Estudo e Avaliação de Métodos de Autenticação EAP na Infraestrutura de Redes de Telecomunicação 5G

Leonardo Azalim de Oliveira[1] **e Edelberto Franco Silva**[1]

[1]Departamento de Ciência da Computação – Universidade Federal de Juiz de Fora (UFJF)
Caixa Postal 15.064 – 91.501-970 – Juiz de Fora – MG – Brazil

{leonardo.azalim,edelberto}@ice.ufjf.br

Resumo. *As redes móveis de quinta geração (5G) tiveram sua exploração comercial iniciada em 2019. Por conta do paradigma orientado a serviços do 5G, é possível utilizar o componente 5G Core Network (5GCN) para conectar dispositivos que fazem parte das chamadas redes não-3GPP (que incluem protocolos como o WiFi). A implementação desse tipo de comunicação requer protocolos específicos que proporcionem interconectividade, autenticação e confiabilidade. Com essas características em foco, é necessário que seja feita a escolha dos algoritmos de criptografia e métodos de autenticação que serão utilizados pelos User Equipments (UEs) não-3GPP ao se conectarem à infraestrutura de 5G. Este trabalho apresenta o estado atual da investigação do tópico em questão.*

1. Introdução

Atualmente, existe suporte às tecnologias Hotspot 2.0 e Passpoint na federação gerida pela RNP. E apesar de não estarem efetivamente em funcionamento na comunidade acadêmica Eduroam no Brasil, as tecnologias adotadas no serviço embasam tal afirmativa. Por conta disso, vem se destacando o crescente interesse da RNP em se tornar membro do *hub* do consórcio OpenRoaming[1]. Porém, há de se levar em consideração alguns requisitos.

O consórcio OpenRoaming possui como um de seus principais pilares a Ciber Segurança. Ela deve atuar de forma que seja possível haver conectividade simples, segura e escalável entre as organizações que são parte do consórcio, e que seja possível realizar o *roaming* entre as milhares de redes de forma segura e criptografada.

Além da entrada no consórcio, existe também a oportunidade da expansão da área de cobertura por meio da integração da infraestrutura atual com as redes 5G. A arquitetura destas redes é definida pelo 3GPP[2], que divulga publicamente as chamadas *Releases*. As *Releases* são documentos que contém detalhes dos aspectos técnicos que servem para nortear a implementação desta tecnologia de telecomunicação em ambiente de produção.

A arquitetura conta, a partir da *Release 15*, com o grupo de componentes *5G Core Network* (5GCN) que engloba diversas funções de rede (*Network Functions* – NFs). As NFs são elementos de rede ou instâncias de *software* que são especificadas e/ou adotadas pelo 3GPP e que possuem comportamento funcional e interfaces claramente definidas. O 5GCN tem como principais objetivos, ser flexível (podendo ser virtualizado) e gerenciar os recursos de rede de forma a conectar o dispositivo do usuário (*User Equipment* – UE) à rede de dados (*Data Network* – DN) e/ou aos demais recursos disponíveis.

[1]https://wballiance.com/openroaming/
[2]https://www.3gpp.org/technologies/5g-system-overview

A partir da *Release 16*, o 3GPP incluiu as chamadas tecnologias não-3GPP à arquitetura do 5G. O principal componente da arquitetura 5G que fornece a funcionalidade de integração de redes e dispositivos não-3GPP é chamado de *Non-3GPP Inter Working Function* (N3IWF). A conexão dos UEs pode ser feita por meio de tecnologias sem fio (como o WiFi) o que, dentre outras coisas, possibilita o suporte à dispositivos legados (conhecidos como dispositivos *Non-5G Cabable* – N5GC). Desse modo, o acesso do UE não-3GPP se dá de forma que este encaminha seu tráfego para um *gateway* confiável dentro da infraestrutura da operadora de rede móvel.

Nesse contexto, estudar os métodos suportados em conjunto com os atributos relacionados e avaliar possíveis melhorias de segurança na integração de tecnologias não-3GPP é fator de suma relevância.

2. Fundamentação Teórica

Como pontos centrais deste estudo, há conceitos relacionados ao *core* 5G e aos métodos EAP, partindo-se do pressuposto que conceitos como Eduroam e WiFi não necessitariam de fundamentação teórica neste documento. Então, o *Extensible Authentication Protocol* (EAP) é um arcabouço de autenticação definido pela `RFC 5247`[3], que atualmente abrange mais de 40 métodos de autenticação distintos sendo amplamente difundido em redes de computadores, e comumente utilizado em, por exemplo, redes WiFi (onde encontra-se implementado dentro do protocolo `IEEE 802.1X`). É ele que será investigado como forma de possibilitar a autenticação do UE no 5G. Além disso, em um ambiente de produção, geralmente emprega-se uma base de dados, ou diretório, que contém atributos relacionados às credenciais de acesso do usuário ou dispositivo. Assim, os processos de autenticação e autorização giram em torno destes atributos, sendo que os métodos disponíveis nas redes 5G podem ser vistos na Figura 1.

	Client Identity Protection	Forward Secrecy / Zero Trust	Authentication	Primary Authentication
5G-AKA	Optional	Not supported	PSK (stored in USIM)	Public or Private
EAP-AKA'	Optional	Not supported	PSK (stored in USIM)	Public or Private
EAP-AKA-PFS	Optional	Mandatory	PSK (stored in USIM)	Private
EAP-TLS 1.2	Optional and slow	Optional	Certificate	Private
EAP-TLS 1.3	Mandatory	Mandatory	Certificate	Private
EAP-TTLS 1.2	Mandatory	Optional	Anything	Private
EAP-TTLS 1.3	Mandatory	Mandatory	Anything	Private

Figura 1. Principais características dos métodos EAP disponíveis nas redes 5G. Fonte: [Mattsson and Arkko 2022].

Por sua vez, no relatório técnico do projeto Brasil 6G [6G 2022b] é apresentada uma análise detalhada de soluções de código aberto para o componente 5GC da infraestrutura de 5G. Entre as possibilidades, duas chamam a atenção: Open5GS e Free5GC.

[3] `https://datatracker.ietf.org/doc/html/rfc5247`

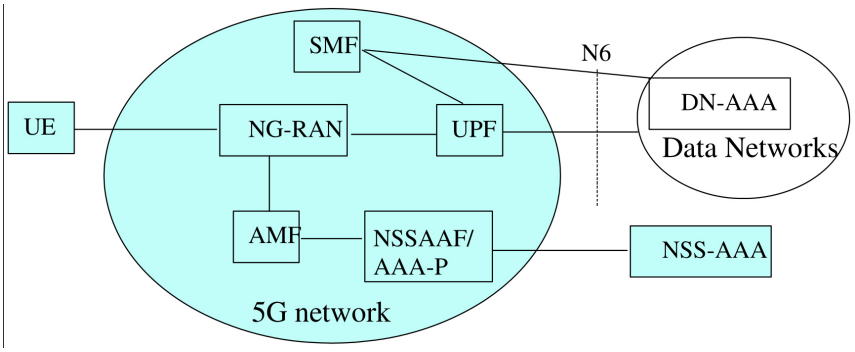

Figura 2. Arquitetura de referência dos módulos envolvidos na autenticação. Fonte: [3GPP 2023].

Como embasamento ilustrativo, a Figura 2 mostra os elementos do *core* responsáveis pela autenticação e autorização, considerando a especificação da *Release 17* [3GPP 2023].

O projeto Open5GS conta com uma boa organização do código fonte e um bom nível de documentação. Porém, com a possibilidade da inserção de um gNodeB (gNB) criado a partir de outro projeto de pesquisa [6G 2022a] e do enfoque na integração da solução com a já existente rede WiFi federada Eduroam, era obrigatória a presença do componente N3IWF. O N3IWF é importante pois no caso tanto de um gNB experimental quanto no de um UE N5GC ou mesmo de um UE conectado via WiFi, o acesso, segundo a especificação do 3GPP [3GPP 2018], deve ser realizado do mesmo modo que o de uma rede não-3GPP. Infelizmente, até a época do início das atividades deste trabalho, o referido componente não se encontrava implementado neste *core*.

Por outro lado, o projeto Free5GC possui um bom nível de modularidade e conta com uma documentação de apoio[4] que contém em boa parte tutoriais de auxílio para os usuários da solução. Este projeto possui o módulo N3IWF implementado e, como bem apontado pelo relatório, conta com uma considerável aceitação por parte da comunidade científica. Ele também possui uma licença de software mais permissiva que possibilitaria, por exemplo, a utilização de uma versão customizada do software sem a necessidade de disponibilizar publicamente o código fonte modificado.

A especificação do 3GPP em relação ao 5GC [3GPP 2018] prevê a presença de algumas NFs. Dentre estas, o presente trabalho focará na utilização daquelas diretamente relacionadas com a autenticação de UEs.

3. Resultados

Por conta das análises que foram mencionadas na Seção 2, optou-se por utilizar a solução de *core* de código aberta Free5GC. Uma instância do Free5GC foi instalada com sucesso em um ambiente de testes.

Além deste achado, é interessante comentar sobre a necessidade de integração entre credenciais dos 2 diferentes ambientes (redes móveis e redes WiFi). Uma credencial em uma rede móvel, em geral, é baseada no IMSI (*International Mobile Subscriber Identity*), porém uma identidade Eduroam é baseada na junção de identificador com *realm* (sendo este último o endereço de domínio do servidor de autenticação).

[4] `https://free5gc.org/guide/`

```
Sun May 22 00:03:13 2022: Access-Reject for user
67243139309747080wlan.mnc031.mcc724.3gppnetwork.org
stationid 84-37-D5-B3-49-F1 from _self_
(Misconfigured client: Unsupported 3G EAP-SIM
client! Rejected by <TLD>.) to eduroam01.ufpe.br
(150.161.50.4)
```

Listing 1: Exemplo de tentativa de autenticação.

De forma ilustrativa, um exemplo de tentativa de autenticação por parte de um UE (rede móvel) na rede Eduroam (WiFi) encontra-se na Listagem 1. Como é possível observar, há a necessidade da investigação da possibilidade da associação dos identificadores, porém também é necessário preservar a privacidade dos usuários. Nesse sentido, pode-se direcionar a investigação em torno da utilização do TMSI (*Temporary MSI*). Contudo, a solução definitiva para lidar com essa situação ainda encontra-se em aberto, mas possivelmente passará por alguma técnica de tradução e/ou encapsulamento de endereços.

4. Conclusão e Próximos Passos

É possível notar que, para lidar com as características disruptivas do 5G (como a mudança de paradigma e a nova arquitetura de rede), o embasamento teórico se torna ainda mais importante. O aprofundamento desse conhecimento permite maior clareza e segurança nas soluções propostas, apesar da complexidade inerente à etapa de implementação.

Como passos seguintes a esta pesquisa, pretende-se finalizar a configuração do ambiente do Core 5G juntamente com a conexão entre UE e gNB/NR para que seja possível realizar a execução de testes que compreendam as diferentes configurações de interesse. Além disso, aproveitar o ambiente para a produção de uma prova de conceito com a coleta de dados de desempenho que possibilitem uma comparação direta das configurações testadas. Por fim, estudar a fundo os métodos EAP suportados pelo 5G e verificar a possibilidade de autenticação nativa das redes móvel e também WiFi. Para o estudo deste cenário propõe-se realizar a simulação de um *handoff* entre as tecnologias.

Referências

3GPP (2018). 3gpp ts 23.502 version 15.2.0 release 15. Technical report, 3rd Generation Partnership Project.

3GPP (2023). 3gpp ts 29.561 version 17.8.0 release 17. Technical report, 3rd Generation Partnership Project.

6G, B. (2022a). Contribuições para a camada física de redes 6g. [Online]. Disponível em: https://inatel.br/brasil6g/documents/brasil6g-meta-3-atividade-3-1-camada-phy.pdf.

6G, B. (2022b). Relatório técnico das atividades 5.1 e 5.2 – projeto e seleção de componentes, plataformas, ferramentas e especificação. [Online]. Disponível em: https://inatel.br/brasil6g/documents/Brasil6G-Meta2-ComponentesPlataformaseFerramentas.pdf.

Mattsson, J. P. and Arkko, J. (2022). Extensible authentication protocol (eap) in next-generation networks.