Ingenieria de software

Seguridad de la aplicación

**ESTANDRES DE SEGURIDAD**

Android es un sistema menos vulnerable. El estudio en cuestión habla de 13 vulnerabilidades graves para Android.

**TrustPort**

Es capaz de escanear bajo demanda cada aplicación instalada o cada archivo descargado. Si un usuario descarga o actualiza una aplicación, TrustPort Mobile Security escanea esta aplicación de forma automática y en caso de ser necesario es posible desinstalar la aplicación sospechosa,

**Estático**

Las [herramientas de pruebas](http://searchdatacenter.techtarget.com/es/opinion/La-seguridad-basada-en-el-riesgo-facilitara-las-pruebas-de-software) estáticas miran la aplicación mientras está en reposo, ya sea el código fuente o el binario de la aplicación. Esto puede ser bueno para la identificación de ciertos tipos de vulnerabilidades en la forma en que el código se ejecutará en el dispositivo, por lo general asociado con el flujo de datos y el manejo del búfer. Algunas herramientas y servicios de análisis de seguridad estática comerciales tienen la capacidad de probar el código de la aplicación móvil.

**Dinámico**

Las herramientas de pruebas dinámicas permiten a los analistas de seguridad observar el comportamiento de los sistemas en funcionamiento con el fin de identificar posibles problemas.

**Forense**

Las herramientas forenses permiten a los analistas de seguridad examinar los artefactos que son dejados de lado por una aplicación después de que se ha ejecutado. Las cosas comunes que pueden buscar los analistas incluyen las contraseñas codificadas fuertemente u otras credenciales almacenadas en los archivos de configuración, los datos sensibles almacenados en bases de datos de aplicaciones, y los datos inesperados almacenados en las memorias caché de componentes del navegador web.

**Seguridad en las comunicaciones**

El protocolo TLS es un protocolo para establecer una conexión segura entre un cliente y un servidor, o entre dos servidores. TLS es capaz de autenticar en ambos lados de la comunicación, y crea una conexión cifrada entre los dos.

La principal propiedad del protocolo TLS, es ofrecer privacidad e integridad de los datos, entre dos aplicaciones que se comunican; el protocolo está compuesto por dos capas, el TLS Record Protocol y el TLS Handshake Protocol.

El TLS Record Protocol: es utilizado para la encapsulación de varios protocolos de nivel superior. Si las conversaciones no estuvieran cifradas sería muy fácil un ataque y podría hacer que se interceptaran de forma fácil las conversaciones.

Si el servidor XMPP tiene habilitada la seguridad TLS, la captura de estos mensajes ya no es por lo menos tan fácil de conseguir.

SASL provee a XMPP de un método generalizado para la autenticación. Para ello se han aplicado ciertas normas:

• Si la autenticación SASL se da entre dos servidores, la comunicación no se establecerá hasta que cada servidor se asegure de la auténtica DNS del otro.

• Si quien quiere autenticarse soporta SASL, deberá incluir el atributo ‘version’ con el valor ‘1.0’ por lo menos, en la cabecera del stream inicial.

• Si el servidor soporta SASL, deberá informar de sus tipos de autentificaciones con la etiqueta <mechanisms/> en la contestación de la etiqueta de inicio de sesión, si es que el cliente soporta la conexión SASL

• Durante la negociación SASL, ninguno de los dos deberá enviar algún carácter en blanco como separación entre elementos, esta prohibición ayuda a asegurar la precisión a nivel de byte.

• Cualquier carácter XML contenido en los elementos XML deberá estar codificado usando el algoritmo base64 (Algoritmo de codificación binaria de textos).

El proceso de autentificación mediante SASL sería el siguiente:

• La entidad que pida una autentificación SASL deberá incluir el atributo ‘version’ en la etiqueta de inicio de sesión enviada al servidor con el valor ‘1.0’ como mínimo.

• Cuando el servidor recibe la etiqueta de inicio de sesión con el atributo ‘version’ deberá comunicar los tipos de autentificación SASL que implementa, cada uno de ellos irá dentro de un hijo del tipo <mechanisms/>.

• El cliente deberá seleccionar uno de los mecanismos enviando el elemento <auth/> con un valor adecuado para el mecanismo de autentificación SASL elegido. Si el cliente debe responder con un elemento vacío, responderá con el carácter ‘=’, que indicará que la respuesta no contiene datos.

• Si fuera necesario, el servidor enviará el elemento <challenge/> al cliente que contendrá datos en formato XML, esto dependerá del tipo de autentificación SASL que el cliente haya elegido.