POLÍTICA DE PRIVACIDAD

La aplicación *AMon* recopila información de su dispositivo Android para la realización del Proyecto de investigación MDSM (*Mobile device Dynamic Security Management*) que tiene por objeto garantizar la seguridad de las redes y sistemas de información dentro en ámbitos públicos institucionales como la Universidad de Granada.

RESPONSABLE DEL TRATAMIENTO:
Pedro García Teodoro
Dpto. Teoría de la Señal, Telemática y Comunicaciones
ETS Ing. Informática y de Telecomunicación
Universidad de Granada

FINALIDAD:
Investigación sobre seguridad de las redes de información y comunicaciones y sobre el uso de dispositivos móviles. Los fines del tratamiento son legítimos, proporcionales y necesarios para la consecución de los objetivos de la investigación y conformes a derecho.

La seguridad en redes y sistemas de información y comunicación constituye una prioridad para las instituciones, los ciudadanos y la sociedad en su conjunto. Ello requiere medidas de prevención, corrección, resiliencia y respuesta frente a incidentes, riesgos y amenazas. Esa necesidad es, incluso, mayor en entornos y redes institucionales o corporativos cuando el usuario necesariamente ha de estar conectado y la seguridad depende no solo, ni principalmente, de su propio comportamiento sino, sobre todo, de la seguridad global del entorno o red en la que opera.

Los sistemas de redes y comunicaciones resultan extraordinariamente complejos por el número y la diversidad de dispositivos, particularmente, en redes institucionales o corporativas donde coexisten percepciones y conductas múltiples y heterogéneas en el uso de ese entorno común.

La seguridad de las redes se sustenta esencialmente en la monitorización y supervisión del entorno. Con esa finalidad, el Proyecto de Investigación MDSM (*Mobile Device Dynamic Security Management*) se explica sobre la base de dos ideas básicas:

1) La red debe conocer el nivel de seguridad del dispositivo y su uso de cara a la provisión de acceso a servicios y recursos. Por ello se realiza un perfil de seguridad para el dispositivo y su uso basado en ciertos atributos de seguridad derivados de su configuración y operación en el tiempo.

2) El perfil de seguridad del dispositivo se monitoriza a lo largo del tiempo, tanto al inicio de la comunicación como durante la misma. El acceso estará condicionado al cumplimiento de las condiciones de seguridad y se renovará periódicamente en base al

nivel de seguridad mantenido a lo largo del tiempo. En caso de determinarse la existencia de algún riesgo de seguridad, el sistema podrá notificarlo al dispositivo con objeto de proceder a la solución del problema de seguridad en cuestión. En caso de no resolverse, el acceso podrá ser restringido o, incluso, denegado por razones de seguridad de la red y del propio dispositivo.

La red de operación será la de la Universidad de Granada (UGR) a la que los dispositivos móviles se conectarán a través de la infraestructura Eduroam. El objetivo es implementar los mecanismos de control para el tráfico de los dispositivos que pretende desarrollar el Proyecto MDSM. El sistema de autenticación de la red permitirá determinar los momentos temporales en los que se realiza la autenticación de un usuario, identificando sus direcciones MAC e IP y permitiendo contar con un listado de accesos a la red identificando el tiempo de acceso y las direcciones MAC e IP asignadas. El listado de conexiones permitirá evaluar la evolución temporal de las conexiones y configurar patrones de comportamiento de los diferentes dispositivos.

La información sobre el usuario concreto que está accediendo queda oculta en este proceso para garantizar el anonimato. En este intercambio de información se anonimiza también la dirección del dispositivo.

LEGITIMACIÓN:
El consentimiento del usuario que se manifiesta al descargar la aplicación es la base jurídica para el tratamiento realizado con fines de investigación científica en el marco del Proyecto MDSM.

DESTINATARIOS:
La gestión de los datos se realizará fundamentalmente en el contexto del Proyecto MDSM. En todo caso, cuando este finalice, y a fin de permitir nuevas propuestas y avances en el campo de la mejora de la seguridad, se podrá disponer la base de datos (con las convenientes medidas de anonimato y protección) para el uso exclusivo de la comunidad científica.

DERECHOS:
Los usuarios de la aplicación tienen garantizados los derechos reconocidos en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018 de Protección de Datos y Derechos Digitales respecto de los datos personales:

- Derecho a solicitar el acceso a los datos personales
- Derecho a solicitar su rectificación o supresión
- Derecho a solicitar la limitación de su tratamiento
- Derecho a oponerse al tratamiento
- Derecho a la portabilidad

PROCEDENCIA:
Los datos se recabarán del dispositivo del usuario garantizando el anonimato de este y su utilización exclusiva con fines de investigación científica.

FUNCIONAMIENTO:
AMon recopila información relativa al estado del teléfono, la conectividad y la seguridad, pero los datos no se asocian directamente con la identidad personal del usuario del teléfono porque se utiliza el MAC del dispositivo como identificador. Tampoco se recopila información alguna relativa a contactos o similar. Los principios de proporcionalidad y necesidad serán escrupulosamente respetados para minimizar el tratamiento de los datos.

AMon recopila los datos estáticos del dispositivo. Esto incluye el modelo del teléfono, las especificaciones básicas del hardware, el uso de la CPU, el consumo de batería, los valores de RAM y un registro de las aplicaciones instaladas, su versión, el funcionamiento automático o no de la aplicación y los permisos requeridos por la misma.

AMon recopila la dirección IP de los sitios visitados, la aplicación que realizó el acceso, la hora de inicio de la conexión, su duración y los puertos utilizados. No se almacena información de la carga útil o credenciales que no son necesarios a efectos de la investigación.

AMon envía información relacionada con las capacidades de conectividad, información sobre uso de redes Wi-Fi y dispositivos Bluetooth vinculados, así como valores específicos relacionados con la seguridad del dispositivo.

AMon opera en segundo plano con independencia de la acción del usuario, pero sin alterar el uso y funcionamiento normal del dispositivo.

AMon puede ser desinstalada en cualquier momento por el propio usuario.

DURACIÓN:
Los datos serán mantenidos, convenientemente anonimizados y protegidos, el tiempo estrictamente requerido para el desarrollo de la investigación científica.

CUMPLIMIENTO NORMATIVO:
El tratamiento se realizará conforme a las obligaciones de protección de datos personales y privacidad establecidas en derecho.