شرح تشفير الواتساب[1] بروتوكول (Signal)

فهد الدريبي

أنواع المفاتيح العامة (مفتاح خاص و آخر عام ينشأ باستخدام Curve25519)

- مفتاح التعريف، يتم إنشاؤه أثناء تركيب التطبيق.
- مفتاح ابتدائي، ينشأ أثناء التركيب و يجدد بشكل دوري وموقع بواسطة مفتاح التعريف.
- مفاتيح الاستخدام الواحد، تنشأ حسب الحاجة.

أنواع مفاتيح الجلسة (مفاتيح تماثلية)

- مفتاح رئيس.
- مفتاح تسلسلي، ينشأ بالمفتاح الرئيس.
- مفاتيح الرسائل، تنشأ بالمفاتيح التسلسلية.

عند تركيب التطبيق يقوم البرنامج بإرسال المفاتيح العامة لكل من مفتاح التعريف والمفتاح الابتدائي ومجموعة من مفاتيح الاستخدام الواحد لخوادم الواتساب. يحتفظ الخادم بهذه المفاتيح مع حساب المستخدم. المفاتيح الخاصة تبقى دائما مع المستخدم فقط.

إعداد جلسة المحادثات بين طرفين

المراسلات في نظام التشفير الجديد كلها مشفرة وذلك يشمل رسائل الإعداد الأولي ولتحقيق ذلك يقوم المرسل باستخدام المفاتيح العامة للمستقبل والتي يحصل عليها من خادم الواتساب[2]. يرسل الخادم للمرسل مفاتيح المستقبل وهي مفتاح التعريف ومفتاح ابتدائي و أحد مفاتيح الاستخدام الواحد[3]. فيقوم المرسل باستخدام مفاتيحه الخاصة و مفاتيح المستقبل العامة لإنشاء المفتاح السري (باستخدام بروتوكول ECDH) ويستخدم المفتاح السري في عملية تشفير الرسائل قبل إرسالها للمستقبل. كما يقوم المرسل بإرفاق مفاتيحه العامة مع الرسائل الأولى إلى أن يتم إنهاء إعداد الجلسة.

عندما تصل الرسائل للمستقبل يقوم باستخدام مفاتيحه الخاصة والمفاتيح العامة للمرسل والتي أرسلت له مع الرسالة وينشئ منها نفس المفتاح السري الذي أنشاءه المرسل (هذه هي عبقرية بروتوكول ديفي-هيلمان) ومن ثم يقوم باستخراج المفتاح الرئيس كما فعل المرسل ويستخدمه في عملية فك تشفير الرسائل وبهذا تكون الجلسة قد أعدت بين الطرفين وكلاهما يحمل مفاتيح تشفير الرسائل.

تشفير الرسائل

لكل رسالة تنشأ مفاتيح تشفير جديدة لدى الطرفين ولها هذه المميزات:

1. المفاتيح لدي الطرفين متشابهة (شكرا لبروتوكول ديفي-هيلمان)و تنشأ من مفاتيحهم العامة والخاصة.
2. مفتاح كل رسالة مستقل عن ما قبله وما بعده، فضياع الرسالة لا يوثر على سير التراسل. واكتشاف احد المفاتيح لا يمكن من فك تشفير الرسائل السابقة.
3. لا يمكن استنباط المفاتيح الأصلية من مفاتيح الرسالة.
4. المفتاح يستخدم لتشفير رسالة واحدة فقط ولا يعاد استخدامه

هذه المميزات تجعل عملية ربط رسالة مشفرة بمرسل معين مستحيلة، فالتحقق من صحة الرسالة ممكن لكن التحقق من هوية المرسل مستحيلة وهذه مفيدة في حال المراسلات الحساسة والتي يخشى فيها المرسل مثلا من محاكمته واتهامه بإرسال تلك الرسائل. لكن في نفس الوقت هذه الميزة تجعل عملية التحقق من هوية الطرف الآخر مستحيلة لذلك يتم استخدام مفتاح الاستخدام الواحد وكذلك خاصية التحقق من خلال تطبيق الواتساب ومطابقة رمز التحقق يدويا مع الطرف الآخر لتجاوز هذه الثغرة.

ملفات الوسائط (الفيديو والصور و الصوت) والمستندات يتم تشفيرها بنفس الأسلوب. وعند استقبال ملف من شخص وتمريره لشخص آخر تتم عملية تشفير الملف بمفاتيح خاصة بالشخص الآخر وإرسال الملف المشفر من جديد.

تشفير رسائل المجموعات

بأسلوب مشابه تقريباً لطريقة المراسلات بين طرفين يقوم المرسل عند إرسال رسالته الأولى بإنشاء جلسة للمجموعة وذلك بالتخاطب مع جميع أعضاء المجموعة كل على حدة وبتشفير مختلف عن الآخرين ويرسل لهم مفتاح موحد خاص به يسمى مفتاح المرسل. يقوم المرسل بعدها باستخدام ذلك المفتاح لإنشاء مفاتيح التشفير لكل رسالة (مفتاح تسلسلي ومفتاح الرسالة) ويستخدم تلك المفاتيح لتشفير رسائله وإرسالها للخادم والذي بدورة يقوم بتوزيع تلك الرسالة لجميع أعضاء المجموعة. جميع الأعضاء يملكون مفتاح المرسل فيقومون باستخدامه لاستخراج المفاتيح التي تتيح لهم فك تشفير تلك الرسالة والرسائل القادمة.

عندما يقوم احدهم بمغادرة المجموعة يقوم بقية الأعضاء بمسح جميع مفاتيح المرسلين وإعادة إنشاء جلسات المجموعة من جديد.

التخاطب مع الخادم

بالإضافة لتشفير الرسائل بين المستخدمين فإن تطبيق الواتساب (في أجهزة الاندرويد والايفون والويندوز فون فقط) يقوم كذلك بتشفير قناة الاتصال مع الخادم وذلك يمنع من لديهم القدرة على التجسس على الشبكة من معرفة مالذي يقوم به المرسل ومع من يتحدث.

هل نثق في التطبيق الآن؟

يوفر تطبيق الواتساب خيار يمكن تفعيلة من خلال صفحة إعدادات الأمان لتنبيه المستخدم عندما يتغير مفتاح التعريف لأي من المستخدمين المعرفين لديه. ومفتاح التعريف يتغير عند تغيير جهاز الهاتف أو إعادة تركيب التطبيق أو قيام احدهم بانتحال شخصية الطرف الآخر لذا يجب التحقق من هوية الطرف الآخر ومطابقة رمز التحقق إذا كانت سرية المحادثة مهمة.

* يصعب الوثوق في تطبيق الواتساب وتشفيره لعدة أسباب منها:

1. كون التطبيق مغلق المصدر مما يصعب عملية التحقق من طريقة عملة ومطابقتها مع ما اعلن عن طريقة عمل بروتوكول التشفير.
2. كون التطبيق لا يزال يدعم التراسل غير المشفر للتوافق مع الإصدارات القديمة التي لا تدعم التشفير وأن وعملية الانتقال للتشفير تمت بشكل تلقائي من الشركة بدون موافقة المستخدم أو القدرة على اختيار نوع التراسل فهذا يعني أن الشركة قادرة على تعطيل التشفير لشخص معين دون علمه. وبما أن التطبيق يدعم التراسل بالطريقتين فالتحقق من ما يقوم به التطبيق صعب ويحتاج مراقبة مستمرة.
3. كون بروتوكول Signal مصمم في الأصل ليوفر خاصية الإنكار (repudiation وهو عكس non-repudiation) والتي تمكن المرسل من إنكار علاقته بالرسائل التي قام هو بإرسالها فإن عملية التحقق تعتمد على الثقة بخادم الواتساب بالإضافة لعملية مطابقة رمز التحقق يدويا من كلا الطرفين.

وضع الآمان في التطبيق بعد إضافة خاصية التشفير يعد افضل من السابق بمراحل عدة خصوصا للمستخدم العادي ويعتبر من أكثر الحلول المتوفرة أمناً في تطبيقات المحادثات المشهورة حالياً. أما من يبحث عن أمان مطلق فعليه استخدام أدوات ووسائل أخرى لا تتطلب الثقة بطرف ثالث أو استخدام عدة حلول بتقنيات مختلفة مع بعض.

المصادر

[1] المصادر: WhatsApp-Security-Whitepaper و whispersystems.org

[2] هذه احد نقاط الضعف في التشفير، إذ يجب الثقة في الخادم وان المفاتيح المرسلة تخص المستقبل الحقيقي.

[3] يقوم الخادم بحذف المفتاح بعد استخدامه ولا يقبل استخدامه مرة أخرى، وفي حال استنفذت جميع مفاتيح الاستخدام الواحد ولم يستطع الخادم طلب مفاتيح جديدة من المستقبل لعدم وجودة online فإن العملية تتم بدونها. وهذه نقطة ضعف أخرى إذ يستطيع المخترق استغلالها بإنشاء طلبات اتصال وهمية حتى تستنفذ جميع مفاتيح الاستخدام الواحد.