PLAKAT INFORMACYJNY PROJEKTU BADAWCZEGO – GRUDZIEŃ 2021

KATEDRA SYSTEMÓW I SIECI RADIOKOMUNIKACYJNYCH

Zespół projektowy: 8@KSSR'2021	**1. Michał Gronau – kierownik** **2. Arkadiusz Bysewski** **3. Jakub Filipiak** **4. Kamil Kobierzyński** **5. Adam Trzebiatowski**
Opiekun:	**dr inż. Piotr Rajchowski**
Klient:	**dr inż. Piotr Rajchowski**
Data zakończenia:	**31.12.2021 r.**
Słowa kluczowe:	**cyberbezpieczeństwo LTE** **symulacja LTE/VoLTE** **ataki i obrona w sieci LTE**

TEMAT PROJEKTU:

Utworzenie stanowiska symulującego działanie sieci 4G-LTE oraz narzędzi ingerujących w przesyłane dane pakietowe.

CELE I ZAKRES PROJEKTU:

Celem projektu jest zweryfikowanie możliwości zaburzenia przesyłania danych pakietowych, w tym podczas transmisji VoLTE, stosując otwarte oprogramowanie umożliwiające uruchomienie punktu dostępowego sieci 4G-LTE. Projekt ma na celu przedstawić potencjalne ataki, zbadać ich skuteczność, a następnie zaproponować metody umożliwiające wykrywanie anomalii w ruchu pakietów lub rozwiązania mogące w części albo w całości wyeliminować badane zagrożenie.

OSIĄGNIĘTE REZULTATY:

W ramach projektu badawczego pomyślnie wykonano 2 scenariusze ataków w sieci 4G-LTE oraz przeprowadzono serię eksperymentów prowadzących do jednoznacznych wniosków. Potwierdzono hipotezę projektu mówiącą o możliwości zaburzania sposobu przesyłania danych pakietowych. Jako że badane ataki były związane z obniżaniem poziomu usług do 2G, zaobserwowano niedoskonałości technologiczne występujące w komercyjnych sieciach GSM w Polsce związane z szyfrowaniem o niskim poziomie bezpieczeństwa. W ramach rozwiązania zaprezentowano konsekwencje wymuszenia na abonencie korzystania z fałszywej sieci GSM zamiast komercyjnej sieci 4G-LTE. Przedstawiono potencjalne rozwiązania zwiększające bezpieczeństwo sieci mobilnych.

CECHY CHARAKTERYSTYCZNE ROZWIĄZANIA, KIERUNKI DALSZYCH PRAC:

Przedstawiane rozwiązanie realizuje 2 ataki w sieciach komórkowych. Pierwszy z nich opiera się na uruchomieniu niezabezpieczonej stacji bazowej GSM zagranicznego operatora. Dzięki temu terminal mobilny z zagraniczną kartą SIM podłącza się do nowej stacji bazowej przedstawiającej się jako stacja macierzysta. Drugi atak dotyczy krajowych abonentów sieci komórkowych i polega na wymuszeniu na terminalu mobilnym łączności z fałszywą siecią GSM przedstawiającą się jako sieć macierzysta. Rozwiązanie wykorzystuje zmodyfikowane oprogramowanie OpenLTE oraz środowisko Osmocom. Dalsze prace mogą obejmować ukończenie implementacji ataku polegającego na wydobyciu numeru telefonu abonenta oraz wytworzenie aplikacji spełniającej funkcję ochronną w związku z wykorzystaniem sieci GSM.

RESEARCH PROJECT INFORMATION FOLDER –DECEMBER 2021

DEPARTMENT OF RADIOCOMMUNICATION SYSTEMS AND NETWORKS

Project team: 8@KSSR'2021	**1. Michał Gronau - leader 2. Arkadiusz Bysewski 3. Jakub Filipiak 4. Kamil Kobierzyński 5. Adam Trzebiatowski**
Supervisor:	**PhD Piotr Rajchowski**
Client:	**PhD Piotr Rajchowski**
Date:	**12.31.2021**
Key words:	**LTE cybersecurity LTE/VoLTE simulation attacks and defence in LTE**

LTE SAFETY
RESEARCH PROJECT

PROJECT TITLE:

Realisation of a test stand simulating 4G-LTE network and tools for interfering with LTE data transmission.

OBJECTIVES AND SCOPE:

The aim of the project is to verify the possibility of disruption of packet data transmission, including VoLTE transmission, using open software enabling running the 4G-LTE network access point. The aim of the project is to present potential attacks, examine their effectiveness and then propose methods for detecting anomalies in packet traffic or solutions that may partially or completely eliminate the analysed threat.

RESULTS:

As a part of the research project, 2 attack scenarios in the 4G-LTE network were successfully performed and a series of experiments were conducted leading to unambiguous conclusions. The project's hypothesis about the possibility of disrupting the packet data transmission was confirmed. As the investigated attacks were relying on lowering the level of services from LTE to 2G, technical imperfections in commercial GSM networks in Poland were observed, related to low-security encryption. As a part of the solution, the consequences of forcing the subscriber to use a fake GSM network instead of the commercial 4G-LTE network were presented. The team showed potential solutions increasing the overall security of mobile networks.

MAIN FEATURES, FUTURE WORKS:

The presented solution carries out 2 attacks within cellular networks. The first of them is based on running an unsecured GSM base station of a foreign mobile network operator. As a result, a mobile station with a foreign SIM card is connecting to the fake base station which presents itself as a home base station. The second attack affects domestic subscribers of mobile networks and consists in forcing the mobile station to connect to a fake GSM network presenting itself as a home network. The solution uses modified OpenLTE software and the Osmocom environment. Future works may include completing the phone number catcher attack implementation and creating an application which would be able to protect the subscriber from various GSM network vulnerabilities.