GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT
centro criptológico nacional

CCN-CERT IA-13/18

Informe de amenazas.
Riesgos de uso de Line.

Junio 2018

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.06.11 16:45:09 +02'00'

© Centro Criptológico Nacional, 2018

Fecha de Edición: junio de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. CONTEXTO DE LA APLICACIÓN

Line es una aplicación de mensajería instantánea que se encuentra disponible tanto para teléfonos móviles, como para PC/Windows y Mac. Además de la mensajería básica que suelen proporcionar esta serie de servicios, a través de Line se pueden realizar envío de imágenes, vídeos y audio, y hacer llamadas VoIP[1]. La aplicación es principalmente reconocida por su singular sistema de pegatinas (stickers), que reemplaza a los tradicionales iconos. En la actualidad, la aplicación tiene más de 500 millones de usuarios en todo el mundo.

[1] VoIP (Voice Over Internet Protocol): protocolo de voz por internet.

Inicialmente fue una aplicación desarrollada para teléfonos móviles con sistemas Android e iOS. Tras su gran acogida y popularidad entre los usuarios, se amplió a Windows Phone, BlackBerry OS, Firefox OS, Mac OS X y Windows. En esta última tiene dos versiones: una de escritorio tradicional; y otra, exclusiva para Windows 8, disponible en Windows Store.

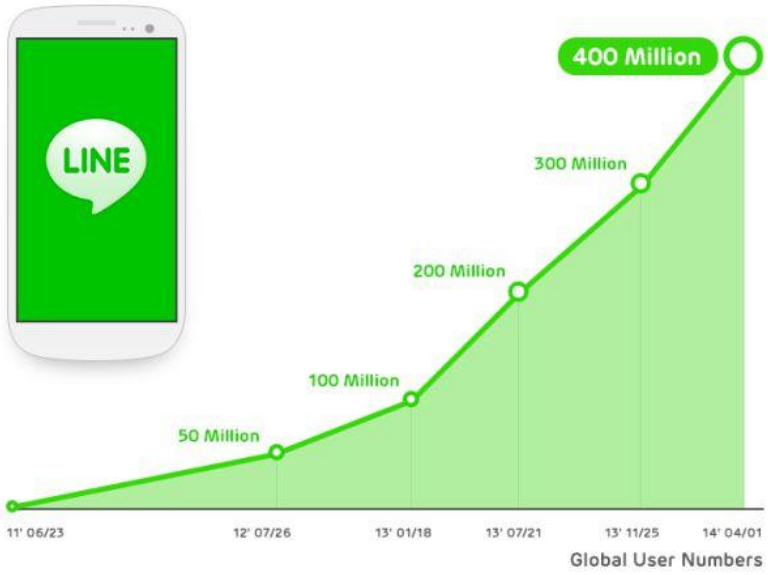


Ilustración 1: Crecimiento de usuarios hasta el año 2014

El servicio nació en Japón, tras la caída de los servicios de telefonía durante el terremoto de marzo de 2011. Los trabajadores de la empresa surcoreana NHN, dueña del buscador Naver, desarrollaron Line para poder comunicarse entre ellos. Dos meses más tarde, salió a la luz al público general.

Su funcionamiento es muy parecido al de WhatsApp o Telegram. La aplicación busca los contactos del teléfono que ya usan el servicio y los agrega directamente, aunque más adelante se pueden eliminar o incluir a otros simplemente utilizando su nombre de usuario.

Entre sus principales características, destacan:

- Sincronización de Microsoft Word.
- Confirmación en tiempo real de envío y entrega de mensajes.
- Permite compartir fotos, vídeos y música.
- Envío de localización.
- Envío de emoticonos y pegatinas (stickers).
- Posibilidad de crear grupos de hasta 100 personas.

- Tablón de noticias.
- Posibilidad de agregar amigos mediante uso de códigos QR y NFC.
- Uso de perfiles y biografías.
- Posibilidad de utilizar el servicio bajo un pseudónimo, sin revelar el número de teléfono del usuario.

3. PROBLEMAS DE SEGURIDAD EN LA ACTUALIDAD

3.1 SECUESTRO DE CUENTAS APROVECHANDO FALLOS DE LA RED

La firma Positive Technologies hizo público un vídeo[2] en el que se mostraba cómo secuestrar cuentas de WhatsApp o de otras aplicaciones como Telegram. La técnica que enseñaban, basada en el empleo de fallos conocidos en el protocolo de comunicaciones SS7, es también aplicable a otros servicios de mensajería, como Line.

El protocolo SS7[3] (Signalling System No. 7) es estándar global para las telecomunicaciones. Fue desarrollado por AT&T en 1975, y define el protocolo y procedimientos mediante los cuales los elementos de una red de telefonía intercambian información sobre una red digital para efectuar el enrutamiento, el establecimiento y el control de llamada; y que forma parte, entre otros, del funcionamiento interno de servicios como los SMS.

Anteriormente, algunos investigadores ya mostraron[4] fallos de seguridad de este protocolo en la conferencia de hacking alemana Chaos Communication Congress, donde se demostró que en el caso de que un atacante consiguiera entrar al sistema SS7 podría interceptar o grabar llamadas, leer SMS, o detectar la localización del dispositivo utilizando el mismo sistema que la red del teléfono.

[2] **How to hack WhatsApp and Telegram:** https://habrahabr.ru/company/pt/blog/283052/
[3] **SS7:** https://es.wikipedia.org/wiki/SS7
[4] **SS7: Locate. Track. Manipulate :** https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

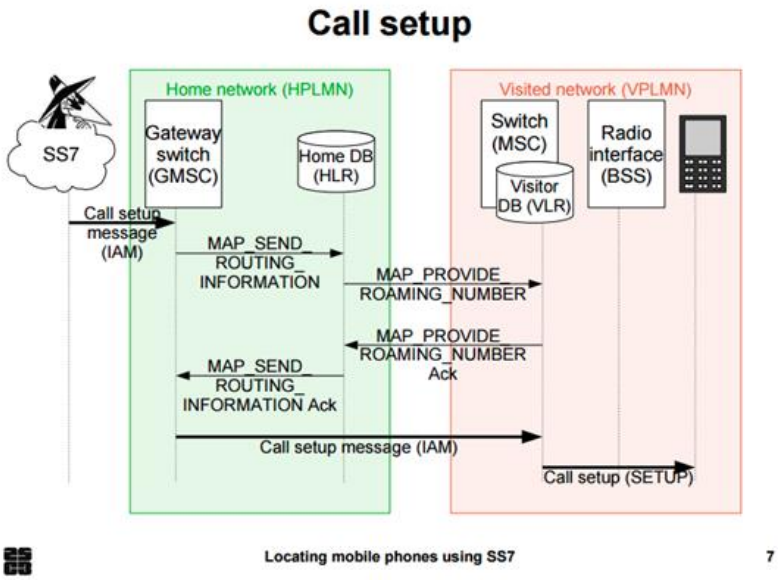


Ilustración 2: Esquema de funcionamiento bajo SS7

Aprovechando estos fallos de seguridad conocidos, aún sin resolver, el ataque se realiza de forma sencilla, haciendo creer a la red telefónica que el dispositivo del atacante dispone del mismo número que la víctima. De esta forma, se consigue recibir un código de verificación de Line válido que permite el acceso completo a la cuenta de la víctima –independientemente del cifrado incluido en las comunicaciones–, siendo posible suplantarla desde ese momento en adelante.

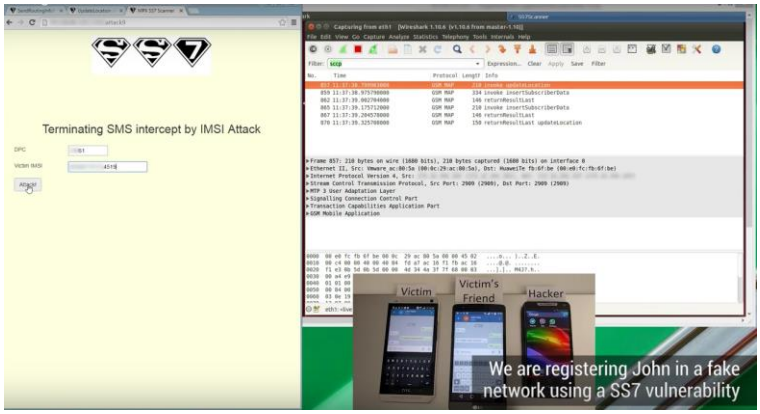


Ilustración 3: Prueba de concepto sobre WhatsApp y Telegram

Al tratarse de un fallo en de red, no dependiente de la aplicación, no existe una forma directa de resolver estos fallos. En algunas versiones de Line es posible activar, desde el menú de preferencias de la aplicación, la autenticación de doble factor para añadir una capa de seguridad adicional.

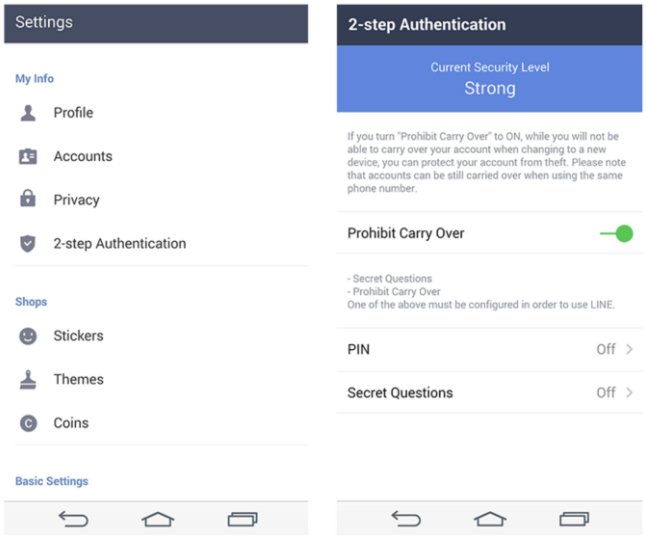
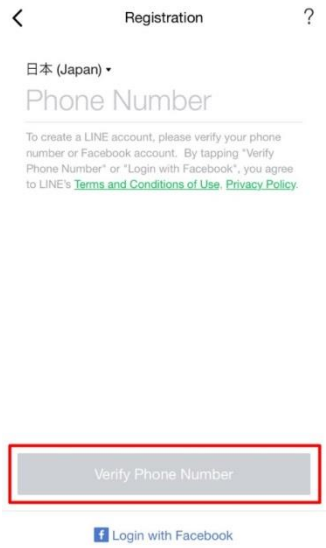


Ilustración 4: Configuración de autenticación de doble factor

El usuario, al activar este doble factor[5], deberá de elegir entre las diferentes medidas de protección disponibles:

- **Carry Over**: evita que la cuenta sea transferida a un nuevo dispositivo con un número de teléfono diferente, mejorando la protección frente a robos.
- **PIN**: es posible configurar un PIN de acceso que se exija cuando se intente acceder desde otra cuenta.
- **Secret Questions**: Como medida adicional para proteger las cuentas del usuario contra inicios de sesión no autorizados, se pueden configurar preguntas secretas. Cuando se transfiera una cuenta, se solicitará a los usuarios que respondan a una de las tres preguntas configuradas de antemano.



[5] **LINE with 2-Step Authentication:** https://linecorp.com/en/pr/news/en/2015/976

3.2 ROBO DE CUENTAS MEDIANTE SMS Y ACCESO FÍSICO

Algunos de los ataques con mayor índice de éxito no implican el uso de vectores de ataque avanzados. Un posible despiste, o pérdida del teléfono –a pesar de tener los mecanismos de bloqueo de pantalla y código de seguridad–, puede permitir a una persona con acceso físico a un dispositivo móvil secuestrar nuestra sesión de Line de forma sencilla.

El primer método tiene que ver con el sistema de registro de la aplicación. Un atacante podría utilizar un teléfono propio, o un emulador de terminal, y comenzar el proceso de registro con el número de la víctima, como si se tratara de un cambio de terminal.

Si el atacante consigue acceso físico al teléfono, y la previsualización de SMS se encuentra activada, podrá observar el código de seguridad que el teléfono reciba, registrando satisfactoriamente su terminal y obteniendo acceso a la sesión de la víctima.

Para evitarlo, se debe desactivar la previsualización del remitente y contenido en la pantalla de bloqueo del terminal. En el caso de utilizar un terminal iPhone, se procederá de la siguiente forma:

1. Se accede a **Ajustes**
2. En el menú **Notificaciones**
3. Se selecciona la opción de **Mensajes**
4. Se desactiva la opción **Previsualización**

En el caso de utilizar un terminal Android, procederemos de la siguiente forma:

1. Se accede a **Ajustes**
2. Se pulsa sobre **Sonido y notificaciones**
3. Dentro del menú **Notificación**, se pulsa sobre **Notificaciones de aplicaciones**
4. Se busca la aplicación por defecto para la gestión de SMS (Hangouts o Messenger) y se cambia la configuración, desactivando la opción de **Permitir vista previa**

3.3 REPLAY ATTACKS

En primer lugar, se explicarán algunos conceptos básicos, como en qué consiste un Ataque de Repetición (conocido como Replay Attack) o un Código de Autenticación de Mensajes (MAC). Un Replay Attack es un ataque en el que un adversario registra mensajes entre dos partes. Este puede reproducir esos mensajes a cualquiera de los miembros de la conversación, como si hubieran sido enviados legítimamente. El atacante no necesita saber el contenido del mensaje para poder reenviarlo.

Los Códigos de Autenticación de Mensajes (MAC) se usan para garantizar la integridad de un mensaje y asegurar que este no ha sido alterado de ninguna manera. Cuando un mensaje es recibido, el receptor calcula de nuevo el valor de MAC y lo comprueba contra el MAC recibido, para certificar que el mensaje recibido es el mismo que el mensaje original enviado. Además, también deben autenticarse datos adicionales, como fuente y destino de información, y un número de mensaje. Esta información adicional protege el mensaje de los ataques de repetición.

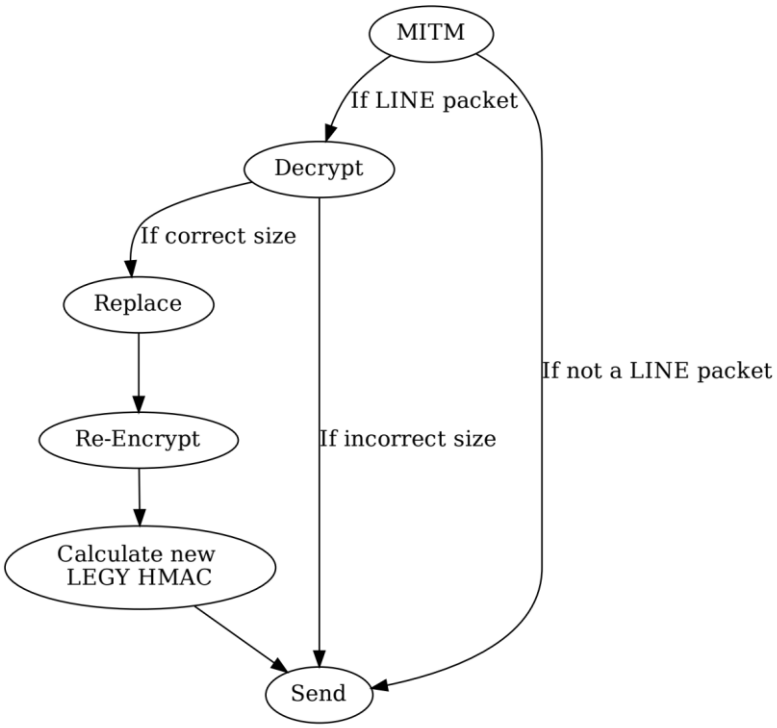


Ilustración 6: Implementación del Replay Attack

Durante las diferentes pruebas realizadas en un estudio llevado a cabo por dos investigadores[6], se ha descubierto que es posible realizar estos ataques de repetición, que permiten reemplazar el cuerpo de un mensaje en tránsito con cualquier mensaje visto anteriormente.

El Replay Attack es posible debido al hecho de que LINE solo autentica el mensaje en sí, posibilitando así ataques de repetición. También hay una desviación de las mejores prácticas de criptografía, ya que LINE utiliza la misma clave para el MAC que para el cifrado. Tanto este ataque, como el que será explicado más adelante, supone que el atacante dispone de los mismos privilegios que el servidor de Line.

[6] **Analysis of end-to-end encryption in the LINE messaging application:**
https://www.usenix.org/system/files/conference/foci17/foci17-paper-espinoza.pdf

Los tres componentes relevantes durante este proceso son:

1. Salt
2. Mensaje cifrado
3. MAC

Cuando el servidor envía un mensaje nuevo, con estos tres campos iguales a los de un mensaje que haya sido enviado con anterioridad, se produce el ataque.

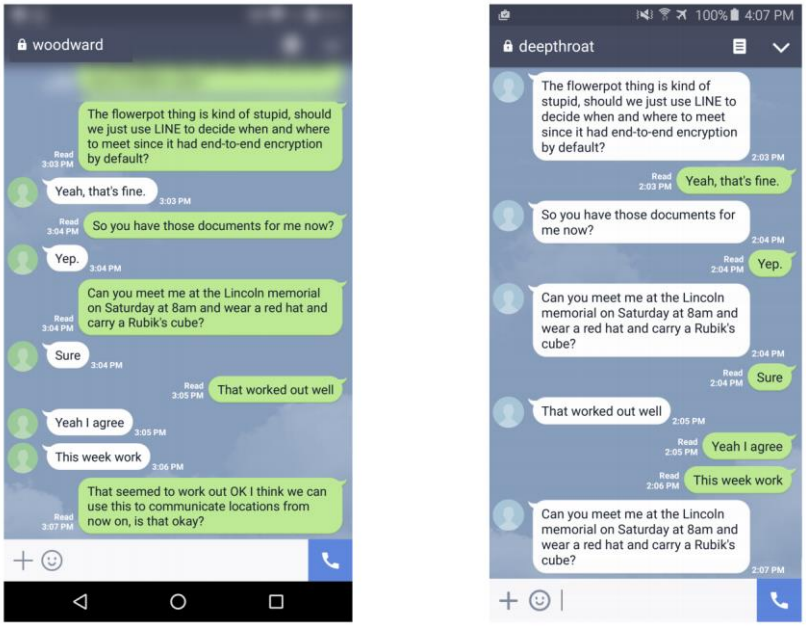


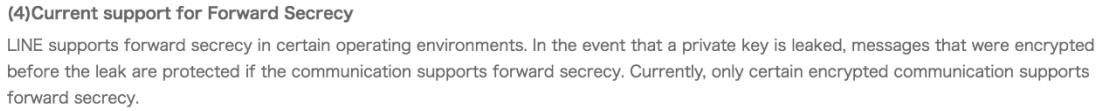
Ilustración 7: Diferencias entre los datos enviados por el emisor y los recibidos por el receptor

3.4 IMPLEMENTACIÓN DE FORWARD SECRECY

Forward Secrecy es una propiedad del sistema de cifrado que impide que un atacante pueda descifrar mensajes pasados o futuros, incluso si las claves privadas de uno o más usuarios están comprometidas.

Para la comunicación de cliente a cliente, Forward Secrecy se implementa generando una nueva clave para cada sesión o mensaje intercambiado entre usuarios (llamada clave efímera). La consideración más importante es que la clave para esta sesión se genera de forma aleatoria, es decir, no es predecible o determinista.

Además, la implementación de esta capa de seguridad es de extremo a extremo (E2E), lo que significa que las comunicaciones están cifradas desde el usuario que envía el mensaje hasta el destinatario previsto.


(4)Current support for Forward Secrecy

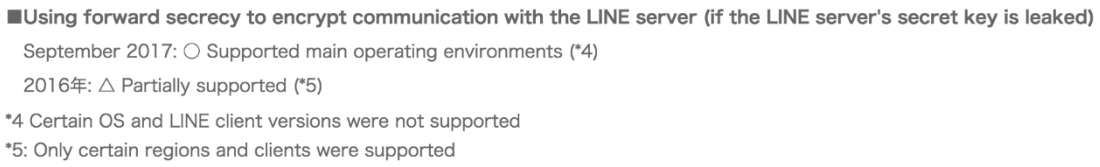
LINE supports forward secrecy in certain operating environments. In the event that a private key is leaked, messages that were encrypted before the leak are protected if the communication supports forward secrecy. Currently, only certain encrypted communication supports forward secrecy.

Ilustración 8: Documentación del protocolo disponible en la web principal de Line

LINE, sin embargo, solo ofrece confidencialidad de cliente a servidor, lo que significa que la capa de seguridad ofrecida por este sistema de claves efímeras no protege al usuario de un posible atacante con los mismos privilegios que el servidor de Line.

Este ataque es posible si el atacante puede acceder a la clave secreta de uno de los dispositivos de los usuarios. Este método requiere el acceso físico a un dispositivo, por la aplicación de la ley, los agentes del gobierno, los empleadores, etc. En cualquier caso, un atacante con una clave privada de un usuario podría recuperar mensajes, incluso si han sido eliminados de los dispositivos de ambos usuarios.

Durante septiembre de 2017 se realizó un cambio en la implementación de Forward Secrecy, como se aprecia en la siguiente imagen de la página oficial de Line, pero quedando limitado a ciertos sistemas operativos y clientes, que no han sido especificados:


■Using forward secrecy to encrypt communication with the LINE server (if the LINE server's secret key is leaked)

September 2017: ○ Supported main operating environments (*4)

2016年: △ Partially supported (*5)

*4 Certain OS and LINE client versions were not supported

*5: Only certain regions and clients were supported

Ilustración 9: Modificaciones en la implementación de Forward Secrecy

3.5 IMPLEMENTACIONES CRIPTOGRÁFICAS CON POSIBLE RIESGO

Existen otra serie de desviaciones sobre el protocolo de Line respecto a los estándares y recomendaciones criptográficas, que pueden llegar a suponer un riesgo de seguridad:

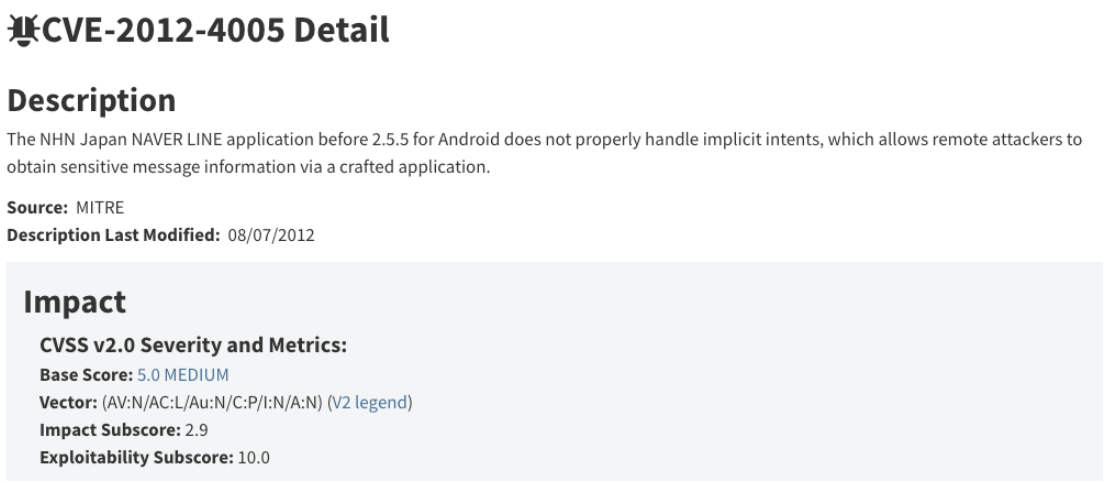
- La documentación oficial indica que la capa de cifrado Cliente a Servidor usa un **Vector de Inicialización** (**IV**) aleatorio junto con la clave efímera de cifrado para AES; pero, en gran parte de las versiones del cliente analizadas, el **IV** está *hardcodeado* y nunca cambia.

- La documentación oficial también indica que la capa de cifrado Cliente a Servidor utiliza **AES**[7] en modo **GCM**[8], pero también se encuentra **AES** en modo **CBC**[9].
- **LEGY-HMAC**, el MAC utilizado para las comunicaciones Cliente a Servidor (no documentadas en el documento técnico), tiene una longitud de 32 bits y se basa en algoritmo hash, que no es criptográficamente fuerte.
- Para el cifrado E2E se utiliza la misma clave, así como para la autenticación de mensajes (MAC). Se considera una práctica recomendada usar claves separadas.
- Para el cifrado E2E, el MAC funciona como "**hash and then encrypt**", comparado con algo como podría ser **HMAC**[10], que protege de diversos tipos de ataques.

3.6 OTROS FALLOS DE SEGURIDAD ANTERIORES

3.6.1. LECTURA DE INFORMACIÓN DESDE APLICACIONES DE TERCEROS

En Julio de 2012, desde el centro de coordinación JPCERT, se notificó una vulnerabilidad que afectaba a la versión 2.5.5 del cliente, y que indicaba un problema de diseño, que permitía a una aplicación maliciosa leer información (salvo el número de teléfono del cliente) de forma ilícita de los mensajes en el momento de su transmisión desde terminales Android. A esta vulnerabilidad se le asignó la referencia CVE-2012-4005[11].



CVE-2012-4005 Detail

Description

The NHN Japan NAVER LINE application before 2.5.5 for Android does not properly handle implicit intents, which allows remote attackers to obtain sensitive message information via a crafted application.

Source: MITRE
Description Last Modified: 08/07/2012

Impact

CVSS v2.0 Severity and Metrics:
Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

Ilustración 10: Información pública de la vulnerabilidad

[7] AES: Advanced Encription Standard
[8] GCM: Google Cloud Messeging
[9] CBC: Cipher-Bloch Chaining
[10] Código de autentificación de mensajes en clave hash
[11] **CVE-2012-4005:** https://www.cvedetails.com/cve/CVE-2012-4005/

3.6.2. TRANSMISIÓN DE INFORMACIÓN EN TEXTO CLARO SOBRE 3G

En agosto de 2013, un equipo de investigadores alertó de que los chats y las comunicaciones entre usuarios de la aplicación viajaban en claro cuando las comunicaciones 3G del terminal del usuario estaban activas; sin embargo, eran cifradas cuando éste se encontraba conectada a una red WiFi. Esto permitía a cualquier agencia gubernamental o compañía telefónica acceder al texto en claro de las conversaciones, violando la confidencialidad de los usuarios.

El equipo desarrolló un script Python de 20 líneas, de algunos de los tokens que registraron de comunicaciones de usuarios, y los empleó para realizar peticiones sobre los servidores de Line. Con una simple solicitud HTTP en formato JSON pudieron acceder a los nuevos mensajes en los chats de grupo y, con un pequeño ajuste de los parámetros, fue posible obtener el histórico del grupo desde hacía unos meses.

Las claves de sesión utilizadas para recuperar los registros de los chats anteriormente indicados debían tener una fecha de caducidad, pero eso no fue evidente durante la duración del estudio. Alrededor de 24 horas después, los mismos tokens lograron extraer los registros de chat de los servidores de Line.

3.6.3. ALMACENAMIENTO INSEGURO DE CHATS OCULTOS

Durante el mes de Julio de 2014[12], Line implementó un nuevo sistema de envío de mensajes denominado chats ocultos (Hidden chats). Los chats ocultos tienen lugar en un chat uno a uno, quedando separados de los chats regulares. Los mensajes de texto e imagen se envían en un estado seguro y, después de que el receptor “toque” el mensaje, los contenidos solo se muestran durante un período de tiempo preestablecido. Excedido ese límite de tiempo, el mensaje se elimina automáticamente.

[12] **LINE Hidden Chats :** http://official-blog.line.me/en/archives/1006361166.html

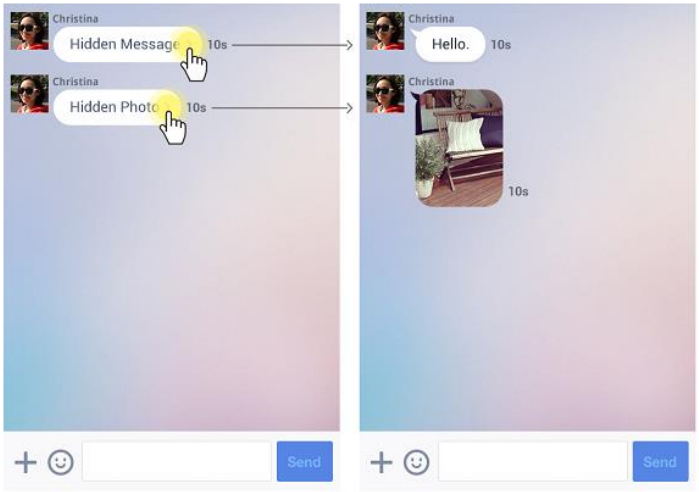


Ilustración 11: Ejemplo de uso de los Hidden chat

Esta función se diseñó para enviar mensajes con información sensible o imágenes que solo se desea que vea el destinatario. Los diversos estudios publicados indican[13] que parte de esta información sensible quedaba almacenada en la base de datos de la aplicación, accesible desde la ruta '/data/data/jp.naver.line.android/', sin necesidad de permisos de root.

Esta base de datos es utilizada para almacenar los mensajes de los chats y multimedia, intercambiados por la aplicación, conteniendo diversos ficheros clasificados por el tipo de información tratada:

Database	***Description***
databases/	This directory holds sqlite database files used by the app
naver_line.db	This file stored chat data in Sqlite 3 file database format, It's structure is discussed below
naver_line_private_chat.db	This file contains data from private messaging feature of the program called "Hidden Message" inside the app. This file and the "Hidden Message" feature are discussed in the next section.

Ilustración 12: Bases de datos utilizadas por los chats y hidden chats

Según el escenario implementado en la investigación, no todos los mensajes ocultos fueron recuperados. No se encontraron elementos en el fichero "naver_line_private_chat.db", ya que los mensajes fueron borrados al finalizar la duración establecida del tiempo de espera del mensaje.

[13] **Forensics:** https://www.researchgate.net/publication/287997487_LINE_IM_app_Forensic_Analysis

No obstante, cerrando la aplicación de forma manual, y en otros casos al tratarse de ficheros multimedia, se pudo localizar la información almacenada en la base de datos, siendo accesible mediante el uso de herramientas forenses:

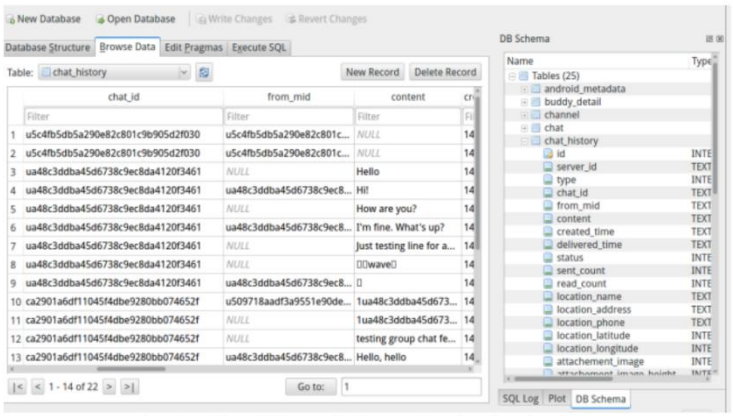


Ilustración 13: Base de datos de conversaciones de LINE

Esta funcionalidad fue sustituida a finales de Junio de 2016[14] por lo que Line ha denominado Letter Sealing, que es realmente un sistema de cifrado E2E. Desde ese momento, la opción de los chats y mensajes ocultos ha sido eliminada de la plataforma, no siendo posible acceder a esta funcionalidad ni a los datos almacenados por ésta.

3.6.4. ATAQUES MITM A TRAVÉS DE CERTIFICADOS MALICIOSOS

Durante octubre del año 2014, también se localizó una vulnerabilidad en la versión 2.3.1.1 del cliente para Android. Al no realizarse verificación sobre los certificados X.509 de los servidores SSL, era posible que un atacante realizara ataques man-in-the-middle para suplantar a los servidores de la aplicación, y así obtener información sensible utilizando un certificado malicioso. A esta vulnerabilidad se le asignó la referencia CVE-2014-6980[15].

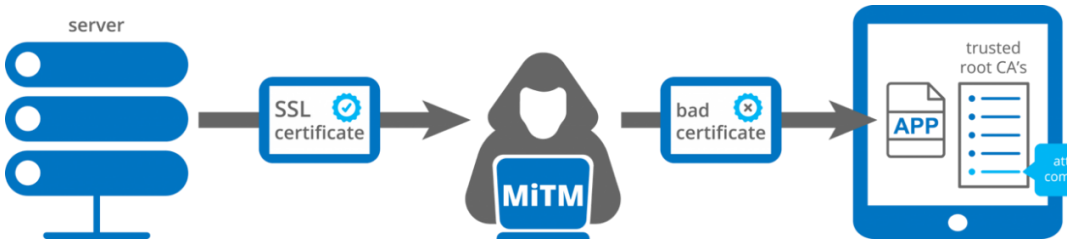


Ilustración 14: Explicación gráfica de un ataque MiTM

[14] **LINE Letter Sealing :** http://official-blog.line.me/en/archives/1058913293.html
[15] **CVE-2014-6980 :** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6980

4. RECOMENDACIONES ADICIONALES PARA TELÉFONOS MÓVILES

Debido a los riesgos de seguridad que implica el uso de la aplicación, resulta necesario adoptar una serie de medidas de precaución, para que la información de los dispositivos móviles quede a salvo de posibles criminales o programas maliciosos. Las siguientes recomendaciones ayudarán en esta tarea:

- Mantener el teléfono bloqueado. De esta forma se reduce el riesgo si el teléfono cae en manos equivocadas. Además, y como se ha visto a lo largo de esta guía, será recomendable impedir las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance. Una simple llamada de teléfono podría comprometer la seguridad de alguna sesión o aplicación que se esté utilizando.
- Extremar el acceso y las solicitudes de permisos de las aplicaciones que se ejecuten en el teléfono, especialmente en terminales Android.
- Considerar los riesgos de realizar un *jailbreaking*[16] o *rooting*[17] del terminal, debido a que se puede comprometer y reducir considerablemente su seguridad.
- Desactivar la conectividad adicional del teléfono, como la conexión WiFi o Bluetooth, cuando no se vaya a utilizar. Así, además de reducir el consumo de batería, disminuye la posible superficie de ataque sobre tu terminal.
- Activar cualquiera de las soluciones de geolocalización y seguridad, que serán de gran ayuda para el acceso remoto en caso de pérdida o robo, pudiendo incluso realizar un borrado seguro en caso necesario.
- Si es posible, instalar un antivirus en el teléfono, puesto que los programas maliciosos no solo afectan a los equipos de sobremesa. La tendencia de los atacantes y estafadores indica que en los próximos años se incrementará exponencialmente el uso de estos programas dañinos en teléfonos móviles.

[16] Jailbreaking: supresión de limitaciones impuestas por Apple
[17] Rooting: supresión de limitaciones impuestas en dispositivos Android