6TH INTERNATIONAL CONFERENCE ON APPLIED RESEARCH IN COMPUTER, ELECTRICAL AND INFORMATION TECHNOLOGY
March 6, 2022
Tbilisi - Georgia
CINVU
Kosar University
Avicenna International Community College LLC

تست نفوذ و بررسی عملیاتی آسیب‌پذیری الگوریتم A5 در مقابل حملات MITM با استفاده از دانگل‌های RTL-SDR

مجید توحیدلو [۱] ، مهدیه هاشمی صدر*[۲]

۱- دانشجوی کارشناسی ارشد مهندسی برق-مخابرات دانشگاه صنعتی مالک اشتر، تهران، ایران

۲- دانشجوی کارشناسی ارشد مهندسی برق-مخابرات دانشگاه صنعتی مالک اشتر، تهران، ایران

چکیده

سیستم‌های ارتباطی نقش مهمی در دنیای امروز دارند و به سرعت رو به پیشرفت هستند. در این میان مسئله امنیت و حفظ حریم خصوصی کاربران از اهمیت بالایی برخوردار است و همزمان با توسعه این سیستم‌ها، افراد سودجو در تلاش هستند تا از راه‌های مختلف به اطلاعات کاربران نفوذ کنند و به آن آسیب برسانند. بنابراین ایده مخابرات سلولی به وجود آمد تا بستری برای ایجاد امنیت فراهم شود. GSM یکی از سامانه‌هایی است که به طور گسترده در مخابرات سلولی مورد استفاده قرار می‌گیرد. این سامانه از الگوریتم A5 به منظور رمزگذاری داده‌های دیجیتال استفاده می‌نماید. با این وجود، الگوریتم A5 می‌تواند در برابر برخی حملات از جمله حمله MITM، که در آن فرد مهاجم در میان یک ارتباط دو سویه قرار می‌گیرد و سعی بر شنود و ثبت اطلاعات کاربر را دارد، آسیب پذیر باشد. در این مقاله به بررسی آسیب پذیری الگوریتم A5 در برابر این نوع حمله و تست نفوذ آن با استفاده از دانگل‌های RTL-SDR پرداخته می‌شود. در انتهای مقاله سناریوی حمله و شنود آورده شده است. همان طور که ملاحظه می‌شود اطلاعاتی از جمله MNC، MCC، TMSI، IMSI، کشور و نام اپراتور استخراج می‌شود که با استفاده از آن‌ها می‌توان سیگنال‌های تبادلی در کانال را رمزگشایی نمود.

واژگان کلیدی: GSM، الگوریتم A5، آسیب‌پذیری، حملات MITM.

*نویسنده مسئول