VoWiFi Security: An Exploration of Non-3GPP Untrusted Access via Public ePDG URLs

F. Zampognaro[1,2,*], D. Verde[3] and G. Bianchi[2,4]

[1] *Link Campus University, Rome, IT*
[2] *University of Rome "Tor Vergata", Rome, IT*
[3] *RomARS s.r.l., Rome, IT*
[4] *CNIT National Network Assurance and Monitoring (NAM) Lab, Rome, IT*

Abstract

Mobile cellular operators strategically view the integration of alternative access technologies, such as Wi-Fi, as essential measures to augment network capacity, enhance service delivery, and ensure a seamless and comprehensive user experience. Voice over Wi-Fi (VoWiFi), a.k.a. Wi-Fi calling, is available in LTE networks via an Evolved Packet Data Gateway (ePDG), accessible through an untrusted public Internet connection which, as such, mandates for security protection during setup. This paper assesses the security of real-world VoWiFi publicly accessible services. After identifying available ePDG URLs for 2523 worldwide mobile network operators, we subsequently tested the 340 ePDGs that provided a response. For each of these, we assessed the possible presence of security criticalities by suitably crafting the messages exchanged during the establishment of IPsec/IKEv2 security associations. Our findings reveal that at least 18% of these gateways accept deprecated (sometimes also broken) ciphers and more than 30% support small-sized (1024 bits or less) Diffie-Hellman groups. These results provide valuable insights into the security posture of convergence technologies, pinpointing areas where critical enhancements are imperative to mitigate potential risks.

Keywords

4G, non-3GPP, Security, VoWiFi, WiFi Calling

1. Introduction

In their historical evolution, cellular networks have consistently aimed to expand their reach and accessibility. This includes efforts to enable access through technologies, such as WiFi, *alternative* to the Radio Access Network standardized by the 3rd Generation Partnership Project (3GPP), and called non-3GPP access. The initial steps to standardize IP-based access through Public Internet Service Providers (ISPs) date back to more than 20 years ago during the 3G era, specifically, 3GPP Rel. 6. However, in practical terms, this early effort was at that time not deemed practically or commercially exploitable by 3G operators.

It wasn't until the advent of LTE networks that this capability began to see deployment, mainly taking the form of the Voice over Wi-Fi (VoWiFi) service, often commercially referred to as Wi-Fi Calling. VoWiFi, as its name implies, enables voice calls to be handled as standard cellular calls, but carried using legacy Wi-Fi access networks and public Internet Service Providers. This service thus introduces alternative pathways for users to connect to mobile networks, extending beyond the confines of traditional cellular networks.

VoWiFi is a great opportunity for mobile network operators to offload the licensed radio spectrum used by the Radio Access Network (RAN), to extend their service over unlicensed Wi-Fi bands, and to reduce the roaming necessity with other licensed operators. Thanks to Wi-Fi Calling via non-3GPP access, User Equipments (UEs) can initiate and receive phone calls using the same subscriber mobile number even in areas with poor coverage, such as underground facilities, large indoor areas with thick walls (e.g., malls, industries), private homes, or via public hot-spots (e.g., in Airports, or Hotels abroad).

ITASEC 2024: The Italian Conference on CyberSecurity

[*] Corresponding author.

zampognaro@ing.uniroma2.it (F. Zampognaro); verde@romars.tech (D. Verde); giuseppe.bianchi@uniroma2.it (G. Bianchi)

Importantly, this is achieved without the need for installing additional applications, as virtually all modern smartphones today include native non-3GPP access procedures.

On a more technical standpoint, there are actually two distinct types of non-3GPP access modes: trusted access, for scenarios where a Mobile Network Operator (MNO) deploys a protected Wi-Fi access point, and untrusted access, i.e. when the service is provided by a third-party (e.g., public) Wi-Fi access via a public Internet connection. In this paper, we focus on this second scenario. Here, the untrusted nature of such approach refers to the fact that the mobile operator has neither control nor, at least in principle, knowledge on the security mechanisms of the specific access network used. This requires the User Equipment (UE) to access the MNO Core Network via a dedicated gateway exposed on the Internet, which is part of the MNO domain and responsibility. These endpoints engage in the setup of an end-to-end security association, to setup both Control plane and User Plane communication

In 4G/LTE networks, this Internet-accessible entry point to the operator's core network is a component named evolved Packet Data Gateway (ePDG) which is reachable at a conventional URLs[1] defined in [1] as:

$$\texttt{epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org} \tag{1}$$

It is worth noting that other ways to provide or announce available ePDGs to the UEs are possible, by means of alternative mechanisms such as static configurations, Protocol Configuration Options (PCO) signaling, local or roaming-based DNS resolutions[2]. Nonetheless, the explicit naming convention presented in (1), called PLMN method, appears to be the most used approach and included in fact in commercial Smartphones (determined by inspection of traffic from real Smartphones contacting the corresponding ePDG).

Starting from 5G (3GPP release 15), the ePDG has evolved into the so-called Non-3GPP Inter Working Function (N3IWF), a function which has the same logical role of the ePDG but provides slightly different and more general access procedures [2]. Both ePDG and N3IWF show commonalities in the protocols in use (IKEv2 and ESP [3]), and the sequence of messages exchanged. Furthermore, at least in its early deployment, N3IWF is supposed to be used to offer the same VoWiFi service already enabled by ePDG. For N3IWFs, the naming convention is similar, and defined as follows:

$$\texttt{n3iwf.5gc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org} \tag{2}$$

In this context, our goal is to test the security posture of ePDGs and N3IWF accessible through the Internet. Acting as a gateway, these can potentially represent a privileged access door to the MNO internal infrastructure, posing risks to both the operator's service and user privacy, if not implemented correctly.

1.1. Motivation, methodology and contribution

In related previous work on VoWiFi security, such as [4, 5], authors have addressed practical attacks aiming at denying the service with e.g., DNS interception, IKE_INIT_SA spoofing/ mangling or exploiting NAT or handover limitations. They also have shown how sensitive data such as the IMSI can be gathered. Nonetheless, the main focus of such works is on attacks involving rogue ePDGs or Access Points, targeting the UE, with only a few real ePDGs tested and without a focus on the cryptographic establishment of the security association.

This paper instead is motivated by two main questions not answered yet: i) what is the deployment status of VoWiFi/non-3GPP untrusted access gateways? and, especially, ii) what is the security posture of all these publicly exposed entry points?

To respond to the first question, we have developed a Python crawler devised to test whether, for each operator tested, an URL in the format (1) or (2) can be resolved by performing DNS queries[3]. 2523

[1] To make an example, Vodafone Italy MNO has been assigned $MCC = 222$ and $MNC = 10$; an LTE UE with a USIM of that MNO will thus try connect to `epdg.epc.mnc010.mcc222.pub.3gppnetwork.org`

[2] See as reference the source code of Android: http://tinyurl.com/55jy7re4

[3] https://github.com/francozamp2/epdg_n3iwf_discoverer

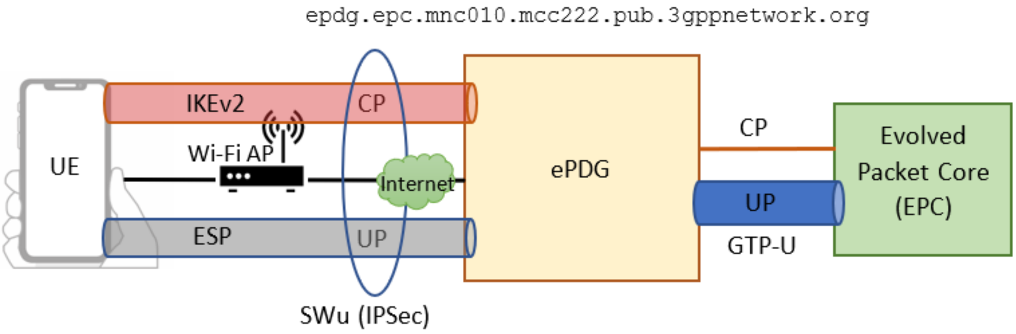

epdg.epc.mnc010.mcc222.pub.3gppnetwork.org
UE
IKEv2
CP
Wi-Fi AP
Internet
ESP
UP
SWu (IPSec)
ePDG
CP
UP
GTP-U
Evolved Packet Core (EPC)

Figure 1: Simplified LTE non-3GPP access Control and User Plane configuration (ePDF URLs example, with MNC/MCC values of Vodafone Italy)

valid combinations of MNC/MCC value pairs of real MNOs worldwide can be defined, considering the MNO list available at https://www.mcc-mnc.com after removing testing and internal MNC values ($MNC = 299$ “Failed Calls” and $MNC = 999$ “Fix Line”). This list has been used as input to the crawler.

By running the crawler we have obtained 340 successful Domain Name resolutions for ePDGs out of the 2523 MNOs identified. That means at least 13.5% of the LTE MNOs worldwide have enabled the optional non-3GPP untrusted access. Instead, at the time of writing, just one N3IWF entry resulted with a valid DNS entry ($MCC = 230$, $MNC = 1$ –“T-Mobile”). Nonetheless, the corresponding N3IWF is not responding to any access requests, so it is assumed in an internal testing mode or geo-blocking requests from other countries.

We then started a comprehensive assessment of the identified LTE ePDGs available worldwide, to respond to the second question. For obvious reasons, our testing strategies are *minimally invasive* and are on purpose limited to testing the configurations of operational gateways that can be inferred by the servers’ response, i.e., without trying to dig further into access attempts. The results discussed in detail in the remainder of the paper show quite significant misconfigurations (such as usage of obsolete or weak cipher suites, or poor protection to Denial of Service attacks), which appear to be at the base of potential security concerns.

Despite having been tested exclusively with real LTE ePDGs so far, it is important to emphasize that our techniques can easily be adapted for testing future N3IWF deployments, as well as extended to assess more possible vulnerabilities. The results of our research hold significance for the early identification of threats and the formal validation of ePDGs and future N3WIFs. This applies both in laboratory setups during the development and configuration of the service, in preparation of the final deployment in testing environments, and if already in production, to ascertain potential upgrades or fixes.

2. Untrusted access overview

In the rest of the paper, we assume that the reader is provided with a baseline background on the working principles and architecture of the 4G Evolved Packet Core (EPC) [6] and the IPSec protocol suite [3]. For completeness, in the Appendix of this paper, we have included supplementary technical details on untrusted non-3GPP type of access in LTE.

For LTE non-3GPP untrusted access, UE connectivity is realized with the ePDG via an Access Network or Internet Service Provider not under the control of the MNO, and without trust on security and confidentiality mechanisms available therein. For this reason, IKEv2 is used to establish a security association between the UE and the ePDG, with the goal of protecting Control Plane (CP) and User Plane (UP) connections, as shown in figure 1. The established security association permits to safely exchange authentication credentials and performs access to the network using USIM/eSIM secrets (Control Plane), in the same way as it is done with the traditional radio access over RAN. After the authentication and access, secure IP data communication via the UP is possible directly between the UE and the ePDG via ESP (i.e., an IPSec tunnel). That tunnel can then be used for instance to carry the IP packets of the VoWiFi service. To provide more details, the untrusted non-3GPP access is best presented via a sequence of simplified stages which are shown in figure 2.

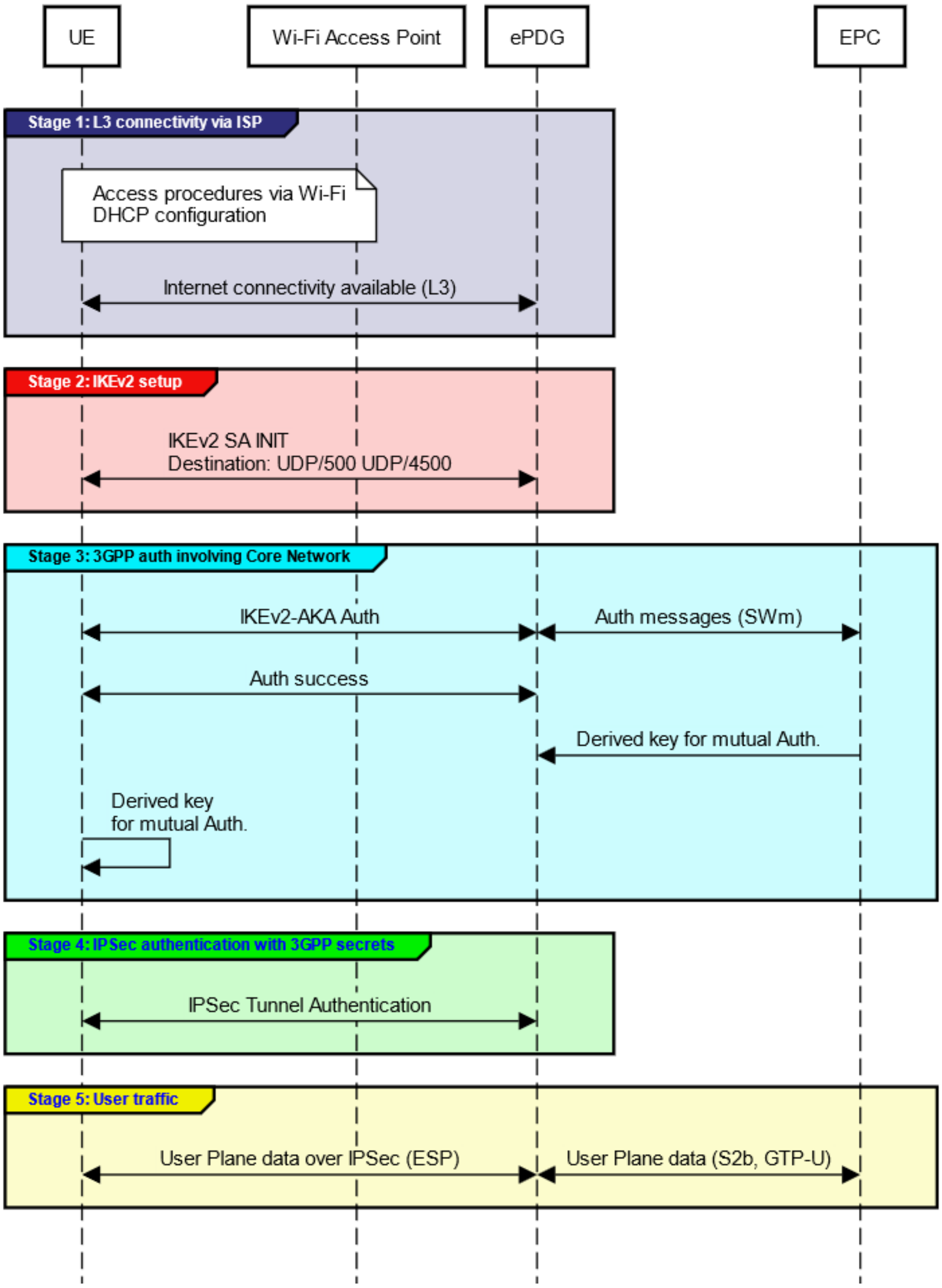

UE
Wi-Fi Access Point
ePDG
EPC
Stage 1: L3 connectivity via ISP
Access procedures via Wi-Fi
DHCP configuration
Internet connectivity available (L3)
Stage 2: IKEv2 setup
IKEv2 SA INIT
Destination: UDP/500 UDP/4500
Stage 3: 3GPP auth involving Core Network
IKEv2-AKA Auth
Auth messages (SWm)
Auth success
Derived key for mutual Auth.
Derived key
for mutual Auth.
Stage 4: IPSec authentication with 3GPP secrets
IPSec Tunnel Authentication
Stage 5: User traffic
User Plane data over IPSec (ESP)
User Plane data (S2b, GTP-U)

Figure 2: Simplified untrusted non-3GPP access procedure steps

The first stage regards obtaining access to the internet via the Wi-Fi access point to which the UE is connected, including L2 authentication (e.g., WPA2) or other authentication mechanisms outside the control of the MNO. Firewalls at the UE side or at the Core Network side must not prevent the use of UDP destination ports 500 and 4500. The second stage involves the establishment of an IKEv2 secure association between the UE and the ePDG. The cipher suites used during the subsequent data transfer are agreed upon at this stage.

Stage 3 involves the interaction with the Core Network (EPC), which is the only other entity owning the UE secrets included in its USIM. Such credentials never leave the designated NFs of the Core network (i.e., the HSS), nor the USIM, and are verified end-to-end with derived keys. This procedure ensures that the UE is entitled to access the MNO network and is performed using the normal EAP-AKA procedure over IKEv2. Next, derived key material from the EPC side and the UE side is calculated. The former is sent by the EPC to the ePDG in preparation for the following stage.

In stage 4, the IPSec security association is finalized by performing mutual authentication using the derived keys obtained as discussed in the previous stage via the IKEv2 protocol. Following a successful mutual authentication, a tunnel is established and data plane traffic can be exchanged between the UE and the PDN of the EPC (stage 5).

In the present study, to ensure minimal invasiveness, we restricted our testing to involve only stage 2. Methods to extend tests and delve deeper into the setup procedure without appearing as a potential threat to the involved operators remain a subject for future research.

3. Security assessment of ePDGs

Using the methodology presented in section 1.1, we have identified 340 successful Domain Name Server (DNS) resolutions out of the known active 2523 MNOs. Anyway, a DNS resolution can be a single IP address, or several IP addresses in case of load balancing enforced by the MNO to distribute UE requests to multiple ePDGs. Indeed, the total number of IP addresses resolved by the Python crawler for available ePDGs was 695. The key idea developed in this work is to perform a non-invasive security assessment of these 695 IPs found, sending forged (but controlled/limited) IKE_SA_INIT proposals. We have considered in our analysis the IPs list regardless of the MNO they serve, since we have experienced different configurations even within the pool of ePDGs of the same MNO. On the basis of the answers received from each ePDG, some of the configurations of the associated IKEv2 server could be inferred, spotting out possible weak configurations or unexpected behaviors.

3.1. Assessing ePDGs security algorithms

The primary goal of the assessment is to verify whether some of the accessible ePDGs support insecure or deprecated encryption and authentication algorithms for Security Association (SA) establishment, as well as vulnerable Diffie-Hellman (DH) Groups for key exchange. For the encryption, we have focused on DES and its successor 3-DES. A notable weakness of DES lies in its short key size (56 bits), rendering the cipher susceptible to brute-force attacks. Over the years, DES has also been subjected to cryptanalysis [7]. In contrast, 3-DES was deprecated by NIST in 2023, and as of January 1, 2024, its usage has been disallowed[4].

Next, we have considered vulnerable DH Groups 1 and 2, due to pre-computation attacks to the shared secret described in [8]. Today, DH Groups 1 and 2 (as well as 5) are considered inadequate also by some major vendors, e.g. Cisco[5]. Finally, we have also pointed the attention to HMAC-MD5. [9] recommends not using HMAC-MD5 in IKEv2 implementations either as Pseudo-Random Function (PRF) or authentication algorithm, due to transcript collision attacks found in [10]. As a reference, examples of IKE_SA_INIT proposals captured from real smartphones are reported in Table 1.

By empirical observation, the UEs analyzed are proposing several options, and the respective ePDGs behave very well since they select the "best" ones. As a sidenote, Xiaomi is also proposing e.g., DH-1024, which is relatively poor, and this proposal is potentially subject to downgrade attacks [3]. Anyway, the question we want to answer is what is the "minimum" algorithms acceptance level of ePDGs?

To reply to this question, it is necessary to send targeted IKE_SA_INIT proposals with different options. In case IKE_SA_INIT proposals are not compatible with the ePDG configuration (i.e., UE proposing only insecure encryption algorithms), it is likely that no answer is received at all. This can also happen in case the source IP of the UE is geo-blocked, with access allowed only if the UE IP geo-localization matches the nationality of the MNO. Otherwise, a negative response is received (i.e., no-proposal chosen). By varying the proposal ranges, it is possible to receive a response from the IKEv2 ePDG server which allows us to understand what are the acceptable/allowed/minimum (but also best) configurations based on whether it agrees on a given proposal option (called transform) or not.

[4] https://csrc.nist.gov/news/2023/nist-to-withdraw-sp-800-67-rev-2

[5] https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography

Table 1
IKE_SA_INIT proposals captured from real UEs. In bold the agreed security association with the MNO ePDG at the end of the INIT phase.

UE Brand/Model	MNO	DH group (bits)	Encr (bits)	Integrity (bits)	PRF (bits)
Xiaomi 12	Wind Italy (222/88)	14 * (2048) 15 (3072) 16 (4096) 17 (6144) **18 (8192)** 5 (1536) 2 (1024)	AES_CBC (128) AES_CBC (256) AES_CTR (128) **AES_CTR (256)**	HMAC_SHA1 (96) AES_XCBC (96) HMAC_SHA2 (256/128) HMAC_SHA2 (384/192) **HMAC_SHA2 (512/256)**	HMAC_MD5 (128) HMAC_SHA2 (256) HMAC_SHA2 (384) **HMAC_SHA2 (512)**
Samsung Galaxy S22	TIM Italy (222/01)	14 * (2048) 15 (3072) **16 (4096)**	AES_CBC (128) AES_CBC (192) **AES_CBC (256)**	HMAC_SHA2 (256/128) HMAC_SHA2 (384/192) **HMAC_SHA2 (512/256)**	HMAC_MD5 (128) HMAC_SHA2 (256) HMAC_SHA2 (384) **HMAC_SHA2 (512)**

* = default

To automate this assessment process, targeting the list of ePDG IPs obtained by the crawler, we developed a custom IKEv2 ePDG scanner in Golang[6], that can send custom IKE_SA_INIT proposals. The software developed is configured so that it can propose in different runs as a unique option the above mentioned weak algorithms and check the reply from all the ePDGs considered.

Anyway, it is important to remark that the availability of an ePDG to accept weak proposals is not a direct security concern per-se, since it must be agreed also by the UE. Nonetheless, it may open to possible side or man-in-the-middle attacks aiming at a potential disclosure or mangling of private users' data.

3.2. Assessing ePDGs DoS protection

In addition to algorithmic evaluations, we also focused on possible Denial of Service characterization of ePDGs. The initial IKE_SA_INIT exchange between an UE and ePDG is shown in Figure 2 in Stage 2, is not subject to particular constraints, being the service publicly exposed on the internet. Thus an attacker can forge an unlimited number of IKE_SA_INIT proposals, spoofing source IPs, that can lead to state/memory and CPU exhaustion associated with a large number of half-open SAs (see [3], section 2.6). If the ePDG supports the use of the IKEv2 Cookie Payload, it can protect itself from processing excessive requests by replying to the first IKE_SA_INIT with a random Cookie. Next, the initiator (i.e., the UE) must re-issue the initial IKE_SA_INIT including the Cookie, proving implicitly its source IP. While waiting for the reply by the initiator, the ePDG is not consuming memory since the Cookie derivation is stateless (of course, it will occupy CPU in handling the requests anyway), and consequent messages without Cookies are neglected.

The test, in this case, is to identify if the DoS prevention by cookie is correctly implemented by the ePDG, using a reasonable threshold value for the requests. Commercial and Open Source IPSec Servers (Cisco, Huawei, PanOS, Strongswan) usually have a default threshold value for half-open SAs, before issuing a Cookie, of a few tens to about 1000 (with in some cases dedicated thresholds per-IP) but some implementations do not enable Cookies at all by default (HPe, SonicWall). A half-open SA state in the ePDG can consume on average 1 to 2 Kbytes or more, required to store the information of the IKE_SA_INIT, so according to the request rate and considering a typical timeout of 30 s before the half-open SAs state is deleted, it is possible to identify practical load conditions which can be problematic for the ePDG and its memory consumption. Of course, MNO can implement other forms of DoS prevention, but we assume that an embedded mechanism offered by IKEv2 is suitable to reduce risks of overloads and would be good to have.

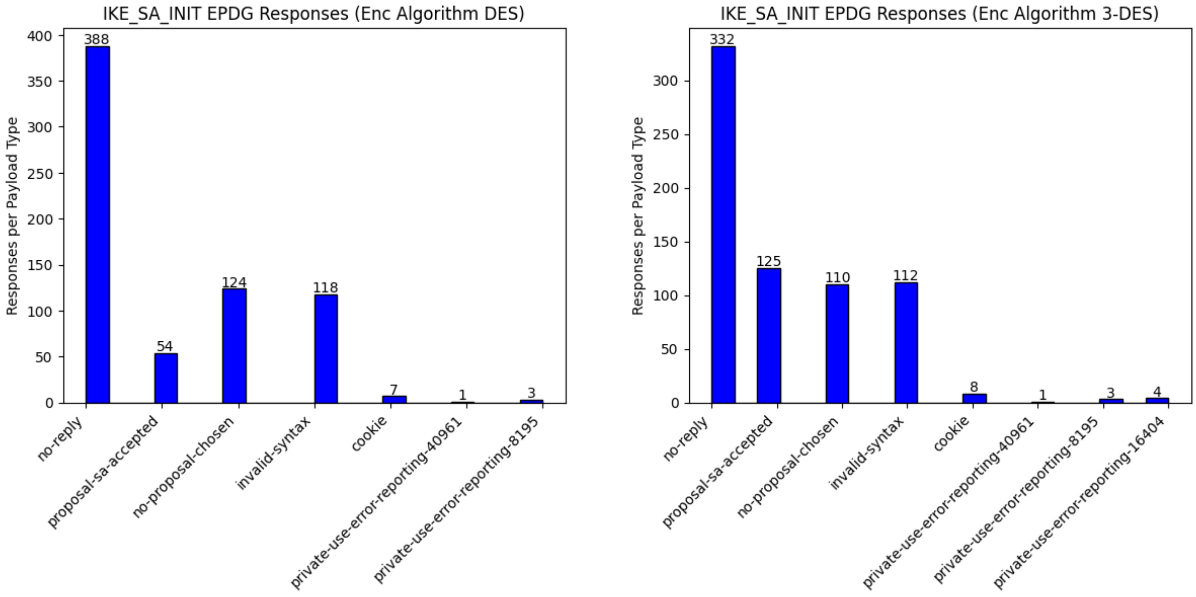
For this aim, we have developed a second software[7] to send several requests at once and identify if a Cookie is correctly received after requests exceed a given threshold. To reduce the impact of this test

[6] https://github.com/DomenicoVerde/epdg-scanner
[7] https://github.com/DomenicoVerde/epdg-stresser

since it is targeting operational ePDGs, we have set an internal maximum value in the SW to stop the test at a certain point avoiding over-flooding excessively MNO servers.

4. Results

The first part of the experiments is to identify ePDGs that support too weak encryption algorithms. In addition to DES and 3DES, we also attempted to request NULL encryption, but fortunately no ePDG accepted that (it is indeed forbidden by the IPSec specification, but possible in principle for debugging purposes). In Figure 3a and 3b, we reported the distribution of the responses provided by all ePDGs when the initiator is proposing the use of (a) DES or (b) 3-DES. 54 (7.8%) ePDGs still support DES, while 125 (18.0%) still support 3-DES. We found that the majority of ePDGs are in fact ignoring unacceptable proposals (no reply), and in lesser cases the ePDGs provided a negative or error response, indicating explicitly that the requested SA could not be accepted.



(a)

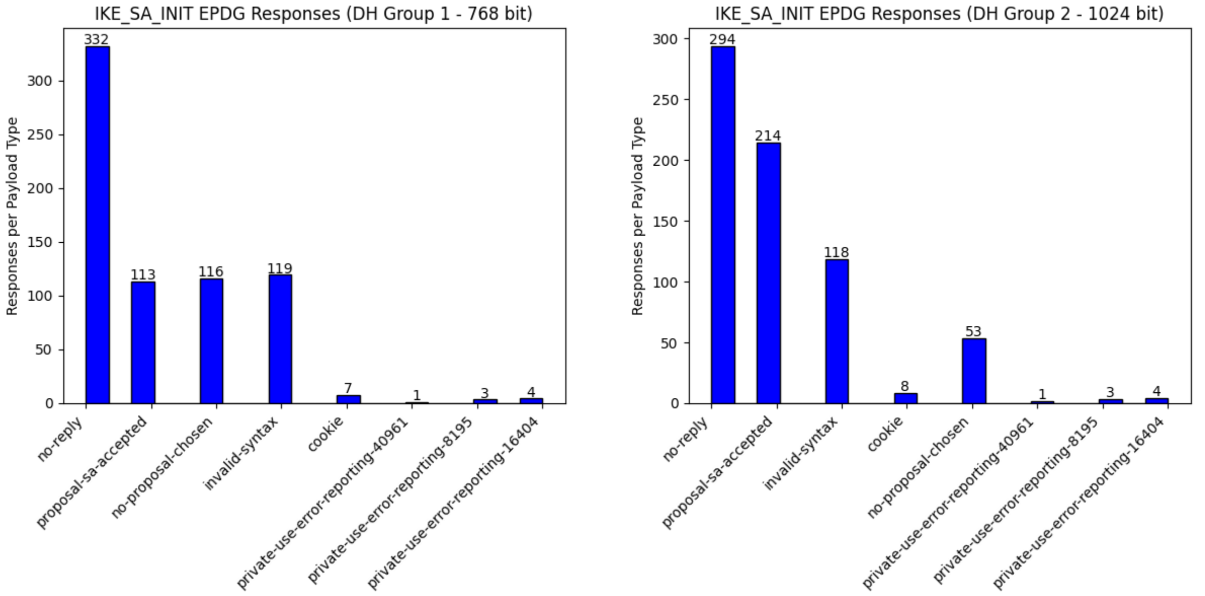
(b)

Figure 3: ePDGs responses to UE proposal to use (a) DES encryption and (b) 3DES encryption

Then we focused on DH Group minimum configuration accepted. 54 ePDGs (16.3%) support DH group 1 and 125 (30.8%) support DH group 2, as showed in Figure 4a and 4b. To provide a more general overview on DH, we included in different proposals, in turn, all the possible groups defined in [11] to gather additional information on typical and highest DH groups supported. All proposals contain also a valid initiator public key $A = g^{a} modp$, where a is randomly generated and p is a safe prime defined in [3], to make it reasonable to the ePDG. The resulting distribution is shown in figure 5, in which it is possible to confirm that DH-14 is the most supported one, whereas in some cases the support of weaker DH Groups is higher than the support of stronger groups.

Finally, we proceeded to the part regarding HMAC-MD5. As done previously, we forged and sent IKE_SA_INIT where HMAC-MD5 is proposed as the only option firstly as (a) authentication algorithm and then as (b) pseudo-random function. Results in Figure 6a and 6b show that 93 or 95 (about 13.4%) ePDGs support HMAC-MD5 either for Auth or as PRF.

Concerning the evaluation of DoS, we found a very limited number of ePDGs (belonging to just 5 MNOs) responding with Cookies, with a low threshold (few requests). In most of the cases instead, we experienced a sort of rate limit (most likely enforced by a firewall or by load limits within the ePDG) so that if 1000 requests are sent in a short time interval, only about 100 of them get a reply. This means that an effective DoS prevention using internal IKEv2 Cookie-based mechanisms is rarely enabled,



(a) (b)

Figure 4: ePDGs responses to UE proposal to use Diffie-Helmann (a) Group 1 (768 bits) and (b) Group 2 (1024 bits)

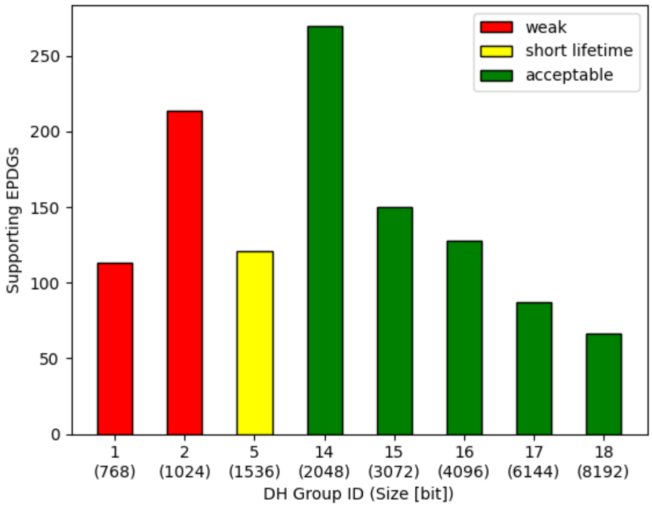


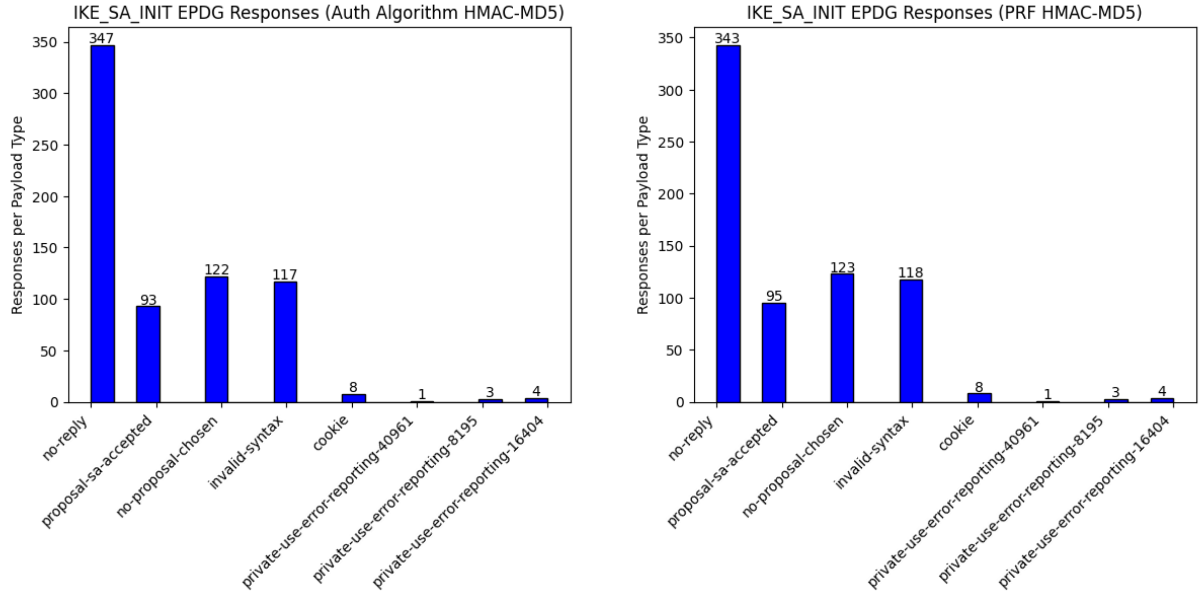
Figure 5: ePDGs overall supported DH groups distribution

thus not avoiding efficient state/memory exhaustion. On the other hand, a rate limit is enforced in most of the cases, which is a good practice, but then it is possible that the ePDG may deny the access to legitimate users while a DoS attack is ongoing. We couldn't characterize the DoS behavior better since we didn't want to overflood public ePDGs which are in fact serving real users, therefore we leave further evaluations as future work (possibly cooperating with MNOs).

5. Final recommendations and future work

During the tests, several ePDGs showed very low levels of crypto-suite allowed, opening to possible man-in-the middle attacks and consequent confidentiality violations. At the same time, we have verified that commercial UEs are able to use very secure and larger-bits algorithms, which must be encouraged during the IKA_SA_INIT negotiation. Even if not associated with direct vulnerabilities, it is suggested to remove weak or obsolete/deprecated algorithms from the range of ePDG accepted ones.

ePDG security, as basement also for N3IWF security in future 5G deployments, is not adequately



(a) (b)

Figure 6: ePDGs responses to UE proposal to use HMAC-MD5 (a) as authentication algorithm and (b) as PRF

addressed yet, even though ePDGs and N3IWF represent a critical/exposed node of MNO's Core Networks. A confirmation of that is the lack of 3GPP Security Assurance Specifications (SCAS) dealing specifically with untrusted non-3GPP access (except for a single simple test defined in [3GPP TS 33.520]). In this direction, SCAS tests shall be enhanced in the next future, and combined with typical public network-related security testing outside the 3GPP context and considering vulnerabilities already found in literature.

In conclusion, as future work we also envisage further and deeper tests of the untrusted access, as well as trusted access, dealing with i) the access stages after the IKA_SA_INIT stage 2 addressed in this work ii) the definition of possible attack scenarios beyond the state of the art iii) the analysis on the UE-side security iv) a more accurate evaluation of DoS robustness and last but not least v) the possible identification and definition of new SCAS tests.

6. Conclusions

This research is motivated by the ever growing interest of mobile network operators in integrating alternative access technologies, particularly Wi-Fi, for enhancing network capacity and coverage also in terrestrial areas hardly reachable by 4G/5G signals, such as isolated venues or private homes or areas. To assess the security posture of currently reachable real-world VoWiFi services, we have crawled 2523 worldwide operators' URLs potentially exposing an entry point for non-3GPP access, and found 340 MNOs with active evolved Packet Data Gateways (ePDGs), which we tested by suitably crafting IKEv2 signaling setup messages. Our experimental assessment highlights notable security concerns. With at least 18% of gateways accepting deprecated (or even broken, such as 56-bit key DES) ciphers, and over 30% supporting small-size Diffie-Hellman groups, our findings unveil a quite critical security landscape, and underscore the importance of more thorough security controls and configuration checks in these convergence technologies.

Acknowledgment

This work has been partially supported by the EU under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership "Telecommunications of the Future" (PE00000001 - program "RESTART") and "SEcurity and RIghts In the CyberSpace" (PE00000014 - program "SERICS"), and by the European Space Agency (ESA) INN3SCO project, contract n. 4000134916/21/NL/AF (https://artes.esa.int/projects/inn3sco). Responsibility of the contents resides with the authors.

References

[1] 3GPP, Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks, Technical Specification (TS) 24.302, 3rd Generation Partnership Project (3GPP), 2016.

[2] M. T. Lemes, A. M. Alberti, C. B. Both, A. C. D. O. Júnior, K. V. Cardoso, A Tutorial on Trusted and Untrusted Non-3GPP Accesses in 5G Systems—First Steps Toward a Unified Communications Infrastructure, IEEE Access 10 (2022) 116662–116685.

[3] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, 2010.

[4] J. Baek, S. Kyung, H. Cho, Z. Zhao, Y. Shoshitaishvili, A. Doupé, G.-J. Ahn, Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling, in: In Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC), San Juan, Puerto Rico, USA, 2018.

[5] H. Lee, I. Karim, N. Li, E. Bertino, VWAnalyzer: A Systematic Security Analysis Framework for the Voice over WiFi Protocol, in: Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, ASIA CCS '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 182–195.

[6] C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J.-F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke, F. Gunnarsson, LTE release 14 outlook, IEEE Communications Magazine 54 (2016) 44–49. doi:10.1109/MCOM.2016.7497765.

[7] T. Güneysu, T. Kasper, M. Novotný, C. Paar, A. Rupp, Cryptanalysis with COPACOBANA, IEEE Transactions on Computers 57 (2008) 1498–1513. doi:10.1109/TC.2008.80.

[8] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin, P. Zimmermann, Imperfect forward secrecy: how Diffie-Hellman fails in practice, Commun. ACM 62 (2018) 106–114. URL: https://doi.org/10.1145/3292035. doi:10.1145/3292035.

[9] Y. Nir, T. Kivinen, P. Wouters, D. Migault, Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2), RFC 8247, 2017. URL: https://www.rfc-editor.org/info/rfc8247. doi:10.17487/RFC8247.

[10] K. Bhargavan, G. Leurent, Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH, in: Network and Distributed System Security Symposium – NDSS 2016, San Diego, United States, 2016. URL: https://inria.hal.science/hal-01244855. doi:10.14722/ndss.2016.23418.

[11] T. Kivinen, M. Kojo, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), RFC 3526, 2003.

[12] 3GPP, Architecture enhancements for non-3GPP accesses, Technical Specification (TS) 24.402, 3rd Generation Partnership Project (3GPP), 2018.

[13] T. Kivinen, A. Huttunen, B. Swander, V. Volpe, Negotiation of NAT-Traversal in the IKE, RFC 3947, 2005. URL: https://www.rfc-editor.org/info/rfc3947. doi:10.17487/RFC3947.

[14] V. Volpe, M. Stenberg, B. Swander, L. DiBurro, A. Huttunen, UDP Encapsulation of IPsec ESP Packets, RFC 3948, 2005. URL: https://www.rfc-editor.org/info/rfc3948. doi:10.17487/RFC3948.

[15] M. Luglio, M. Quadrini, C. Roseti, D. Verde, F. Zampognaro, Performance evaluation of untrusted non-3GPP Access to a 5G Core Network via satellite, in: 2022 International Symposium on Networks, Computers and Communications (ISNCC), 2022, pp. 1–6.

[16] Y. Hu, M.-Y. Chen, G.-H. Tu, C.-Y. Li, S. Wang, J. Shi, T. Xie, L. Xiao, C. Peng, Z. Tan, S. Lu, Uncovering insecure designs of cellular emergency services (911), in: Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, MobiCom '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 703–715. URL: https://doi.org/10.1145/3495243.3560534.

Appendix – Untrusted access details

The reference architecture for untrusted non-3GPP access in 4G is described by 3GPP TS 23.401, from which we extracted figure 7. The access gateway functionality for untrusted access is implemented by the Evolved Packet Data Gateway (ePDG), at the border of the MNO EPC.

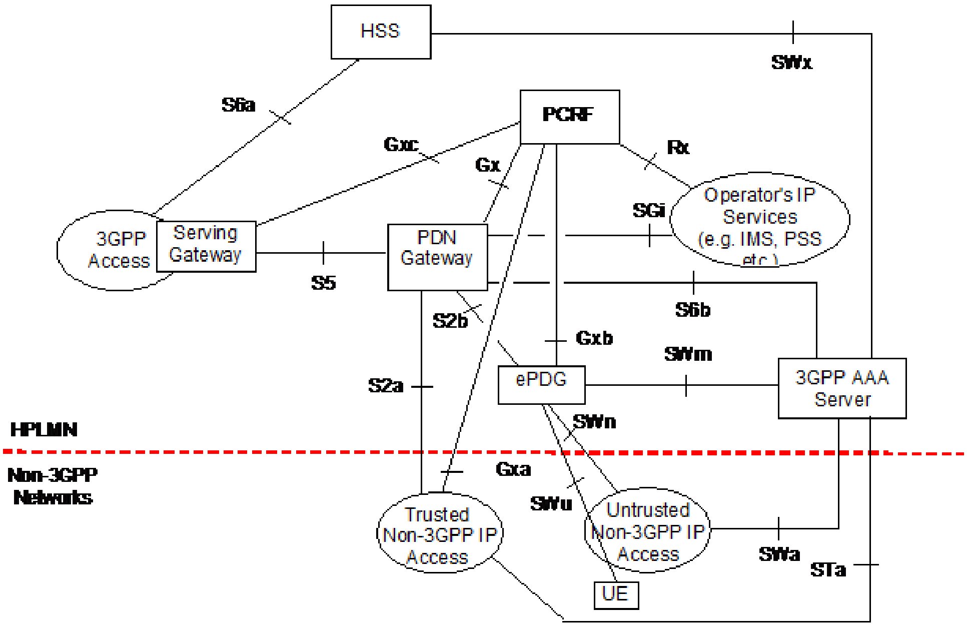


Figure 7: Reference 4G untrusted (and trusted) non-3GPP access architecture (Source: [1])

ePDGs are exposed on the Internet and their interfaces with the UE represent the main focus of our security assessment, since it is easily accessible by legitimate or rogue UEs. In particular, we are interested in the interface between the ePDG and the UE, called SWu, and defined in [1] and [12]. Active ePDGs worldwide, for all MNOs who have decided to implement this non-mandatory access option, are opening the ports associated with the IKEv2 service, which are UDP ports 500 and 4500 [13, 14]. IKEv2 protocol is used to manage and establish IPSec tunnels for the secure communication of the UE with the corresponding ePDG.

Concerning untrusted non-3GPP access in 5G, the Non-3GPP Inter-Working Function (N3IWF) is defined, with an equivalent role but different interfaces towards the 5GC (called NWu). Interested readers can refer to [15] for further information.

It is worth noting that in 4G/LTE trusted options were introduced later on by 3GPP, via the TWAG Gateway in Release-8. Nonetheless, even if it shares some common aspects with regard to untrusted access, it is not addressed in the current study since it is not yet commercially available, and is subject to future work. Similarly, 5G introduced dedicated trusted options, such as the Trusted Non-3GPP Gateway Function (TNGF), which will be subject to analysis in future works as well.

To perform the access procedures, including proving to the EPC the UE identity leveraging 3GPP secrets included into its USIM, mutual authentication between UE and ePDG, and User Plane connectivity establishment, a sequence of messages and controls are necessary. They are accurately described by 3GPP and reported in figure 8. Figure 2 of section 2 is a simplification of this sequence diagram. In particular, the paper only covers the initial IKEv2 establishment messages and algorithms proposal/agreement, as well as possible issues in case of flooding requests (DoS).

Finally, in addition to the URLs introduced in this work and associated with untrusted non-3GPP access, other classes of URLs are defined by 3GPP for emergency, localization-based access, and roaming. Of our interest in future works will be the first class, which is obtained by prepending `sos.` to the ePDG or N3IWF URLs. An example considering TIM MNO in Italy for emergency voice LTE services

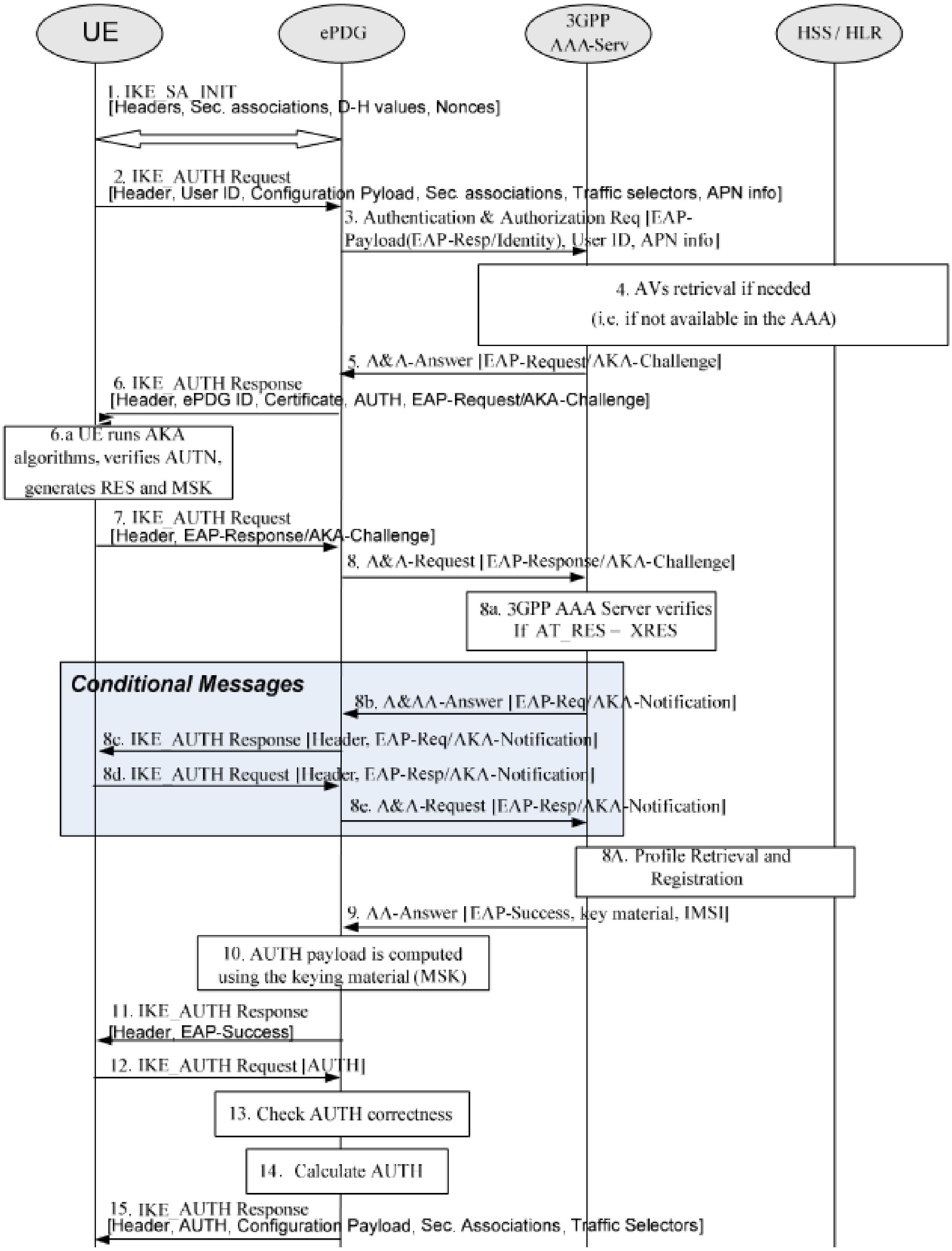

UE
ePDG
3GPP AAA-Serv
HSS / HLR
1. IKE_SA_INIT [Headers, Sec. associations, D-H values, Nonces]
2. IKE_AUTH Request [Header, User ID, Configuration Pyload, Sec. associations, Traffic selectors, APN info]
3. Authentication & Authorization Req [EAP-Payload(EAP-Resp/Identity), User ID, APN info]
4. AVs retrieval if needed (i.e. if not available in the AAA)
5. A&A-Answer [EAP-Request/AKA-Challenge]
6. IKE_AUTH Response [Header, ePDG ID, Certificate, AUTH, EAP-Request/AKA-Challenge]
6.a UE runs AKA algorithms, verifies AUTN, generates RES and MSK
7. IKE_AUTH Request [Header, EAP-Response/AKA-Challenge]
8. A&A-Request [EAP-Response/AKA-Challenge]
8a. 3GPP AAA Server verifies If AT_RES = XRES
Conditional Messages
8b. A&AA-Answer [EAP-Req/AKA-Notification]
8c. IKE_AUTH Response [Header, EAP-Req/AKA-Notification]
8d. IKE_AUTH Request [Header, EAP-Resp/AKA-Notification]
8e. A&A-Request [EAP-Resp/AKA-Notification]
8A. Profile Retrieval and Registration
9. AA-Answer [EAP-Success, key material, IMSI]
10. AUTH payload is computed using the keying material (MSK)
11. IKE_AUTH Response [Header, EAP-Success]
12. IKE_AUTH Request [AUTH]
13. Check AUTH correctness
14. Calculate AUTH
15. IKE_AUTH Response [Header, AUTH, Configuration Payload, Sec. Associations, Traffic Selectors]

Figure 8: Reference 4G untrusted non-3GPP access procedure (Source: [12] – Figure 8.2.2-1)

would be:

`sos.epdg.epc.mnc001.mcc222.pub.3gppnetwork.org`

These latter types of URLs are used to perform emergency calls to e.g., 112 (in Europe), or 911 (in the US) also in case of missing USIM and no subscription with the MNO, via the non-3GPP untrusted access. In this case, just 11 DNS entries for ePDG supporting emergency services were found, and they might be potentially more vulnerable [16].