, P. (eds.) Talleres OTM 2006. LNCS, vol. 4277,
págs. 352–361. Springer, Heidelberg (2006)
10. Phan, R.: Criptoanálisis de un nuevo protocolo de autenticación RFID ultraligero
- SASI. Transacciones IEEE sobre computación confiable y segura (2008), doi:
10.1109/TDSC.2008.33

Apéndice

Aproximaciones a K1, K2 e ID (10.000 pruebas)

incógnita	dist(X, K1) 49,4	dist(X, K2) dist(X, ID)	
A	± 1,8547 48,3 ± 4,3829	49,3 ± 5,1196	
B	49,4 ± 5,0990 48,3 ±	6,2578 49,3 ± 3,9560	
D	34,0 ± 1,9493 35,1 ±	3,8587 52,4 ± 3,8000	
mi	47,8 ± 4,284	46,2 ± 4,6861 49,3 ± 4,1485	
F	36,1 ± 3,3600 35,6 ±	3,1686 50,8 ± 5,0160	
A B	48,6 ± 4,055	47,9 ± 5,1662 49,0 ± 3,7148	
A D	37,2 ± 3,4293 61,6 ±	2,2000 48,7 ± 2,9343	
A E	42,8 ± 3,628	48,3 ± 2,052	50,6 ± 4,3174
A F	61,3 ± 3,769 37,7 ± 4	,6054 48,9 ± 3,0806	
B D	61,8 ± 4,3543 36,9 ±	4,2532 47,1 ± 3,4771	
B E	47,6 ± 3,8262 47,8 ±	3,1874 47,6 ± 7,1722	
B F	37,7 ± 2,6851 60,8 ±	4,5343 46,9 ± 2,3000	
D E	42,6 ± 2,9732 45,7 ±	3,5228 52,3 ± 5,3675	
D F	47,1 ± 1,9723 46,7 ±	4,0509 51,6 ± 2,8355	
mi f	41,9 ± 4,5705 56,2 ±	4,1665 67,7 ± 5,4598	
A B D 37,6 ± 5	,8173 36,8 ± 2,4000	48,2 ± 5,8617	
A B E 56,0 ± 2	,1448 44,5 ± 3,4132	24,5 ± 3,6946	
A B F 35,5 ± 3	,2939 36,3 ± 3,0348	49,8 ± 3,6824	
A D E 47,2 ± 3	,1875 38,4 ± 3,9294	35,8 ± 4,9759	
A D F 47,5 ± 3	,5284 47,0 ± 5,0398	50,3 ± 6,4195	
A E F 48,5 ± 3	,3838 48,1 ± 2,6627	22,2 ± 1,7205	
B D E 51,2 ± 4	,7286 45,7 ± 3,1953	34,0 ± 3,7947	
B D F 49,9 ± 4	,5706 47,5 ± 4,7802	47,5 ± 3,4424	
B E F 49,9 ± 5	,1662 45,6 ± 4,200 D	E F 50,3	47,6 ± 6,9022
± 3,9762 45,3 ± 4,5	177 31,1 ± 3,5903		
A B D E 47,6 ± 4	,5211 55,4 ± 4,8208	61,1 ± 4,3920	
A B D F 44,5 ± 3	,9812 49,2 ± 3,3106	49,4 ± 3,555	
A B E F 48,3 ± 5	,2354 44,9 ± 5,6643	45,7 ± 5,0408	
A D E F 44,9 ± 3	,8066 40,6 ± 2,7276	35,8 ± 6,1449	
B D E F 45,5 ± 1	,8028 55,5 ± 4,7592	62,4 ± 2,7276	
A B D E F 53,5 ± 5,0843 45,4 ± 5,5534		42,7 ± 3,06757	