Politechnika Gdańska

POLITECHNIKA GDAŃSKA

PLAKAT INFORMACYJNY PROJEKTU BADAWCZEGO – MAJ 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:	**23.05.2021 r.**
Słowa kluczowe:	**cyberbezpieczeństwo LTE** **symulacja LTE/VoLTE** **ataki i obrona w sieci LTE**

BEZPIECZEŃSTWO LTE

PROJEKT BADAWCZY

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 symulujące działanie sieci 4G-LTE oraz narzędzia własne. Dodatkowym celem jest przedstawienie propozycji metody umożliwiającej wykrywanie anomalii w ruchu pakietów. Zakres projektu obejmuje działające sieci 4G-LTE razem z rozszerzeniem funkcjonalności przenoszenia mowy w ramach standardu VoLTE.

OSIĄGNIĘTE REZULTATY:

W ramach projektu badawczego sporządzono scenariusz ataku w sieci 4G-LTE oraz skompletowano niezbędne do jego realizacji oprogramowanie. Pomyślnie skompilowano i zainstalowano komponenty oprogramowania niezbędne do wykonania zaplanowanego ataku na przeznaczonym do tego komputerze klasy PC wchodzącego w skład zaprojektowanego stanowiska badawczego. W ramach badania pilotażowego oraz następujących po nich badań, skrupulatnie manipulując parametrami zainstalowanego oprogramowania, pomyślnie uruchomiono działający punkt dostępowy sieci 4G-LTE. Następnie za pomocą dedykowanej aplikacji, jednocześnie konfigurując środowisko punktu dostępowego 4G-LTE, uzyskano numer identyfikacyjny abonenta (IMSI).

CECHY CHARAKTERYSTYCZNE ROZWIĄZANIA, KIERUNKI DALSZYCH PRAC:

Przedstawiane rozwiązanie stanowi podstawę do przeprowadzenia ataku przekierowującego do sieci 2G. W ramach rozwiązania wymagane są cztery jednostki radia programowalnego, komputer klasy PC oraz terminal mobilny Motorola (np. model C139). Dodatkowo wykorzystywany jest szeroki zakres urządzeń pomiarowych i dodatkowych urządzeń teleinformatycznych oraz telekomunikacyjnych. Projekt w obecnej formie skupia się na aktywnym ataku ukierunkowanym na pojedynczego użytkownika sieci 4G-LTE. Dalsze prace projektowe pozwolą na otrzymanie numeru telefonu dzięki już uzyskanemu numerowi IMSI. W następnej kolejności zostaną przeprowadzone ataki w obszarze działania technologii VoLTE. Mając kompletne oprogramowanie symulujące atak w sieci 4G-LTE, będzie możliwe wytworzenie aplikacji przeciwdziałającej atakom.

Gdansk University of Technology

POLITECHNIKA GDAŃSKA

RESEARCH PROJECT INFORMATION FOLDER – MAY 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:	**05.23.2021**
Key words:	**LTE cybersecurity LTE/VoLTE simulation attacks and defence in LTE**

PROJECT TITLE:

Realization 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 disrupting packet data transmission, including the VoLTE transmission, using open software simulating the operation of the 4G-LTE network and dedicated tools. An additional goal is to propose a method for detecting anomalies in packet traffic. The scope of the project includes operating 4G-LTE networks with the extension of speech transmission functionality within the VoLTE standard.

RESULTS:

As part of the research project, an attack scenario was prepared in the 4G-LTE network and all necessary software for its implementation was gathered. The software components needed to perform the planned attack on a dedicated PC computer included in the designed test stand have been successfully compiled and installed. As a part of the pilot study and subsequent studies, a working 4G-LTE network node was successfully created and launched by manipulating the parameters of the installed software. Then, using a dedicated application and configuring the 4G LTE network node software environment, the subscriber identification number (IMSI) was obtained.

MAIN FEATURES, FUTURE WORKS:

The presented solution is the basis for a redirection attack from 4G-LTE to the 2G network. The solution requires four software defined radios, a PC and Motorola mobile station (e.g. Motorola C139). Additionally, a wide range of measuring apparatus and additional telecommunication devices are used. The project in its current state focuses on an active attack targeting a single user of the 4G-LTE network. Further project work will allow to obtain a phone number thanks to the already obtained IMSI number. Later, attacks in the area of VoLTE technology will be launched. Having a complete software that simulates an attack in the 4G-LTE network, it will be possible to create an anti-attack protecting application.