طريقة لاكتشاف خاطف هوية مستخدم الشبكة الخلوية

حمد مرزوق حيي الرشيدي

بإشراف

د. رياض أحمد شيخ

المستخلص

شبكات الهاتف الخلوية (الجوال) ليست آمنة وموثوقة بالقدر الذي يظنه اكثر مستخدمين هذه الشبكات. جهاز خاطف هوية مستخدم شبكة الجوال (IMSI Catcher) يعتبر من اكبر التهديدات التي تواجه مستخدمين هذه الشبكات. هذا الجهاز يعتبر جهاز لاسلكي له القدرة على التظاهر انه برج اتصالات حقيقي مما يسمح لأجهزة الجوال القريبة منه بالاتصال فيه بدلا عن أبراج الاتصالات الحقيقية وبذلك يستطيع تنفيذ الهجوم الشهير بهجوم (رجل في الوسط). بعد تنفيذ هذا الهجوم واتمام الاتصال بين الضحية و شبكة الجوال يستطيع هذا الجهاز عمل كل شيء تقريبا تجاه ضحاياه مثل التنصت على المكالمات وتسجيلها و اعتراض الرسائل القصيرة وإعادة توجيهها و تحديد موقع مستخدم الجوال و العديد من الأشياء الأخرى. هذه الأجهزة تستخدم نظاميا من قبل العديد من الجهات الحكومية حول العالم لتتبع المجرمين والإرهابيين للحد من مخاطرهم لكن في الوقت الحاضر أصبحت هذه الاجهزة تستخدم من قبل اشخاص غير مصرح لهم و منظمات إرهابية لأغراض متعددة. هناك العديد من الأبحاث العلمية التي تمت للحد من مخاطر هذه الأجهزة لكن معظم هذه الأبحاث تعتمد على خصائص أبراج الاتصالات الحقيقية للكشف عن وجود أبراج مزيفة. تختلف هذا الرسالة عن الأبحاث السابقة كونها تعتمد على مزايا وصفات الموقع الجغرافي لأبراج الشبكة وعددها لبناء بصمة لكل موقع تختلف عن غيرها من المواقع الأخرى و تستخدم هذه البصمة للكشف عن وجود أي برج دخيل على ذلك الموقع قبل الاتصال به و قبل إرسال الهوية الخاصة بالمستخدم وهذا ما يجعل الرسالة و البحث فريد من نوعة مقارنة مع الأبحاث الاخرى.

IMSI Catcher Detection Method for Cellular Networks

Hamad Marzoq Alrashede

Supervised By

Dr. Riaz Ahmed Shaikh

Abstract

Mobile communications are not trustful as many people think about it. The IMSI catcher is one of the most effective threat that can compromise the security of mobile communications. It is a radio device that acts as a fake cellular base station allowing near mobiles to connect to it instead of legitimate base station. This type of attack is called man in the middle attack (MITM). The IMSI catcher can do almost everything after being connected to its victims, such as eavesdropping calls, intercepting SMS messages, locating phone's location and so many. It is widely used by government agencies legally to track criminals and terrorists, but nowadays it could be used by unauthorized individuals and criminal organizations for different purposes. Several of countermeasures against this threat have been proposed by many researchers but most of them are reliant on real base station features to expose fake base stations. Those features are limited and could be easily imitated by IMSI catcher device. This thesis presents a new IMSI catcher detection method, which relies on location area features to build a unique fingerprint for each area that makes it unique as compared to most of the existing schemes.