Investigación matemática por combinatoria para conocer el tipo de seguridad más eficiente en un teléfono celular Android 5.1

Joel Alejandro Espinoza Sánchez

Centro de Educación Media

Resumen:

Estás sentado platicando con una compañía que de repente toma tu celular y ella trata de acceder al celular. Al ver que el mismo tiene contraseña procede a preguntarte: "¿Cuál es tu contraseña?" y al negarte te pide una pista: "Es un número de 6 dígitos" y al hacer un comentario espontáneo surge una investigación interesante: "La cantidad de números de 6 dígitos es muy grande.

La seguridad en el celular surge debido a la cantidad de información que éste guarda de nuestras vidas personales y la importancia que tiene para nosotros, tan es así que se han inventado distintos tipos de seguridad para proteger al teléfono celular, sin embargo, alguien no se pone a pensar en el día a día cuál tipo de seguridad le será más eficiente ante alguien que trate de desbloquear este aparato, por lo que en esta investigación he calculado cuál de entre el PIN, Contraseña y Patrón, en un teléfono con sistema operativo Android 5.1 es el más eficiente.

Palabras clave:

Combinatoria, Permutaciones, Seguridad Telefónica, Android 5.1, PIN, Contraseña, Patrón.

Abstract:

You're next to someone talking about nothing important but then suddenly she takes your cell phone and she tries to access to it. After seeing that it has a password, she asks you: "What is your password?" And when you refuse to tell her, she asks you for a clue: "It's a 6-digit number" then she makes a spontaneous comment, and this comment is how an interesting investigation emerges: "The amount of 6-digit numbers is very large". How large can this amount could be?

The security in the cell phone arises due to the amount of information that this saves our personal lives and the importance it has for us, so much so that they have invented different types of security to protect the cell phone, however, someone does not puts to think in the day to day which type of security will be more efficient before someone trying to unlock this device, so in this research I have calculated which of the PIN, Password and Pattern, in a phone with Android operating system 5.1 is the most efficient.

Key words:

Combinatorial, Permutations, Telephone Security, Android 5.1, PIN, Password, Pattern

Introducción:

Hoy en día, la tecnología ha alcanzado avances increíbles permitiendo a que cada vez más personas tengan en su posesión tantísimos dispositivos electrónicos, como computadoras, consolas de videojuegos o celulares. Sin embargo, nadie está exento de que alguien entre a estos aparatos electrónicos y ahora, estos poseen información personal muy valiosa como los correos electrónicos, cuentas de redes sociales, la nube o el mismo almacenamiento del dispositivo que guarda fotos, lugares, la ubicación, a veces hasta cuentas de banco y otra información de alto valor en los mismos dispositivos. Un artefacto que ahora gran parte de la población sobretodo adulta y adolescente pero que ahora ha alcanzado hasta a los infantes es el teléfono celular, el cual es el artefacto que corre más riesgo de ser robado y de tener la mayor cantidad de datos personales y, por consiguiente, robar mucha información de ellos. Es por ello que se han creado diferentes aplicaciones de seguridad que en algunos casos vienen predeterminadas en el mismo dispositivo, pero ¿qué tipo de seguridad de estos aparatos es la más eficaz?

Un teléfono Android común tiene 3 tipos de seguridad preinstalados: Contraseña, PIN y Patrón, con los cuáles es más que suficiente preguntarnos: ¿cuál de las anteriores es la más segura? Para ello tendría que contar de una por una todas las combinaciones posibles de cada tipo de seguridad y concluir algo a partir de este largo proceso, pero afortunadamente, el conteo, concretamente, la combinatoria facilita en una gran medida este trabajo.

Método:

Teórico, en el cual se probará una breve experimentación con cada tipo de seguridad para observar el comportamiento de cada uno en cuanto a posibilidad de combinaciones, repeticiones y arreglos posibles para determinar los arreglos totales de cada tipo de seguridad

Descripción de la Investigación:

PIN

Comenzando por el primer tipo de seguridad, el PIN, consisten en el uso de números del 0 al 9 para hacer una única combinación que dé acceso a la información del teléfono. Observando entonces que, en una primera elección de un número cualquiera, se tiene una posibilidad de 10 elementos diferentes de los cuales se puede escoger en una primera elección, de la misma manera que se puede hacer esto en una segunda elección y así sucesivamente, lo cual causa que se haga una multiplicación entre la cantidad de elementos posibles a elegir la primera vez multiplicado por los de la segunda vez y así sucesivamente, debido a que son eventos que pueden ocurrir simultáneamente, por lo que un arreglo de combinatoria sin restricciones sería la sumatoria de las combinaciones posibles desde que se escoge un elemento hasta que se escogen infinitos, sin embargo, el sistema restringe al usuario a usar un mínimo de cuatro números y un máximo de 16, por lo que esta sumatoria queda de la siguiente manera:

$$\sum_{n=4}^{16}(10^{n})$$

Lo cual proporciona la cantidad de 11,111,111,111,110,000 distintos tipos de combinaciones en el caso del PIN.

Contraseña

Para la contraseña es un caso similar, puesto que las casillas y su comportamiento se mantienen de manera similar, sin embargo, la cantidad de caracteres que se pueden usar son más con un total de 112 diferentes caracteres. Por lo tanto, observándolo como el caso anterior, como su comportamiento es el mismo, pero la cantidad de elementos es diferente, su notación es similar, siendo la siguiente:

$$\sum_{n=4}^{16}(112^{n})$$

Esta operación nos da como resultado que, para la contraseña, el número de combinaciones totales posibles es $6.185622422 \times 10^{32}$. Lo cual es un número increíblemente mayor en comparación al PIN, siendo posiblemente el tipo de seguridad más eficaz entre los tres, pero todavía queda un caso más, que es el más conocido entre los usuarios que hacen uso de la seguridad en los teléfonos celulares y es el patrón.

Patrón

El patrón es un tipo de seguridad muy diferente a los vistos anteriormente, posee 9 puntos distribuidos en la pantalla que se pueden enlazar para formar una figura la cual sea esta la única que desbloqueé al dispositivo. El sistema permite unir como mínimo 4 puntos hasta el máximo que son los 9 puntos, sin embargo, éste trabaja con restricciones que vuelven el conteo de sus combinaciones complicado y lento, por lo que se optó por numerar cada punto como un número de la siguiente manera:

1	2	3
4	5	6
7	8	9

Lo lógico para un conteo de casos del patrón sería la división de diferentes casos, para entonces observar el comportamiento individual cuando se recorre un distinto camino, puesto que es imposible volver a elegir un mismo punto que ya fue elegido debido a restricción del sistema, sin embargo al explorar esta posibilidad, uno se encuentra con que cada caso es muy específico por lo que sería muy lento analizar un aproximado de 630 casos diferentes sólo para cuando se es esperando que cada uno diera aproximadamente 576 arreglos diferentes, ya que así es la manera en la que se acercaría a el número que se espera, pues en un caso ideal, sin restricciones, se esperaría poder seleccionar cualquiera de los 9 puntos, en la segunda elección, cualquiera de los 8 puntos restantes, en la tercera, cualquiera de los 7 puntos que quedan y así sucesivamente, lo cual resulta en un 9!, que es lo mismo que $9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$, sin embargo no es así, pues como se observa, no es posible ir del punto 7 al 1 sin antes haber pasado por el 4 marcado en la figura anterior, de otra manera, sería necesario pasar por el 4, lo que da una combinación imposible, demostrando así que el total de combinaciones que se buscan para el caso en el que se escogen los 9 puntos es menor a 9! Podría decirse por una combinación (la anteriormente demostrada) pero hay muchas combinaciones imposibles debido a este comportamiento de este tipo de seguridad, por lo que fue necesario primeramente encontrar estas restricciones que causan que haya combinaciones imposibles.

Antes de hallar estas restricciones, hay que pensar cada tipo de "dibujo" en el patrón como un arreglo de números en casillas de la siguiente manera:

__ __ __ __ __ __ __ __ __

De modo que la primera casilla represente el primer punto que se selecciona, la segunda casilla sería el punto al que se va directamente después de haber seleccionado este punto y así sucesivamente hasta el final.

Por lo que, hemos observado entonces, que en cualquier casilla que se encuentren, los elementos 7, 1 y 4 en este específico orden no se pueden encontrar, debido a que no es posible llevar a cabo estos arreglos. De esta manera encontramos que todas las restricciones que hacen que haya combinaciones imposibles son:

No es posible ir directamente de	Hasta el punto	Sin antes haber pasar
7	1	4
3	1	2
9	1	5
3	7	5
9	7	8
9	3	6
8	2	5
6	4	5

Hay que tener en cuenta las inversas de cada una, por ejemplo 714 y 174.

Al pensar entonces que estas restricciones vuelven complicado el procedimiento para el conteo de cada caso, se decidió descontar aquellas combinaciones que fueran imposibles sabiendo qué arreglos son imposibles de efectuarse. Haciendo un diagrama de casillas para los casos en los que se quieren escoger los nueve puntos:

								Conteo	Total
71								$1 \times 7!$	5,040
	71							$6 \times 1 \times 6!$	4,320
		71						$6 \times 5 \times 1 \times 5!$	3,600
			71					$6 \times 5 \times 4 \times 1 \times 4!$	2,880
				71				$6 \times 5 \times 4 \times 3 \times 1 \times 3!$	2,160
					71			$6 \times 5 \times 4 \times 3 \times 2 \times 1 \times 2!$	1,440
						71		$6 \times 5 \times 4 \times 3 \times 2 \times 1 \times 1 \times 1$	7,20
									20,160

Sin embargo, se observan diferentes intersecciones al caso, donde una misma combinación se encuentra ya contada dos veces puesto que podríamos directamente restar este número las veces necesarias que tuviéramos alguna restricción, sin embargo, estaríamos contando dos veces las restricciones conjuntas, es decir, hay casos donde puede haber dos o hasta tres restricciones, como por ejemplo el arreglo: 7 1 8 2 9 3 4 5 6 donde tenemos la restricción 714, 825 y 936. Así que es necesario tener en cuenta dichos casos.

Primeramente, observamos que hay casos donde hay una intersección de hasta 3 tríos de elementos imposibles, por lo que habrá que hacer estos y también contar donde hay una intersección de 2 tríos de elementos imposibles. Haciendo primero la intersección de 3 tríos imposibles. Sean 71, 82 y 93 "R" y 4, 5 y 6 "r" donde forzosamente 4 debe ir después de 71, 5 después de 82 y 6 después de 93.

Elección 1	Elección 2	Elección 3	Elección 4	Conteo	Total
R_1	R_1 r_1	R_1 r_1 R_2 r_2	R_1 r_1 R_2 r_2 R_3 r_3	$3 \times 3 \times 2 \times 2 \times 1 \times 1$	36
	R_1 r_1	R_1 r_1 R_2 R3	R_1 r_1 R_2 R_3 r_2 r_3	$3 \times 3 \times 2 \times 1 \times 2 \times 1$	36
	R_1 R_2	R_1 R_2 R_3	R_1 R_2 R_3 r_1 r_2 r_3	$3 \times 2 \times 1 \times 3 \times 2 \times 1$	36
		R_1 R_2 r_1	R_1 R_2 r_1 R_3 r_2 r_3	$3 \times 2 \times 3 \times 1 \times 2 \times 1$	36
			R_1 R_2 r_1 r_2 R_3 r_3	$3 \times 2 \times 3 \times 2 \times 1 \times 1$	36
					180

Por lo tanto, hay 180 combinaciones en los que ocurren tres restricciones posibles en un mismo caso. Esto será necesario para descontar ciertos casos posteriormente. También hay que descontar los casos donde se encuentran dos restricciones en ellos, haciendo un cuadro similar al anterior, señalando nuevamente que las casillas sombreadas en sus respectivos casos son donde no puede ir ninguna "r" en ellos. Lógicamente "r_2" no puede estar antes de "R_2" para que esta restricción sea "imposible". También ocurre lo mismo con intersecciones dobles, lo cual causa otra operación para conocer las mismas muy similar a la anterior:

							Conteo	Total
R_1	R_2						$2 \times 1 \times 5!$	240
R_1		R_2					$2 \times 4 \times 1 \times 4!$	192
R_1			R_2				$2 \times 4 \times 3 \times 1 \times 3!$	144
R_1				R_2			$2 \times 4 \times 3 \times 2 \times 1 \times 2!$	96
R_1					R_2	r_2	$2 \times 4 \times 3 \times 2 \times 1 \times 1 \times 1$	48
	R_1	R_2					$3 \times 2 \times 1 \times 4!$	144
	R_1		R_2				$3 \times 2 \times 3 \times 1 \times 3!$	108
	R_1			R_2			$3 \times 2 \times 3 \times 2 \times 1 \times 2!$	72
	R_1				R_2	r_2	$3 \times 2 \times 3 \times 2 \times 1 \times 1 \times 1$	36
		R_1	R_2				$3 \times 2 \times 2 \times 1 \times 3!$	72
		R_1		R_2			$3 \times 2 \times 2 \times 2 \times 1 \times 2!$	48
		R_1			R_2	r_2	$3 \times 2 \times 2 \times 2 \times 1 \times 1 \times 1$	24
			R_1	R_2	r_1	r_2	$3 \times 2 \times 1 \times 2 \times 1 \times 2 \times 1$	24
			R_1	r_1	R_2	r_2	$3 \times 2 \times 1 \times 2 \times 1 \times 1 \times 1$	12
								1,260

Ahora conociendo estos datos numéricos será necesario tomar en cuenta, como un diagrama de Venn, sabiendo que tenemos ciertos puntos de intersección en los conjuntos, sin embargo, ya conocemos estos valores. Cabe resaltar que hay muchos puntos de intersección: Los elementos de dos puntos de intersección de tres elementos ya están contados en un punto de intersección de dos elementos, por lo que fueron descontados. Asimismo, cuatro puntos de intersección de dos elementos, contando los elementos del punto de intersección de tres elementos ya están contados en las 20,160 combinaciones que se originan de un caso individual.

Es entonces que hemos obtenido la cantidad de 107,280 casos imposibles totales para cuando se escogen 9 puntos en el patrón. Lo siguiente será restar a 9! este número multiplicado por dos, ya que sólo estamos contando así los casos de restricciones verticales, pero también están los casos horizontales (132 por ejemplo) y a su vez, cuatro veces el número 20,160, esto debido a que también hay que contar los casos diagonales (195, 915, 375 y 735). Para obtener de esta manera los casos que si se pueden hacer:

$$9! - [(2 \times 107280) + (4 \times 20160)] = 67680$$

Así conocemos que la cantidad de combinaciones posibles para hacer un patrón con los nueve puntos es de 67,680 posibilidades. Para el caso en el que se escogen ocho puntos de los nueve totales el número de posibilidades será 67,680 también. Esto es porque el principio de 9! = ${}_9P_8$ puesto que tomar o no este último punto propicia a mantener las características y posibilidades de manera igualitaria al caso en el que si se tomara este último punto.

Repitiendo este procedimiento, pero tomando en cuenta las diferentes elecciones que se tienen ante cada caso se realizaron obteniendo los siguientes resultados:

Caso: Escoger 7 puntos

$$\left[\frac{9!}{(9-7)!}\right] - [(2 \times 51000) + (4 \times 9720)] = 40560$$

Caso: Escoger 6 puntos

$$\left[\frac{9!}{(9-6)!}\right] - [(2 \times 16248) + (4 \times 3000)] = 15984$$

Caso: Escoger 5 puntos

$$\left[\frac{9!}{(9-5)!}\right] - [(2 \times 3672) + (4 \times 660)] = 5136$$

Caso: Escoger 4 puntos

$$\left[\frac{9!}{(9-4)!}\right] - [(2 \times 624) + (4 \times 108)] = 1344$$

Finalmente, con todos estos números obtenidos de cada suma de cada caso, se concluye con la suma de los seis casos para así obtener el número total y definitivo:

$$67680 + 67680 + 40560 + 15984 + 5136 + 1344 = 198384$$

Por lo que concluimos que el número total de posibilidades en el patrón son 198,384 combinaciones.

Conclusión:

Con los números obtenidos podemos concluir que la seguridad más eficiente para un teléfono celular es la contraseña, pues tiene quintillones de diferentes posibilidades, haciendo que se vuelva más difícil tratar de descifrar una combinación de este tipo de seguridad.

Con el uso de las contraseñas, desde lo cotidiano, como la importancia de tener en cuenta la seguridad del teléfono celular, pues es ahora donde gran parte de la vida personal es almacenada, por lo que a veces tener en cuenta algunos números ayuda al conocimiento humano personal y así poder inclinarse a un sistema de contraseñas que le propicie al usuario mayor seguridad si éste siente que la necesita, hasta lo matemático, donde por este tema que parece cotidiano y sencillo se puede aprender una gran cantidad de cosas de combinatoria, como el hecho y la importancia de la interpretación de la combinatoria, el conteo, e incluso observar a veces las facilidades que la combinatoria puede ofrecerle a una persona para evitar hacer un conteo largo, pues no es eficiente hacer un conteo por cada tipo diferente de combinación que puede hacerse, por ejemplo en el PIN.

Agradecimientos:

Agradezco enormemente al Ingeniero Bioquímico Edgar Ahmed Muñoz Guzmán por la ayuda en la verificación de procedimientos en esta investigación, así como el seguimiento continuo y arduo que se llevó a cabo en el mismo. De la misma manera, agradezco infinitamente al Ingeniero Mecánico Electricista José Luis Espinoza González por la ayuda que me brindó en el tramo completo que tuvo que recorrerse mientras se llevaba a cabo esta investigación, así como en cada tropiezo ante cada obstáculo que me encontraba para realizar un determinado cálculo.