Aspectos de Segurança Cibernética em Redes Móveis 5G

Ítalo A. S. Tacca, Evandro C. Vilas Boas, Guilherme P. Aquino

***Resumo*— A arquitetura de rede 5G traz novos desafios em segurança cibernética quando comparada às redes legadas, cujo histórico demonstra vulnerabilidades em comunicações fim-a-fim. Nesse contexto, esse trabalho apresenta uma breve discussão sobre os aspectos de segurança cibernética em redes 5G relacionados à autenticação de assinante por meio de criptografia do SUPI (*Subscriber Permanent Identifier*), processo de *Roaming* empregando o SEPP (*Security Edge Protection Proxy*) e implementação do eSIM (*Embedded Subscriber Identity Module*). Além disso, discutem-se as possíveis vulnerabilidades introduzidas pelas redes definidas por *software* e virtualização de funções de rede, assim como recomendações de implementação segura.**

***Palavras-Chave*— 5G, GUTI, SUCI, SEPP, segurança cibernética.**

***Abstract*— The 5G network architecture brings new challenges in cybersecurity compared to legacy networks, whose history demonstrates end-to-end communication vulnerabilities. Therefore, this work presents a brief discussion on cybersecurity aspects in 5G networks related to subscriber authentication through SUPI (*Subscriber Permanent Identifier*) encryption mechanisms, *Roaming* process using SEPP (*Security Edge Protection Proxy*) and eSIM (*Embedded Subscriber Identity Module*) implementation. Furthermore, vulnerabilities introduced by software-defined networks (SND) and network functions virtualization (NFV) are discussed, along with recommendations for secure deployment.**

***Keywords*— 5G, cyber security, GUTI, SUCI, SEPP.**

I. Introdução

As redes de telefonia móvel de quinta geração (5G) apresentam como principal característica a flexibilidade na alocação de recursos. Portanto, a padronização das redes 5G visa atender aos requisitos de grupos de tecnologias, serviços e aplicações emergentes em relação à latência, taxa de transmissão, número de conexões de dispositivos e extensão da cobertura geográfica para regiões remotas [1], [2]. A flexibilidade das redes 5G oferece suporte para diversas verticais de mercado com a possibilidade de alocar recursos sob demanda. A heterogeneidade de serviços e aplicações exige a introdução e integração de diferentes tecnologias para prover escalabilidade, flexibilidade e programabilidade nas redes 5G. Obtém-se essas características por meio de redes definidas por *software* (*software defined network*, SDN) e virtualização de funções de rede (*network function virtualization*, NFV), que possibilitam o fatiamento dos recursos de rede [1]. Dessa forma, isolam-se logicamente diferentes serviços e aplicações com requisitos de comunicação distintos, enquanto coexistem em uma mesma infraestrutura física.

A arquitetura de rede 5G traz novos desafios em relação a segurança cibernética quando comparada às redes legadas, cujo histórico demonstra vulnerabilidades relacionadas à segurança em comunicações fim-a-fim. A segurança no tráfego de informações (voz e dados) é um importante aspecto em redes e sistemas de telefonia móvel e não se limita somente à interceptação e modificação da informação como vulnerabilidades. Historicamente, a primeira geração de telefonia móvel (1G) não incluía aspectos de criptografia no tráfego de informações, sendo susceptível à interceptação de chamadas e a clonagem de números. Nas redes 2G, introduziram-se técnicas de criptografia, mitigando as vulnerabilidades a nível de camada física. Contudo, a exploração de vulnerabilidades em protocolos relacionados aos procedimentos de controle e sinalização revelaram a interceptação do IMSI (*international mobile subscriber identity*), mensagens de sinalização inseguras com o protocolo SS7 [3], e falsificação de estações rádio base como possíveis abordagens de ataque [4].

A transição entre o 2G e 3G introduziu o tráfego de dados e acesso à Internet banda larga. Dessa forma, as arquiteturas passaram a realizar tanto a comutação de circuito (voz) quanto de pacotes (dados). Consequentemente, as redes 3G herdaram a superfície de ataque das redes de computadores devido à comutação de pacotes [5]. Porém, implementaram-se novas soluções em segurança como a autenticação mútua entre o UE (*User Equipment*) e a rede e procedimentos para garantir a integridade das mensagens de controle [6]. Essas abordagens reduziram os riscos relacionados aos ataques de negação de serviço (*Deny of Service*, DoS). Contudo, o tráfego de dados dos usuários não possui verificação de integridade, apenas encriptação. Dessa forma, assume-se que os dados não sofram alterações e sejam conhecidos apenas pelas entidades envolvidas no processo de comunicação [7].

As redes móveis 4G estão expostas aos mesmos problemas das redes de computadores como DoS, falsificação de endereços IP (*Internet Protocol*), e acesso à identificação do usuário [8]. A ênfase na comutação de pacotes culminou em uma arquitetura baseada em IP, cujas funções de rede são facilmente acessíveis via endereçamento IP. Entretanto, aplicam-se mecanismos de segurança como regras de acesso, filtragem de pacotes e criptografia para proteger o núcleo da rede. Dentre as vulnerabilidades mencionadas, a interceptação do IMSI persistiu, pois o processo de inicialização do UE envolve a sua transmissão sem criptografia pela interface

Ítalo A. S. Tacca, Evandro C. Vilas Boas, Guilherme P. Aquino, Centro de Segurança Cibernética do Inatel (CxSC Telecom), Instituto Nacional de Telecomunicações - Inatel, Santa Rita do Sapucaí - MG, e-mail: italo_augusto@get.inatel.br, evandro.cesar@inatel.br, guilherme-aquino@inatel.br. Este trabalho foi financiado pelo Centro de Segurança Cibernética do Inatel (CxSC Telecom) do Instituto Nacional de Telecomunicações (Inatel).

aérea. Essa vulnerabilidade pode revelar a identidade e a localização do usuário, informações que podem ser utilizadas para possíveis abordagens de ataque [8].

As redes 5G apresentam diversos mecanismos de segurança para mitigar as vulnerabilidades persistentes nos processo de sinalização das redes legadas, assim como para prover proteção contra ataques cibernéticos de outra natureza. Neste trabalho, apresenta-se uma breve discussão sobre os mecanismos de segurança introduzidos nas redes 5G, estruturando-a em sete Seções. Na Seção II, discutem-se os aspectos de comunicação segura durante a autenticação do assinante no núcleo da rede 5G. Apresentam-se as soluções em comunicação segura para processos de *Roaming* na Seção III. Discutem-se os mecanismos de implementação segura do eSIM (*Embedded Subscriber Identity Module*) na Seção IV. Nas Seção V e Seção VI, abordam-se as possíveis vulnerabilidades introduzidas pelos conceitos de NFV e SDN nas redes 5G e recomendam-se abordagens para implementação segura. Por fim, apresentam-se os comentários finais na Seção VII.

II. Autenticação de assinantes

O início da comunicação entre um UE e a rede 5G inclui processos de autenticação criptográfica, envolvendo criptografia simétrica e assimétrica. Um assinante móvel é identificado em uma rede 5G por meio do seu identificador permanente (*Subscriber Permanent Identifier*, SUPI) composto por 15 dígitos no formato IMSI [9]. Os três primeiros dígitos correspondem ao código móvel do país (*Mobile Coutry Code*, MCC), seguidos pelos dois dígitos de código da rede móvel (*Mobile Network Code*, MNC) e pelos dígitos de identificação do assinante (*Mobile Subscription Identification Number*, MSIN). O SUPI também pode assumir o formato de identificador de acesso à rede (*Network Access Identifier*, NAI), sendo composto por um nome de usuário (*username*) correspondente a um identificador como IMSI, NAI, GCI (*Global Cable Identifier*) ou GLI (*Global Line Identifier*) e por um domínio (*realm*) como identificação da operadora.

A. Subscription Concealed Identifier - SUCI

O envio do SUPI no formato IMSI inclui o uso de esquemas de criptografia assimétrica baseada em curvas elípticas (*Elliptic Curve Integrated Encryption Scheme*, ECIES) para encriptar o MSIN [10]. O resultado desse processo é combinado com o MCC e o MNC, que permanecem em texto claro, formando o identificador oculto do assinante (*Subscription Concealed Identifier*, SUCI) [9]. Na Figura 1, apresentam-se os seis campos que compõem o SUCI.

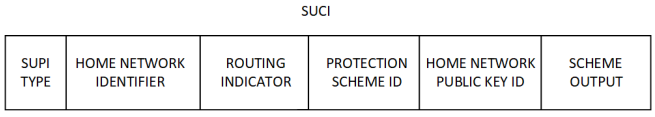

Fig. 1. Campos do identificador SUCI

O campo SUPI *type* indica o formato do SUPI e assume oito possíveis valores, sendo 0 - IMSI, 1 - NAI, 2 - GLI e 3 - GCI. Os demais valores são reservados para uso em novos formatos. O campo *Home Network Identifier* identifica a rede doméstica do assinante (MCC e MNC para formato IMSI e nome de domínio para formato NAI). O campo *Routing Indicator* assume valores decimais entre um e quatro dígitos provisionados pela aplicação USIM (*Universal Subscriber Identity Module*) presente no cartão SIM. Esse campo é utilizado em conjunto com o *Home Network Identifier* para possibilitar o roteamento das mensagens de sinalização da rede para as funções de autenticação e gerenciamento de dados presentes no núcleo da rede [9].

O campo *Protection Scheme ID* é formado por 15 dígitos e indica qual tipo de processo de encriptação é empregado na transmissão do SUCI [11]. Especificaram-se dois esquemas denominados de *Profile A* e *Profile B*, sendo possível não empregá-los em uma abordagem de proteção nula, não recomendada. Uma quarta abordagem considera um processo especificado pela HPLMN (*Home Public Land Mobile Network*). O valor do campo *Protection Scheme ID* varia de acordo com o esquema implementado: 0x00 - esquema nulo; 0x01- *Profile A*; 0x02 - *Profile B*; e 0xC à 0xF - esquemas de proteção especiais definidos pela operadora. Reservaram-se os demais valores para esquemas de encriptação futuros. O campo *Home Network Public Key Identifier* carrega a identificação da chave pública utilizada no processo de encriptação, cujos valores possíveis estão entre 0 e 255. O campo *Scheme Output* contém o resultado do processo de encriptação para o MSIN (formato IMSI) ou nome de usuário (formato NAI). Esse campo pode assumir formato de *string* ou número em uma base hexadecimal.

O SUPI é enviado pelo UE apenas quando o assinante não possui um identificador temporário único global (*Globally Unique Temporary Identity*, GUTI) associado ao cartão SIM. O GUTI é provido pela função de gerenciamento de mobilidade e acesso (*Access and Mobility Management Function*, AMF) e tem como objetivo fornecer uma identificação temporária ao UE [12]. Dessa forma, mantêm-se o SUPI em anonimato durante os processos de sinalização entre UE e a rede. A AMF oferece um novo GUTI para um UE sempre que recebe uma mensagem de requisição de registro inicial ou periódica, ou ainda, ao receber uma mensagem em resposta à uma solicitação de *paging* [11].

B. Elliptic Curve Integrated Encryption Scheme - ECIES

Para implementar a criptografia do SUPI quando é necessário enviá-lo pela rede, o UE emprega o esquema de criptografia assimétrica ECIES [10]. Considera-se o uso de funções e algorítimos associados em esquemas de criptografia e decriptografia entre duas entidades no processo de comunicação. Dessa forma, realiza-se um acordo de chaves baseado em Diffie-Hellman para se estabelecer um canal de comunicação seguro, por onde o identificador do assinante pode ser transmitido.

No processo de criptografia, definem-se as funcionalidades KA (*Key Agreement*), KDF (*Key Derivation Function*), ENC (*Encryption*), MAC (*Message Authentication Code*) e *Hash*. A função KA gera senhas compartilhadas entre as entidades no processo de comunicação, a função KDF permite obter o conjunto de chaves pública e privada, o algoritmo ENC

introduz a criptografia simétrica, o algoritmo MAC origina uma tag de autenticação e o *Hash* opera sobre o MAC e KDF para obter parâmetros *Hash* de comprimento fixo.

Considerando a comunicação entre duas entidades A e B, ambas entidades possuem um par de chaves privada (PR-A e PR-B), sendo as respectivas chaves públicas (PU-A e PU-B) derivada da operação entre a chave privada e um gerador de curva elíptica (G): PU-A = PR-A*G e PU-B = PR-B*G. As chaves públicas são temporárias e geradas aleatoriamente. Após gerar a chave pública, a entidade A usa a função KA para obter uma senha secreta para compartilhamento, empregando o produto escalar entre a PR-A e a PU-B. Aplica-se esse resultado à função KDF para derivar a chave de criptografia simétrica (kENC) e chave MAC (kMAC). O algoritmo ENC emprega a kENC para encriptar o texto claro, resultando na mensagem C. A função MAC emprega a kMAC e a mensagem C para obter a *tag* de verificação de integridade da mensagem. Posteriormente, concatena-se a mensagem C com a PU-A e a *tag*.

Na recepção, a entidade B extrai a mensagem C, a PU-A e a *tag* do criptograma recebido. Por conseguinte, utiliza-se a função KA para obter o produto escalar entre a PR-B e PU-A, cujo resultado esperado deve ser idêntico ao obtido no processo de criptografia. Dessa forma, aplica-se o valor à função KDF para derivar a kENC e a kMAC. Utilizando a função e fornecendo a mensagem C e a kMAC, obtêm-se a *tag* de verificação de integridade para fins de comparação com a *tag* recebida. Caso sejam iguais, a entidade B segue com decriptografia da mensagem C por meio da função ENC utilizando a kENC. Caso contrário, descarta-se o criptograma e assume-se falha na verificação MAC, indicando possível violação da mensagem.

Considera-se o ECIES como um processo de criptografia seguro aplicado ao processo de autenticação do UE, sendo robusto à ataques de força bruta. Contudo, abordagens modernas como emprego do aprendizado de máquina podem comprometer a segurança do processo de autenticação e expor o SUPI [13]. Nesse tipo de ataque, treina-se um algoritmo para reconhecer padrões de encriptação baseado no esquema ECIES, utilizando-o para obter o SUPI que gerou o SUCI em intervalos de minuto. Portanto, verifica-se uma vulnerabilidade no processo de proteção do SUPI em redes 5G, mesmo que o identificador seja enviado apenas no início da comunicação.

III. *Roaming*

O *Roaming* é um processo que permite ao assinante se comunicar fora da área de cobertura de sua rede doméstica por meio de uma rede visitada. Essa comunicação é pautada por uma troca de sinalização entre a rede doméstica e a visitada. Durante esse processo, empregam-se protocolos de comunicação que podem não possuir mecanismos de segurança. Logo, verificam-se vulnerabilidades principalmente quando se envolvem redes IP externas ao domínio das operadoras. Dentre os protocolos de comunicação empregados no *Roaming* em redes legadas, tem-se o protocolo SS7 (*Signalling System No.7*) introduzido nas redes 2G e 3G e o protocolo *Diameter* aplicado às redes 4G.

O protocolo SS7 caracteriza-se por não implementar aspectos de segurança na comunicação como criptografia e autenticação. O protocolo *Diameter* substitui o SS7 em redes 4G e também possui falhas de segurança, pois a encriptação obrigatória nas mensagens é feita ponto-a-ponto ao invés de fim-a-fim. Dessa forma, viabiliza-se a interceptação por substituição de uma fonte de requisições legítimas por outra fraudulenta [14]. No 4G, tem-se a possibilidade de empregar o *Voice over LTE* (VoLTE) como recurso para transmissão de chamadas por meio de pacote de dados e uso de protocolo IP, garantindo os aspectos de comunicação segura. Contudo, os requisitos de qualidade de serviço para operação do VoLTE dificultam seu uso pelas redes 4G, que se apoiam em redes 2G e 3G coexistentes para realizar processos de *Roaming* durante encaminhamento de chamadas [15]. Novamente, emprega-se o protocolo SS7 e expõem-se a comunicação às suas vulnerabilidades de segurança.

Nas redes 5G, as implementações *Non Standalone* (NSA) e *Standalone* (SA) derivam análises distintas para os processos de segurança no *Roaming*. O 5G NSA reutiliza os recursos do núcleo das redes 4G e, portanto, sujeita-se às vulnerabilidades encontradas no processo de sinalização de *Roaming* empregando o protocolo *Diameter* e eventualmente o SS7. O 5G-SA introduz novas funcionalidades por meio do *New Generation Core* (NGC) com o objetivo de incrementar a segurança, além da utilização de novos protocolos para sinalização nos processos de *Roaming*. O 5G SA utiliza o SEPP (*Security Edge Protection Proxy*) para estabelecer conexões seguras com núcleos de redes externas para a troca de mensagens de sinalização através dos mecanismos disponibilizados pelos protocolos TLS (*Transport Layer Security*) e IPsec (*IP Security*). O SEEP age como uma espécie de *gateway* ou *firewall* de borda.

A comunicação entre as funções de rede do 5G baseia-se no modelo cliente/servidor do HTTP. Dessa forma, o SEPP protege o tráfego de sinalização do plano de controle entre diferentes 5G-PLMNs (*5G Public Land Mobile Network*) durante o *Roaming*. O SEPP realiza a filtragem de pacotes, a autenticação ponta a ponta, a criptografia da conexão, incluindo a negociação e o gerenciamento de chaves, e a ocultação de topologia, limitando a visibilidade que as partes externas da rede têm da topologia interna. Essa última funcionalidade evita que atacantes explorem a topologia da rede e obtenham informações sensíveis sobre as funções implementadas [11]. A filtragem de pacotes no SEPP inclui a validação dos endereços de origem e destino das mensagens e verificação de autorização do uso de números de identificação pelo SEPPs de outras PLMNs. As taxas de comunicação podem ser controladas para evitar sinalização excessiva, incluindo possíveis ataques de DoS [11].

Para estabelecer comunicação segura entre funções de rede diferentes, define-se uma interface lógica denominada N32 através dos SEPPs e IPXs (*IP Exchange Services*) das respectivas redes produtoras (pSEPP e pIPX) e consumidoras (cSEPP e cIPX) de serviços. Essa comunicação utiliza a criptografia JWE (JSON *Web Encryption*) para proteger mensagens contra ataques de *eavesdropping* e de repetição. Além disso, os IPXs podem realizar modificações de acordo com uma

política de modificação especificada pelas redes, que devem ser registradas e assinadas digitalmente pelo mecanismo JSON *Web Signature* (JWS). Caso um IPX intermediário não suporte encriptação, utiliza-se o protocolo TLS para proteger as mensagens de sinalização [11].

As redes 5G implementam procedimentos de segurança sobre as mensagens de sinalização trocadas entre duas PLMNs distintas, protegendo tanto os dados trafegados quanto suas topologias lógicas. Vale destacar, que protocolos JWS e TLS utilizados para a troca de mensagens de sinalização foram concebidos inicialmente para aplicações de redes de computadores clássicas. Portanto, deve-se analisar suas vulnerabilidades e consequências de uso em redes 5G, considerando o impacto na segurança geral da rede.

IV. *Embedded Subscriber Identity Module* - eSIM

O eSIM (*Embedded Subscriber Identity Module*) é uma solução com foco no UE, que tem como objetivo simplificar e tornar seguros o processo de conexão entre assinante e operadora, e diferentemente dos cartões SIM tradicionais, pode ser embarcado no UE com a utilização de eUICC (*Embedded Universal Integrated Circuit Card*). Para isso, verificam-se duas soluções na implementação do eSIM, sendo uma abordagem para aparelhos celulares e outra para aplicações M2M (*machine-to-machine*). Essas soluções apresentam arquiteturas distintas em relação à organização das funções.

O eSIM provê funções tradicionais de autenticação e acesso à rede, contratação de serviços de diferentes operadoras, uso de múltiplos perfis de usuário e fácil integração com dispositivos IoT (*Internet of Things*) [16]. Esse conjunto de novas funcionalidades introduzem vulnerabilidades em sua utilização. Por exemplo, utiliza-se o recurso de atualização de perfis de assinante ou provisionamento remoto sempre que necessário implementar um novo perfil de usuário. Nesse processo, deve-se garantir a integridade e confidencialidade dos perfis entre o momento em que é criado pela operadora e o armazenamento no dispositivo do assinante.

As abordagens de implemetação do eSIM fazem uso de métodos de criptografia baseados em PSK (*Pre-Shared Key*), solução M2M, e PKI (*Public Key Infrastructure*), aparelho móvel. Ambas soluções exigem um CI (*Certificate Issuer*) para prover comunicação segura e autenticação mútua através da emissão de certificados digitais. Assim como o eUICC, que inclui alguns elementos para implementação dos processos de comunicação e armazenamento seguro de dados, denominados de domínios.

O ECASD (*Embedded UICC Controlling Authority Security Domain*) é responsável pelo armazenamento seguro das credenciais utilizadas para os diferentes níveis de segurança nos outros domínios. Logo, contém chaves privadas para assinaturas digitais, certificados de associação para autenticação do eSIM e chaves públicas de autenticação na rede. O ISD-P consiste em um domínio seguro para armazenamento dos perfis do assinante, evitando a visualização por componentes externos à estrutura interna. O ISD-R, é o domínio responsável pela criação de novos ISD-Ps e pelo gerenciamento de ISD-Ps. O MNO-SD se comporta como uma espécie de representante da operadora no chip, contendo as chaves OTA (*Over-The-Air*) da operadora que possibilitam estabelecer canais seguros para atualizações no eSIM. O *Telecom Framework* provê algoritmos de autenticação padronizados para os NAAs (*Network Access Application*) armazenados nos ISD-Ps [17].

As funções de rede utilizam autenticação mútua para o transporte seguro dos perfis. Portanto, transportam-se os perfis pela rede móvel e carregam-nos no eUICC do assinante apenas após estabelecimento de uma autenticação mútua baseada em encriptação entre o servidor de provisionamento e o UE [17]. Essa autenticação pode ser feita utilizando um ECKA-DH (*Elliptic Curve Key Agreement based on Diffie-Hellman*) ou ECKA-EG (*Elliptic Curve Key Agreement based on ElGamal*). Com o acordo de chaves, um canal de comunicação seguro é estabelecido utilizando criptografia simétrica [18].

Apesar dos procedimentos de segurança por meio de autenticação, a tecnologia possui vulnerabilidades. Caso um atacante obtenha uma posição privilegiada na rede, pode-se utilizar dessa vantagem para realizar ataques aos assinantes por meio do envio de perfis não solicitados, comprometendo a segurança das informações e a privacidade dos usuários. Embora seja pouco provável, um ataque dessa natureza depende de aspectos de segurança de outras funções da rede 5G, e até mesmo das políticas de segurança da operadora. Além disso, assinantes maliciosos ou *malwares* podem realizar deleções de perfis no UE e sucessivas solicitações de provisionamento remoto, ocasionando sobrecarga no servidor e a sua inoperação, deixando solicitações legítimas sem resposta [19].

V. Redes definidas por software e virtualização de funções de rede no 5G

A introdução do conceito de SDN nas redes 5G permite realizar a separação dos planos de controle (plano de sinalização) e dados (plano de usuário). Essa abordagem garante as características de flexibilidade e programabilidade das redes 5G em conjunto com outras tecnologias. O plano de controle é responsável por coordenar a dinâmica geral da rede, comportando o tráfego de funções de roteamento, com a decisão de encaminhamento de pacotes, e da aplicação de políticas de qualidade de serviço e segurança. Tem-se como figura central o controlador, um dispositivo que domina todos os nós da rede. Já o plano de dados transporta a informação das aplicações em execução na infraestrutura. Por isso, é onde atuam as funções tradicionais de segurança como *firewalls* e dispositivos de detecção de intrusão [20].

O controle centralizado introduz a possibilidade de um atacante controlar toda a rede. Enquanto, a programabilidade pode ocasionar vulnerabilidades em caso de implementação inconsistente de isolamento de tráfego e dos recursos. Para mitigar estes riscos, deve-se isolar funções de acordo com o nível de sensibilidade a segurança e exposição, delimitando domínios. Além disso, incluí-se o controle de acessos por meio de uma estrutura de identificação que permita a autenticação do usuário, garantindo a segurança principalmente de funções de controle e de dados usados para a tomada de decisões [21].

A infraestrutura NFV é composta pelas funções de rede virtualizadas (*Virtualized Network Functions*, VNFs), orquestrador NFV, gerenciador NFV e o gerenciador de infraestrutura

virtual (*Virtual Infrastructure Manager*, VIM). O orquestrador NFV coordena a execução dos elementos da arquitetura. Enquanto o gerenciador é responsável pelo ciclo de vida das funções virtualizadas, incluindo a criação e configuração. O VIM aloca recursos físicos e virtuais de computação, de armazenamento e de rede da infraestrutura para as VNFs.

Essa infraestrutura de rede pode herdar vulnerabilidades tanto da infraestrutura de virtualização quanto das funções e protocolos de rede. Por exemplo, a falha de isolação possibilita a um agente malicioso invadir o hipervisor hospedeiro e executar uma série de ataques que inicialmente comprometem uma ou mais VNFs e, posteriormente, a interface de gerenciamento desse hipervisor. VNFs comprometidas podem ser utilizadas para disparar ataques DoS, interrompendo os serviços da própria infraestrutura. Outras vulnerabilidades podem existir de acordo com o tipo de aplicação e protocolos de rede implementados nas VNFs [22].

No contexto das redes 5G, há recomendações contidas na TR 33848 para prover segurança em uma infraestrutura baseada em NFV. Inclui-se a definição de domínios confiáveis com a separação de funções com base na sensibilidade à segurança. Dessa forma, isolam-se funções com níveis críticos de segurança e exposição de outras funções. Consideram-se a separação física de equipamentos para reduzir o nível de intrusão de um atacante em caso de invasão e programas das VNFs para maior controle sobre o tráfego. Deve-se restringir os recursos físicos para evitar que as VNFs tenham acesso direto a esses recursos no hospedeiro. Assim como, implementar o bloqueio da camada de virtualização e o uso de criptografia, para que apenas as comunicações necessárias aos serviços das VNFs sejam realizadas. O privilégio de administrador e tempo de sessão devem ser restritos, com monitoramento e registro de atividades. Além disso, recomenda-se executar as funções de administração e segurança em *hardwares* separados, considerando-as críticas [23]. Logo, aplicam-se políticas de segurança no ambiente NFV tanto a nível físico quanto virtual. Assegura-se a implementação adequada das funções utilizadas e das configurações do hipervisor, eliminando a violação do perímetro das VNFs e exploração de privilégios de acesso não autorizado em qualquer ponto da infraestrutura.

VI. Conclusões

Esse trabalho apresentou uma breve discussão sobre os mecanismos de segurança implementados nas redes 5G. Abordou-se o processo de autenticação do assinante, ressaltando uso do esquema de criptografia ECIES para transmissão segura do SUCI. Verificou-se o uso do SEPP para viabilizar o processo de *Roaming*. Enquanto, explorou-se os aspectos de arquitetura segura do eSIM. Em relação aos conceitos de SDN e NFV, discutiram-se pontos de vulnerabilidades e recomendações para implementação segura. Por fim, verificou-se que a padronização das redes 5G introduziu mecanismos de comunicação segura fim-a-fim. Contudo, a evolução dos ataques cibernéticos demandaram a evolução dessas abordagens.

Agradecimentos

Os autores agradecem ao Centro de Segurança Cibernética do Inatel (CxSC Telecom) do Instituto Nacional de Telecomunicações (Inatel) por fomentar esse trabalho e ao Inatel por prover os meios necessários à sua realização, assim como o suporte da empresa Huawei.

Referências

[1] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View," *IEEE Access*, vol. 6, pp. 55 765–55 779, 2018.

[2] J. Hwang, L. Nkenyereye, N. Sung, J. Kim, and J. Song, "IoT Service Slicing and Task Offloading for Edge Computing," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 526–11 547, 2021.

[3] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash, and H. Abbas, "SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1337–1371, 2020.

[4] M. Pannu, R. Bird, B. Gill, and K. Patel, "Investigating vulnerabilities in GSM security," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 2015, pp. 1–7.

[5] C. Landwehr and D. Goldschlag, "Security issues in networks with Internet access," *Proceedings of the IEEE*, vol. 85, no. 12, pp. 2034–2051, 1997.

[6] D. Caragata, S. El Assad, C. Shoniregun, and G. Akmayeva, "UMTS security: Enhancement of identification, authentication and key agreement protocols," in *2011 International Conference for Internet Technology and Secured Transactions*, 2011, pp. 278–282.

[7] M. Khan, A. Ahmed, and A. R. Cheema, "Vulnerabilities of UMTS Access Domain Security Architecture," in *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2008, pp. 350–355.

[8] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[9] 3GPP, "Numbering, addressing and identification," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.003, 03 2021, version 17.1.0.

[10] L. H. E. V. Gayoso Martínez and C. S. Ávila, "A Survey of the Elliptic Curve Integrated Encryption Scheme," in *JOURNAL OF COMPUTER SCIENCE AND ENGINEERING*, vol. 2, no. 2, 2010, pp. 7–13.

[11] 3GPP, "Security architecture and procedures for 5G System," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 33.501, 04 2021, version 17.1.0.

[12] 3GPP, "System architecture for the 5G System (5GS)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501, 03 2021, version 17.0.0.

[13] V. H. Tea, "Unmasking Concealed 5G Privacy Identity with Machine Learning and GPU in 12 mins," in *TechRxiv*, 11 2020.

[14] Positive Technologies, "Diameter Vulnerabilities Exposure Report," Positive Technologies, Technical Report, 2018.

[15] O. Kadatskaya and S. Saburova, "Research of requirements to QoS for voice over LTE," in *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, 2014, pp. 135–138.

[16] GSMA, "eSIM Whitepaper," GSM Association (GSMA), Whitepaper, 03 2018.

[17] GSMA, "RSP Technical Specification," GSM Association (GSMA), Technical Specification (TS) SGP.22, 06 2020, version 2.2.2.

[18] G. S. for Mobile Communications Association, "Embedded SIM Remote Provisioning Architecture ," GSM Association (GSMA), Technical Specification (TS) SGP.01, 07 2020, version 4.2.

[19] GSMA, "RSP Architecture," GSM Association (GSMA), Technical Specification (TS) SGP.21, 09 2017, version 2.2.

[20] G. Pujolle, "Software Networks: Virtualization, SDN, 5G, and Security," in *Advanced Networks Set*, vol. 1, 2020, pp. 15–48.

[21] ONF, "Principles and Practices for Securing Software-Defined Networks ," Open Networking Foundation, Technical Report (TR) 511, 01 2015, version 1.0.

[22] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[23] 3GPP, "Study on security impacts of virtualisation," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 33.848, 06 2021, version 0.8.0.