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

رمزگشایی عملیاتی الگوریتم A5 شبکه مخابرات سلولی داخلی در یک حمله غیرفعال MITM مبتنی بر دانگل 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

سیستم جهانی ارتباطات سیار (GSM) به طور گسترده در مخابرات سلولی استفاده می‌گردد. مسئله حریم خصوصی و امنیت کاربران یکی از مهم‌ترین موضوعات حائز اهمیت در چنین سیستم‌هایی است. برای این منظور الگوریتم‌هایی مختلفی به وجود آمدند تا از اطلاعات کاربران در مقابل حملات و آسیب‌هایی که شبکه GSM را تهدید می‌کند، محافظت کنند. الگوریتم A5 یکی از الگوریتم‌هایی است که برای رمزگذاری به کار می‌رود. این الگوریتم پنج نسخه متفاوت تحت عنوان A5/0، A5/1، A5/2، A5/3 و A5/4 را شامل می‌شود. به طور کلی طیف وسیعی از حملات علیه ارتباطات سیار وجود دارد که اغلب آن‌ها الگوریتم A5 را هدف قرار می‌دهند و به دو دسته حملات فعال و غیرفعال تقسیم می‌شوند. در این مقاله به بررسی عملیاتی شنود و رمزگشایی الگوریتم A5 در یک حمله غیرفعال MITM پرداخته می‌شود که در سناریوی حمله و شنود مورد نظر از دانگل‌های RTL—SDR استفاده شده است. نتایج حاصل شده نشان-دهنده عملکرد موفقیت‌آمیز این سناریو است که بیان‌گر آسیب‌پذیری الگوریتم A5 در برابر چنین حملاتی است.

واژگان کلیدی: GSM، رمزگشایی الگوریتم A5، حملات غیرفعال، حملات MITM

* نویسنده مسئول