Even or Odd: A Simple Graphical Authentication System

N. López, M. Rodríguez, C. Fellegi, D. Long, *Fellow Member, IEEE* and T. Schwarz, *Senior Member*, *IEEE*

***Abstract*— Many portable devices need a simple authentication system to protect them from being used by an unauthenticated person such as a thief. The security of traditional methods such as pin codes or passwords is limited by shoulder surfing where a casual or intentional observer observes an authentication session and derives all information necessary for authentication. Graphical authentication systems have been developed to forestall this attack. We present here an especially simple variant of a graphical authentication system based on the capacity of humans to recognize faces well. In our challenge-response scheme, a user is presented with a row of typically three faces and needs to decide whether the number of "friends" is even or odd. We present here an analysis of security and usability of this scheme.**

***Keywords*— Authentication, Usability, Graphical Passwords**

I. Introducción

Es muy importante diseñar un protocolo que permita impedir el uso de los dispositivos móviles, y por ende preservar la privacidad de los datos en caso de hurto o pérdida. Los mecanismos están orientados a imposibilitar su uso sin autenticación, y así disuadir al individuo de la acción delictiva. A menudo los dispositivos móviles se utilizan en público, por lo tanto un adversario tiene la oportunidad de observar el proceso de autenticación. El mismo se denomina en Inglés *shoulder surfing* o *peeping* (atisbar o espiar). Un adversario sagaz puede incluso observar la ligera decoloración de las teclas durante la digitación de un pin o filmarla con un teléfono celular. Entretanto la autenticación biométrica no se torne en una realidad segura, es necesario crear esquemas de seguridad que resistan el peeping.

Un diseñador de sistema debe buscar un punto de equilibrio entre la seguridad y la facilidad de uso durante la autenticación. En inteligencia artificial se han desarrollado soluciones robustas como los solucionadores 3-SAT [1] por medio del cual se puede extraer información de un conjunto de observaciones de sesiones de autenticación. Pero lo que es fácil con solucionadores 3-SAT, supera las capacidades de un observador humano. Con el fin de que estas metodologías prevalezcan sobre otras, es necesario diseñar esquemas que no sean excesivamente complicados para un usuario medio. Nos inclinamos a favor de la usabilidad y proponemos una solución usable que proteja al usuario de una observación intencional pero limitada. Un ladrón potencial necesita filmar más que una sesión de autenticación para obtener una probabilidad útil para desbloquear el dispositivo. Un conocido de la víctima si puede observar la autenticación suficiente cantidad de veces o derivar el conocimiento necesario para desbloquearlo por interacción con la víctima. Este caso en particular escapa al alcance de nuestro protocolo de autenticación.

Nuestra propuesta se denomina, *Even or Odd* (*Par o Impar*), en la misma se le presenta al usuario un número de líneas con k rostros ($k \geq 3$) tomados de un conjunto de "amigos" y de "desconocidos" seleccionado anteriormente. Por defecto, $k=3$. El usuario utiliza dos botones para indicar si el número de amigos en una línea es par o impar. Este protocolo es una versión de *aprender a calcular la paridad* [3] que utiliza la facilidad humana para reconocer rostros.

A continuación presentaremos el trabajo relacionado y luego expondremos nuestro esquema en detalle. En la Sección 4, analizaremos la seguridad aplicando las premisas de la teoría de la información. En la Sección 5 presentaremos un informe con los resultados del experimento aplicando las propuestas relacionadas a la usabilidad tratados en este artículo. Posteriormente, se incorporarán mejoras al esquema de seguridad inicialmente propuesto.

II. TRABAJO RELACIONADO

Matsumoto e Imai [8] fueron los primeros autores en proponer un esquema de autenticación segura contra el shoulder-surfing, pero como Wang y sus colegas lograron forzar dicho esquema de seguridad [14] Matsumoto debía incorporar mejoras [9]. El esquema mejorado es del tipo desafío-respuesta. La solución reside en aplicar un vector de campos de Galois y la respuesta se obtiene calculando sus productos escalares. A pesar de la mejora introducida a la propuesta original, aún persisten dudas sobre si la misma es viable para ser utilizado por un usuario común. Hopper y Blum [3] y Li y Teng [6] mejoran la seguridad del sistema de Matsumoto. Hopper y Blum lo basan en un problema NP-duro, pero admiten que el resultado es poco usable. El esquema de Li y Teng tampoco parece intuitivo.

Li y Shum [5] le adicionan dos componentes. En el primero proponen la aplicación de gemelos donde los desafíos se plantean por pares. El usuario selecciona un desafío al azar para responder como verdadero y a otro como falso. El segundo (Foxtail) consiste en ocultar la respuesta. El protocolo que hemos elegido es del tipo Foxtail, debido a que el usuario no debe identificar en forma directa los rostros que se les presentan.

Weinshall [13] utiliza una partición secreta de un conjunto de

N. López, Universidad Católica del Uruguay, Montevideo, Uruguay, nicolas.eduardo.lopez@gmail.com

M. Rodriguez, Universidad Católica del Uruguay, Montevideo, Uruguay, matias.rodrigo.rodriguez@gmail.com

C. Fellegi, Universidad Católica del Uruguay, Montevideo, Uruguay, cfellegi@ucu.edu.uy

D. Long, University of California, Santa Cruz, USA, darrell@cs.ucsc.edu

T. Schwarz, Universidad Centroamericana, La Libertad, El Salvador, tschwarz@jesuits.org

íconos entre un subconjunto F y su complemento que comparte el autenticado con el dispositivo. Por ejemplo, en el dispositivo, se le presenta al usuario una grilla de 8 por 10 íconos con preguntas del tipo múltiple opción. El usuario inicia mentalmente un camino comenzando por el ícono en la esquina arriba-derecha hacia el borde izquierdo o abajo definido por la afiliación de los íconos y los va recorriendo en la medida que halla la respuesta. Esta solución es segura contra ataques del tipo shoulder-surfing, si no se graban sesiones de autenticación. Golle y Wagner [1] han demostrado que con un solucionador 3-SAT se puede obtener la partición en un número limitado de observaciones.

Li y sus colegas [7] utilizan un método de memorización *Método de Loci* el cual afilia un objeto o un hecho a una ubicación en un ambiente familiar. Con el fin de brindar más seguridad le añaden un objeto y un color. Por ejemplo una contraseña podría ser "Una muñeca con pelo rojo en la cocina". Con el fin de dificultar el shoulder-surfing, la respuesta a los colores se presenta en grupos.

Wiedenbeck y colegas [14] también utilizan una partición compuesta por un conjunto de íconos. Se le presenta al usuario una pantalla completa de íconos y se le solicita que cliquee los íconos que conforman un polígono convexo definido por del subconjunto primario. Para ello es necesario realizar un análisis formal de este esquema, el cual a priori parece ser difícil. Cabe destacar, que un observador puede excluir un número de íconos en cada una de las observaciones.

Roth y colegas [10] han desarrollado un método en el cual se le solicita al usuario que ingrese un PINs de cuatro dígitos. Siendo el teclado numérico y la mitad de las teclas son coloradas sobre blanco y las otras coloradas sobre negro. En lugar de registrar el dígito, el usuario debe seleccionar el color del dígito. Luego de 16 rondas, el sistema puede reconstruir el PIN. Desafortunadamente, un shoulder-surfer también puede replicar estas mismas acciones.

Tan et al. [11] proponen implementar un teclado de modo tal que le torne muy difícil a un espía reconstruir la clave por medio de la observación, pero los resultados obtenidos no son los esperados, si se da el caso en el cual el observador graba dicha interacción.

Por su parte Kim y colegas [4] desarrollaron el método ColorRings, en el cual se le solicita al usuario que recuerde un conjunto de íconos para autenticarse. Para ello se le presenta una pantalla completa con íconos y se le solicita que halle cuatro anillos elípticos colorados de modo que rodeen los íconos del conjunto que componen la contraseña. Un anillo debe contener entre seis o siete íconos, con una sola observación el adversario posee el 0.056% de probabilidad de identificar los íconos de la contraseña. Se considera que esta solución posee como debilidad - en términos generales - que los usuarios tienen tendencia a centrar los anillos alrededor de los íconos que identifican a la contraseña, por lo tanto se pierde seguridad.

Gridsure (http://www.gridsure.com) es un sistema comercial en el cual la contraseña se compone de un patrón de cuatro a seis cuadrados en una grilla de cinco por cinco. Con el fin de que el usuario pueda autenticarse, se le exhibe una grilla la cual contiene 25 dígitos decimales aleatorios y se le solicita que registre los dígitos mostrados en el patrón. En una única ronda de observación, se posee el 2.5% de probabilidad de poder identificar el patrón. En caso que se pueda realizar una segunda observación, es posible que se obtenga el mismo resultado.

A partir de nuestro estudio (incompleto) se puede concluir que la seguridad y la usabilidad son dos metas antagónicas. La existencia de métodos más robustos de IA y particularmente la disponibilidad de los solucionadores 3-SAT le permite a un adversario (que no cuente con recursos de gran porte informáticos) solucionar problemas que son poco complejos por causa de la usabilidad. Concluimos que los esquemas que incluyen en su solución aspectos de usabilidad se han demostrado que tienen seguridad limitada y que aquellos que se ha demostrado que son seguros, no poseen las bondades de la usabilidad.

II. EVEN OR ODD

Even or Odd utiliza un sistema de desafíos y respuestas con una interface gráfica para reemplazar el uso de un PIN para desbloquear un dispositivo móvil. Se basa en la capacidad humana para reconocer rostros con facilidad. Solamente un 2.5% de la población sufre de una incapacidad para reconocer rostros, sea por una condición neurológica – la prosopagnosia – o por lesiones cerebrales [2] y no podrían utilizar nuestro sistema.

El usuario debe haber ingresado un conjunto de caras desconocidas y de amigos. El desafío consiste en presentar tres caras por cada fila (Fig. 1) y la respuesta binaria a brindar es: si el número de amigos se encuentra en una fila es par o impar. Cada respuesta va filtrando la información, de forma tal que es muy difícil memorizarlo.

Una variante interesante es solicitarle al usuario que mienta, vale decir, responder a un desafío de forma falsa [7]. En la primera versión de la variante, la mentira se hace en cualquier momento. Ello reduce la resistencia en contra de un adversario

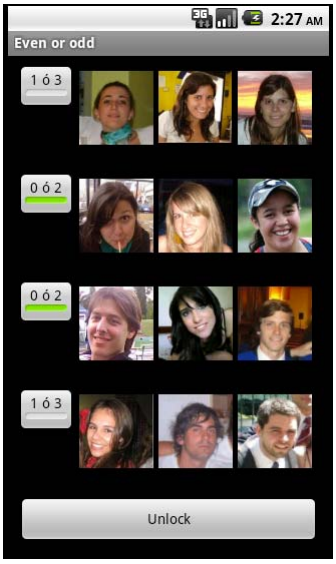

Figura 1. Pantalla de Even or Odd.

que responde a los desafíos aleatoriamente, pero a su vez dificulta el análisis del shoulder-surfer. Desafortunadamente, los experimentos con usuarios han demostrado que los mismos tienen una marcada tendencia a seleccionar al último desafío

como falso y hesitar significativamente antes de ingresar la respuesta. La segunda variante siempre pone la mentira en el mismo lugar, pero eso no soluciona el problema porque los usuarios que observamos hesitaron marcadamente más antes de responder a la mentira y así advirtieron a un adversario el lugar de la mentira.

III. ANÁLISIS DE SEGURIDAD

Asumiremos un adversario que roba el dispositivo y quiere falsamente autenticarse para preparar el dispositivo para venderlo o acceder a la información privada contenida en el dispositivo.

A. *Resistencia a Adivinación*

En primera instancia, calcularemos la probabilidad de autenticarse exitosamente al azar. La probabilidad de elegir "par" depende de la proporción de amigos del conjunto de las fotos como se muestra en la Fig. 2 para un conjunto de 50 fotos. Si "par" es más probable, entonces un adversario optará como mejor estrategia seleccionar siempre "par". Ello nos permite calcular la fórmula de la resistencia de nuestro método. La probabilidad de que ocurra una autenticación exitosa depende de la probabilidad p de "par" y el número de pruebas n

(1) $\text{Prob(Éxito)} = \max(p, 1-p)^n$

La Fig. 2 muestra que en un conjunto de 50 caras, la probabilidad de que la respuesta a un desafío aleatorio sea par es aproximadamente la mitad, para un rango de valores. Para comparar la seguridad de Even-Odd con un pin, medimos la resistencia en número de nueves y obtenemos:

(2) $\text{resistencia} = -n \log_{10}(\max(p, 1-p))$

Un pin de n dígitos puede ser adivinado con una probabilidad de 10^{-n} y tiene por ende una resistencia de n. Por ejemplo, si tenemos 15 amigos en un conjunto de 50 fotos y realizamos 20 pruebas obtenemos como resistencia 5.6561 nueves que es mejor que la resistencia de un PIN de 5 dígitos. Como se muestra Fig. 3 para el caso en que $N = 50$ y se realizan 10 pruebas (fila de caras), la probabilidad de adivinación es relativamente constante 0.001 para un rango de números F de amigos que se encuentra entre las N fotos. Eso corresponde a una resistencia de 3 y al uso de un PIN de tres dígitos.

B. *Resistencia a Peeping*

Even or Odd combate la amenaza del shoulder-surfing. A la gran mayoría de las personas le falta la capacidad mental para reconstruir el conjunto de amigos de las respuestas dadas por un adversario. Pero si se graban las sesiones de autenticación, es posible excluir al conjunto de amigos en cada una de las respuestas. Formalmente, podemos conformar el conjunto $\boldsymbol{F}$ de todos los subconjuntos posibles de "amigos" en un conjunto de N fotos. En cada respuesta se excluye aproximadamente la mitad de los elementos de $\boldsymbol{F}$ como posibles conjuntos de amigos.

Hemos simulado la tarea de un adversario. Para ello representamos a los conjuntos posibles de amigos con cadenas de bits. Simularemos los desafíos aleatorios y excluiremos

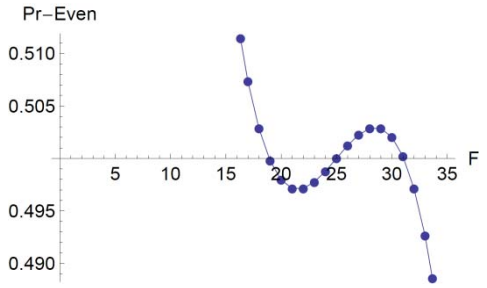

Figura 2. Probabilidad de "par" en dependencia del número F de amigos en un conjunto de 50 fotos.

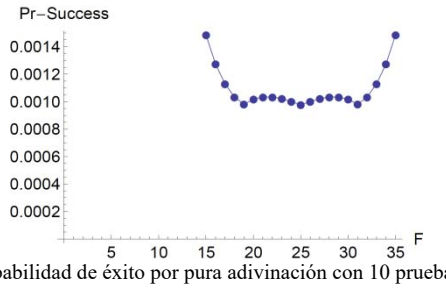

Figura 3. Probabilidad de éxito por pura adivinación con 10 pruebas.

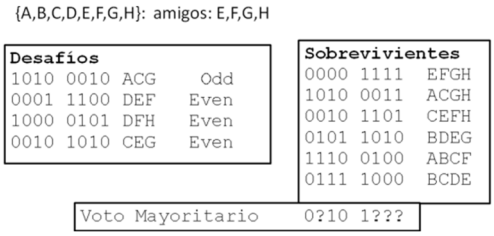

Figura 4. Ejemplo acotado del análisis de Even-ODD.

todas las cadenas de bits que no concuerden con las respuestas de los desafíos. Luego de un cierto número de desafíos-respuestas, se obtiene un conjunto de tamaño reducido de conjuntos posibles de amigos.

C. *Ejemplo*

Dado un conjunto de 8 caras A, B, C, D, E, F, G, y H entre los cuales E, F, G, y H son amigos. Emplearemos cuatro desafíos aleatorios los cuales consisten de ACG, DEF, DFH, y CEG. En Fig. 4 representamos cadenas de bits para representar los desafíos y el conjuntos de amigos. Por ejemplo, ACG corresponde a la cadena (1,0,1,0,0,0,1,0) porque A es el primer elemento, C el tercero y G el penúltimo elemento en el conjunto de caras. La cadena (0,0,0,0,1,1,1,1) representa al conjunto {E,F,G,H}.

D. *Interpretación Matemática de las Respuestas*

Los subconjuntos de un conjunto finito con N elementos $\{a_1, a_2, \ldots a_n\}$ pueden ser representados como cadenas de bits o vectores en el espacio vectorial $\boldsymbol{Z}_2^n$ de dimensión n sobre el cuerpo finito $\{0, 1\}$. Si el conjunto es F, se define un vector $\mathbf{f}$ por la correspondencia

(2) $a_i \in F \Leftrightarrow \mathbf{f}_i = 1$

donde $\mathbf{f}_i$ es la coordenada i del vector $\mathbf{f} \in \boldsymbol{Z}_2^n$. La paridad del número de coordenadas es 1, lo cual representa el producto escalar con el vector (1,1, ..., 1). La conjunción de conjuntos corresponde a la conjunción booleana de los dos vectores. Si $\mathbf{f}$ y $\mathbf{g}$ son dos vectores correspondientes a dos subconjuntos,

entonces el producto escalar $\mathbf{f}\cdot\mathbf{g}$ da la paridad de la conjunción de los dos subconjuntos.

E. *Ejemplo continuado*

Tomando las ${}_8C_4=70$ posibilidades de elegir cuatro amigos entre 8 personas, de ellos sobreviven seis como posibles conjuntos de amigos. En Fig. 4 presentamos un ejemplo empleando cadenas de bits utilizando la descripción más natural por medio del nombre del rostro. En el primer desafío aplicado al último conjunto {BCDE} tiene como intersección {C}, con los amigos es {G}, pero la única información brindada por el usuario es que la intersección consiste de una o tres caras.

El segundo desafío DEF equivale al vector (00011100) $\in \boldsymbol{Z_2^8}$. Para calcular la paridad de la intersección con el conjunto {A, C, D, E} que corresponde al vector (10111000), se calcula el producto escalar

(3) $$(0\ 0\ 0\ 1\ 1\ 1\ 0\ 0)\cdot(1\ 0\ 1\ 1\ 1\ 0\ 0\ 0)=1+1=0$$

para obtener el resultado "par". Un conjunto que cumpla con todos los desafíos de forma exacta si es una solución de la ecuación lineal

(4) $$\begin{pmatrix}1&0&1&0&0&0&1&0\\0&0&0&1&1&1&0&0\\1&0&0&0&0&1&0&1\\0&0&1&0&1&0&1&0\end{pmatrix}\cdot\mathbf{x}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

Como la matriz tiene rango 4, el espacio de soluciones tiene dimensión 4 y por ende 16 elementos. Pero solamente seis de esas 16 soluciones corresponden a subconjuntos de cardinalidad 4.

TABLA I. PROMEDIO Y DESVIACIÓN ESTÁNDAR DEL NÚMERO DE POSIBLES CONJUNTOS DE AMIGOS DESPUÉS DE OBSERVAR LOS RESULTADOS DE UN CIERTO NÚMERO DE PRUEBAS (30 CARAS, 15 (IZQ.) O 12 (DER.) DE ELLAS DE AMIGOS).

Pruebas	Promedio	Desviación Estándar	Promedio	Desviación Estándar
	15 de 30 amigos		12 de 30 amigos	
28	1.71	1.42	2.27	1.89
27	2.20	1.84	2.89	2.23
26	3.67	3.49	3.99	3.03
25	6.26	6.29	5.83	4.38
24	10.81	8.07	9.10	5.76
23	21.37	15.80	16.05	10.83
22	41.10	23.36	28.50	14.36
21	80.07	45.38	52.66	27.02
20	156.52	62.53	97.81	38.50
19	311.68	109.83	188.62	62.42
18	621.86	189.63	364.32	108.43
17	1263.02	389.12	724.89	213.20
16	2458.59	562.55	1389.13	324.34

F. *Interpretación Matemática de las Respuestas (continuada)*

El conjunto que incluye al conjunto de amigos posibles equivale a la solución de un sistema lineal dado por los vectores correspondientes a los desafíos y a las respuestas. En general, si se utiliza un número pequeño de desafíos aleatorios, el rango r del sistema es igual al número de desafíos. Tal sistema lineal tiene 2^{N-r} soluciones, pero solamente una parte de esas soluciones equivale a un subconjunto con la misma cardinalidad que posee el conjunto de amigos. Si tenemos por ejemplo 30 caras en total y entre ellas 15 son amigos, entonces en poco más de 30 desafíos se van a identificar de forma única a los amigos. Un experimento cuyos resultados presentamos en Tabla I muestra el promedio del tamaño del número de conjuntos "amigos" consistente con todas las respuestas. La observación de 28 desafíos brinda en general suficiente información para determinar el conjunto verdadero de "amigos".

G. *Ejemplo continuado*

Si se analizan los conjuntos sobrevivientes, se puede constatar que muchas veces la afiliación de una cara al conjunto de amigos es siempre la misma y por ende el conjunto determina la afiliación de algunas caras. Para verificar si esa observación le provee al adversario capacidades adicionales, es que introduciremos el concepto del conjunto *votado* por el conjunto de sobrevivientes. En el ejemplo de Fig. 4, la cara A está en 2 de los seis conjuntos y el voto de todos es que A no sea la de un amigo. En el caso de B, los últimos tres conjuntos contienen B, pero los primeros tres no. En ese caso, el voto es un empate, indicado por la marca de pregunta.

H. *Peligro de un conjunto de sobrevivientes*

Un adversario que ha observado y analizado un número de desafíos-respuestas insuficientes para la determinación del conjunto de amigos, puede sin embargo utilizar dicha información. Un primer intento es utilizar el conjunto *votado* por los conjuntos sobrevivientes. El cual consiste en el conjunto formado por las caras que estén presentes en la mayoría de los conjuntos sobrevivientes. En general, el número de elementos en el conjunto votado es menor que el número de amigos. El adversario substituye el conjunto votado por el conjunto desconocido de los amigos.

Otra estrategia del adversario para responder los desafíos es utilizar al azar uno de los conjuntos sobrevivientes en lugar del de los amigos para responder a las respuestas. Hicimos una simulación de 1000 conjuntos sobrevivientes y 10000 desafíos adicionales, cuyos resultados presentamos en Tabla II.

Ello nos arroja que la probabilidad de un conjunto arbitrario sobreviviente o el conjunto votado pase una sola prueba (la paridad / imparidad de una sola fila). La razón para obtener poco éxito en el conjunto votado, se produce en el caso en que no se utiliza toda la información posible, debido a que el número de sus elementos puede ser menor al número de amigos conocido. La posibilidad de obtener resultados exitosos es mayor si se realiza mayor cantidad de pruebas que cuenten con la presencia del verdadero conjunto de amigos entre los sobrevivientes. En general, el adversario necesita determinar el conjunto de amigos para dar respuestas adecuadas a los desafíos.

TABLA II. PROBABILIDAD DE SOBREVIVIR UN DESAFÍO ALEATORIO EN EL CONJUNTO DE LOS AMIGOS.

Prueba	Promedio sobreviviente	Promedio votado
24	60.001%	56.354%
23	56.508%	53.709%
22	54.260%	52.021%
20	51.983%	50.644%
18	50.993%	50.055%

I. *Conclusiones*

En un total de n desafíos Even or Odd presenta una probabilidad de 2^{-n} de que un adversario pueda desbloquear

un dispositivo adivinando las respuestas. Con 12 filas (tres rondas en nuestra implementación) posee una resistencia similar a la de un PIN de 3 y 4 dígitos Con la incorporación de una ronda adicional, Even or Odd equivale al uso de un PIN de 4 dígitos.

Si se utilizan en total *N* caras y aproximadamente *N/2* son amigos, el adversario necesita ~ *N* respuestas observadas para determinar el conjunto de amigos. En general, podrá alcanzar cierta determinación del conjunto si le faltan una o dos respuestas, pero esta condición se da únicamente si se conoce el número (pero no la identidad) de amigos. Más aún si el número de posibles conjuntos (los sobrevivientes) es pequeño, la resistencia al desbloqueo permanece alta. Si elegimos 30 caras y utilizamos 16 desafíos aleatorios, tenemos la misma seguridad que un PIN de 4 dígitos. En estas condiciones aún resiste a un adversario que ha filmado una sesión de autenticación. El escenario más probable, es que el adversario no conozca a la víctima.

III. Análisis de Usabilidad

Para analizar la usabilidad, hemos implementado un prototipo Even or Odd en un celular inteligente utilizando Android 1.6 (Fig. 1). En cada pantalla se presentan cuatro filas con tres rostros y además se ha incorporado un botón en el margen izquierdo. En la primera reacción los usuarios constatamos que los botones deberían estar ubicados en el margen derecho. Con el fin de no utilizar términos matemáticos, se decidió cambiar

TABLA III. NÚMERO DE LOS ERRORES COMETIDOS EN DIEZ RONDAS DE PRUEBAS.

Voluntario	Pr. 1	Pr. 2	Pr. 3
1	1	0	1
2	1	0	1
3	2	0	0
4	1	0	1
5	0	1	0
6	2	0	0
7	1	0	1
8	1	0	1
9	1	0	1
10	0	1	0
11	1	0	1
Total	11	2	7

TABLA IV. ACIERTOS EN EL GRUPO DE ADULTOS MAYORES.

Prueba	Aciertos	Tiempo promedio
1	90%	10.1 seg
2	92.7%	10.0 seg
3	94.5%	9.92 seg

la denominación de los botones por los textos "1 ó 3" y "0 ó 2". Luego se realizó un estudio con dos grupos de usuarios. El primer grupo se conformó con once personas que poseían conocimiento en informática. Mientras que en el segundo grupo se seleccionaron quince personas de edad madura y de tercera edad, las cuales son consideradas como usuarios con dificultades en el empleo de dispositivos electrónicos.

Al primer grupo (con competencia en informática) se les solicitó que realizaran tres pruebas con el protocolo que incluye una "mentira". Las pruebas se aplicaron en intervalos de una semana. Cada prueba consistió en diez rondas (Tabla III). Durante el experimento los voluntarios lograron desbloquear el dispositivo superando la probabilidad del 90% en las diez rondas. Cabe destacar que cuatro de los once voluntarios no recordaban el protocolo durante la segunda prueba, apenas un vago recuerdo fue suficiente. En la segunda prueba se observó que los sujetos interactuaron con los dispositivos con relativa facilidad. Durante las entrevistas realizadas a este grupo y las observaciones ejecutadas se extrajo la siguiente información: (1) Más de los 80% de los individuos insertaron una mentira en el mismo lugar y un 70% lo hicieron en el último conjunto. Muchos resolvieron el acertijo y luego marcaron la mentira lo cual sería evidente para que un observador detecte la posición donde se decidió que fuera una mentira. (2) El 70% de los sujetos hubieran preferido que los botones se denominaran "par" e "impar" por considerarles más intuitivos. (3) El 60% de los personas marcaron como incorrecta la ubicación de los botones que contenía la respuesta.

Los individuos sin competencia en informática tenían aproximadamente entre 47 y 60 años a los cuales también se los sometió a tres pruebas. La segunda prueba se aplicó a la semana siguiente de efectuada la primera y la tercera un mes después. A pesar de que solamente el 24.44% de los sujetos lograron desbloquear el dispositivo en cada uno de cinco retos; la mayoría logró el objetivo entre la cuarta y quinta ronda.

Los involucrados en el experimento manifestaron que aproximadamente el 50% no usa o no usaría este tipo de dispositivo. A pesar de ello, todos señalaron que el protocolo es fácil de entender. En cambio aquellos que si lo utilizan o utilizarían dicho dispositivo indicaron que (salvo por una excepción) lo emplearían a diario. La mayor dificultad que debieron enfrentar fue en la manipulación del dispositivo. La mayoría expresó que no cambiaría la aplicación, excepto que se cambie el texto de los botones por "par" e "impar" o que en su defecto se presenten dos botones diferentes.

El tiempo que insumió el desbloqueo fue similar en ambos grupos. Dos de los autores que desarrollaron la aplicación utilizaban la misma en forma diaria, luego de una semana lograron alcanzar un promedio de 4.1 segundos para cada autenticación. Este tiempo sería lo esperado para un usuario que está acostumbrado a utilizar Even or Odd.

TABLA V. CANTIDAD DE DESBLOQUEOS CON CINCO RONDAS Y CINCO RETOS.

Prueba	0	1	2	3	4	5
1	0	2	2	3	5	3
2	0	1	0	6	4	4
3	0	0	1	3	7	4

TABLA VI. TIEMPOS PROMEDIO POR RETO.

Prueba	Promedio
1	11.98 seg
2	9.39 seg
3	10.44 seg

IV. Variantes

El protocolo utiliza la paridad de la intersección que es una propiedad lineal ayudando el análisis de los resultados del shoulder surfing. Es sencillo introducir un cambio en el protocolo para presentar cuatro caras por fila y preguntar si el número de amigos se encuentra entre {0, 1, 4} o entre {2, 3}. Pero para un número razonable de caras (≤ 40), el adversario puede enumerar todos los conjuntos posibles de amigos y eliminar cada una de las respuestas observadas. Con 40 caras, esa tarea le insumiría a una sola computadora alrededor de un día, si extrapolamos el tiempo que insume (en segundos) para 30 caras.

Incorporar "mentiras" es una variación eficaz para mejorar la seguridad contra el shoulder surfing. Desafortunadamente, la naturaleza -básicamente honesta- de los usuarios no permite que su uso sea efectivo. En nuestro experimento, los usuarios casi siempre optaron por seleccionar al último desafío como una "mentira".

V. Conclusión

Hemos presentado Even or Odd, un protocolo que combina el reconocimiento de rostros con la paridad de la intersección de conjuntos. Hemos demostrado que posee resistencia al shoulder surfing ocasional porque se requieren dos o tres sesiones de autorizaciones grabadas para tener una probabilidad razonable de autenticación, como ocurrió en la muestra realizada en nuestro análisis. Hemos investigado e implementado un prototipo "Even or Odd" para demostrar su usabilidad y hemos medido el tiempo para autenticarse. Se estima que el mismo se reduzca con el uso diario. La seguridad que ofrece es suficiente para transformar el dispositivo en inservible, para un ladrón que solamente ha observado una sesión de autenticación. Por lo tanto se elimina en gran parte el incentivo al robo.

References

[1] P. Golle and D. Wagner. Cryptanalysis of a cognitive authentication scheme. In Security and Privacy, 2007. SP'07. IEEE Symposium on, pp. 66-70. 2007.

[2] T. Grüter, M. Grüter, C.C. Carbon: Neural and genetic foundations of face recognition and prosopagnosia. In Journal of Neuropsychology, Vol 2(1), pp. 79-97. 2008

[3] N. Hopper and M. Blum. Secure human identification protocols. Advances in cryptology—ASIACRYPT 2001 (2001): 52-66.

[4] D. Kim, P. Dunphy, P. Briggs, J. Hook, J.W. Nicholson, J. Nicholson, and P. Olivier. Multi-touch authentication on tabletops. In Proceedings of the 28th international conference on Human factors in computing systems (pp. 1093-1102). 2010

[5] S. Li and H.Y. Shum. Secure human-computer identification (interface) systems against peeping attacks: SecHCI. IACR's Cryptology ePrint Archive: Report 268, 2005.

[6] Xiang-Yang Li and Shang-Hua Teng. Practical human-machine identification over insecure channels. Journal of Combinatorial Optimization 3.4 (1999): 347-361.

[7] Z. Li, Q. Sun, Y. Lian, and D.D. Giusto. An association-based graphical password design resistant to shoulder-surfing attack. In Proceedings, Multimedia and Expo, 2005. ICME 2005.

[8] T. Matsumoto. Human-computer cryptography: An attempt. Proceedings of the 3rd ACM conference on Computer and communications security. 1996.

[9] T. Matsumoto and I. Hideki. Human identification through insecure channel. Advances in Cryptology—EUROCRYPT'91. Springer Berlin/Heidelberg, 1991.

[10] V. Roth, K. Richter, and R. Freidinger. "A PIN-entry method resilient against shoulder surfing." Proceedings of the 11th ACM conference on Computer and communications security. 2004.

[11] D. Tan, P. Keyani, and M. Czerwinski. Spy-resistant keyboard. Proceedings of the 17th Australia conference on Computer-Human Interaction. 2005.

[12] C.-H. Wang, T. Hwang, and J.-J. Tsai. On the Matsumoto and Imai's human identification scheme. Advances in Cryptology—EUROCRYPT'95. Springer Berlin/Heidelberg, 1995.

[13] D. Weinshall. Cognitive authentication schemes safe against spyware." Security and Privacy, 2006 IEEE Symposium on. IEEE, 2006.

[14] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces, pp. 177-184. 2006.

Nicolás López received the Engineer's degree in Informatics and Computer Science from the Universidad Católica del Uruguay, Montevideo, in 2011, and is now working in the local software industry.

Matías Rodríguez received the Engineer's degree in Informatics and Computer Science from the Universidad Católica del Uruguay, Montevideo, in 2013, and is now working in project in all of Latin America.

Catalina Fellegi Paccard received the Engineer's degree in Informatics and Computer Science from the Universidad Católica del Uruguay, Montevideo, in 1991 and holds Masters degrees from Universidad Politècnica de Catalunya, Instituto Tecnológico de Buenos Aires and Universidad de Jaén. She is professor at the Universidad Católica del Uruguay.

Darrell D. E. Long (Ph.D, UCSD, 1988) is a fellow of IEEE and the Kumar Malavalli professor of Computer Science at UCSC. He is member of the Center for Research in Storage Systems at UCSC.

Thomas Schwarz, SJ, (Dr. rer. nat. in Mathematics, Fernuniversität Hagen 1984, Ph.D. Computer Sience, UCSD 1994) is professor of Computer Science at the Universidad Centroamericana in El Salvador. His research interests are in storage systems, cyber-security, and databases.