Security Issues and Counter Measures In 3G Mobile Networks

Dr. Prabhat Kumar Vishwakarma

Department of Computer Science and Information Technology, IEC-GI, Knowledge Park-I, Greater Noida 201306 UP India
prof.dr.prabhat@gmail.com

Abstract -- Internet has given the new way of commercial activities as E-Commerce. These online activities with the emergence of 3G enabled smart phones have been increased drastically. 3G-systems play a key role in this network evolution, and, thus the security level supports in the new emerging mobile environment are seriously needed to all the stakeholders involved directly or indirectly in online commercial activities. This paper initially elaborates security framework in 3G mobile networks and then security requirements needed by stakeholders as well as end-users. The security architecture along with security mechanisms proposed by Universal Mobile Telecommunication System (UMTS) network, have also been analyzed. Furthermore the paper focuses on to identify Critical points in the 3G-security architecture that may cause network and service vulnerability are identified and proposes for the enhancement of the 3G-security architecture, and the provision of advanced security services to end-user data traffic within and outside the UMTS core network. The proposed security measure can easily be accommodated in the existing network infrastructure, and can flawlessly improve the UMTS network functionality.

Keywords: Mobile Security, Universal Mobile Telecommunication System; Authentication; Virtual Private Network

I. INTRODUCTION

Mobile/Wireless Internet is becoming available with the advent of third generation (3G) mobile communication systems. Along with the variety of new perspectives, mobile Internet also raises new concerns on security issues. Wireless access is inherently less secure, and mobility implies higher security risks compared to those encountered in fixed networks. The advanced wireless and wired network infrastructure, which supports higher access rates, and the complex network topologies, which enable ‘anywhere– anytime’ connectivity, may increase the number and the ferocity of potential attacks. The introduction of IP-based transport technology to the core of 3G mobile networks brings along new vulnerabilities and potential threats. Presently, mobile network operators do not deploy their own private networks, but they rather rely on the existing Internet infrastructure for the establishment of intra-network and inter-network communications. The major security concern in this approach is that the ‘shared’ Internet links are exposed to a large population of smart phone users, who have direct access to them. To counter against these vulnerable points, 3G systems have incorporated specific security architecture. This architecture is built on the security principles of 2G systems with improvements and enhancements in certain points in order to provide advanced security services. Its main objective is to ensure that all information generated by or relating to a user, as well as the resources and services provided by the serving network (SN) and the home environment (HE), are adequately protected against misuse or misappropriation. This paper examines and analyses the security framework in 3G mobile networks. The security requirements imposed by the different types of traffic, and by the different players involved (mobile users, SN and service providers) are investigated. The security architecture, which comprises all the security mechanisms that are projected for the Universal Mobile Telecommunication System (UMTS) network [2], is presented and elaborated.

II. UMTS NETWORK

Network Architecture: UMTS comprises a realization of 3G-mobile systems, which is compatible with the evolved Global System for Mobile communication/General Packet Radio Services (GSM/GPRS) [1] network. The basic architecture is shown in Figure 1. Its main objective is to provide a wide range of real-time multimedia applications with differentiated levels of quality of service and advanced service features to mobile users. The fundamental difference between GSM/GPRS and UMTS R99 is that the latter supports higher access rates (up to 2 Mbps) [2]. This is achieved through a new Wideband Code Division Multiple Access radio interface for the land based communication system, named UMTS Terrestrial Radio Access Network (UTRAN) [3]. While UMTS R99 is a logical evolution from the 2G-system architecture, UMTS Rel-4 and Rel-5 are revolutionary, introducing new concepts and advanced features [4,5]. A major point of differentiation is the shift towards an all-IP network architecture that eventually will replace the circuit-
switched (CS) transport technology, which is partially used in UMTS R99, by packet-switched (PS).

Figure 1. UMTS network architecture.

3G Security Specifications and Architecture: Security protection in 3G-networks requires the consideration of several aspects and issues, such as the wireless access, the end-user mobility, the particular security threats, the type of information to be protected, and the complexity of the network architecture. The radio transmission is by nature more susceptible to eavesdropping and fraud in use than wireline transmission. The user mobility and the universal network access certainly provoke security threats. The different types of data, such as user data, charging and billing data, customer information data, and network management data, which are conveyed or are resident in mobile networks, require different type and level of protection.

Figure 2 gives an overview of the complete 3G-security architecture, illustrating five major security classes: (I) network access security, (II) NDS, (III) user domain security, (IV) application domain security and (V) visibility and configurability of security [13].

Although mobile networks differ in nature from fixed terrestrial networks, their security measures should also support the principles defined for traditional IP networking, such as confidentiality, integrity, authentication, availability, authorization and accounting [6]. These measures counteract against a number of potential attacks like masquerading, unauthorized use of resources, unauthorized disclosure of information, unauthorized alteration of information, repudiation of actions and denial of service [7, 8].

III. Network Security in 3G Mobile Network

Network access security is a key component in the 3G-security architecture. This class deals with the set of security mechanisms that provide users with secure access to 3G services, as well as protect against attacks on the radio interface. Such mechanisms include: (i) user identity confidentiality, (ii) authentication and key agreement (iii) data confidentiality and (iv) integrity protection of signaling messages. Network access security takes place independently in each service domain.

User identity confidentiality: User identity confidentiality allows the identification of a user on the radio access link by means of a Temporary Mobile Subscriber Identity (TMSI) This implies that confidentiality of the user identity is protected almost always against passive eavesdroppers. A TMSI in the CS domain or P-TMSI in PS domain has a local significance only in the location area or the routing area, in which the user is registered. The association between the permanent and temporary user identities is stored in the Visited Location Register or the Serving GPRS Support Node (VLR/SGSN). If the mobile user arrives into a new area, then, the association between the permanent and the temporary identity can be fetched from the old location or routing area. If the address of the old area is not known or the connection cannot be established, then, the permanent identity must be requested from the mobile user. To avoid user traceability, which may lead to the compromise of user identity confidentiality as well as to user location tracking, the user should not be identified for a long period by means of the same temporary identity. Additionally, any signaling or user data that might reveal the user’s identity are ciphered on the radio access link.

Authentication and Key Agreement: Authentication and key agreement mechanism achieves mutual authentication between the mobile user and the SN showing knowledge of a secret key, K, as well derives ciphering and integrity keys. The authentication method
is composed of a challenge/response protocol (Figure 3), and was chosen in such a way as to achieve maximum compatibility with the GSM/GPRS security architecture facilitating the migration from GSM/ GPRS to UMTS. Furthermore, the User Service Identity Module (USIM) [14] and the HE keep track of counters SQNMS and SQNHE, respectively, to support the network authentication. The sequence number SQNHE is an individual counter for each user, while the SQNMS denotes the highest sequence number that the USIM has accepted.

Upon receipt of a request from the VLR/SGSN, the HE authentication center (HE/AuC) forwards an ordered array of authentication vectors (AV) to the VLR/SGSN. Each AV, which is used in the authentication and key agreement procedure between the VLR/SGSN and the USIM, consists of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK, and an authentication token AUTN.

Figure 4 shows an AV generation by the HE/AuC. The HE/AuC starts with generating a fresh sequence number SQN, which proves to the user that the generated AV has not been used before, and an unpredictable challenge RAND. Then, using the secret key K it computes: The Message Authentication Code MAC, and the Authentication and key Management Field (AMF) is used to fine tune the performance or bring a new Authentication key stored in the USIM into use. The VLR/SGSN compares the received RES with the XRES field of the AV. If they match, it considers that the authentication and key agreement exchange has been successfully completed.

Finally, the USIM and the VLR/SGSN transfer the established encryption and integrity protection keys (CK and IK) to the mobile equipment and the Radio Network Controller (RNC) that perform ciphering and integrity functions.

Data confidentiality: Once the user and the network have authenticated each other, they may begin secure communication. The cipher key is shared between the core network and the terminal after a successful authentication event. User and signaling data sent over the radio interface are subject to ciphering using the function f 8 (Fig 5): The encryption/decryption process takes place in the MS and the RNC on the network side. The f 8 is a symmetric synchronous stream cipher algorithm that is used to encrypt frames of variable length. The main input to the f 8 is a 128-bit secret cipher key CK. Additional inputs, which are used to ensure that two frames are encrypted using different keystreams, are a 32-bit value COUNT, a 5-bit value BEARER and a 1-bit value DIRECTION (Fig. 5). The output is a sequence of bits (the ‘keystream’) of the same length as the frame. The frame is encrypted by XORing the data with the keystream. For UMTS R99, f 8 is based on the Kasumi algorithm [15].

Authentication key stored in the USIM into use. The VLR/SGSN compares the received RES with the XRES field of the AV. If they match, it considers that the authentication and key agreement exchange has been successfully completed.

Figure 4. Generation of authentication vectors.

Figure 5. Ciphering over the radio access link.

Integrity protection of signaling messages: The radio interface in 3G-mobile systems has also been designed to support integrity protection on the signaling channels. This enables the receiving entity to be able to verify that
the signaling data has not been modified in an unauthorized way since it was sent. The function $f_9$ (Figure 5) is used to authenticate the integrity and the origin of signaling data between the MS and the RNC in UMTS. It computes a 32-bit Message Authentication Code (MAC) (Fig. 6), which is appended to the frame, and is checked by the receiver. The main inputs to the algorithm are an 128-bit secret integrity key $IK$, and the variable-length frame content $MESSAGE$. Additional inputs, which are used to ensure that MACs for two frames with identical content are different, are a 32-bit value $COUNT$, a 32-bit value $FRESH$, and an 1-bit value $DIRECTION$. In the UMTS R99, the $f_9$ is based on the Kasumi algorithm [15].

IV. NETWORK DOMAIN SECURITY
NDS features ensure that signaling exchanges within the UMTS core, as well as in the whole wireline network are protected. Various protocols and interfaces are used for the control plane signaling inside, and between core networks, such as the Mobile Application Part (MAP) [16] and the GPRS Tunneling Protocol [1] protocols. These will be protected by standard procedures based on the existing cryptographic techniques. Specifically, the IP-based protocols shall be protected at network level by means of IPsec [6], while the realization of protection for the SS7-based protocols shall be accomplished at the application layer.

**IP-based protocol:** The UMTS network domain control plane is sectioned into security domains, which typically coincide with the operator borders. Security gateways (SEGs) are entities at the borders of the IP security domains used for securing native IP-based protocols. It is noted that NDS does not extend to the user plane, which means that packet flows over the Gi [2] interface will not be protected by the SEGs. The key management functionality is logically separate from the SEG. Key administration centers (KACs) negotiate the IPsec security associations (SAs) by using the Internet Key Exchange (IKE) protocol [19] in a client mode, on behalf of the network entities (NEs) and the SEGs. The KACs also distribute SAs parameters to the NEs or the SEGs through standard interfaces.

In Figure 7 the UMTS NDS architecture for IP-based protocols is depicted. To secure the IP traffic between two NEs, either a hop-by-hop or an end-to-end scheme may be applied. The first requires the originating NE to establish an IPsec tunnel to the appropriate SEG in the same security domain and forward the data to it. The SEG terminates this tunnel and sends the data through another IPsec tunnel to the receiving network. The second tunnel is terminated by the SEG in the receiving domain, which in turn uses IPsec to pass the data to its final destination (Fig. 7(a)). The end-to-end scheme implies that an IPsec SA is established between the two NEs (Fig. 7(b)). This scheme can also be applied in case that the two parties belong to the same security domain. Node authentication can be accomplished using either pre-shared symmetric keys, or public keys [19]. Using preshared symmetric keys means that the KACs or the NEs do not have to perform public key operations, as well as there is no need for establishing a public key infrastructure.

![Figure 6. Derivation of MAC on a signaling message.](image)

Figure 6. Derivation of MAC on a signaling message.

![Figure 7. NDS architecture for IP-based protocols.](image)

Figure 7. NDS architecture for IP-based protocols.

The IPsec can be configured either in transport mode or in tunnel mode [6]. Whenever at least one endpoint is a gateway, then, the tunnel mode suits better. Finally, the IPsec protocol shall always be Encapsulation Security Payload [6], given that it can provide confidentiality and integrity protection as well.

**SS7-based protocols:** NDS for SS7-based protocols is mainly found at the application layer. Specifically, in case that the transport relies on SS7, or on a combination of SS7 and IP, then, security shall be provided at the application layer. On the other hand, whenever the transport is based on IP only, security may be provided at the network layer exclusively, or in addition to the application layer security, by using IPsec. For signaling protection at the application layer the necessary SAs will be network-wide and they are negotiated by KAC, similarly to the IP-based architecture (Figure 8).
End-to-end protected signaling will be indistinguishable to unprotected signaling traffic to all parties, except for the sending and receiving sides. It is worth noticing that in Rel-4 the only protocol that is to be protected is the MAP. The complete set of enhancements and extensions that facilitate the MAP security is termed MAPsec [18]. The MAPsec covers the security management procedures, as well as the security of the transport protocol including data integrity, data origin authentication, anti-reply protection and confidentiality. Finally, for IKE adaptation a specific Domain of Interpretation is required.

**Traditional network security feature:** Besides the security features that are included in the 3Gsecurity architecture, the mobile network operators can apply traditional security technologies used in terrestrial networking to safeguard the UMTS core network, as well as the inter-network communications. User data in the UMTS backbone network are conveyed in clear-text exposing them to various external threats.

![Fig. 8. NDS architecture for SS7 and mixed SS7/IP-based protocols.](image)

Figure 8. NDS architecture for SS7 and mixed SS7/IP-based protocols.

Moreover, inter-network communication is based on the public Internet, which enables IP spoofing to any malicious third party who gets access to the network. Thus, to counteract against these vulnerable points the mobile operators can use two complementary technologies: firewalls, and VPNs [21].

Firewalls can be characterized as a technology providing a set of mechanisms to enforce a security policy on data from and to a corporate network. They are established at the borders of core network allowing traffic originated from specific foreign IP addresses. Thus, firewalls protect the UMTS backbone from unauthorized penetration. Since firewalls do not provide privacy and confidentiality, VPNs have to complement them to protect data in transit.

VPN establishes a secure tunnel between two points, encapsulates and encrypts data, and authenticates and authorizes user access of the corporate resources on the network. Thus, they extend dedicated connections between remote branches, or remote access to mobile users, over a shared infrastructure. Implementing a VPN makes security issues such as confidentiality, integrity, and authentication, paramount. There is a two-fold benefit that arises from VPN deployment: the low cost and security. A number of different mechanisms that provide VPN over IP networks exist. Application-layer security builds security features into individual applications, and they operate independently of any network security measures.

Many applications have special security requirements that simply cannot be met by network security services. Security at this level is by far the easiest to deploy, as long as all users are running a homogeneous application on a standard platform. While these methods are effective for solving specific security problems, such solutions are by their nature limited to specific niches. For instance, Transport Layer Security (TLS) [21] works fine for simple client-service cases, but, in case that the service contains a considerable number of cross references to other servers, for each one a separate key exchange operations is needed overloading unnecessarily the client.

Link-layer techniques are often applied within wireless link. Their limitation pertains to the fact that link-layer end-to-end security cannot be consistently realized in the context of a network utilizing various types of radio and wired transmission segments. On the other hand, the IPsec [6] standard aims at securing the network layer, and guarantees security for any application that uses it. It facilitates transparent encryption and integrity protection on both IPv4 and IPv6, and authentication of the communicating peers. It is especially useful for implementing VPNs, and for remote access to private networks.

**V. USER AND APPLICATION DOMAIN SECURITY FEATURES**

*User domain security:* User domain security [13] ensures secure access to the MS. It is based on a physical device called UMTS Integrated Circuit Card, which can be easily inserted and removed from terminal equipment, containing security applications such as the USIM [14]. The USIM represents and identifies a user and his association to an HE. It is responsible for performing subscriber and network authentication, as well as key agreement, when 3G services are accessed. It may also contain a copy of the user’s profile.

The USIM access is restricted to an authorized user, or to a number of authorized users. To accomplish this feature, the user and the USIM must share a secret (e.g. a PIN). The user gets access to the USIM only if he proves knowledge of the secret. Furthermore, access to a terminal or to other user equipment can be restricted to an authorized USIM. To this end, the USIM and the terminal must also share a secret. If a USIM fails to
prove its knowledge of the secret, then, access to the terminal is denied.

**Application domain security:** On the other hand, application domain security [13] deals with secure messaging between the MS and the SN or the SP over the network with the level of security chosen by the network operator or the application provider. A remote application should authenticate a user before allowing him to utilize the application services, and it could also provide for application-level data confidentiality.

Application-level security mechanisms are needed because the lower layers’ functionality may not guarantee end-to-end security provision. Lack of end-to-end security could be envisioned when, for instance, the remote party is accessible through the Internet. USIM Application Toolkit [20] provides the capability for operators or third party providers to create applications that are resident on the USIM. To assure secure transactions between the MS and the SN or the SP, a number of basic security mechanisms such as entity authentication, message authentication, replay detection, sequence integrity, confidentiality assurance, and proof of receipt, have been specified and integrated in the USIM Application Toolkit.

Wireless Application Protocol (WAP) is a suite of standards for delivery and presentation of Internet services on wireless terminals, taking into account the limited bandwidth of mobile networks, as well as the limited processing capabilities of mobile devices. To connect the wireless domain to the Internet, a WAP gateway is needed to translate the protocols used in WAP segment to the protocols used in the public Internet. The WAP architecture has been standardized in two releases (versions 1.2.1 and 2.0) [24].

To secure data transmission in the WAP architecture (version 1.2.1), the Wireless Transport Layer Security (WTLS) protocol [24], which is based upon the TLS protocol, is employed. WTLS has been optimized for use over narrow-band communication channels providing also datagram support. It ensures data integrity, privacy, authentication, and denial-of-service protection.

For Web applications that employ standard Internet security techniques with TLS, the WAP gateway automatically and transparently manages wireless security, and conveys protected data between the WTLS and TLS security channels (Figure 9a). Thus, this scheme does not support end-to-end security. WAP 2.0 proceeds to the re-design of the WAP architecture by introducing the existing Internet protocol stack, including the Transmission Control Protocol (TCP), into the WAP environment. The new architecture allows a range of different gateways, which enables conversion between the two protocol stacks anywhere from the top to the bottom of the stack. A TCP-level gateway allows for two versions of TCP, one for the wired and another for the wireless network, on top of which a secure TLS channel can be established all the way from the mobile device to the server (Fig. 9b). The availability of a wireless profile of the TLS protocol, which includes cipher suites, certificate formats, signing algorithms, and the use of session resume,

![Figure 9(a). WAP 121 architecture (b) WAP 20 architecture.](image)

enables end-to-end security support at the transport level allowing interoperability for secure transactions.

**Security visibility and configurability:** Although the security measures provided by the SN should be transparent to the end user, visibility of the security operations as well as the supported security features should be provided. This may include: (a) indication of access network encryption; (b) indication of network wide encryption; (c) indication of the level of security (e.g. when a user moves from 3G to 2G).

Configurability enables the mobile user and the HE to configure whether a service provision should depend on the activation of certain security features. A service can only be used when all the relevant security features are in operation. The configurability features that are suggested include: (a) enabling/disabling user-USIM authentication for certain services; (b) accepting/rejecting incoming non-ciphered calls; (c) setting up or not setting up non-ciphered calls; (d) accepting/rejecting the use of certain ciphering algorithms.

**Network-wide user data confidentiality:** Network-wide confidentiality is an option that provides a protected mode of transmission of user data across the entire network. It protects data against eavesdropping on every link within the network, and not only on the vulnerable radio links. Whenever network-wide confidentiality is applied, access link confidentiality on user data between the MS and the RNC is disabled to avoid replication. However, access link confidentiality for signaling information, as well as user identity confidentiality is retained to facilitate the establishment of the encryption process. In Fig. 10, the network-wide encryption deployment is depicted. Network-wide confidentiality uses a synchronous stream cipher algorithm similar to
that employed in the access link encryption. Initially, a
data channel is established between the communicating
peers indicating also the intention for network-wide
encryption. VLRa and VLRb exchange cipher keys (Ka
and Kb) for users a and b, respectively, using cross
boundaries signaling protection, and then, pass them to
the MSs over protected signaling channels. When each
MS has received the other party’s key, the end-to-end
session key, Ks, is calculated as a function of Ka and Kb.
Alternatively, VLRs can mutually agree on the Ks using
an appropriate key agreement protocol. Both key
management schemes satisfy the lawful interception
requirement, since Ks can be generated by the VLRs. Fig.
9. (a) WAP 1.2.1 architecture; (b) WAP 2.0 architecture.

VI. 3G-SECURITY ARCHITECTURE

EVALUATION

The existing UMTS security architecture provides
advanced security services, and addresses many security
concerns that have been listed in the context of next
generation mobile networks. However, there are critical
points, which need further elaboration and
improvements. In the following, some security
weaknesses that may cause network and service
vulnerability are identified, as well as evolution
perspectives that aim to enhance the level of security
services and can be easily integrated in the 3G security
architecture are outlined.

Weaknesses: The mobile user identity and location is
valuable information that requires protection. A possible
weakness in 3G-security architecture is the backup
procedure for TMSI reallocation [22]. Specifically,
whenever the SN/VLR cannot associate the TMSI with
the International Mobile Subscribers Identity (IMSI)
because of TMSI corruption or database failure, the VLR
should request the user to identify itself by means of
IMSI on the radio-path.

Furthermore, when the user roams, and the SN/ VLRn
cannot contact the previous VLRo, or cannot retrieve
the user identity; the SN/VLRn should also request the
user to identify itself by means of IMSI on the radio path [13].
This may lead an active attacker to pretend to be a new
SN to which the user has to reveal his permanent
identity. In both cases, the IMSI, which represents the
permanent user identity, is conveyed in clear-text on the
radio interface violating user identity confidentiality.
Another critical point is that the users may be identified
by means of the IMSI in signaling conversations in the
wireline path.

Moreover, the firewalls security value is limited because
they allow direct connection to ports and cannot
distinguish services. Similarly, the current type of VPN
fails to provide the necessary flexibility to establish
reliable secure connections for typical mobile users. VPN
services for UMTS subscribers can be established in a
static manner between the border gateway of the UMTS
core network and a remote corporate security gateway.
This makes the realization of VPN services feasible only
between the security gateway of a large organization and
a mobile operator, when a considerable amount of traffic
requires protection. Thus, if the static VPN parameters or
the VPN topology has to be changed, then the network
administrators in both ends must reconfigure it.

Furthermore, the aforementioned security scheme can
provide VPN service neither to individual mobile users,
that may require on demand VPN establishment, nor to
enterprise users that may roam internationally. In case
that a mobile user uses the WAP architecture (version
1.2.1), data privacy is not guaranteed. Although
encryption is used, the WAP gateway constitutes a
security hole since, inside the gateway data are
transmitted unencrypted.

WTLS is only used between the mobile device and the
gateway, while TLS can be used between the gateway
and the web server. From a security point of view, the
gateway should be considered as an entity-in-the-middle.
This means that data exchanged may be available to
people with privileged access to the WAP gateway, and,
thus, the privacy of the data depends the gateway’s
internal security policy.

WAP 2.0 does address the ‘gap’ in security caused by
protocol translation at the WAP gateway. However, the
mobile phone would have to use an IP protocol stack, at
the expense of larger latency and bandwidth
consumption. Although TLS can be used to secure the
communication of any application, it must be integrated
into the application, and, thus, to a large extent it is used
for web-based applications. Interaction with the end-user
is needed, for example, to check with whom a secure
session has been established, or to explicitly request the
client to authenticate with the server.

TLS is generally a resource consuming protocol for
deployment in mobile devices with limited processing
capabilities, and low bandwidth/high latency wireless
networks. Moreover, the operation overhead may be
increased by complex key-exchange procedures in case
that the protected service contains cross-references to
other services. The network-wide encryption may also
encounter problems when transcoding is used.

Voice calls may need to be transcoded when they cross
network borders, meaning that voice data may have to
undergo change, such as, bit rate change or some other
transformation. It is not possible to apply such
transformation on an encrypted signal, which implies that
the signal has to be decrypted before transcoding.
Furthermore, the network-wide confidentiality lacks
flexibility, and it is not applicable to all types of service
in different mobile scenarios. Specifically, it is limited to
protecting the communication between mobile subscribers. Consequently, there is a lack of a general-purpose mechanism that can provide advanced security services to user data traffic according to the particular end-user needs, inside and outside the UMTS core network.

Firewall technology cannot adequately ensure data transfer within the UMTS core network. Static VPN deployment and the network-wide confidentiality option cannot be applied to all mobile scenarios protecting all type of potential services. Moreover, the WAP architecture and application layer security are mainly related to web-based applications, which can integrate TLS or WTLS functionality.

Next generation mobile subscribers require dynamic, flexible, client initiated security mechanisms, which will be available anywhere–anytime. They should provide customized security services to data traffic, and guarantee interworking with existing and forthcoming network infrastructure, taking into account the end-user mobility and the mobile network characteristics.

*Proposed improvements:* The weak points in the 3G-security architecture, identified earlier, may lead to compromises of end-user or mobile network security. In this section, enhancements that aim to improve the 3G-security architecture, as well as to provide advanced security services to end-user data traffic within and outside the UMTS core network are outlined. The proposed enhancements can be easily integrated in the existing network infrastructure and operate transparently to UMTS network functionality.

To prevent the exposure to threats of the permanent mobile user identity, where the clear-text IMSI paging procedure is being used, the employment of two additional temporary user identities has been proposed. Specifically, when the SN/VLR has failed to page a mobile user using the current TMSI, it can try to page him using an alternative temporary identity that also resides in the VLR, and thus, the use of IMSI can be avoided.

If none of the TMSI is valid, or both TMSI are corrupted, the user is not attached to the network. In case of a VLR database recovery, or a corruption of the TMSI in the VLR, the SN/VLR requires a second temporary identity by which it can page the user. This temporary identity has to be provided by the user’s HE, otherwise it cannot be assured that it is available at the SN/VLR after a database recovery. For similar reasons, it cannot be provided to the SN/VLR in advance. The TMSIHE should have a limited lifetime to prevent potential intruders to link it to the permanent user’s identity [9]. NDS features protect signaling exchange in the wireline network architecture over IP and SS7 technologies.

However, these features are considered for the later versions of the UMTS standardization process, leaving the first one unprotected. UMTS R99 is the precursor of 3G networks and needs to prove the necessity of transition from 2Gþ to 3G. Apart from the higher access rate and the advanced QoS features, another reason that should enforce this transition would be the enhanced security services that 3G systems offer to the involved parties. Therefore, it is necessary that signaling exchange protection in the wireline network architecture be applied to the entire set of the UMTS releases.

Another issue that will empower the security services being provided in 3G networks is the advanced protection of user data traffic, either globally (end-to-end) or within the wireline network, according to the end-user needs. Complementary to the network-wide confidentiality option and the WAP security, the incorporation of VPN technology in the 3G-security framework will further increase the supported level of protection by providing general-purpose security services at the network layer.

On demand, customized VPN services are well suited to mobile users, which require anywhere–anytime connectivity. Moreover, VPN technology guarantees interworking with existing and forthcoming IP terrestrial network infrastructure. The end-to-end VPN scheme [10] enhances mobile users’ privacy in both the radio path and wireline network. The VPN functionality, which is based on the IPsec protocol suite, is integrated in the communicating peers, and thus, data traffic remains encrypted for the entire route between them. It has minimal impact on the existing network infrastructure, and provides the best security services to the end users.

On the other hand, the main drawback of this scheme derives from the fact that each MS must have the appropriate software (IPsec) in order to apply the required security policy. This imposes computational costs on the lightweight end-user devices, and duplicates encryption (packet encapsulation) over the expensive radio interface. Moreover, the end-user must be aware of when encryption is required. An alternative approach to the end-to-end VPN scheme pertains to a network-based scheme [11, 12].

This scheme integrates VPN functionality into the network infrastructure, and eliminates the need for end-user involvement. procedures an IKE protocol proxy scheme has been proposed, which enables the mobile user to initiate a VPN, while shifting complex key negotiation to the network infrastructure. The deployed VPNs provide maximal security services to end users, operate transparently to the MSs movement, and are compatible with the legal interception option. The required enhancements for security service provision can be integrated in the existing network infrastructure, and
therefore, the security scheme can be used as an add-on feature of the UMTS. There is significant interest in such solutions both by customers, seeking to reduce support costs, and by network operators, seeking new revenue sources. By placing security functionality in the UMTS access network or in the UMTS border, the network-wide or the border-based VPN scheme are deployed, respectively [11,12]. In the network-wide scheme the deployed VPN is extended over the UMTS backbone and the public Internet, while in the border-based it expands only in the public Internet segment. The particular scheme that will be selected in a potential deployment scenario depends on the required level of security services, as well as the network topology.

VII. CONCLUSION
The evolution of 3G-networks signifies a shift towards open and easily accessible network architectures, which raises major security concerns. Thus, all stakeholders are interested in the security level supported in 3G-systems because of the identified risk that prospective users might perceive 3G-networks as not trustworthy, and not use them. This paper has elaborated on the security framework in 3G mobile networks.

The security requirements imposed by the different types of traffic, and by the different players involved (mobile users, SN and service providers) have been outlined. The security architecture, which comprises all the security mechanisms that are projected for the next generation mobile networks, has been presented and analyzed. 3G-security attempts to ensure that all information generated by or relating to a user, as well as the resources and services provided by the SN and the home environment, are adequately protected against misuse or misappropriation.

The employment of traditional security technologies, originally designed for fixed networking, such as firewalls, and static VPN, in order to safeguard the UMTS core network from external attacks, as well as to protect user data when conveyed over the public Internet have been examined. Critical points in the 3G-security architecture that may cause network and service vulnerability have been identified. Finally it is possible to provide secure data transfer without requiring an extra tunnel overhead on the radio link, or the implementation of computationally intense encryption algorithms in the MS. The VPN functionality is also based on IPsec. For VPN initialization and key agreement aim to enhance the 3G-security architecture, as well as to provide advanced security services to end-user data traffic within and outside the UMTS core network have been briefly discussed. The proposed enhancements can be easily integrated in the existing network infrastructure, and operate transparently to UMTS network functionality.

VI. REFERENCES

[1]. GSM 03.60, GPRS, Service Description, Stage 2, 1998.


[24]. Wireless Application Forum (WAP), WAP Specifications.URL:
http://www.wapforum.org/what/technical.htm

Dr Prabhat Kumar Vishwakarma
is currently working as Professor and Head of Department (CSE & IT) in IEC College of Engineering and Technology, Greater Noida. He completed his PhD in Computer Science discipline from Mahatma Gandhi Kashi Vidyapith Varanasi after receiving his MCA from MNREC Allahabad and M.Tech (CSE) from AAI-DU respectively. He has 18 years of vast teaching experience with International exposure in academics.

Published seven national and three International research papers. Participated and presented 10 research articles in national level seminar/conference as well as three research articles in International conferences.