LTE/SAE Security Issues on 4G Wireless Networks

Anastasios N. Bikos | University of Patras
Nicolas Sklavos | Technological Educational Institute of Patras

An overview of the potential security issues that can occur in the deployment of the Long-Term Evolution/System Architecture Evolution protocol in emerging 4G wireless technologies gives a snapshot of the current state of the art.

The recent expansion of wireless network technologies and the emergence of novel applications such as mobile TV, Web 2.0, and streaming content have led to the standardization of the (pre-4G) Long-Term Evolution (LTE) protocol to become operational with the 3rd Generation Partnership Project (3GPP). The 3GPP has also begun the study of the standard's future development, called System Architecture Evolution (SAE), set to evolve into the new era of 4G. LTE is, in fact, the latest standard in the mobile network core technology that now accounts for more than 85 percent of all mobile subscribers.[1,2]

The next-generation mobile telecommunication system, universally recognized as 4G, is being prototyped for increased security and reliable communication. Yet, 4G wireless technologies have several key differences compared to 3G and other preceding versions. One elementary difference is that 4G wireless networks will operate entirely on the TCP/IP architectural suite, thus becoming totally IP based. This decision represents an effort to work more with interoperability across heterogeneous network environments, both wired and wireless, thus solving many compatibility issues in terms of architectural design. However, one consequence of making this transition to an open suite of communication protocols is that it poses greater risks in terms of safety and reliability.[3]

The 4G evolution of LTE with the launch of its newest add-on—the evolved packet system (EPS), which is the relevant aspect of the LTE/SAE main core network architecture—demands that security functions should be optimally and efficiently embedded into the overall architecture. The 2G standards—the Global System for Mobile Communications (GSM)—and 3G security mechanisms offer a solid basis for EPS security architecture, but their ciphering algorithms and integrity methods still possess significant weaknesses. Moreover, because they are exposed to new and advanced communication threats, there's certainly room for further improvement. Here, we review the state of the art of the current encryption and authentication techniques that utilize a layered security approach, as well as examine security weaknesses and challenges that emerge from those ciphers' deployment in 4G wireless networks.

LTE/SAE 4G Network Security Architecture

The 3GPP general packet radio service (GPRS) core network allows 2G GSM and 3G LTE mobile networks to have IP interconnectivity with public networks such as the Internet. SAE, whose network architecture is illustrated in Figure 1, is the evolution of GPRS infrastructure, which enables LTE to become functional within the 4G era. The main component of the LTE/SAE network architecture, also known as the EPS, is the evolved packet core (EPC). The EPC contains the mobility management entity (MME) unit, the serving gateway (SGW), the packet data network (PDN)

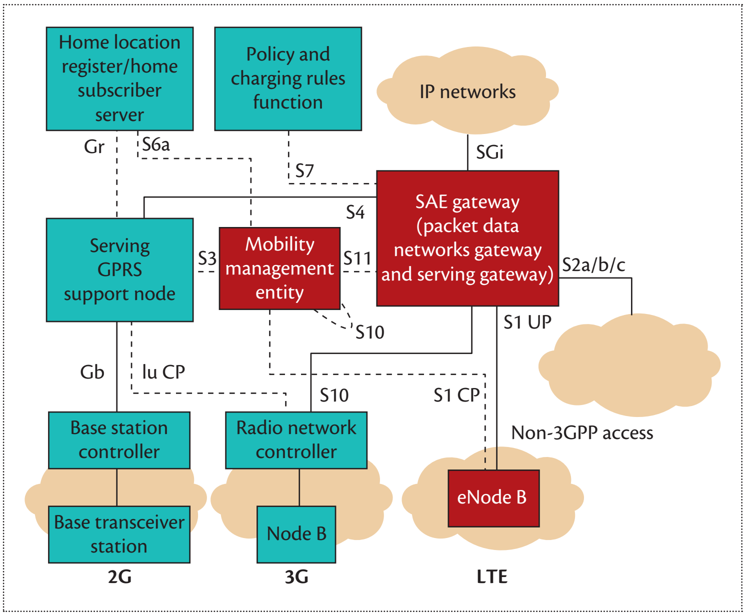
Home location register/home subscriber server
Policy and charging rules function
IP networks
Gr
S6a
S7
SGi
SAE gateway (packet data networks gateway and serving gateway)
S4
Serving GPRS support node
S3
Mobility management entity
S11
S2a/b/c
S10
S1 UP
Gb
Iu CP
S10
S1 CP
Non-3GPP access
Base station controller
Radio network controller
eNode B
Base transceiver station
Node B
2G
3G
LTE

Figure 1. The SAE evolved packet system's (EPS) architecture (LTE/SAE). The user plane functionality is represented by the entities inside the colored boxes. Solid and dashed lines correspond to traffic and signaling purposes for the SAE protocol.

gateway (PGW) units—both SGW and PGW are now unified as SAE gateway—and the policy and charging rules function (PCRF). The latter supports service policies for dataflow detection, enforcement, and flow-based client charging.

This architectural evolution reduces the number of nodes and manages to better distribute the processing load, minimizing latency in the network. Compared to the previous design, which involved more entity nodes (four in total), the system architecture is more simplified and contains two network elements—enhanced NodeBs (eNBs) and EPC—that implement the all-IP mobile core network for 3GPP LTE. In addition, the control plane is totally separated through a well-defined open-signaling interface (S11) between the MME node and gateway.[4,5]

Traditionally having minimum functionalities, the eNB, as the hardware presence of a user client inside the mobile network, now encompasses more critical operations—for example, Radio Resource Management, the routing capability of the user data toward the SGWs, and scheduling and transmissions of signaling messages. Likewise, the MME unit plays a key role in the control-related operations of LTE/SAE. Apart from being a termination point for the signaling (control) plane interfaces of SAE, as well as SAE's ciphering/integrity protection mechanisms, its main responsibility is user authentication and the optimal selection of an SGW for user equipment (UE) at the initial attaching phase. On its behalf, the SGW acts as a mobility anchor for both inter- and intra-handover connectivity across eNBs and other 3GPP technologies. It forwards and routes packets while the PGW simultaneously offers connectivity for the mobile user to external packet data networks.

It's worth noting that the home location register (HLR) of the original GSM (2G) and Universal Mobile Telecommunication System (UMTS; 3G) architecture is extended to the home subscriber server (HSS). The static subscriber information is maintained there and is integrated with the authentication center (AuC). The AuC also creates temporary authentication and security data that can be used for subscriber authentication and user traffic encryption.

For the smooth and consistent operation of the LTE/SAE network architecture, it is necessary for the previously described entities to connect each other with reference or termination points. We can easily identify them as solid or dashed single lines between the network entities. Links with a continuous line on them function as user traffic transmission connections, whereas dashed links are used for signaling purposes. 3GPP utilizes labels for each reference point such as S6a, S3, S4, S10, SGi, and Gr. The S6a interface, between MME and HSS, exchanges data related to the location of the mobile station and the management state of the subscriber. The SGi point might be an external or intra-operator packet data network. The S10 interface between multiple MMEs supports MME transmission of user information and MME relocation.[5] To provide a mutual authentication scheme between the UE and MME through the Evolved-UMTS Terrestrial Radio Access Network—the 4G wireless access network—the LTE/SAE reuses UMTS authentication and key agreement (UMTS-AKA). This authentication protocol, called *evolved packet system-authentication and key agreement* (EPS-AKA), is used to generate all the ciphering and integrity keys needed to ensure encryption and integrity protection. All the keys are derived via the key derivation function.

Although there are several known security weaknesses on the basic AKA protocol, the UE/universal subscriber identity module (UE/USIM)—the card embedded into subscribers' mobile phones used for their identification and authentication—always implements an AKA algorithm to create the mutual authentication with mobile core networks. In fact, although the authentication protocols might be different, they all implement the AKA algorithm on UE/USIM.[6]

LTE/SAE 3G Cryptographic Algorithms

Although 3G security specifications have already been standardized for the LTE protocol, extensible research is still carried out by the European Telecommunications Standards Institute (ETSI)—experts for the 4G stan-

Table 1. Advantages and disadvantages of Long-Term Evolution/System Architecture Evolution (LTE/SAE) encryption schemes.

LTE/SAE ciphers	Advantages	Disadvantages
Kasumi	Fits the requirements of the 3G security environment	Lacks adequate protection against new forms of attacks (like algebraic attacks)
	Offers strong encryption via 128-bit keys	Requires a trade-off between performance and complexity (in terms of space) owing to the implementation flexibility
	Is optimized for hardware implementation using previous block cipher Misty1	
	Offers strong resistance against most common block cipher attack methods	
SNOW 3G	Fits the requirements of the 3G security environment	Is more computationally complicated in terms of hardware area space regarding an application for integrity protection
	Offers adequate protection against new forms of algebraic attacks	
	Avoids similar design principles with Kasumi (like the atomic nonlinear functions)	
Milenage	Fits the requirements of the 3G security environment	Requires interoperability of different universal subscriber identity module implementations
	Offers strong encryption via 128-bit keys	For compatibility purposes, it would be easier if a standard algorithm was used
	Offers secure implementation and protection against side-channel attacks via Advanced Encryption Standard as core function	
ZUC	Fits the requirements of the 3G security environment	Requires more analysis to gain further confidence
	Offers strong encryption via 128-bit keys	
	Appears to have a sound design with a large security spectrum	
	Builds on design principles of well-known ciphering algorithms	

dard of LTE/SAE. The Security Algorithms Group of Experts (SAGE) task force analyzed the basic 3G algorithms for encryption and integrity protection for the LTE network standard. Table 1 presents the advantages and disadvantages of each.

The Kasumi Algorithm

The first ciphering algorithm for the LTE standard, the Kasumi algorithm, is mainly a block cipher algorithm that uses a key size of 128 bits. The algorithm utilizes two mapping functions to produce the ciphertext, which are called *S-boxes*. Kasumi was specifically designed as a building block for the UMTS encryption algorithms (UEA1) and integrity algorithms (UIA1).

SNOW 3G

SNOW 3G was designed as a second cryptographic solution in response to the appearance of newer forms of attacks—algebraic attacks—that would decrease Kasumi-based algorithms' security. Similar to the case of Kasumi, some changes were made to the original SNOW 2.0 to adapt it to the requirements of the demanding 3G environment and defend itself successfully against the newly discovered algebraic attacks. SNOW 3G is used as the core component of both UEA2 and UIA2.

The Milenage Algorithm

The Milenage encryption algorithm is the third 3G security algorithm deployed in LTE that uses a core function of a block cipher in which both block size and key size are 128 bits. Here, we can use the basic form of the Advanced Encryption Standard encryption algorithm as the core function.[6]

The ZUC Algorithm

In addition to the previous 3G cryptographic algorithms, the ETSI SAGE task force, together with Chinese cryptography experts, have already started the design work for a third algorithm pair specifically for 4G security. This beyond-3G cryptographic component is the ZUC algorithm, and it will be the core cipher block for UEA3/UIA3 set.

Vulnerabilities of LTE/SAE Security Algorithms and Procedures

Several EPS-specific threats that concern the whole EPS architecture and trust model have emerged with the characteristics of radio interface—thus posing great risks for the standards integrity environment. We further classify the main threat and risk categories that degrade the EPS security reliability as follows:

- *Threats against user identity and privacy.* A common threat category is defined by the illegal usage of user and mobile equipment identities to access network services. In particular, the potential malefic user could gain illegal access and usage of the security procedure keys to access network services. Another example might be the malicious modification of UE parameters to lock out the user from idle usage of services.[7]
- *Threats of UE/USIM tracking.* An example of this is tracking a user based on an IP address that could potentially be linked to an International Mobile Subscriber Identity (IMSI) or another identity.[8]
- *Threats related to base stations and handovers.* An example of this would be forcing a handover to a compromised base station via a powerful signal.
- *Threats related to broadcast or multicast signaling.* One method for this is to broadcast false system information across the network, causing disorder in the signaling plane.[7]
- *Threats related to denial of service (DoS).* One example of DoS threats could be causing DoS attacks against other UEs.
- *Threats against manipulation of control plane data.* One high-risk case of data manipulation is changing the signaling data of the EPS protocol to become comprehensible to eavesdroppers or to be modified in transit.
- *Threats of unauthorized access to the network.* In case there was illegal access to the EPS core network, malefic users can establish communication through the system for further security degradation.
- *Compromise of eNB credentials as well as physical attacks on an eNB.* False configuration data, faked or cloned credentials, and data associated with remote algorithmic attacks can severely compromise security.
- *Protocol attacks on an eNB.* These include security attacks that might involve dropping fake messages to the eNB (similar to DoS) by exploiting any protocol vulnerabilities.
- *Attacks on the core network, including eNB location-based attacks.* In an effort to report a false location of an eNB, this form of threat could lead to configuring the network with wrong parameters.

Most of the threats listed above are already addressed by the high-level requirements of the LTE/SAE security architecture specifications.

> **There's a possibility of malicious actors gaining improper access to 3G networks by exploiting AKA compatibility with GSM authentication.**

Target Objectives

So how secure are 3G systems? This is important to consider because all the specifications concerning the transition to the next generation (4G) of LTE security will be derived from practical aspects of applied 3G cryptographic algorithms' fidelity and reliability. But to fully answer this question, we need to focus on how well 3G telecommunication systems meet the availability, confidentiality, and integrity of key security objectives.

Availability

Availability is very critical for LTE/SAE: as the number of new subscribers radically increases, so do the security objectives with the authentication of users and network operators. On one hand, AKA is considered to be secure with the algorithms used by UMTS, but on the other hand, an IP-based operator network is not, nor is Internet Protocol security (IPsec) usage mandatory. This can create a potential vulnerability issue, particularly for DoS attacks. An example of this type of attack is flooding the radio frequencies with fake requests for wireless connection establishment.[3,7]

Confidentiality

Confidentiality might be the most achieved target of these three objectives, but several weaknesses occur in the LTE system—for example, there's a possibility of malicious actors gaining improper access to 3G networks by exploiting AKA compatibility with GSM authentication (related key attack).

Furthermore, the Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) uses a symmetric key (K), which is shared between the UE and the HSS to perform authentication and key agreement. All derived keys (such as CK, IK, MK, and MSK) were generated using K. For this reason, the disclosure of K is equal to the disclosure of all EAP-AKA's security procedures. The conclusion is that EAP-AKA doesn't provide perfect forward secrecy, referring to the security property that a session key derived from a set of long-term public and private keys is guaranteed to not be compromised if one of those keys should be compromised in the future.[8] Despite strong encryption offered by 128-bit keys, the confidentiality objective is not fully accomplished in LTE 3G networks.

Integrity

Integrity is primarily provided only for signaling channels, making this aspect the least achieved target of all three objectives.[9,10]

Security Enhancements in LTE/SAE Standard

For most security attacks, many crucial security features came along with the security standardization of the LTE/SAE. Many of those requirements led to the EPS security architecture being quite different from the 3G security architecture. Some of the design decisions are as follows:

- *Permanent security association.* One crucial security principle that must be kept in EPS is that the permanent key used in the AKA protocol should never be visible outside the security module and the AuC in the HLR because there's a permanent security association between the UE/USIM and the HLR.[6,11,12]
- *New key hierarchy in EPS.* In contrast to GSM and 3G, the novel introduction of a local master key serves many advantages, such as fulfilling the requirements of cryptographic network separation. Furthermore, this master key is less exposed because it is never transferred to the radio access network; therefore it remains in the core network.[11,12]
- *Need for mutual authentication mechanisms.* This is a cornerstone of the proper function of the whole EPS core because it lets the UE verify the authenticity of the network it is attached to and vice versa. In addition to the mutual identity-verification of both the terminal and the network, additional shared ciphering material between them allows for the confidentiality and integrity-protection of transmitted data.[6]
- *Trusted environment and secure execution.* All sensitive functions used for device authentication, such as operations involving the private key of the eNB, must be ensured in such a way that they will never leave the trusted environment. Another security feature, autonomous validation, in which the network is assured after successful authentication that only an integrity-checked device could have performed, should also be supported.[11,12]
- *DoS protection of network.* The restriction of the number of connections per eNB to the network must be performed; only validated eNBs should be allowed into the core network.[6,11,12]
- *User privacy.* IMSI should be kept secret both inside the device and over the air. Additionally, the confidentiality of signaling and user data must be retained.[11,12]
- *Authorization.* Authorization is necessary for the connection to core networks and for software integrity.

While the EPS security architecture has changed from the 3G architecture, there is still room for improvement, especially when considering the possibility of subsequent changes to mobile network security.

4G Security Architecture Proposals for LTE/SAE

We can't neglect future prospects that will likely shape the next generation of mobile network security architecture—for example, multilayered, end-to-end, framework-based protection—for LTE/SAE standards. Research efforts like the Handover Keying working group (Hokey WG) operating out of the Internet Engineering Task Force (IETF), IEEE Y-Comm, and the ITU X.805 framework are still in the draft process.

IETF Hokey Workgroup Project

A common procedure among wireless networks such as LTE/SAE is the handover, or handoff, which refers to the process of transferring an ongoing call or data session from one connected cell of the core network to another. A mobile device must reauthenticate each time it reattaches to the network. The authentication process is perhaps one of the most latency-consuming sources that prevents seamless handovers. This latency is partly due to the signaling overhead for authentication and association purposes between a user and the new access point. When the device goes through the full procedure of reauthentication, it creates a series of security vulnerabilities due to the UE. It's possible, however, to minimize the time it takes to reauthenticate by reusing the initial key authentication information produced from the first authentication.

The Hokey WG is currently undergoing comprehensive research, developing procedures for faster key reuse and authentication, while still maintaining adequate security practices. Although this research group has not yet implemented the complete suite of protocols, standards, and procedures needed for real security environment scenarios, it has already specified some concrete solutions, which are classified into different categories based on timing and mechanism issues.

One suggestion is that the authentication and key management take place before handoff, when latency is much less critical. Alternatively, they both could occur during handoff, when latency is indeed critical. In the first early authentication effort to reduce handover delay, the main advantage is that authentication and key agreement does not need to be performed during

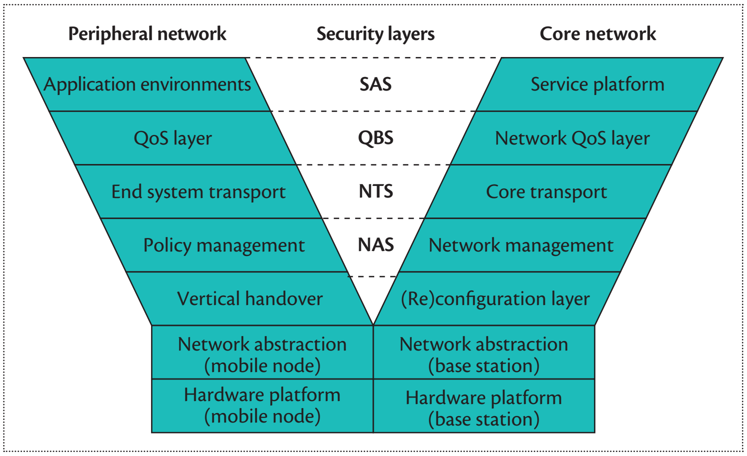

Figure 2. Y-Comm's overall architecture. Comm uses a four-layer security model, which is integrated into the two frameworks, peripheral and core. This allows Y-Comm to explore new security concepts. By using three separate security layers—network architecture security, network transport security, and service and application security—Y-Comm manages to ensure more secure packet transmission by taking all the necessary security measures first, taking the form of intrusion detection systems, firewalls, and IPsec, and manipulating network resources in an intelligent manner using sophisticated authentication protocols.

handoffs. In the second approach, the reuse of ciphering material generated during the initial authentication saves time during reauthentications. These solutions can also further minimize the total number of referrals to AAA servers as well as avoid the re-execution of size-consuming EAP information exchanges. This could be implemented by offering a more sophisticated management of the cryptographic keying material in conjunction with a protocol for the timely delivery of the corresponding keys to the corresponding entities. Such solutions could include practices like handover keying, low-latency reauthentication, preauthentication, or early authentication.

The Hokey WG is making efforts to define an extended master session key (EMSK)-based hierarchy for both authenticated and seamless handovers. This produced key is also referred to as the reauthentication Root Key (rRK). The rRK is used to derive the reauthentication Integrity Key and a reauthentication MSK that is specifically associated to each authenticator. The first key mainly plays the role of proof validation between the peer and the AAA server, whereas the second is used to derive the access link security-key material after the reauthentication procedure.

Concerning the milestones of the Hokey project, extensive standardization has been implemented over the past two years, with perhaps the most considerable event being the submission of the Hokey architecture draft to the Internet Engineering Steering Group in November 2011 (https://datatracker.ietf.org/wg/hokey/charter).

IEEE 802.21 Y-Comm Architecture

So how would you eventually build a commercial network to provide consistent, ubiquitous connectivity along with a necessary, adequate security level? Following many interconnectivity efforts, like the interworking procedure of LTE/SAE with non-3GPP networks and the security concerns that particularly arise, it soon became clear that traditional frameworks, such as the open systems interconnection model, aren't equipped to meet these challenges. As a result, a rather different approach became adaptable with the birth of Y-Comm architecture.

Y-Comm is a brand new communication architecture implemented in the Cambridge wireless testbed from the University of Cambridge. It is designed to provide coherent heterogeneous communication on a global scale. This new Internet generation will provide continuous connectivity through the seamless operation of multiple mobile networks. It will be accessible by mobile nodes, providing features like cognitive radio and vertical handover, while at the same time fostering all the QoS-aware mechanisms.

As illustrated in Figure 2, Y-Comm cements this new reality as an architecture based on two frameworks. The first, the peripheral framework, runs on the mobile node and interacts with wireless access networks. The second, the core framework, runs in a distributed fashion in the core infrastructure. Furthermore, in addition to this double-organized framework, Y-Comm has a multilayer security system that interacts with those two frameworks to provide a fully secure environment.

In March 2004, IEEE defined the 802.21 working group (published in 2008) to examine the possibility of standardizing this interface to different wireless media access controls.[9]

ITU X.805 Framework

One relevant research effort to unveil the security challenges that emerge in 4G networks was the development of the International Telecommunications Union X.805 standard as a systematic analysis tool based on the Bell Labs security model.[13,14] Based on the philosophy that threats to cellular systems can happen in any layer, as well as architectural planes, the X.805 builds a structured framework that considers and enhances multilayered, end-to-end network security features across eight security dimensions, serving as protection against all possible attacks and vulnerabilities.

In X.805, the network security is, as illustrated in Figure 3, organized in three layers (application, services, and infrastructure), three planes (end user, control, and management), and eight dimensions (access

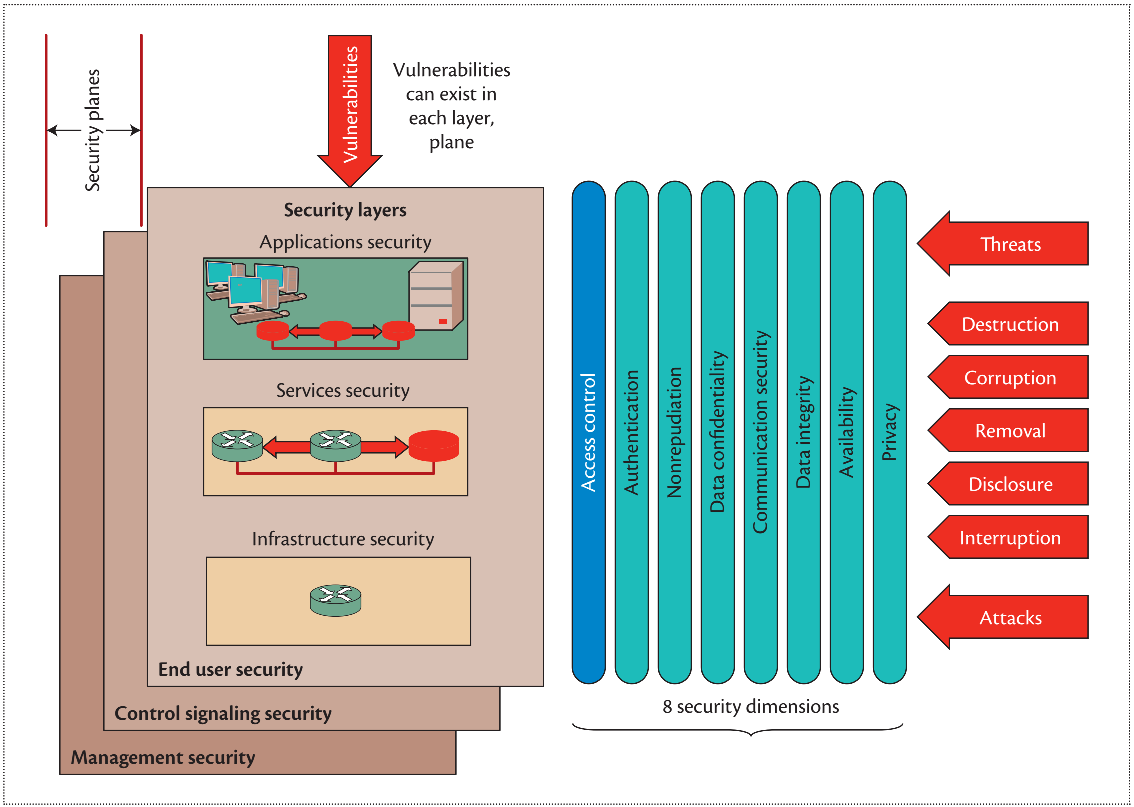

Figure 3. The ITU X.805 framework architecture. X.805 is built on nine modules, which are defined by three planes and three layers, where each module is analyzed using eight security dimensions. Regarding this architectural design, nine modules are defined by three planes and three layers, and each module is analyzed using the eight security dimensions. Each security dimension of each security module has different objectives, corresponding to different sets of security measures.[13,14] The Bell Labs security framework eventually became the ITU-T Recommendation X.805 standard in October 2003.

control, authentication, nonrepudiation, data confidentiality, communication security, data integrity, availability, and privacy).

Most of the research projects we mentioned in this article could easily integrate with the upcoming SAE/LTE protocol deployment in the 4G wireless network environment (that is, the service layers usage) in an effective, layered, and intelligent manner to confront the rising challenges of new asymmetric security threats. This work, though, still leaves us with the need to study the best compromise for including a mobility protocol and key management solution that best fits the SAE/LTE architecture, while at the same time maintaining a multilayered and multidimensional security approach. These two aspects—the selection of a straightforward ciphering key hierarchy distribution mechanism (Hokey project) and providing a layered network security architecture (Y-Comm and X.805 recommendations)—emerge as probably the most promising and novel solutions for tackling LTE/SAE security issues on 4G wireless networks. ■

References

1. I.S. Comsa et al., “Reinforcement Learning Based Radio Resource Scheduling in LTE-Advanced,” *Proc. 17th Int’l Conf. Automation and Computing* (ICAC 11), IEEE, 2011, pp. 219–224.
2. J. Berkmann et al., “On 3G LTE Terminal Implementation—Standard, Algorithms, Complexities and Challenges,” *Proc. Int’l Wireless Communications and Mobile Computing Conf.* (IWCMC 08), IEEE, 2008; doi:10.1109/IWCMC.2008.168.
3. Z. Shi et al., “Layered Security Approach in LTE and Simulation,” *Proc. 3rd Int’l Conf. Anti-counterfeiting, Security, and Identification in Communication* (ASID 09), IEEE, 2009; doi:10.1109/ICASID.2009.5276930.
4. C. Vintilă, V. Patriciu, and I. Bica, “Security Analysis of LTE Access Network,” *Proc. 10th Int’l Conf. Networks* (ICN 11), Int’l Academy, Research, and Industry Assoc., 2011, pp. 29–34.

5. *Network Architecture,* tech. specification 3GPP TS 23.002 V9.1.0, 3GPP, 2009.
6. D. Forsberg, *LTE Security,* John Wiley, 2010.
7. H. Mun, K.Han, and K. Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement Based on EAP-AKA," *Wireless Telecommunications Symp.* (WTS 2009), IEEE, 2009; doi:10.1109/WTS.2009.5068983.
8. N. Seddigh et al., "Security Advances and Challenges in 4G Wireless Networks," *Proc. 8th Conf. Privacy Security and Trust* (PST 10), 2010, IEEE; doi:10.1109/PST.2010.5593244.
9. L. Huang et al., "Performance of Authentication Protocols in LTE Environments," *Proc. Int'l Conf. Computational Intelligence and Security* (CIS 09), IEEE, 2009; doi:10.1109/CIS.2009.50.
10. L. Hui and B. Shuo, "Research and Implementation of LTE NAS Security," *Proc. Int'l Conf. Educational and Information Technology* (ICEIT 10), IEEE, 2010; doi:10.1109/ICEIT.2010.5607551.
11. *3G Security: Security Threats and Requirements,* tech. specification TS 21.133, 3GPP, 2001.
12. *3G Security: Security Principles and Objectives,* tech. specification TS 33.120, 3GPP, 2001.
13. Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," *Proc. Globecom Workshops,* IEEE, 2007; doi:10.1109/GLOCOMW.2007.4437813.
14. N. Sklavos and X. Zhang, eds., *Wireless Security & Cryptography: Specifications and Implementations,* CRC Press, 2007.

Anastasios N. Bikos is an undergraduate student in the Polytechnic School's Computer Engineering and Informatics Department at the University of Patras, Greece. His research interests include optical network protocols, wireless computer networks, cryptography, and wireless communications security. He's a member of IEEE. Contact him at mpikos@ceid.upatras.gr.

Nicolas Sklavos is an assistant professor with the Technological Educational Institute's Informatics and Mass Media Department in Patras, Greece. His research interests include system-on-chip design, computer architecture, VLSI design, and the security of computers and networks. Sklavos received a PhD in electrical and computer engineering from the University of Patras. He's a member of IEEE, IACR, and HIPEAC. Contact him at nsklavos@ieee.org.