Descubrimiento automatizado de patrones de acceso en dispositivos móviles Android

Leopoldo Sebastián Gómez [1, 2]

[1] Poder Judicial de Neuquén
sebastian.gomez@jusneuquen.gov.ar
[2] Universidad Nacional de Río Negro
sgomez@unrn.edu.ar

Resumen. La protección de dispositivos móviles Android mediante un patrón de acceso plantea dificultades para la extracción y análisis de evidencia digital. Las aplicaciones disponibles para tareas de informática forense ofrecen prestaciones limitadas cuando el dispositivo móvil se encuentra bloqueado con este mecanismo de seguridad. A diferencia del sistema operativo iOS, la protección de un dispositivo móvil Android mediante patrón de acceso mantiene un tiempo constante de penalidad en caso de que se efectúen intentos fallidos y en muchos casos no exige el ingreso de un segundo factor de autenticación. La implementación de una solución de bajo costo utilizando el hardware Arduino Leonardo ha permitido realizar una automatización del proceso de descubrimiento de patrones de acceso desconocidos en dispositivos móviles con sistema operativo Android. El software combina técnicas de ataque por diccionario y por fuerza bruta, procurando el acceso al dispositivo en tiempos que resultan aceptables para la investigación penal. El código desarrollado permite que sea adaptado mediante parámetros para su aplicación sobre dispositivos móviles que estén bloqueados a través de la protección por patrón de acceso ofrecida por el sistema operativo Android.

1 Métodos de protección de dispositivos móviles Android

El sistema operativo Android utiliza principalmente tres mecanismos de seguridad para dispositivos móviles: el bloqueo del bootloader, el encriptado y la protección mediante un código de acceso.

El bootloader es el código que se ejecuta al encender un dispositivo móvil y se encarga de seleccionar la partición de inicio que contiene la imagen del sistema operativo o bien la de recuperación. Asimismo, es responsable de establecer una conexión y la ejecución de comandos en modo fastboot. Este código puede chequear la integridad del siguiente código ejecutable del sistema operativo -el kernel- y si falla la verificación, el proceso de inicio queda trunco. Si el código del bootloader está bloqueado los usuarios no pueden modificar las particiones del sistema ni tampoco iniciar el dispositivo móvil con una imagen modificada del sistema operativo -conocidos como custom recovery- vía comandos fastboot o intentar algún bypass de los chequeos de seguridad habilitados por el fabricante. Generalmente el desbloqueo del bootloader destruye las claves criptográficas que son usadas para desencriptar la partición de datos, por ello ésta no es una opción válida para la extracción de

evidencia digital. Aún si fuera viable el desbloqueo del bootloader, la protección adicional conocida como FRP (Factory Reset Protection) incluída a partir de Android 5.1 impide la posibilidad de iniciar el teléfono con una imagen modificada del sistema operativo.

El encriptado de los datos en los dispositivos móviles Android, conocido como FDE (Full Disk Encryption), ha pasado a ser obligatorio a partir de la versión 7 y no existe forma de ser desactivado por el usuario. Si el usuario no utiliza una protección de acceso por PIN, el sistema operativo mantiene una clave por defecto y se calcula a partir de ella un hash criptográfico que queda almacenado sobre el hardware del dispositivo móvil en un entorno de ejecución confiable y seguro, conocido como TEE (Trusted Execution Environment). Aún logrando extraer una imagen forense del dispositivo móvil, ésta no podría ser descifrada ya que el módulo TEE no expone el dato requerido para el cálculo de la clave de descifrado. Existen técnicas para acceder a los datos de dispositivos móviles si ellos utilizan un chipset específico (v.gr. Qalcomm) en su circuitería. Qualcomm admite un modo de acceso abierto llamado EDL (Emergency DownLoad mode), el que permite mapear el almacenamiento de un dispositivo Android al conectarlo a una computadora, por lo que eventualmente se facilita la realización de una imagen forense. Aunque estas técnicas puedan ser aplicadas en algunos modelos de dispositivos móviles, a partir de la versión 7 el sistema operativo Android utiliza encriptado automático y obligatorio en la partición de datos del usuario. La clave de encriptado es almacenada en el dispositivo pero también se mantiene cifrada, restringiendo en muchos casos las posibilidades de efectuar una imagen forense que pueda a posteriori ser accedida para el análisis de los contenidos digitales.

Finalmente, es viable utilizar algún método de protección mediante un código de acceso (PIN, patrón de acceso, contraseña, huella dactilar o algún otro dato biométrico). En caso de que un usuario haga uso de este mecanismo de seguridad, la partición de datos de usuario no estará disponible y el dispositivo móvil no iniciará hasta que se ingrese correctamente la clave de acceso.

2 Protección por patrón de acceso

En el año 2008 Google introdujo en el mercado un nuevo sistema de protección de dispositivos móviles mediante patrones de acceso, conocido como ALP (Android Lock Pattern) en conjunto con el lanzamiento del sistema operativo Android. Se trata de un método de autenticación en el que se presentan nueve puntos en la pantalla táctil del dispositivo, los que están dispuestos en forma de cuadrícula de 3x3, de forma similar al juego de mesa Tres en Línea o Tic-Tac-Toe. El método para otorgar el acceso al sistema operativo consiste en interconectar un subconjunto de de estos puntos, cuyo patrón es definido previamente por el usuario.

La especificación de Google indica que un patrón de acceso debe respetar las siguientes reglas:

R1: Un patrón de acceso debe conectar como mínimo cuatro puntos.

R2: Un punto solamente puede ser conectado una sola vez, lo que implica que un patrón de acceso no puede conectar más de nueve puntos.

R3: Un patrón de acceso siempre conectará al primer punto no conectado en su camino y luego podría conectar otros puntos restantes.

R4: Un patrón de acceso puede pasar a través de un punto previamente conectado para poder alcanzar otros puntos sin conexión.

Es importante tener presente que el número de combinaciones posibles aumenta en forma exponencial con la longitud del patrón de acceso, en forma similar a lo que ocurre con la protección de acceso mediante contraseñas.

Longitud del patrón de acceso	**Combinaciones posibles**
4	1624
5	7152
6	26016
7	72912
8	140704
9	140704

Tabla 1. Combinaciones de patrones de acceso

Debido a la complejidad de las restricciones entre puntos de contacto intermedios este resultado es calculado mediante métodos de fuerza bruta. El mínimo de ALPs que pueden conectarse son cuatro nodos y el máximo son nueve, totalizando 389.112 combinaciones posibles [Aviv et al., 2010].

Las personas tienen comportamientos predecibles y ello ha sido demostrado en diversos trabajos de investigación. Løge analizó que el 44% de los patrones de acceso utilizado por los usuarios parten del nodo superior-izquierdo y que un 77% de los usuarios inician el patrón de acceso en alguno de los cuatro nodos que conforman los bordes del cuadrado. Estadísticamente el número promedio de nodos interconectados en un patrón de acceso asciende a cinco nodos, lo que permite aseverar considerando todas las combinaciones de 4 y 5 nodos, que existen menos de 9000 combinaciones que deben ser intentadas para descubrir el patrón de acceso válido [Løge, 2015].

En la elección del patrón de acceso el usuario debe hacer un balance entre seguridad y usabilidad. Los modelos de Markov se basan en la premisa de que en una cadena de texto, o bien los nodos que conforman un patrón de acceso para el tema en cuestión, los elementos que conforman la secuencia no son elegidos por las personas en forma independiente y aislada sino que tienen alguna vinculación y por ello puede establecerse un modelo estocástico que permita explicar este fenómeno a partir de observaciones previas. Se han publicado estudios [Løge et al., 2016], [Aviv and Kuber, 2018] que han utilizado cadenas de Markov para determinar la fortaleza del patrón de acceso y se ha aplicado este modelo estadístico para identificar los patrones de acceso más frecuentemente utilizados por los usuarios [Cha et al., 2017], [Cho et al., 2017]. En este mismo sentido se han desarrollado métodos para medir la fortaleza de los patrones de acceso mediante fórmulas y estimadores estadísticos como el cálculo de la entropía [Uellenbeck et al., 2013], así como también se ha elaborado un

ranking de ALPs considerando la complejidad visual de cada uno de ellos [Sun et al, 2014].

Otras líneas de investigación [Ye et al., 2017] se orientan a estudiar la posibilidad de descubrir el patrón de acceso a través del análisis de la marca aceitosa -smudge- que queda en la pantalla táctil, mediante la utilización de imágenes digitales tomadas con cámaras DSLR en conjunto con fuentes de luz omnidireccionales orientadas hacia la pantalla táctil. También se han realizado experimentos con cámaras termales que intentan capturar la traza de calor. Se han realizado experimentos exitosos para el descifrado de ALPs realizando un primer examen de la pantalla del dispositivo móvil mediante una cámara digital y un microscopio. Esta técnica ha permitido detectar el nodo de inicio, el nodo final o secuencias parciales del patrón de acceso [Andriotis et al., 2017].

3 Escenario de aplicación del descubrimiento automatizado de patrones de acceso

Una de las primeras técnicas utilizadas en informática forense para realizar una extracción de datos desde dispositivos móviles protegidos con patrón de acceso se apoyaba en la utilización del entorno de desarrollo de Android SDK para poder hacer uso del comando ADB en caso de que estuviese habilitada esta característica a priori en el dispositivo y se contara con privilegios de root, o bien mediante alguna aplicación para gestión de archivos instalada desde la memoria externa o vía USB, con el objeto de modificar o eliminar el archivo gesture.key utilizado para validar el patrón de acceso. Una vez que se lograba el acceso al dispositivo móvil se continuaba con la utilización de las técnicas y herramientas de informática forense usuales para la extracción de datos. Este método de desbloqueo no es viable en las versiones actuales de Android, ya que el archivo que contiene codificado el patrón de acceso se encuentra en una partición gestionada en forma exclusiva por el sistema operativo y no es posible extraerlo o modificarlo si no se cuenta con alguna técnica especial para traspasar esta protección.

Alternativamente se ha podido efectuar la extracción de datos mediante la generación de una copia de respaldo completo del sistema de archivos - conocida como NANDroid backup- pero para ello el bootloader debe estar desbloqueado y se requiere instalar una custom recovery -CWM o TWRP-, o bien si el dispositivo está rooteado es viable lograr el mismo resultado mediante la instalación del paquete BusyBox y alguna aplicación que realice copias de seguridad NANDroid, siempre que el dispositivo no esté bloqueado para acceso.

Las técnicas de chip-off, métodos JTAG o métodos similares no ofrecen alternativas para la extracción de datos ya que los nuevos dispositivos móviles utilizan el cifrado de datos en forma permanente. Como corolario, la multiplicidad de métodos de protección utilizadas en los dispositivos móviles generan una alta dependencia de las herramientas comerciales de informática forense para el logro de una extracción física de datos.

A la fecha unas pocas herramientas comerciales son capaces de abordar el problema del desbloqueo de un dispositivo móvil mediante el descubrimiento del

patrón de acceso por métodos de fuerza bruta o ataque por diccionario. XPINClip[1] es un hardware forense que permite el descubrimiento de protecciones de acceso (v.gr. PIN, patrón de acceso o contraseña), posibilitando ataques por fuerza bruta y búsquedas por rango. Esta herramienta posibilita el desbloqueo de varios modelos de iPhone y iPad, así como también actúa sobre dispositivos con sistema operativo Android. El hardware posee un sensor de luz para detener el procedimiento de desbloqueo una vez que se detecta un cambio en la pantalla del dispositivo móvil. El kit ofrece cables OTG con opción de carga simultánea para lograr que el equipo permanezca encendido mientas se efectúa el procedimiento. De manera similar, la herramienta comercial SvStrike[2] posibilita el desbloqueo de dispositivos móviles protegidos por PIN, patrón de acceso o contraseña. Se trata de un software que se vale de la capacidad de conexión USB Host ofrecida por los sistemas operativos Android e iOS, y permite a través de un cable OTG realizar el desbloqueo del dispositivo móvil. Esta herramienta ofrece algunas funcionalidades adicionales, como la configuración de un email para el envío del PIN o el patrón de acceso descubierto una vez que finaliza la búsqueda. Burner Breaker[3] es un hardware forense que permite la ejecución de pulsaciones y desplazamientos del puntero sobre la pantalla del dispositivo móvil mediante un brazo robótico. Esta herramienta brinda una la solución adecuada para aquellos dispositivos móviles cuyo sistema operativo no admite el método de conexión vía USB Host.

En caso de no contar con herramientas comerciales de informática forense que permitan realizar una extracción física de los datos almacenados un el dispositivo móvil Android bloqueado por patrón de acceso, la técnica de descubrimiento automatizado de patrones de acceso mediante el hardware Arduino puede ser aplicable bajo las siguiente premisas: a) El dispositivo móvil se encuentra bloqueado por patrón de acceso; b) El bootloader está bloqueado y no es viable cargar una custom recovery; c) El dispositivo móvil no está habilitado para la ejecución de comandos ADB; d) El sistema operativo Android admite la conexión con cable OTG; e) El sistema operativo Android mantiene un tiempo de penalidad constante para intentos fallidos y no elimina datos del usuario al llegar a un máximo de intentos erróneos.

[1] XPinClip es una solución forense de ataque por fuerza bruta (Accesible en: http://xpinclip.com/).

[2] SvStrike es un kit forense para descubrimiento de PIN, patrones de acceso y contraseñas (Accesible en: https://www.secureview.us/sv_strike.html).

[3] Burner Breaker es un hardware que permite mimetizar los movimientos de una mano posibilitando el ingreso automatizado de patrones de acceso, PIN o contraseñas sobre dispositivos móviles (Accesible en: https://www.secureview.us/burner_breaker.html).

4 Experimentación y resultados

Se desarrolló una solución de automatización denominada ALPFinder[4], la que ha quedado disponible en GitHub para su descarga. Para la implementación de la herramienta de informática forense se utilizó el hardware Arduino[5]. Se optó por el modelo Arduino Leonardo ya que cuenta con una entrada USB integrada en la placa y ello facilita la interconexión con dispositivos móviles a través de un cable OTG. En el desarrollo del código se incorporó un método de ataque por diccionario considerando los resultados obtenidos en diferentes trabajos de investigación, los que han determinado los patrones de acceso más frecuentemente utilizados por los usuarios de dispositivos móviles y otros estudios sobre fortaleza de ALPs [Cha et al, 2017]. Asimismo, el software desarrollado realiza un ataque por fuerza bruta sobre el dispositivo móvil bloqueado por ALP, conectando patrones de cuatro a nueve puntos. Se efectuaron pruebas de concepto con diferentes dispositivos móviles obteniendo resultados satisfactorios (cfr. Figura 1).

Figura 1. Pruebas de concepto sobre dispositivos móviles Android

Una vez finalizadas las pruebas de concepto sobre los dispositivos móviles Android utilizados para la experimentación, la placa Arduino Leonardo fue conectada a una computadora a través del puerto USB para validar su funcionamiento sobre máquinas virtuales de dispositivos móviles con versiones recientes de Android (v.gr.

[4] ALPFinder es el software desarrollado para el descubrimiento de patrones de acceso en dispositivos móviles Android, pudiendo ser integrado con el hardware Arduino Leonardo (Accesible en: https://github.com/lpinqn/alpfinder).

[5] Arduino es una plataforma de código abierto diseñada para una integración simple entre hardware y software (Accesible en: https://www.arduino.cc/).

Samsung Galaxy S8 con sistema operativo Android 7) utilizando el software Genymotion[6] (cfr. Figura 2).

Figura 2. Pruebas de concepto sobre máquinas virtuales de dispositivos móviles Android

Si bien para cada dispositivo móvil Android que deba ser desbloqueado en primer lugar se debe ajustar el código fuente mediante parámetros específicos, el procedimiento no es complejo para un profesional informático. Considerando las limitaciones de Arduino, para el calibrado de la herramienta se requiere hacer cambios mínimos en el código fuente, recompilarlo y cargar el código ejecutable en la memoria integrada de este hardware, realizando estos pasos en forma repetida hasta que se logre el posicionamiento y desplazamiento del puntero sobre los nueve puntos desplegados en la pantalla del dispositivo móvil para el ingreso de ALPs.

Se efectuaron pruebas de rendimiento sobre el código implementado en Arduino a fin de obtener las cotas máximas de demora para el desbloqueo de un dispositivo

[6] Genymotion es un emulador de dispositivos Android mediante máquinas virtuales (Accesible en: https://www.genymotion.com/).

móvil. Se ha definido un tiempo de espera de dos segundos para que el puntero realice los movimientos de un patrón y se ha contemplado una penalidad de treinta segundos cada cinco intentos fallidos. A diferencia del sistema operativo iOS, Android no incrementa la penalidad del tiempo de espera al aumentar el número de intentos fallidos. En sus versiones más recientes Android impone una penalidad de 30 segundos para cada patrón de acceso inválido. El tiempo estimado para hacer intentos de desbloqueo del patrón de acceso en dispositivos móviles Android resulta aceptable dentro de los plazos que usualmente se prevén para la investigación en los nuevos códigos procesales penales (cfr. Figura 3).

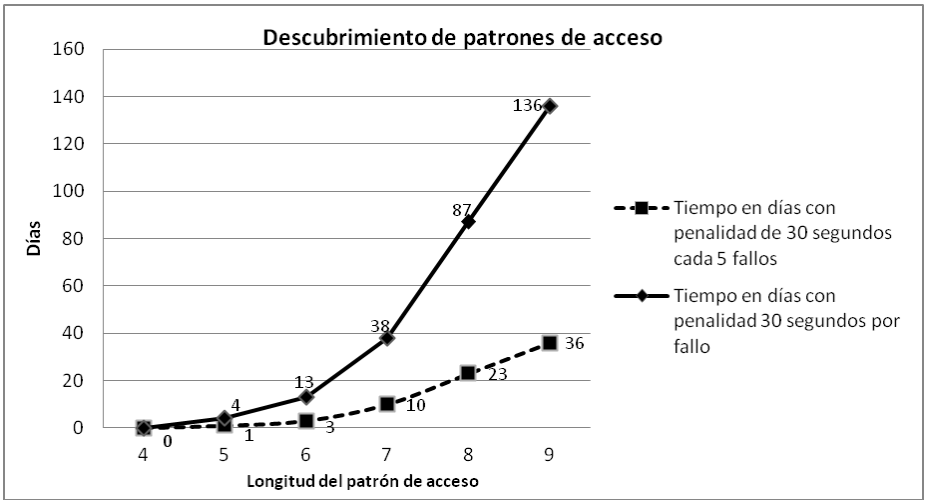

Figura 1. Tiempo máximo para el descubrimiento de un patrón de acceso incluyendo intentos con ALPs de menor longitud

5 Limitaciones

Las medidas de seguridad evolucionan constantemente y los fabricantes de dispositivos móviles ofrecen métodos de control de acceso más sofisticados. Sin perjuicio del avance en materia de métodos de protección de acceso mediante datos biométricos, actualmente existe una importante cantidad de usuarios de dispositivos móviles que hace uso del método de protección por patrón de acceso. La aplicación de la técnica descripta requiere que el sistema operativo Android admita la modalidad de conexión USB Host.

Si bien la implementación desarrollada ha funcionado correctamente en dispositivos móviles Android que actualmente están vigentes en el mercado, la técnica de descubrimiento automatizado de patrones de acceso no puede ser aplicada para casos en que el sistema operativo limite el número de intentos fallidos a un número fijo de oportunidades para luego realizar un reinicio a valores de fábrica del dispositivo eliminando en forma permanente los datos del usuario o bien si luego de un número limitado de accesos inválidos por ALP se solicita el ingreso de usuario y contraseña de Gmail para el desbloqueo.

La autonomía de las baterías de los dispositivos móviles es una limitante a la hora de aplicar la técnica de desbloqueo del patrón de acceso ya que requiere que el equipo se mantenga encendido. Dentro de las alternativas para mitigar este problema se realizaron pruebas de concepto con cables OTG. Aunque la mayoría de ellos no admiten ser utilizados para carga y operación en forma simultánea, se han reportado casos puntuales de OTG modificados que permiten esta doble función en paralelo, pero sólo es viable su aplicación para modelos específicos de dispositivos móviles. Durante la experimentación efectuada se ha comprobado que es posible mantener la carga de los dispositivos móviles mediante la aplicación directa de una fuente de energía externa sobre los bornes que conectan con la batería. Para los dispositivos móviles que no cuenten con batería desmontable el procedimiento resulta más laborioso ya que es necesario desarmar el equipo. Una alternativa técnicamente viable para estos casos consiste en alternar ciclos de descubrimiento automatizado y de carga del dispositivo móvil, ajustando los parámetros que definen el rango de búsqueda en el código fuente para luego continuar con el ataque por fuerza bruta desde el último patrón de acceso que fue intentado antes de efectuar la recarga de la batería.

Aunque no es estrictamente requerido, el sistema implementado no tiene incorporado un sensor para detectar un cambio de luz en la pantalla del dispositivo móvil que permita detener la búsqueda del patrón de acceso. Aunque esta limitante no permite conocer en concreto el ALP descubierto, ello no impide que una vez que esté desbloqueado el dispositivo móvil se pueda realizar una extracción de datos con otras herramientas de informática forense. Una posible variante para conocer la secuencia consiste en complementar el hardware con una cámara externa y software de grabación para identificar a posteriori el patrón de acceso válido.

6 Conclusiones

La era dorada de la informática forense sobre dispositivos móviles ha finalizado y el panorama se vuelve cada vez más desafiante. En dispositivos móviles Android, la configuración de un patrón de acceso es un método frecuentemente utilizado por los usuarios para la protección de datos personales. Se ha presentado una solución tecnológica de bajo costo mediante Arduino Leonardo que realiza una automatización para el descubrimiento de patrones de acceso desconocidos en dispositivos móviles Android a través de un cable OTG, posibilitando que el hardware se comporte como un periférico de entrada de datos y realice movimientos del puntero sobre la pantalla en forma autónoma.

La herramienta de informática forense desarrollada propone una alternativa para escenarios complejos en los que las herramientas líderes del mercado no brindan posibilidad de extracción de datos, siempre que el sistema operativo Android admita una conexión OTG, mantenga una tasa de penalidad constante para accesos fallidos mediante patrones de acceso y no se efectúe el borrado permanente de los datos del usuario luego de una cantidad predeterminada de intentos erróneos. Para el descubrimiento de un patrón de acceso desconocido la automatización combina un ataque por diccionario y por fuerza bruta. Los resultados de la experimentación con casos reales y sobre configuraciones de dispositivos móviles Android ejecutadas en

entornos virtuales para pruebas han sido satisfactorios. Los estudios actuales sobre la fortaleza de los patrones de acceso utilizados por los usuarios han determinado que la longitud promedio es de cinco nodos. Considerando todas las posibles combinaciones de ALPs en la búsqueda por fuerza bruta, el tiempo que se requiere para el descubrimiento de un patrón de acceso mediante la automatización implementada sobre Arduino hace técnicamente posible la solución propuesta y adecuada a los plazos que usualmente son establecidos para la investigación penal en los códigos procesales actuales.

Referencias

Andriotis, P., Tryfonas, T., Oikonomou, G. and Yildiz, C. (2013), "A pilot study on the security of pattern screen-lock methods and soft side channel attacks". In: Buttyan, L., Sadeghi, A.-R. and Gruteser, M., eds. (2013) *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Network*s. ACM, pp. 1-6.

Aviv, A., Gibson, K., Mossop (2010), E., Blaze, M. and Smith, J., "Smudge Attacks on Smartphone Touch Screens". *4th Workshop on Offensive Technologies. Washington*, DC: [s.n.].

Aviv, A. and Kuber, R. (2018), "Towards Understanding Connections between Security/Privacy Attitudes and Unlock Authentication" *Article to appear at the Workshop on Usable Security (USEC)*, Feb. 2018.

Cha,S., Kwag, S., Kim, H. and Huh, J. (2017), "Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks" In: ASIA CCS '17 Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Pages 313-326.

Cho, G., Huh, J., Cho, J., Oh, S., Song, Y., and Kim, H. (2017), "SysPal: System-Guided Pattern Locks for Android", In: I*EEE Symposium on Security and Privacy (SP)*, pp. 338-35, 2017.

Løge, M. (2015), "Tell Me Who You Are and I Will Tell You Your Unlock Pattern". Master of Science in Computer Science. Supervisor: Lillian Røstad, IDI. Department of Computer and Information Science. Submission date: July 2015. Norwegian University of Science and Technology

Løge, M., Duermuth, M. and Rostad, L. (2016), "On User Choice for Android Unlock Patterns", In: *1st European Workshop on Usable Security*.

Sun,C., Wang, Y. and Zheng, J. (2014), "Dissecting pattern unlock: The effect of pattern strength meter on pattern selection", *Journal of Information Security and Applications*, Volume 19, Issues 4-5, November 2014, pp-308-320.

Uellenbeck, S., Dürmuth, M., Wolf, C. and Holz, T. (2013), "Quantifying the security of graphical passwords: the case of android unlock patterns". In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (CCS '13). ACM, New York, NY, USA, 161-172. DOI: http://dx.doi.org/10.1145/2508859.2516700

Ye, G., Tang, Z., Fang, D., Chen, X., Kim, K., Taylor, B. and Wang, Z. (2017), "Cracking Android pattern lock in five attempts". In: *The Network and Distributed System Security Symposium 2017* (NDSS'17).