Τμήμα Ψηφιακών Συστημάτων – Πανεπιστήμιο Πειραιά

Ανάλυση ρίσκου και προτεινόμενη αρχιτεκτονική συνεργασίας των παρόχων για μεγαλύτερη ασφάλεια σε 4G δίκτυα

Μια κριτική στο project ASMONIA

Αρχοντούλα Γκουτζιούλη

Ασφάλεια Ψηφιακών Συστημάτων

ΑΜ: 0905

Επιβλέπων: Χρήστος Ξενάκης

10 Νοεμβρίου 2012

Περιεχόμενα

Σύνοψη

Στα πλαίσια του project ASMONIA παρουσιάζεται μία ανάλυση ρίσκου για τηλεπικοινωνιακά δίκτυα τέταρτης γενιάς (4G) και προτείνεται μία αρχιτεκτονική η οποία επιτρέπει σε παρόχους τηλεπικοινωνιακών δικτύων, κυβερνητικούς και άλλους φορείς να συνεργαστούν προκειμένου να επιτευχθεί μεγαλύτερη ασφάλεια μέσω της διαμοίρασης πληροφοριών σχετικά με περιστατικά ασφάλειας. Η ανάλυση ρίσκου ακολουθεί μία ποσοτική μέθοδο η οποία όμως κρίνεται αδύναμη καθώς ο παράγοντας των συνεπειών (impact) δεν ερμηνεύεται μέσω μίας αντικειμενικής κλίμακας και για το λόγο αυτό προτείνεται μία πιθανή ερμηνεία της κλίμακας. Η αρχιτεκτονική που προτείνεται περιλαμβάνει τον σχηματισμό ενός δικτύου ACN (ASMONIA Collaborative Network) το οποίο προϋποθέτει επιπλέον υποδομές και τεχνικά μέσα προκειμένου η ανταλλαγή των πληροφοριών να γίνεται με ασφάλεια. Οι προτάσεις που παρουσιάζονται αποτελούν μία αρκετά καλή πρώτη προσέγγιση αφήνουν όμως αρκετά κενά, γεγονός που καθιστά δύσκολη την εφαρμογή τους, η οποία καθίσταται ακόμη πιο δύσκολη λόγω κυρίως του κόστους αλλά και της φύσης των σχέσεων των συμμετεχόντων, οι οποίες είναι ανταγωνιστικές.

Acknowledgements

Θα ήθελα να ευχαριστήσω τον καθηγητή Χρήστο Ξενάκη για την καθοδήγηση και υπομονή του και τον Χριστόφορο Νταντογιάν για την βοήθεια και την υποστήριξη που μου προσέφερε για την ολοκλήρωση αυτής της εργασίας. Ιδιαίτερες ευχαριστίες στον προϊστάμενο μου Μανώλη Μαραγκό αλλά και στους συνεργάτες μου, Γιώργο Ζαρογιάννη και Χαράλαμπο Πέτρου με τους οποίους συνεργαστήκαμε άψογα αυτά τα χρόνια. Θα ήθελα να ευχαριστήσω επίσης τους φίλους μου και ιδιαίτερα αγαπημένους μου Σωτήρη Πολυζόπουλο, Χριστίνα Δεληβορριά, Γιώργο Βλάχο, Δήμητρα Παππά και Νίκο Λάππα οι οποίοι ήταν πάντα πρόθυμοι να με βοηθήσουν σε τεχνικά και ακαδημαϊκά ζητήματα, αλλά και υποστηρικτικοί όταν τα πράγματα δεν ήταν τόσο ομαλά. Τέλος οφείλω απέραντη ευγνωμοσύνη στην οικογένεια μου η οποία με στηρίζει πάντα.

Glossary

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
AAA	Authentication Authorization and Accounting
ACGW	ASMONIA Collaboration Gateway
ACN	ASMONIA Collaboration Network
ACN-I	ACN Interface
ARIB	Association of Radio Industries and Business
AS	Application Server
ASMONIA	**A**ttack analysis and **S**ecurity concepts for **MO**bile **N**etwork infrastructures, supported by collaborative **I**nformation exch**A**nge
ATIS	Alliance for Telecommunications Industry Solutions
AuC	Authentication Center
BSC	Base Station Controller
BSI	British Standards Institution
BSS	Base Station System
BTS	Base Transceiver Station
CBC	Cell broadcast Center
CCSA	China Communications Standards Association
CK	Ciphering Key
CS	Circuit Switched
DHCP	dynamic Host Configuration protocol

DSL	Digital Subscriber Line
EAP	Extensible Authentication protocol
EIR	Equipment Identity Register
EMM	EPS Mobility Management
eNB	Evolved NodeB
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESM	EPS Session Management
E-SMLC	Evolved Serving Mobile Center
ETSI	European Telecommunication Standards Institute
e-UTRAN	Evolved Universal Terrestrial Radio Access Network
EWS	Early Warning System
FC CC	Functional Cluster Collaborative Cloud
FC IP	Functional Cluster IP
FC MA	Functional Cluster Monitor and Analysis
FDMA	Frequency Division Multiple Access
GAP	Generic Access Protocol
GERAN	GSM Edge Radio Access Network
GMLC	Gateway Mobile Location Centre
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HE	Home Environment
HeMS	HeNB Management System
HeNB	Home eNB

HeNB-GW	Home eNB Gateway
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server
IK	Integrity key
IKEv2	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPSec	Internet Protocol Security
ITU	International Telecommunication Union
LTE	Long Term Evolution
MME	Mobility Management Entity
MPC	Multiparty Computation
MS	Mobile Station
MSC	Mobile Switching Center
NAS	Non Access Stratum
NIST	National Institute of Standards and Technology
OAM	Operation And Maintenance
OFDMA	Orthogonal Frequency Division Multiple Access
ON	Operator Network
PCEF	Policy and Charging Enforcement Point
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN-GW	Packet Data Network Gateway
PKI	Public Key Infrastructure

PLMN	Public Land Mobile Network
PMIPv6	Proxy Mobile IPv6
PS	Packet Switched
P-TMSI	Packet TMSI
RMM	Reputation Monitoring Module
RADIUS	Remote Authentication Dial In User Service
RN	Relay Node
RNC	Radio Network Controllers
SAE	System Architecture Evolution
SAE-GW	SAE Gateway
SC-FDMA	Single Carrier FDMA
SDO	Standards Development Organization
SeGW	Security Gateway
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SIM	Subscriber Identity module
SN	Serving Network
SQM	Sequence number Management
TAC	Traceable Anonymous Certificate
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
UE	User Equipment

USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Netwrork
VLR	Visitor Location register
VPLMN	Visited PLMN
VPN	Virtual private Network
WCDMA	Wideband Code Division Multiple Access

1. Εισαγωγή

Το ερευνητικό έργο (research project) ASMONIA (**A**ttack analysis and **S**ecurity concepts for **MO**bile **N**etwork infrastructures, supported by collaborative **I**nformation exch**A**nge) πραγματεύεται τη δυνατότητα για συνεργασία μεταξύ των παρόχων, των κατασκευαστών, των χρηστών, των κυβερνητικών υπηρεσιών αλλά και άλλων φορέων οι οποίοι αντιμετωπίζουν ίδιου τύπου απειλές ασφάλειας, προκειμένου να επιτευχθεί μεγαλύτερη ασφάλεια σε ένα τηλεπικοινωνιακό δίκτυο τέταρτης γενιάς (4G Network). Στα πλαίσια του έργου συνεργάζονται οι ακόλουθοι φορείς:

- Cassidian, ERNW GmbH
- Fraunhofer Research Institution for Applied and Integrated Security AISEC
- University of AppliedAugsburg
- Nokia Siemens Networks
- RWTH Aachen University
- Federal Agency for Digital Radio of Security Authorities and Organizations
- Federal Office for Information Security
- Deutsche Telekom AG

Κύριος στόχος του έργου είναι η ανάπτυξη μιας διευρυμένης έννοιας του όρου ασφάλειας των υποδομών δικτύων κινητής τηλεφωνίας, η οποία θα ικανοποιεί τις ποικίλες απαιτήσεις των σύγχρονων δικτύων. Το έργο στοχεύει στην βελτίωση της ανθεκτικότητας, της αξιοπιστίας και της ασφάλειας, τόσο των παρόντων όσο και των μελλοντικών δικτύων κινητών τηλεπικοινωνιών. Οι επιμέρους στόχοι του έργου ASMONIA είναι οι εξής:

- Ανάλυση ρίσκου κινητών δικτύων και τερματικών συσκευών (Risk analysis of mobile networks and end devices)
- Ορισμός εννοιών προστασίας υπό το πρίσμα της συνεργασίας
- Προστασία της ακεραιότητας των δικτυακών συσκευών
- Ενσωμάτωση ανθεκτικών και ευέλικτων συστημάτων ως βασικών συστατικών μονάδων
- Ανάπτυξη τεχνικών ανίχνευσης επιθέσεων και αξιολόγησής τους

Απώτερος σκοπός του ASMONIA είναι να επιτευχθεί η επικοινωνία με τα υπάρχοντα Συστήματα Έγκαιρης Προειδοποίησης (Early Warning Systems, EWSs) ούτως ώστε να ανταλλάζονται πληροφορίες σχετικές με επιθέσεις που έχουν ήδη καταγραφεί από τα συστήματα αυτά, οι οποίες θα μπορούν να χρησιμοποιηθούν και από τους συμμετέχοντες στο ASMONIA.

Στα πλαίσια του ASMONIA πραγματοποιείται μία σειρά από δημοσιεύσεις η οποία περιλαμβάνει τα ακόλουθα [1], [2], [3], [4], [5], [6], [7] και [8] στα οποία παρουσιάζονται με λεπτομέρεια οι ερευνητικές προσπάθειες που έλαβαν χώρα για τους σκοπούς του συγκεκριμένου project. Η παρούσα εργασία εστιάζει στα [1], [5] και [8] στα οποία παρουσιάζεται η προτεινόμενη αρχιτεκτονική και η ανάλυση ρίσκου σε 4G δίκτυο. Στις υπόλοιπες δημοσιεύσεις παρουσιάζονται οι ερευνητικές προσπάθειες που καλύπτουν περιοχές όπως τα λειτουργικά συστήματα και η τεχνολογία cloud και ως εκ τούτου δεν αποτελούν βασική περιοχή μελέτης για την παρούσα εργασία.

Η δομή της εργασίας στηρίζεται στις δημοσιεύσεις του ASMONIA αλλά δεν περιορίζεται σε αυτές. Στο δεύτερο κεφάλαιο παρουσιάζονται πληροφορίες σχετικά με τον οργανισμό 3GPP και τα κινητά δίκτυα τηλεπικοινωνιών όπως διαμορφώνονται στις τεχνολογίες GSM και UMTS. Η αρχιτεκτονική του 4G δικτύου στο δίκτυο πρόσβασης και στο δίκτυο κορμού παρουσιάζεται στο κεφάλαιο 3. Στη συνέχεια ακολουθεί η ανάλυση ρίσκου όπως παρουσιάζεται στο [8] και μία κριτική σε αυτήν. Στο κεφάλαιο 5 παρουσιάζεται η προτεινόμενη αρχιτεκτονική η οποία θα επιτρέπει τη συνεργασία μεταξύ των συμμετεχόντων ενώ το κεφάλαιο 6 περιλαμβάνει τα τεχνικά μέσα και τις απαιτήσεις που θα πρέπει να καλύπτει η συγκεκριμένη αρχιτεκτονική καθώς και την κριτική που γίνεται σε αυτήν. Τέλος, το κεφάλαιο 7 περιλαμβάνει τα συμπεράσματα που προκύπτουν από την μελέτη του συγκεκριμένου project.

2. Background

2.1 Οργανισμός προτυποποίησης 3GPP

Ο οργανισμός προτυποποίησης 3GPP (3rd Generation Partnership Project) ιδρύθηκε το 1998 από πέντε υπάρχοντες οργανισμούς ανάπτυξης προτύπων (SDOs, Standards Development Organizations) με σκοπό να εξασφαλιστεί η δημιουργία ενός προτύπου, εφαρμόσιμου από τα δίκτυα 3G, που θα υιοθετηθεί από όλους τους οργανισμούς. Οι ιδρυτικοί οργανισμοί είναι οι ETSI (European Telecommunication Standards Institute), ARIB (Association of Radio Industries and Business, Japan), TTC (Telecommunication Technology Committee, Japan), ATIS (Alliance for Telecommunications Industry Solutions, North America) και TTA (Telecommunications Technology Association, South Korea), ενώ στη συνέχεια προστέθηκε και ο CCSA (China Communications Standards Association).

Το 1999 έγινε η πρώτη δημοσίευση προτύπων, γνωστή ως Release 99 (το όνομα της έκδοσης εναρμονίζεται με το έτος δημοσίευσης). Έκτοτε ο οργανισμός δημοσιεύει νέες εκδόσεις (Release 4,5, κτλ.) ενώ παράλληλα διορθώνονται και ενημερώνονται οι υπάρχουσες εκδόσεις οπότε και δημοσιεύονται οι ενημερωμένες εκδοχές τους. Οι δημοσιεύσεις του οργανισμού είναι ελεύθερα διαθέσιμες μέσω της ιστοσελίδας τους [9].

Σχήμα 1 3GPP logo

Η πρώτη από τις εκδόσεις στην οποία ορίζεται το LTE/SAE είναι η όγδοη έκδοση (Release 8). Τυπικά, τα δίκτυα 4G συμμορφώνονται με τις προδιαγραφές που καθορίζονται από την δέκατη έκδοση (Release 10) και έπειτα, και είναι γνωστά και ως LTE-advanced. Για αρκετά δίκτυα ωστόσο χρησιμοποιείται ο όρος 4G χωρίς αυτά να είναι συμβατά με τη Release 10, αλλά με τη Release 8 όπου και παρουσιάστηκε το σύστημα EPS. Στη συνέχεια της εργασίας το δίκτυο 4G δεν θα αναφέρεται αποκλειστικά στα δίκτυα LTE-advanced, αλλά θα αναφέρεται σε οποιοδήποτε δίκτυο υιοθετεί την αρχιτεκτονική SAE.

Η μετάβαση από τα δίκτυα 2G/3G στα 4G αναμένεται να μην πραγματοποιηθεί από τη μία μέρα στην άλλη και αυτό είναι κάτι που προβλέπεται και από τα πρότυπα 3GPP.

Στα πρότυπα λοιπόν ορίζονται τρόποι που καθιστούν δυνατή την πρόσβαση στο EPC δίκτυο μέσω των 2G/3G δικτύων.

2.2 Κινητά δίκτυα επικοινωνιών

Τα πρώτα κινητά δίκτυα επικοινωνιών εμφανίστηκαν περίπου στις αρχές της δεκαετίας του ’80 στις Η.Π.Α. και σε χώρες της βορείου Ευρώπης. Αυτά τα δίκτυα πρώτης γενιάς επέτρεπαν ήδη την ταυτόχρονη πρόσβαση σε πολλούς χρήστες από το ίδιο κελί μέσω της τεχνολογίας FDMA (Frequency Division Multiple Access), αλλά και την εναλλαγή κελιών κατά τη διάρκεια μιας σύνδεσης. Αντιπροσωπευτικό παράδειγμα αποτελεί η τηλεφωνική κλήση από το αυτοκίνητο.

Τα κινητά δίκτυα δεύτερης γενιάς (2G) έκαναν την εμφάνισή τους μια δεκαετία περίπου αργότερα. Χρησιμοποιούν την τεχνολογία Global System for Mobile (GSM), το σήμα μεταδίδεται ψηφιακά ανάμεσα στη συσκευή και τον σταθμό βάσης και η πολλαπλή πρόσβαση επιτυγχάνεται μέσω της τεχνολογίας TDMA (Time Division Multiple Access), εξασφαλίζοντας έτσι μεγαλύτερη χωρητικότητα δικτύου, καλύτερη ποιότητα κατά τις κλήσεις ενώ γίνεται παράλληλα και η εισαγωγή κάποιων βασικών χαρακτηριστικών ασφάλειας.

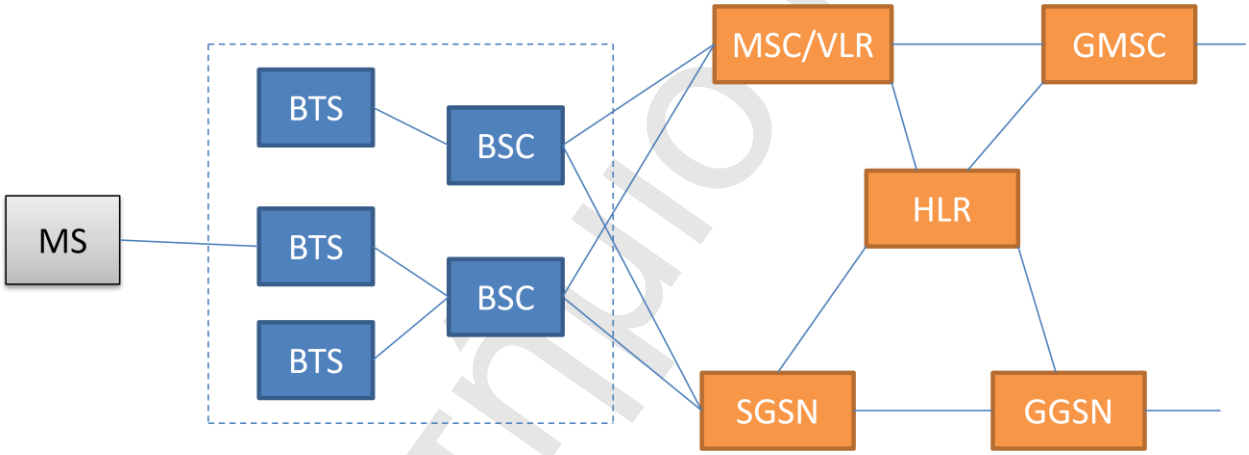
Στις αρχές της επόμενης δεκαετίας εμφανίζονται οι τεχνολογίες τρίτης γενιάς (3G) και έχουν σαν στόχο να επιτρέπουν την παγκόσμια περιαγωγή ώστε να μπορούν οι χρήστες να χρησιμοποιούν τις υπηρεσίες των κινητών δικτύων από οπουδήποτε στον κόσμο. Για την προτυποποίηση των τεχνολογιών συστάθηκε ο οργανισμός 3GPP. Τα δίκτυα 3G παρέχουν αυξημένο ρυθμό δεδομένων (2Mbps στην πρώτη έκδοση). Η πολλαπλή πρόσβαση ακολουθεί την τεχνολογία WCDMA (Wideband Code Division Multiple Access). Τόσο τα δίκτυα 3G όσο και τα δίκτυα 2G αποτελούνται από δύο κατηγορίες δικτύων οι οποίες διακρίνονται από την τεχνολογία μεταγωγής που χρησιμοποιούν. Οι δύο αυτές κατηγορίες είναι το δίκτυο μεταγωγής κυκλώματος (CS, Circuit Switched) το οποίο χρησιμοποιείται για την μεταφορά ομιλίας, και το δίκτυο μεταγωγής πακέτων (PS, Packet Switched) το οποίο χρησιμοποιείται για την μεταφορά δεδομένων.

Η επόμενη δεκαετία (2010) είναι η δεκαετία που αναπτύσσονται τα δίκτυα τέταρτης γενιάς (4G) από τον οργανισμό 3GPP. Οι όροι LTE (Long Term Evolution) και SAE (System Architecture Evolution) χρησιμοποιούνται για να περιγράψουν αυτή την εξέλιξη. Το νέο σύστημα είναι διαφορετικό ως προς το δίκτυο μετάδοση σήματος, το οποίο καλείται E-UTRAN (Evolved Universal Terrestrial Radio Access Netwrork) και το δίκτυο κορμού, το οποίο καλείται EPC (Evolved Packet Core). Το νέο σύστημα καλείται EPS

(Evolved Packet System) και είναι βασισμένο εξολοκλήρου στην αρχιτεκτονική διευθυνσιοδότησης δικτύου (all-IP based architecture). Προσφέρει ιδιαίτερα αυξημένο ρυθμό δεδομένων (100 Mbps) και η πολλαπλή πρόσβαση επιτυγχάνεται μέσω της τεχνολογίας OFDMA (Orthogonal Frequency Division Multiple Access) στην κατερχόμενη ζεύξη (downlink) και της τεχνολογίας SC-FDMA (Single Carrier FDMA) στην ανερχόμενη ζεύξη [10].

2.3 GSM (2G)

Σε ένα 2G δίκτυο, το δίκτυο πρόσβασης καλείται BSS (Base Station System). Τα συστατικά μέρη του BSS είναι τα BTS (Base Transceiver Station) και BSC (Base Station Controller).



Σχήμα 2 2G Architecture

Στο Σχήμα 2 η τερματική συσκευή MS (Mobile Station όπως αποκαλείται στο 2G) είναι εξοπλισμένη με μία κάρτα SIM (Subscriber Identity module) και συνδέεται με τον σταθμό βάσης σηματοδοσίας BTS. Ο BTS είναι υπεύθυνος για την σηματοδοσία και για την κρυπτογράφηση και αποκρυπτογράφηση της επικοινωνίας μεταξύ αυτού και του BSC.

Ο σταθμός ελέγχου βάσης BSC μπορεί να υποστηρίξει τη σύνδεση με περισσότερους από ένα BTS, τυπικά κάποιες εκατοντάδες. Υλοποιεί την απαιτούμενη λογική πίσω από το BTS και είναι υπεύθυνος για το χειρισμό των ραδιοσυχνοτήτων και την εναλλαγή μεταξύ των BTS (handover). Όπως φαίνεται και στο Σχήμα 2, μέσω του BSC το σήμα μεταφέρεται στο MSC/VLR εάν πρόκειται για υπηρεσίες που υλοποιούνται πάνω από το CS, ή στο SGSN εάν οι υπηρεσίες υλοποιούνται πάνω από το PS.

Τα βασικά χαρακτηριστικά ασφάλειας που υλοποιούνται στο GSM είναι

- η αυθεντικοποίηση του χρήστη στο δίκτυο
- η κρυπτογράφηση κατά τη μετάδοση σήματος για εμπιστευτικότητα της επικοινωνίας και
- η χρήση προσωρινών αναγνωριστικών για ανωνυμία του χρήστη

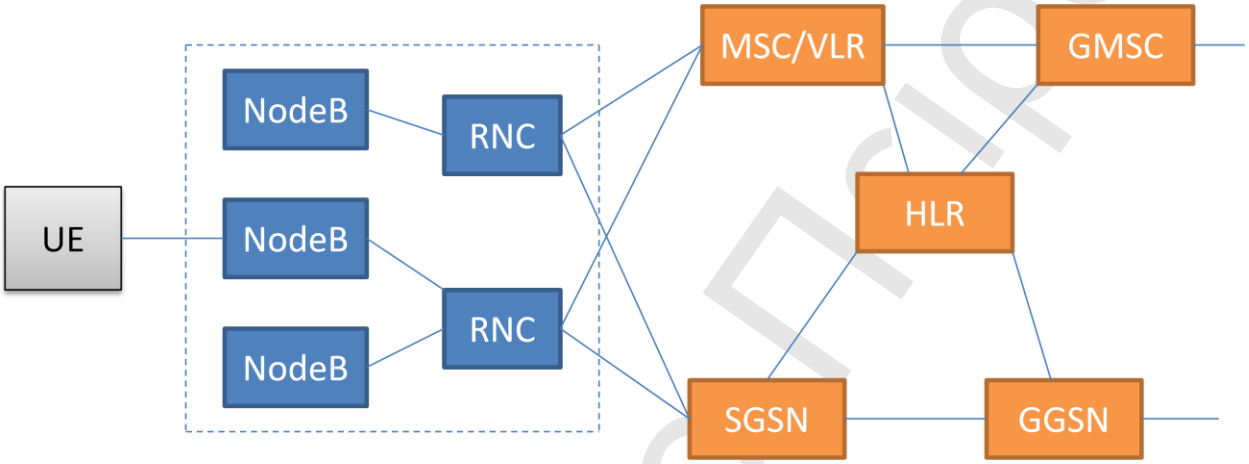
Η αυθεντικοποίηση γίνεται μέσω ενός κλειδιού Ki το οποίο βρίσκεται στην κάρτα SIM και στο AuC (Authentication Center) που βρίσκεται στην HLR (Home Location register). Το κλειδί αυτό είναι μοναδικό και παραμένει το ίδιο στο πέρασμα του χρόνου. Ο αλγόριθμος που χρησιμοποιείται κατά τη διαδικασία της αυθεντικοποίησης είναι ο A3 ο οποίος περιγράφεται στο παράρτημα Α. Η αδυναμία του GSM ως προς την αυθεντικοποίηση έγκειται στο γεγονός ότι μόνο ο χρήστης αυθεντικοποιείται στο δίκτυο και όχι το δίκτυο στο χρήστη. Συνεπώς είναι πιθανές επιθέσεις τύπου masquerade network μέσω faked BTS.

Κατά τη διαδικασία της αυθεντικοποίησης παράγεται επίσης το κλειδί Kc μέσω του αλγόριθμου A8. Το κλειδί αυτό είναι είσοδος για τους αλγόριθμους A5 (A5/0, A5/1, A5/2, A5/3) από τους οποίους παράγεται το κρυπτογραφημένο μήνυμα. Με τον τρόπο αυτό, η επικοινωνία ανάμεσα στο MS και το BTS είναι κρυπτογραφημένη. Εξετάζοντας τους αλγόριθμους ως προς την ασφάλεια που προσφέρουν παρατηρείται ότι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται από το GSM για μεγάλο διάστημα παρέμεναν μυστικοί (security by obscurity) καθιστώντας την μελέτη τους από την κοινότητα αδύνατη. Επίσης έχει αποδειχθεί ότι οι αλγόριθμοι είναι δυνατό να «σπάσουν», αποκαλύπτοντας έτσι το κλειδί Ki όπως παρουσιάζεται και στα [11], [12], [13], [14] και σε παρόμοιες εργασίες. Άλλη μια αδυναμία πηγάζει από το γεγονός ότι το κλειδί Kc μεταφέρεται μη κρυπτογραφημένο μέσω διάφορων στοιχείων του δικτύου.

Η ταυτότητα του χρήστη στο δίκτυο είναι ο αριθμός IMSI (International Mobile Subscriber Identity) ο οποίος βρίσκεται στην κάρτα SIM του χρήστη. Για να μην μεταφέρεται ο αριθμός IMSI στο δίκτυο, χρησιμοποιείται ένα προσωρινό αναγνωριστικό, το TMSI (Temporary Mobile Subscriber Identity). Στην περίπτωση του PS, το προσωρινό αναγνωριστικό είναι το P-TMSI (Packet TMSI). Το TMSI βασίζεται στο IMSI και παράγεται από το δίκτυο κατά τη διαδικασία αυθεντικοποίησης του χρήστη (από το SGSN το P-TMSI). Και αυτό το χαρακτηριστικό ασφάλειας του GSM αποδεικνύεται ότι παραβιάζεται μέσω επιθέσεων man-in-the-middle, όπου ένας μη νόμιμος BTS καταφέρνει να αποσπάσει το IMSI.

2.4 UMTS (3G)

Το 3G δίκτυο έχει βασιστεί στο δίκτυο 2G και αποτελεί ουσιαστικά την εξέλιξή του. Αυτό που αλλάζει είναι το δίκτυο πρόσβασης σε ένα 3G δίκτυο το οποίο αποτελείται από τους σταθμούς βάσης, οι οποίοι καλούνται NodeB, και από τους ελεγκτές του δικτύου σήματος (Radio Network Controllers, RNCs). Η τερματική συσκευή στο 3G δίκτυο ονομάζεται UE (User Equipment). Στο Σχήμα 3 παρουσιάζεται το δίκτυο πρόσβασης που συναντάται σε 3G δίκτυα.



Σχήμα 3 3G Αρχιτεκτονική

Στη συσκευή του χρήστη βρίσκεται η USIM (Universal Subscriber Identity Module) η οποία αντικαθιστά την SIM και προσφέρει κάποιες λειτουργίες ασφάλειας. Οι σταθμοί βάσης NodeB δεν προσφέρουν κάποια χαρακτηριστικά ασφάλειας και οι λειτουργίες τους επικεντρώνονται στο να επικοινωνούν με τις μονάδες ελέγχου σηματοδοσίας του δικτύου, RNC. Όπως και στο δίκτυο 2G, το σήμα μεταφέρεται στο MSC/VLR εάν πρόκειται για υπηρεσίες που υλοποιούνται πάνω από το CS, ή στο SGSN εάν οι υπηρεσίες υλοποιούνται πάνω από το PS.

Οι βελτιώσεις του 3G δικτύου ως προς τα χαρακτηριστικά ασφάλειας σε σχέση με το 2G δίκτυο είναι

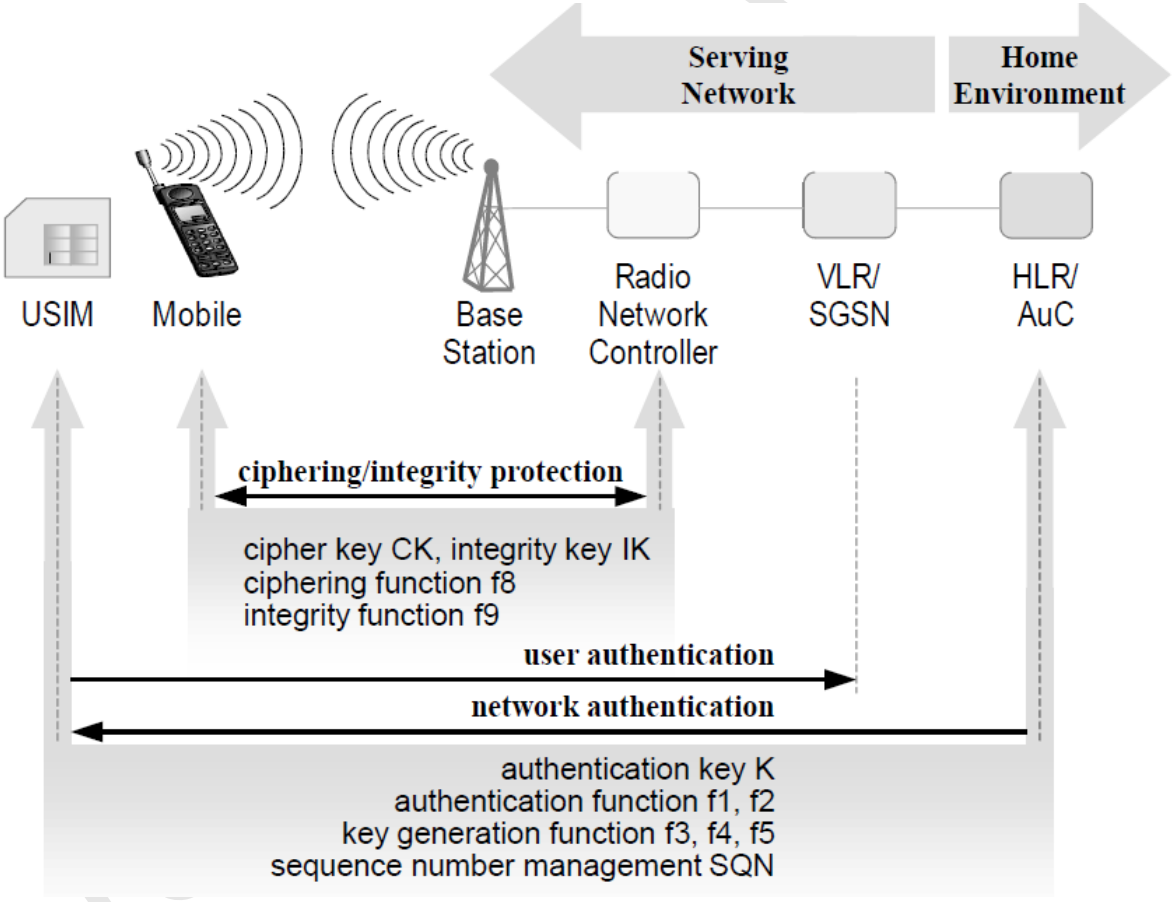
- η αμοιβαία αυθεντικοποίηση
- η ανανέωση των κλειδιών που χρησιμοποιούνται κατά την αυθεντικοποίηση
- η προστασία της ακεραιότητας των μηνυμάτων σηματοδοσίας
- η χρήση ισχυρότερων αλγορίθμων κρυπτογράφησης
- η κρυπτογράφηση η οποία επεκτείνεται στο δίκτυο κορμού

Για την αυθεντικοποίηση και για τη συμφωνία κλειδιών στο 3G χρησιμοποιείται το πρωτόκολλο UMTS AKA (Authentication and Key Agreement) το οποίο περιγράφεται στο [15]. Η αμοιβαία αυθεντικοποίηση επιτυγχάνεται μεταξύ της USIM και του δικτύου εξυπηρέτησης SN (Serving Network). Στη διαδικασία αυθεντικοποίησης συμμετέχει

επίσης το HE (Home Environment) μέσω του AuC. Η διαδικασία στηρίζεται στο γεγονός ότι ο χρήστης μέσω της USIM και το SN αποδεικνύουν τη γνώση ενός κλειδιού K χωρίς να αποκαλύπτεται το ίδιο το κλειδί. Κατά την αυθεντικοποίηση παράγονται επίσης τα κλειδιά CK (Ciphering key) και IK (Integrity key) τα οποία χρησιμοποιούνται για την κρυπτογράφηση και την ακεραιότητα των μηνυμάτων σηματοδοσίας.

Η ανανέωση των κλειδιών επιτυγχάνεται χάρη στη χρήση τυχαίων αριθμών RAND κατά τη διαδικασία της αυθεντικοποίησης. Κάθε φορά που θα πραγματοποιείται η διαδικασία της αυθεντικοποίησης θα χρησιμοποιείται ένα νέο RAND το οποίο εξασφαλίζεται ότι δεν έχει επαναχρησιμοποιηθεί μέσω των αριθμών σειράς (sequence numbers) που χρησιμοποιούνται από το πρωτόκολλο. Τα sequence numbers διαχειρίζονται από το SQM (Sequence number Management) το οποίο βρίσκεται στη USIM και στο AuC.

Στο Σχήμα 4 παρουσιάζονται οι προαναφερθέντες μηχανισμοί ασφάλειας καθώς και τα στοιχεία του δικτύου που αποτελούν τα όρια εφαρμογής τους.



Σχήμα 4 Μηχανισμοί ασφάλειας στο UMTS

Όπως και στο δίκτυο 2G, έτσι και στο 3G, η ανωνυμία του χρήστη επιτυγχάνεται με τη χρήση των προσωρινών αναγνωριστικών TMSI και P-TMSI. Και σε αυτή την περίπτωση

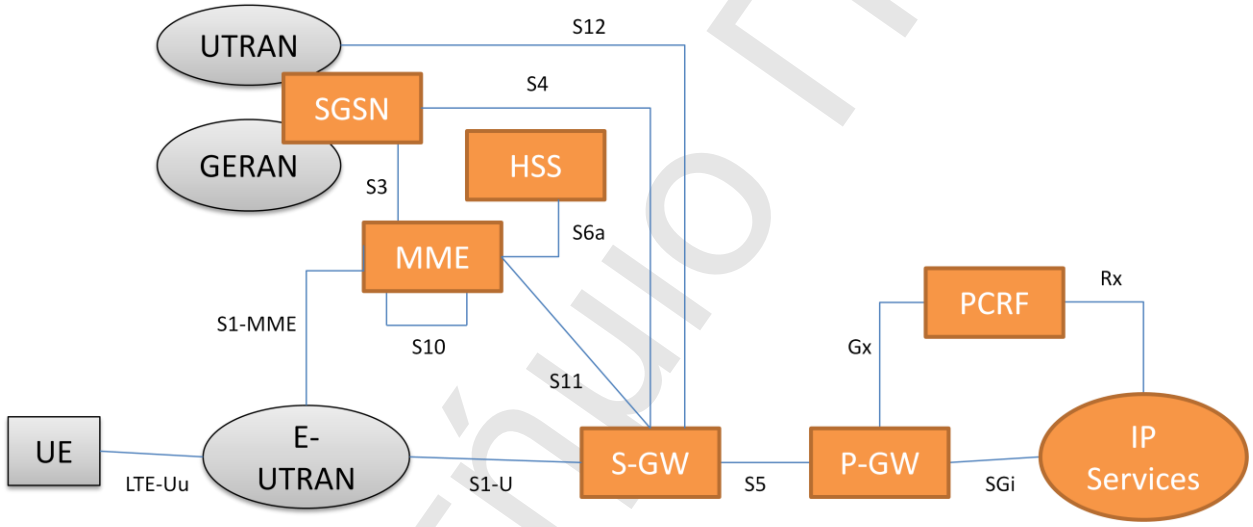
ο συγκεκριμένος μηχανισμός δεν είναι επαρκής αφού το πραγματικό αναγνωριστικό χρήστη, IMSI, μεταφέρεται στο δίκτυο. Επιπλέον, και η θέση του χρήστη μπορεί να αποκαλυφθεί κατά τη διαδικασία όπου το SN ζητά το IMSI όπως περιγράφεται στο [16].

Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται στο 3G δίκτυο είναι βασισμένοι στον αλγόριθμο KASUMI για τον οποίο λεπτομέρειες περιέχονται στο [17]. Πρόκειται για έναν αλγόριθμο που είναι προϊόν σχεδιασμού του οργανισμού 3GPP στα πλαίσια συγκεκριμένου project και οι λεπτομέρειες βρίσκονται στο [18]. Χρησιμοποιεί blocks μεγέθους 64 bits και ένα κλειδί μεγέθους 128 bits. Για τον ίδιο σκοπό, ο ίδιος οργανισμός προχώρησε και στο σχεδιασμό επιπλέον αλγορίθμων βασισμένων στον αλγόριθμο SNOW3G, για τον οποίο οι λεπτομέρειες βρίσκονται στο [19].

Αν και δημοσιεύονται επιθέσεις για τον αλγόριθμο KASUMI, η μεγαλύτερη αδυναμία του δικτύου 3G εξακολουθεί να είναι η αναγκαία συμβατότητα με το δίκτυο 2G, από το οποίο κληρονομεί και τις αδυναμίες που παρατηρούνται σε αυτό και περιγράφονται στο [20].

3. Αρχιτεκτονική δικτύου

Ο οργανισμός 3GPP ορίζει την αρχιτεκτονική LTE/SAE όπως παρουσιάζεται στο Σχήμα 5. Στο σχήμα παρουσιάζεται η γενική εικόνα ενώ διακρίνονται από αριστερά προς τα δεξιά η τερματική συσκευή UE (User Equipment), τα δίκτυα πρόσβασης GERAN (GSM Edge Radio Access Network), UTRAN (UMTS Radio Access Network) και E-UTRAN (Enhanced UTRAN) και οι καινούριες οντότητες που εισάγονται από τη νέα αρχιτεκτονική οι οποίες είναι οι MME (Mobility Management Entity), HSS (Home Subscriber Server), S-GW (Serving Gateway) και P-GW (Packet Data Network Gateway). Τα SGSN, PCRF και IP Services συνεχίζουν να υφίστανται όπως και στις προγενέστερες τεχνολογίες.



Σχήμα 5 Αρχιτεκτονική LTE/SAE

Αυτό που χαρακτηρίζει την εξέλιξη της αρχιτεκτονικής είναι το νέο δίκτυο πρόσβασης E-UTRAN, το οποίο και επιτρέπει την υλοποίηση ενός νέου δικτύου σήματος (RAN, Radio Access Network). Η καινοτομία αυτού του νέου δικτύου είναι ότι λειτουργεί αποκλειστικά ως δίκτυο μεταγωγής πακέτων (PS).

Στο παραπάνω σχήμα περιλαμβάνονται επίσης τα δίκτυα πρόσβασης GERAN για δίκτυα 2G και UTRAN για δίκτυα 3G. Μέσω των GERAN και UTRAN είναι δυνατή η χρήση του σχηματιζόμενου δικτύου από συσκευές που δεν υποστηρίζουν την σύνδεση στο νέο δίκτυο πρόσβασης E-UTRAN. Η διατήρηση των προηγούμενων δικτύων πρόσβασης είναι αναγκαία προκειμένου η νέα τεχνολογία να είναι συμβατή με τις παλαιότερες συσκευές. Ο λόγος που προκύπτει αυτή η ανάγκη είναι μάλλον εμπορικός καθώς η αναβάθμιση του δικτύου ενός παρόχου σε δίκτυο LTE δεν μπορεί να πραγματοποιηθεί αγνοώντας την πλειοψηφία των χρηστών οι οποίοι δεν διαθέτουν

τερματική συσκευή, συμβατή με την τεχνολογία LTE. Επιπλέον το κόστος της αναβάθμισης του δικτύου είναι μεγάλο, επομένως είναι λογικό και αναμενόμενο η αναβάθμιση να πραγματοποιηθεί σταδιακά. Συνεπώς για μεγάλο διάστημα το δίκτυο θα λειτουργεί ως συνδυασμός 2G/3G στο δίκτυο πρόσβασης και EPC στο δίκτυο κορμού.

Η νέα αρχιτεκτονική χαρακτηρίζεται all flat IP architecture επειδή στηρίζεται αποκλειστικά στη χρήση διευθύνσεων IP μεταξύ των δομικών στοιχείων. Ακόμη και στην περίπτωση της κίνησης δεδομένων στο επίπεδο χρήστη (user plane traffic) αυτό επιτυγχάνεται απλώς με τη χρήση των δύο νέων στοιχείων eNodeB και S-GW.

eNodeB (ή αλλιώς eNB) καλείται ο σταθμός βάσης στο 4G δίκτυο. Το eNB επικοινωνεί με το MME και το S-GW. Το MME είναι το βασικό στοιχείο ελέγχου για την πρόσβαση στο 4G δίκτυο. Είναι υπεύθυνο για το control plane traffic και για την είσοδο του χρήστη στο δίκτυο (attach). Το S-GW είναι υπεύθυνο για τη διαχείριση του user plane traffic. Το S-GW συνδέεται με το P-GW (μπορεί να υλοποιούνται και ως ένα στοιχείο), το οποίο παρέχει τη σύνδεση προς τα εξωτερικά δίκτυα δεδομένων (παραδείγματος χάρη το Internet) στο χρήστη. Το HSS αποτελεί την εξέλιξη του HLR από το 2G/3G καθώς είναι η βάση στην οποία γίνεται η αυθεντικοποίηση του χρήστη.

Το 4G δίκτυο μπορεί να διαχωριστεί λογικά στις τερματικές συσκευές (UE), στο δίκτυο πρόσβασης, στο δίκτυο κορμού και στο δίκτυο υπηρεσιών. Οι ενότητες που ακολουθούν περιγράφουν το δίκτυο πρόσβασης και το δίκτυο κορμού ενώ στο τέλος του κεφαλαίου παρουσιάζεται η γενική εικόνα του δικτύου.

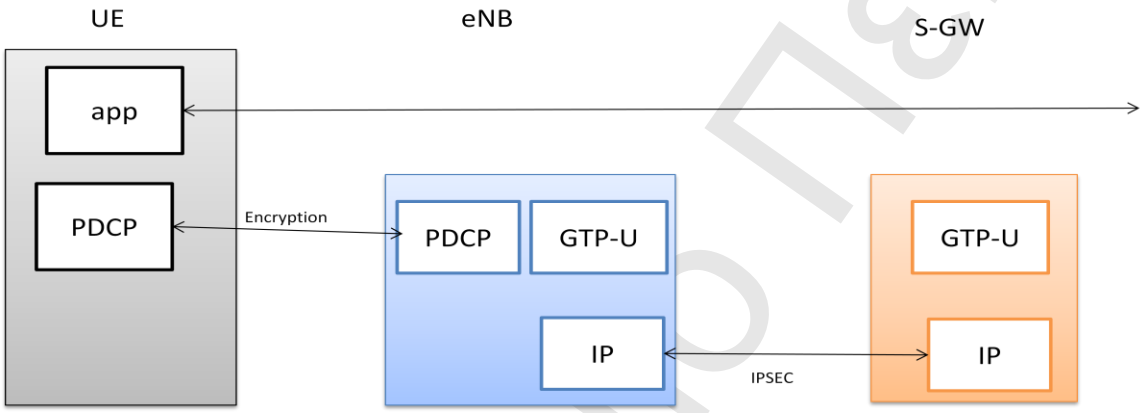
3.1 Δίκτυο πρόσβασης

Το βασικό στοιχείο στο δίκτυο πρόσβασης E-UTRAN είναι το eNodeB το οποίο και αποτελεί το τερματικό σημείο κρυπτογράφησης για το δίκτυο ραδιοσήματος. Για την καλύτερη κάλυψη ραδιοσήματος χρησιμοποιούνται τα Relay nodes (RN). Όμοια με τα eNodeB υπάρχουν τα HeNBs (Home eNodeBs) τα οποία είναι μικρογραφίες των eNodeBs που εγκαθίστανται συνήθως σε εταιρείες και επιτρέπουν την σύνδεση στο 4G δίκτυο μέσω Internet. Προκειμένου να πραγματοποιηθεί αυτή η σύνδεση απαιτείται η χρήση του SeGW (Security Gateway) και προαιρετικά η χρήση των HeNB-GW (HeNB Gateway), HeMS (HeNB Management System) και AAA server (Authentication, Authorization, Accounting).

3.1.1 eNodeB

Στα eNB υλοποιούνται τρία interfaces: το interface προς την τερματική συσκευή (UE, User equipment) το οποίο καλείται LTE-Uu, το interface προς το δίκτυο κορμού (S1) και το interface μεταξύ των eNBs (X2). Το S1 interface διακρίνεται στα S1-MME και S1-U τα οποία είναι τα interfaces προς το MME και το S-GW αντίστοιχα.

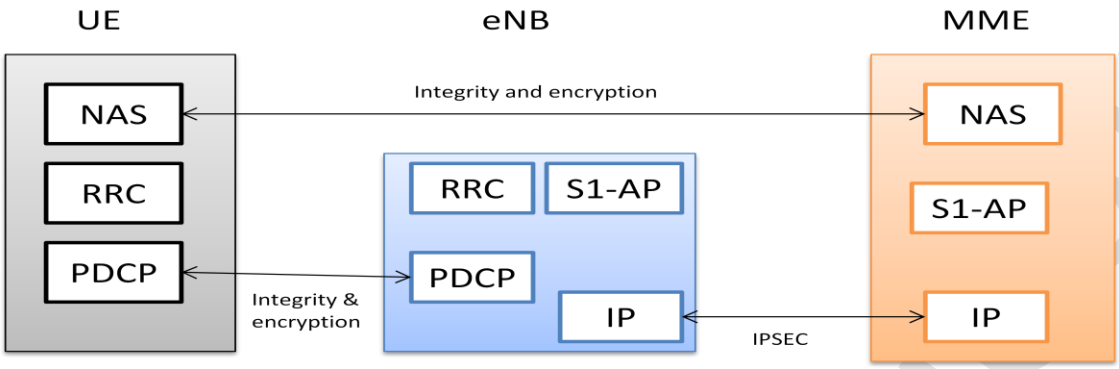
Το S1-U interface χρησιμοποιείται για τη μεταφορά της κίνησης του χρήστη προς το Internet μέσω του S-GW, ενώ το S1-MME χρησιμοποιείται για τη σηματοδοσία προς το MME. Στο Σχήμα 6 και Σχήμα 7 φαίνονται οι στοίβες πρωτοκόλλων που χρησιμοποιούνται στο user plane και στο control plane αντίστοιχα, καθώς και οι μηχανισμοί ασφάλειας που ενσωματώνονται στη στοίβα.



Σχήμα 6 Στοίβα πρωτοκόλλων στο user plane

Στην περίπτωση του user plane τα δεδομένα που μεταφέρονται από το UE στο eNB είναι κρυπτογραφημένα στο επίπεδο του PDCP (Packet Data Convergence Protocol). Με τον τρόπο αυτό εξασφαλίζεται η εμπιστευτικότητα των δεδομένων. Για την κρυπτογράφηση των δεδομένων από το eNB στο S-GW χρησιμοποιείται IPSec.

Όμοια με το user plane, για το control plane ανάμεσα στο UE και στο eNB εξασφαλίζεται η προστασία της εμπιστευτικότητας στο επίπεδο του PDCP. Στο ίδιο επίπεδο ενσωματώνεται και η προστασία της ακεραιότητας. Οι ίδιες αρχές ασφάλειας εφαρμόζονται και στο επίπεδο του NAS (Non-Access Stratum) μεταξύ του UE και του MME. Το IPSec χρησιμοποιείται για την κρυπτογράφηση ανάμεσα στο eNB και το MME αλλά και στο X2 interface.

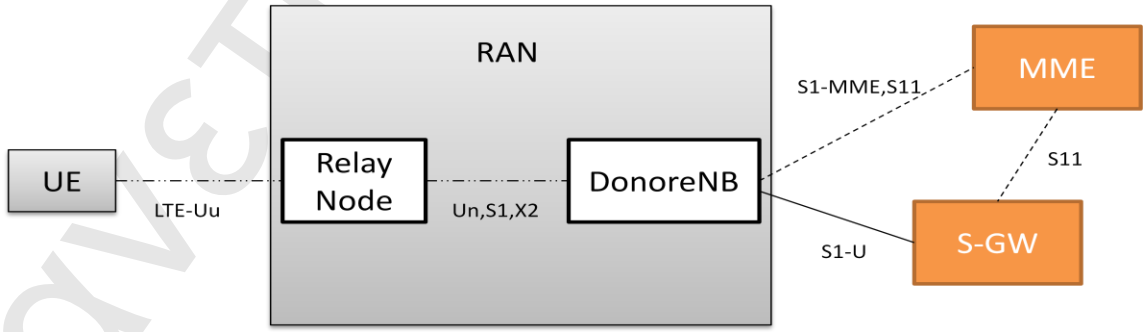


Σχήμα 7 Στοίβα πρωτοκόλλων στο control plane

Το NAS υποδηλώνει τα πρωτοκόλλα που χρησιμοποιούνται για τη σηματοδοσία και την κίνηση των δεδομένων του χρήστη μεταξύ του χρήστη και του δικτύου κορμού. Στο 4G δίκτυο ορίζονται δύο νέα πρωτόκολλα από τον οργανισμό 3GPP, τα οποία είναι το EMM (EPS Mobility Management) και το ESM (EPS Session Management). Μέσω του EMM υλοποιούνται λειτουργίες όπως έλεγχος της κινητικότητας, ανίχνευση της θέσης του χρήστη και αυθεντικοποίηση του UE στο δίκτυο. Μέσω του ESM υλοποιούνται λειτουργίες ελέγχου και διαχείρισης των εικονικών συνδέσεων πάνω από τις οποίες πραγματοποιείται η κίνηση του χρήστη. Στα 4G δίκτυα οι συνδέσεις αυτές ονομάζονται EPS Bearers.

3.1.2 Relay Node

Στόχος του RN είναι να βελτιώσει την κάλυψη του ραδιοσήματος σε περιοχές που δεν καλύπτονται από τα eNBs. Το RN συμπεριφέρεται όπως το eNB προς το UE και αποτελεί σημείο τερματισμού του ραδιοσήματος. Ωστόσο δεν συνδέεται απευθείας με το υπόλοιπο δίκτυο αλλά συνδέεται σε κάποιο eNB μέσω του interface Un. Το eNB στο οποίο συνδέεται το RN καλείται Donor eNB.

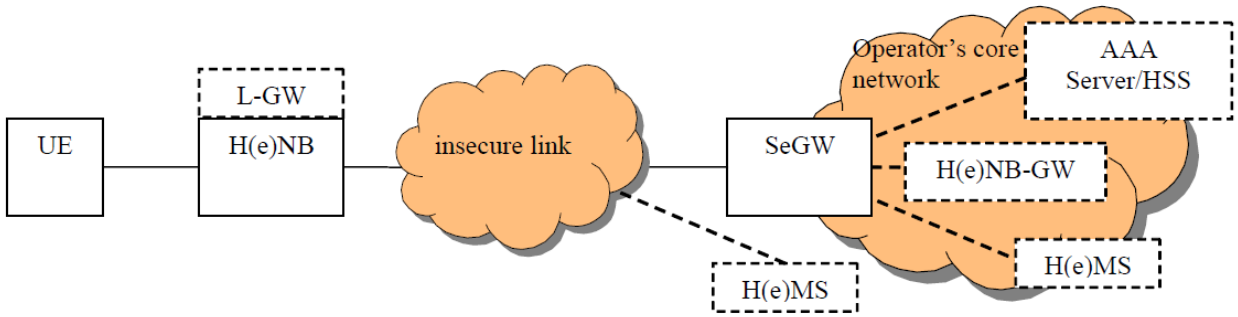


Σχήμα 8 Relay node και Donor eNB

Στο Σχήμα 8 παρουσιάζονται τα RN και Donor eNB καθώς και τα interfaces που υλοποιούνται. Το Un interface υλοποιεί παρόμοιες λειτουργίες με αυτές του LTE-Uu. Έτσι από το RN μεταφέρεται user traffic μέσω στοίβας πρωτοκόλλων όμοιας με αυτή του S1-U και control plane traffic μέσω στοίβας πρωτοκόλλων όμοιας με αυτή του S1-MME. Το ίδιο ισχύει και για το X2 interface. Τέλος, στο Donor eNB υλοποιούνται λειτουργίες που του επιτρέπουν να διαχωρίσει την κίνηση σε user plane και control plane προκειμένου να αναμεταδώσει το κάθε είδος στο αντίστοιχο στοιχείο του δικτύου, δηλαδή το control plane στο MME και το user plane στο S-GW.

3.1.3 Home eNodeB

Τα HeNB είναι πολύ μικρά eNBs τα οποία χρησιμοποιούνται σε οικιακά δίκτυα η σε δίκτυα εταιρειών προκειμένου να παρέχουν σύνδεση σε 4G δίκτυο μέσω σύνδεσης στο Internet, παραδείγματος χάρη μέσω DSL σύνδεσης. Με τον τρόπο αυτό χρησιμοποιούνται οι υποδομές του παρόχου της DSL σύνδεσης μέχρι το σημείο σύνδεσης με το δίκτυο 4G.



Σχήμα 9 Αρχιτεκτονική HeNB και SeGW

Το σημείο σύνδεσης με το δίκτυο κορμού είναι το SeGW. Στο Σχήμα 9 εμφανίζεται η προτεινόμενη από το 3GPP αρχιτεκτονική. Στην αρχιτεκτονική περιλαμβάνονται τα HeNB και SeGW αλλά και με διακεκομμένο πλαίσιο τα προαιρετικά στοιχεία HeMS, HeNB-GW και AAA.

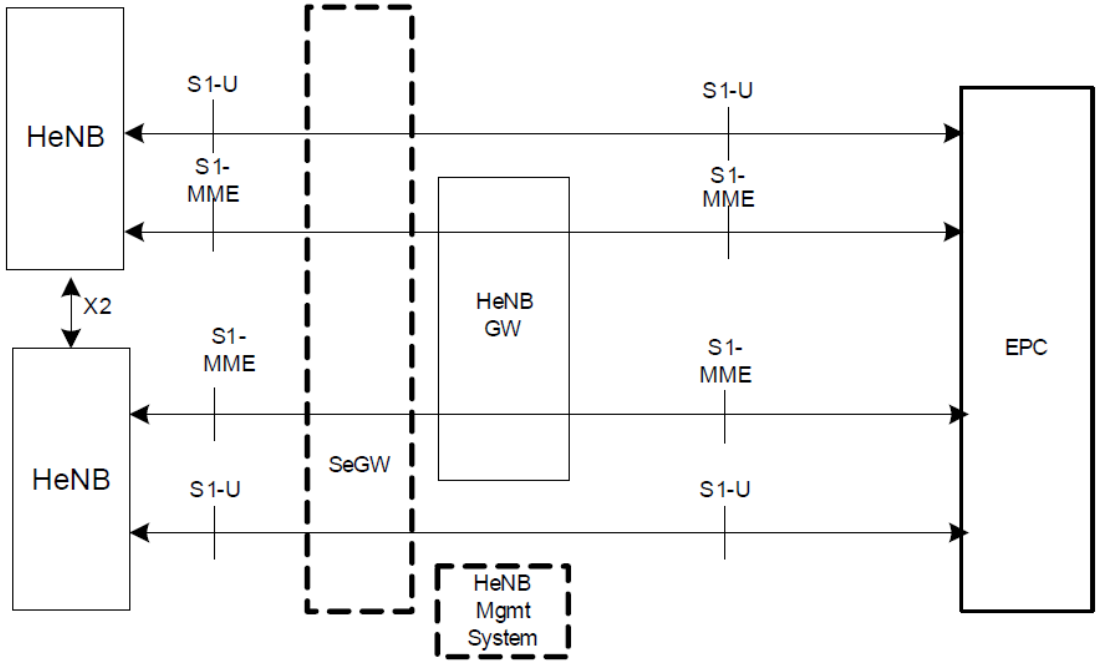
Όλη η προερχόμενη από το HeNB κίνηση διέρχεται πάνω από μη ασφαλή ζεύξη για να καταλήξει στο SeGW. Το SeGW ίσως χρησιμοποιήσει τον AAA για την αυθεντικοποίηση. Επίσης ενδέχεται η κίνηση από πολλαπλά HeNB να συναθροιστεί αρχικά στο HeNB-GW και στη συνέχεια να προσπελάσει από εκεί το δίκτυο κορμού. Στην περίπτωση που δεν χρησιμοποιείται το HeNB-GW η κίνηση από τα HeNBs θα περάσει απευθείας στο δίκτυο κορμού από το SeGW. Η διαχείριση των HeNBs γίνεται

μέσω των HeMS. Τα HeMS ενδέχεται να αποτελούν στοιχεία του δικτύου του παρόχου. Είναι όμως πιθανών να μην αποτελούν μέρος του δικτύου αλλά να αποκτούν πρόσβαση στα HeNBs απευθείας μέσω της σύνδεσης Internet όταν η διαχείριση τους γίνεται από τον πάροχο των HeNBs.

Για την ασφαλή μεταφορά της κίνησης από το HeNB στο SeGW συνιστάται η χρήση IPSec. Από το 3GPP συνιστάται επίσης η χρήση συσκευής που θα πραγματοποιεί την αμοιβαία αυθεντικοποίηση που είναι απαραίτητη για τα HeNBs και το SeGW όπως περιγράφεται και στο [21]. Στην περίπτωση που το HeMS δεν αποτελεί μέρος του δικτύου του παρόχου, συνιστάται η χρήση σύνδεσης TLS προκειμένου να επιτευχθεί η αμοιβαία αυθεντικοποίηση.

3.1.4 Home eNodeB Gateway

Το HeNB-GW αποτελέι ένα κεντρικό σημείο του δικτύου στο οποίο συγκεντρώνεται η κίνηση από τα HeNBs. Το πλεονέκτημα από αυτού του είδους την τοπολογία είναι ότι η κίνηση από όλα τα HeNBs παρουσιάζεται στο MME ως κίνηση από ένα μόνο στοιχείο. Με τον τρόπο αυτό καθίσταται δυνατόν να συνδεθούν πολλαπλά HeNB χωρίς να επηρεαστεί το MME. Το HeNB-GW υλοποιεί την ίδια στοίβα πρωτοκόλλων για τα S1-U και S1-MME interfaces.



Σχήμα 10 Αρχιτεκτονική HeNB-GW

Στο Σχήμα 10 παρουσιάζεται η αρχιτεκτονική που προτείνεται για το HeNB-GW από το 3GPP στο [22]. Το S1-MME interface υλοποιείται και για τις δύο κατευθύνσεις (MME και HeNB). Το S1-U interface ενδέχεται να μην υλοποιείται μέσω του HeNB-GW αλλά να αποτελεί ένα άμεσο interface ανάμεσα στα HeNB και MME.

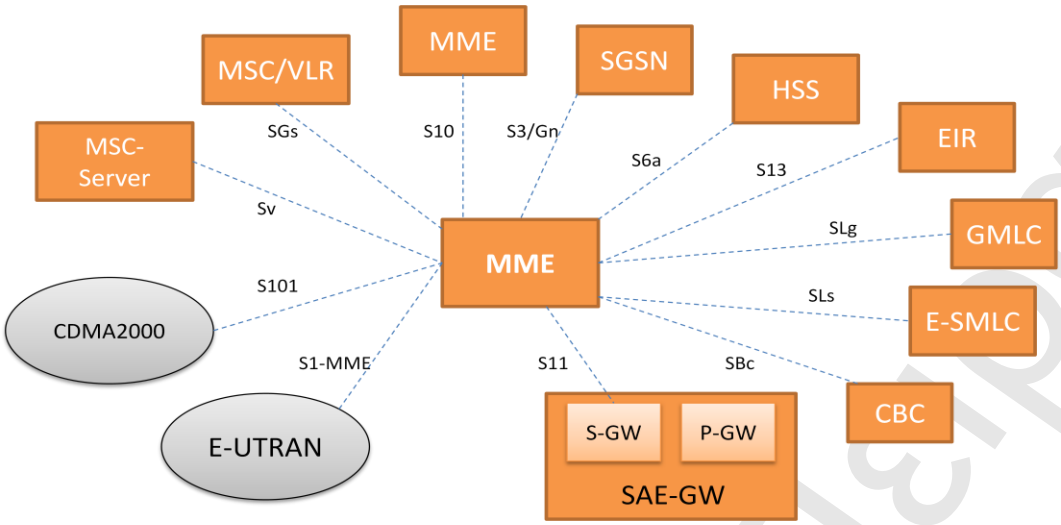
3.2 Δίκτυο κορμού

Το δίκτυο κορμού στο 4G δίκτυο καλείται EPC (Evolved Packet Core). Τα βασικά στοιχεία είναι το MME και το SAE-GW (ως SAE-GW αναφέρεται το S-GW και το P-GW). Το MME είναι το στοιχείο που ελέγχει την πρόσβαση στο δίκτυο και γενικότερα το control plane traffic. Το SAE-GW είναι το κεντρικό στοιχείο του δικτύου που είναι αρμόδιο για το user plane traffic. Λειτουργίες σχετικές με τη διαχείριση των συνδρομητών πραγματοποιούνται από το HSS και το EIR (Equipment Identity Register). Τα 3GPP ορίζουν το PCRF (Policy and Charging Rules Function) για την διαχείριση της πολιτικής του δικτύου και τις υπηρεσίες χρέωσης.

Όπως αναφέρθηκε προηγουμένως, η πρόσβαση στο δίκτυο είναι δυνατή και μέσω τεχνολογιών 2G/3G. Αυτό επιτυγχάνεται μέσω του SGSN το οποίο επιτρέπει τη σύνδεση στο δίκτυο κορμού. Επιπλέον επιτρέπεται η πρόσβαση μέσω τεχνολογιών που δεν ορίζονται από τα 3GPP (non-3GPP access). Για την περίπτωση αυτή χρησιμοποιείται το στοιχείο ePDG (evolved Packet Data Gateway) το οποίο επιτρέπει την πρόσβαση στο 4G δίκτυο από δίκτυο πρόσβασης non-3GPP, με την υποστήριξη και του AAA ο οποίος παρέχει τις υπηρεσίες αυθεντικοποίησης.

3.2.1 Mobility Management Entity

Από το MME διέρχεται μόνο control plane traffic. Είναι το στοιχείο του δικτύου που είναι υπεύθυνο για τη διαχείριση της κινητικότητας (mobility management) στο δίκτυο. Στο Σχήμα 11 παρουσιάζεται το MME και τα interfaces που έχει με τα άλλα στοιχεία του δικτύου.



Σχήμα 11 Το MME στο δίκτυο

Τα interfaces τα οποία ενώνουν τα δίκτυα πρόσβασης με το MME είναι τα S1-MME και S101. Το S1-MME χρησιμοποιείται για την επικοινωνία μεταξύ MME και eNodeB αλλά και για τη μεταφορά του κλειδιού *KeNB* που παράγεται από το MME στο eNodeB προκειμένου να χρησιμοποιηθεί για την παραγωγή των κλειδιών κρυπτογράφησης του ραδιοσήματος. Το S101 interface επιτρέπει στο MME να συνδέεται στο CDMA2000 δίκτυο πρόσβασης.

Η σύνδεση του MME με τα MSC-Server (Mobile Switching Center Server) και MSC/VLR (Visitor Location register) επιτρέπει τη συνέχιση μιας κλήσης φωνής (CS) στην περίπτωση που ο χρήστης μεταβαίνει από 2G/3G δίκτυο πρόσβασης σε 4G, και γίνεται μέσω των interfaces Sv και SGs αντίστοιχα.

Τα MME επικοινωνούν μεταξύ τους μέσω του S10 interface. Η επικοινωνία τους περιλαμβάνει λειτουργίες που επιτρέπουν την εναλλαγή του MME στο οποίο είναι συνδεδεμένος ο χρήστης και την μεταφορά των σχετικών πληροφοριών. Τα SGSN που βρίσκονται στο δίκτυο για την υποστήριξη των GERAN και UTRAN επικοινωνούν με το MME μέσω του S3/Gn interface.

Στα HSS και EIR βρίσκονται οι πληροφορίες σχετικά με τους συνδρομητές. Συγκεκριμένα στο HSS γίνεται η αυθεντικοποίηση του χρήστη και παράγεται επίσης το κλειδί από το οποίο θα προκύψουν τα κλειδιά κρυπτογράφησης ραδιοσήματος και NAS, ενώ στο EIR βρίσκονται πληροφορίες σχετικά με τις τερματικές συσκευές που χρησιμοποιούνται από τους χρήστες του δικτύου. Για τη σύνδεση τους με το MME, τα HSS και EIR χρησιμοποιούν τα interfaces S6a και S13.

Η επικοινωνία με τα GMLC (Gateway Mobile Location Center) και E-SMLC (Evolved Serving Mobile Center) γίνεται μέσω των SLg και SLs αντίστοιχα για την υποστήριξη

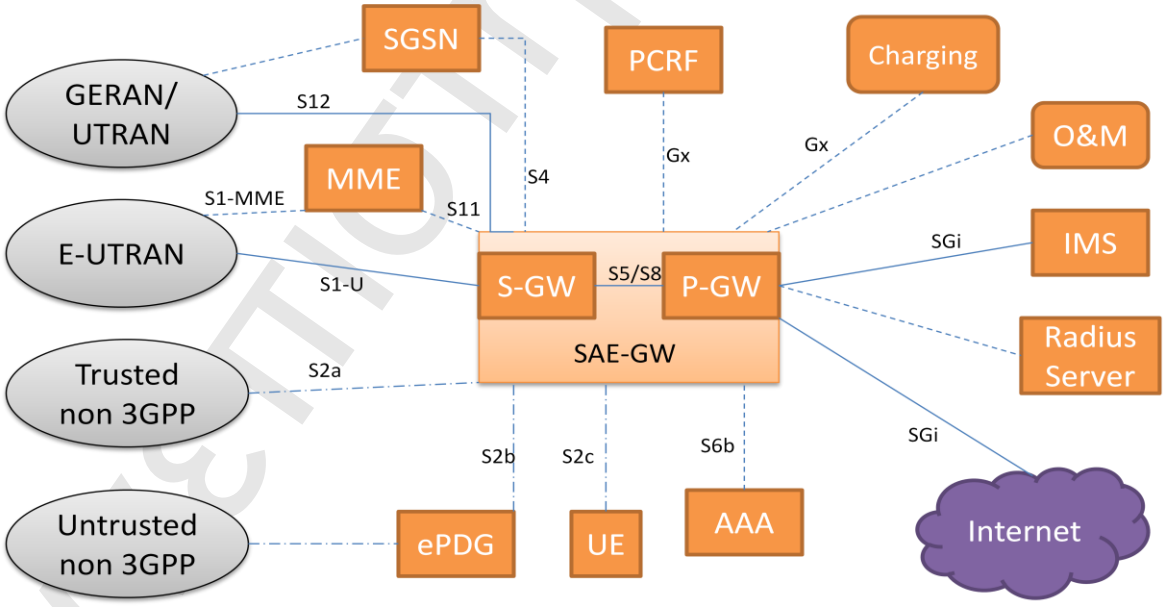
υπηρεσιών βασισμένες στην τοποθεσία (locations services). Για την επικοινωνία με το CBC (Cell Broadcast Center), το οποίο διατηρεί πληροφορίες σχετικά με το κελί στο οποίο βρίσκεται ο χρήστης όταν η πρόσβαση γίνεται μέσω GERAN ή UTRAN, χρησιμοποιείται το SBc interface.

Το S11 interface χρησιμοποιείται για τη σύνδεση του MME με το SAE-GW και πιο συγκεκριμένα με το S-GW.

Το MME αποτελεί το τελικό σημείο για την κρυπτογράφηση και την προστασία της ακεραιότητας στη σηματοδοσία των πρωτοκόλλων NAS. Τέλος, είναι το στοιχείο που υλοποιεί τη διαχείριση των κλειδιών ασφαλείας.

3.2.2 System Architecture Evolution Gateway

Ως SAE-GW θεωρούνται τα S-GW και P-GW. Είναι πιθανό να υλοποιούνται στο ίδιο hardware και να λειτουργούν ως ένα ενιαίο σύστημα. Στην περίπτωση αυτή, το interface που επικοινωνούν είναι το S5. Όταν υλοποιούνται σε διαφορετικά συστήματα, το interface που επικοινωνούν είναι λειτουργικά ακριβώς το ίδιο με το S5 αλλά καλείται S8. S8 καλείται επίσης και στην περίπτωση που ένα από τα δύο στοιχεία ανήκει στο δίκτυο διαφορετικού παρόχου, κάτι που παρατηρείται σε περιπτώσεις περιαγωγής. Στο Σχήμα 12 παρουσιάζεται η θέση του SAE-GW στο δίκτυο και όλα τα interfaces που υλοποιούνται σε αυτό.



Σχήμα 12 Το SAE-GW στο δίκτυο

Το S-GW είναι το στοιχείο το οποίο επικοινωνεί με τα υπόλοιπα στοιχεία στο δίκτυο κορμού καθώς και με στοιχεία δικτύου από διαφορετικό πάροχο, ενώ το P-GW είναι κυρίως η πύλη προς το Internet. Έτσι στο S-GW υλοποιούνται τα S1-U και S12 interfaces μέσω των οποίων συνδέονται τα δίκτυα πρόσβασης E-UTRAN και GERAN/UTRAN τα οποία χρησιμοποιούνται για user plane traffic (user plane traffic στα GERAN/UTRAN μέσω Direct Tunnel, λεπτομέρειες για το οποίο βρίσκονται στο [23]). Επίσης υλοποιούνται και τα S11 και S4 interfaces τα οποία χρησιμοποιούνται για την επικοινωνία με τα MME και SGSN αντίστοιχα.

Στο P-GW υλοποιείται το SGi interface το οποίο είναι το interface που παρέχει την πρόσβαση στο Internet και γενικότερα την πρόσβαση σε οποιοδήποτε δίκτυο πακέτων δεδομένων (packet data network) όπως λόγου χάρη το IMS (IP Multimedia Subsystem). Το Gx interface (ενδεχομένως να αναφερθεί και ως S7 interface στην βιβλιογραφία) παρέχει την μεταφορά των κανόνων χρέωσης και πολιτικής που εφαρμόζεται από το PCRF στο PCEF (Policy and Charging Enforcement Point) το οποίο είναι module που υλοποιείται στο SAE-GW.

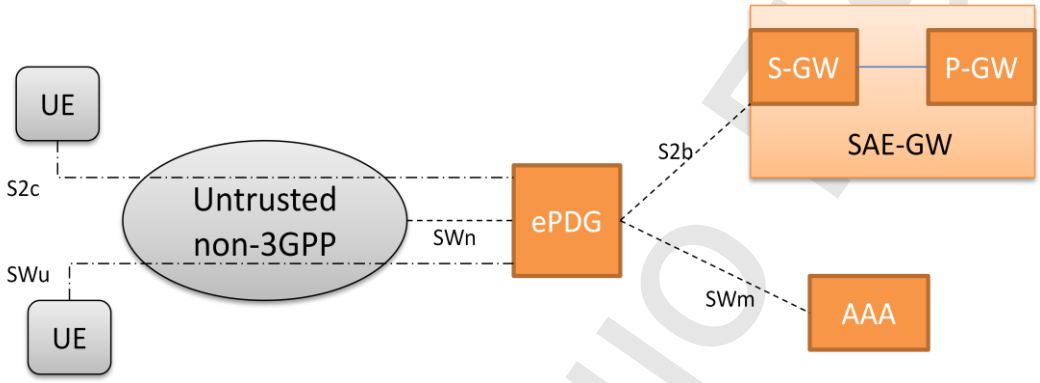
Στο P-GW υλοποιούνται τα S2a, S2b, S2c και S6a interfaces. Τα συγκεκριμένα interfaces επιτρέπουν την πρόσβαση στο P-GW σε δίκτυα πρόσβασης τα οποία δεν είναι ορισμένα από τον οργανισμό 3GPP αλλά είτε θεωρούνται έμπιστα από τον πάροχο (trusted non-3GPP), είτε όχι (untrusted non-3GPP). Στην πρώτη περίπτωση τα interfaces που χρησιμοποιούνται είναι τα S2a και S2c. Το S2c χρησιμοποιείται και για την δεύτερη περίπτωση αλλά και όταν ο χρήστης προσπελαύνει το P-GW μέσω πρόσβασης ορισμένης από το 3GPP αλλά χρησιμοποιεί το DSMIP πρωτόκολλο (Dual Stack Mobile IP). Το S2b interface υλοποιείται μεταξύ του P-GW και του ePDG (Evolved Packet Data Gateway), το οποίο αποτελεί το ενδιάμεσο στοιχείο για την πρόσβαση στο P-GW από untrusted non-3GPP δίκτυα πρόσβασης. Τα S2a, S2b και S2c interfaces μεταφέρουν control και user plane traffic. Το S6b interface μεταφέρει μόνο control plane traffic μεταξύ του P-GW και του AAA server.

Το SAE-GW υλοποιεί επίσης interfaces που επιτρέπουν την διαχείρισή του (OAM, Operation and Maintenance) και την σύνδεσή του με RADIUS server (Remote Authentication Dial In User Service). Άλλα interfaces που ενδέχεται να χρησιμοποιούνται είναι προς διάφορους servers, όπως λόγου χάρη προς DHCP server (Dynamic Host Configuration Protocol), και interface για την υποστήριξη νόμιμων συνακροάσεων (lawful interception).

Καθώς το SAE-GW αποτελεί το σημείο τερματισμού των «τούνελ» (tunnel όπως είναι η δόκιμη ορολογία για το δίκτυο) για το user plane traffic προς τον χρήστη, συνίσταται η χρήση IPSec στα συγκεκριμένα interfaces και ειδικότερα στο S1-U, προκειμένου να διασφαλιστεί η προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

3.2.3 Evolved Packet Data Gateway

Η βασική λειτουργία του ePDG είναι να διασφαλίσει την μεταφορά δεδομένων από την τερματική συσκευή στο δίκτυο κορμού, όταν η πρόσβαση γίνεται μέσω μη έμπιστου και μη προτυποποιημένου από το 3GPP (untrusted non-3GPP), δικτύου πρόσβασης. Το αν ένα δίκτυο θεωρείται ή όχι έμπιστο καθορίζεται από τον εκάστοτε πάροχο και δεν υπάρχει σαφής και αυστηρή διάκριση ως προς αυτό. Στο Σχήμα 13 παρουσιάζεται το ePDG και τα interfaces που υποστηρίζει.



Σχήμα 13 Το ePDG στο δίκτυο

Το ePDG συνδέεται με το SAE-GW μέσω του S2b interface. Στο interface αυτό υλοποιείται το tunnel για το user plane traffic και το signaling για τον έλεγχο του. Το πρωτόκολλο πάνω στο οποίο βασίζεται το S2b είναι το Proxy Mobile IP Protocol (PMIPv6). Το άλλο interface του ePDG προς το δίκτυο κορμού είναι το SWm και χρησιμοποιείται για την επικοινωνία με το AAA. Μέσω αυτού του interface πραγματοποιείται η αυθεντικοποίηση του UE στο δίκτυο.

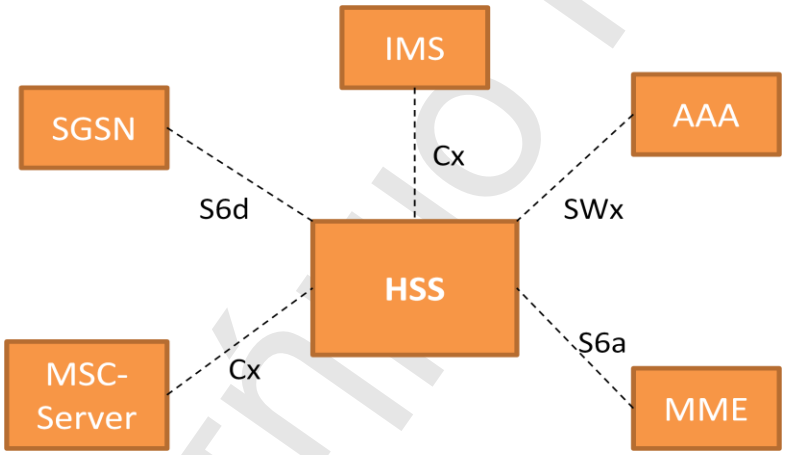
Το S2c interface επιτρέπει την δημιουργία tunnel από το UE στο P-GW το οποίο στην περίπτωση του untrusted non-3GPP δικτύου πρόσβασης, περνάει υποχρεωτικά μέσα από το ePDG. Υποστηρίζει user plane traffic και control traffic για τον έλεγχο του tunnel. Όμοια ορίζεται και το SWu interface το οποίο ενώνει το UE με το ePDG. Το interface αυτό υποστηρίζει την πρόσβαση μέσω untrusted non-3GPP IP δικτύου πρόσβασης για τη δημιουργία tunnel μεταξύ των UE και ePDG. Στη συνέχεια η πρόσβαση στο δίκτυο κορμού ολοκληρώνεται μέσω του S2b interface. Τέλος, το SWn interface υλοποιείται μεταξύ του ePDG και του untrusted non-3GPP δικτύου πρόσβασης.

Προκειμένου να είναι ασφαλής η πρόσβαση μέσω μη έμπιστων δικτύων πρόσβασης, είναι αναγκαία η δημιουργία IPSec tunnel ανάμεσα στο UE και το ePDG. Έτσι το ePDG

αποτελεί και το σημείο τερματισμού αυτών των tunnels. Το πρωτόκολλο που χρησιμοποιείται είναι το IKEv2 (Internet Key Exchange).

3.2.4 Home Subscriber Server

Το HSS είναι η κεντρική βάση όπου βρίσκονται οι πληροφορίες σχετικά με τον χρήστη και την συνδρομή του. Μεταξύ των πληροφοριών βρίσκονται και πληροφορίες σχετικά με την ταυτότητα του χρήστη, την θέση του και πληροφορίες σχετικές με την παρεχόμενη ασφάλεια, όπως είναι τα κλειδιά της αμοιβαίας αυθεντικοποίησης. Οι λειτουργίες που υποστηρίζονται βασίζονται κυρίως στα HLR και AuC των προγενέστερων δικτύων. Στο Σχήμα 14 διακρίνονται το HSS και τα interfaces που υλοποιούνται σε αυτό.



Σχήμα 14 Το HSS στο δίκτυο

Το S6a interface παρουσιάστηκε στην παράγραφο του MME. Το S6d interface είναι παρόμοιο με το S6a και χρησιμοποιείται για την σύνδεση του HSS με το 2G/3G SGSN. Και στις δύο περιπτώσεις τα interfaces βασίζονται στο πρωτόκολλο Diameter.

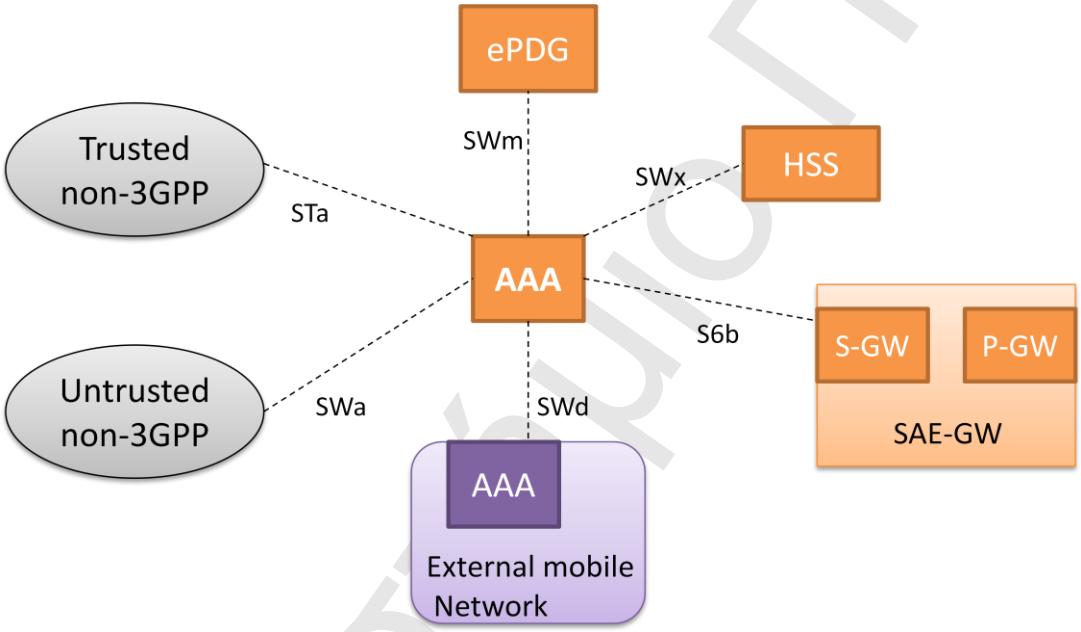
Στο πρωτόκολλο Diameter βασίζεται και το SWx interface, το οποίο χρησιμοποιείται για την επικοινωνία του HSS με τον AAA server. Πάνω από αυτό το interface υλοποιούνται λειτουργίες σχετικές με την αυθεντικοποίηση του χρήστη, το σχηματιζόμενο προφίλ του χρήστη αλλά και λειτουργίες σχετικές με την πρόσβαση στο EPC δίκτυο κορμού από non-3GPP δίκτυο πρόσβασης (παραδείγματος χάρη UE Registration Notification).

Στο HSS υλοποιείται επίσης το Cx interface για την επικοινωνία με το IMS αλλά και το MSC-Server. Μέσω αυτού στέλνονται τα δεδομένα του συνδρομητή, αιτήματα για πληροφορίες θέσης και φυσικά δεδομένα αυθεντικοποίησης. Τέλος, στο HSS

υλοποιούνται και άλλα interfaces που επιτρέπουν στο HSS να επικοινωνεί με στοιχεία εκτός του δικτύου κορμού, όπως λόγου χάρη το Sh interface που υλοποιείται μεταξύ του HSS και των Application Servers (AS) όπως ορίζεται και στο [24].

3.2.5 3GPP AAA server/proxy

Ο AAA server είναι ένας server στον οποίο πραγματοποιούνται οι λειτουργίες της αυθεντικοποίησης (authentication), της εξουσιοδότησης χρήσης (authorization) και διαχείρισης λογαριασμού (accounting). Στο Σχήμα 15 παρουσιάζεται η τοποθέτηση του AAA στο δίκτυο και τα interfaces που υλοποιούνται από αυτό.



Σχήμα 15 Το AAA στο δίκτυο

Από τα interfaces που υλοποιούνται, το SWx interface παρουσιάστηκε στην παράγραφο του HSS, το SWm interface παρουσιάστηκε στην παράγραφο του ePDG και το S6b interface παρουσιάστηκε στην παράγραφο του SAE-GW.

Τα trusted networks επικοινωνούν με το AAA μέσω του STa interface. Σε αυτή την περίπτωση το AAA λειτουργεί ως AAA-Server εκτελώντας την αυθεντικοποίηση η οποία βασίζεται στο πρωτόκολλο EAP (Encryption Authentication Protocol). Στην περίπτωση των untrusted δικτύων, η αυθεντικοποίηση μπορεί να πραγματοποιηθεί είτε στο ePDG, είτε στο AAA. Στη δεύτερη περίπτωση το AAA λειτουργεί ως AAA-Server και το interface που χρησιμοποιείται είναι το SWa.

Στο AAA υλοποιείται τέλος και το SWd interface. Χρησιμοποιείται για την επικοινωνία του AAA με άλλα AAA που όμως ανήκουν σε διαφορετικό δίκτυο κορμού και κατ' επέκταση σε διαφορετικό πάροχο. Το AAA που ανήκει σε διαφορετικό δίκτυο καλείται 3GPP AAA-Proxy. Μέσω του SWd interface ανταλλάσσονται πληροφορίες σχετικά με τους χρήστες όταν αυτοί εκτελούν λειτουργίες του δικτύου από την κατάσταση της περιαγωγής (roaming). Προκύπτει τελικά ότι το AAA λειτουργεί ως 3GPP AAA-Server όταν εξυπηρετεί το δίκτυο στο οποίο ανήκει (HPLMN, Home Public Land Mobile Network) και ως 3GPP AAA-Proxy όταν εξυπηρετεί διαφορετικό δίκτυο (VPLMN, Visited PLMN).

3.2.6 Equipment Identity Register

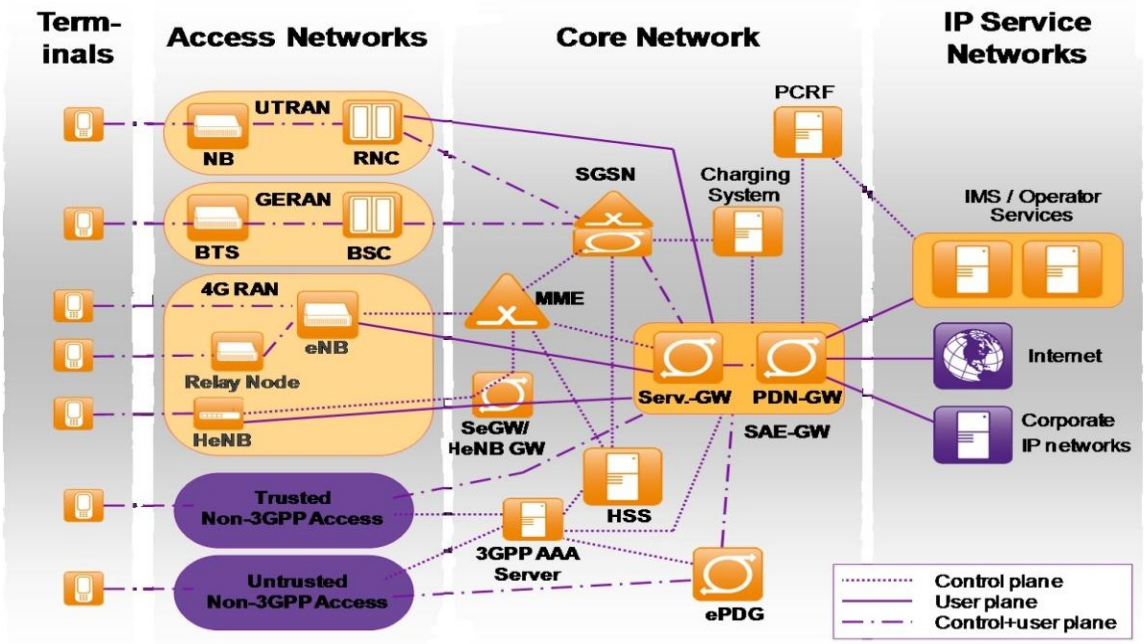
Το EIR είναι ένα προαιρετικό στοιχείο στο δίκτυο κορμού του παρόχου. Διατηρεί πληροφορίες σχετικά με το αναγνωριστικό της συσκευής IMEI (International mobile Equipment Identity) ώστε να μπορεί ο πάροχος να εξαιρέσει συγκεκριμένα IMEI από το δίκτυό του. Η εξαίρεση γίνεται βάση λίστας όπου διατηρούνται τα αναγνωριστικά εκείνα τα οποία αναφέρονται ως κλεμμένα. Στο Σχήμα 16 παρουσιάζεται το EIR καθώς και τα interfaces που υλοποιούνται από αυτό.

Σχήμα 16 Το EIR στο δίκτυο

Καθώς πρόκειται για προαιρετικό στοιχείο του δικτύου, τα interfaces που υλοποιούνται είναι αρκετά περιορισμένα. Έτσι διακρίνονται τα S13 και S13' για την επικοινωνία με το MME και το SGSN αντίστοιχα. Μέσω αυτών οι πληροφορίες που διατηρούνται στο EIR μεταφέρονται στα αντίστοιχα στοιχεία που ελέγχουν την πρόσβαση στο δίκτυο ανάλογα με το δίκτυο πρόσβασης.

3.3 Γενική εικόνα

Στο Σχήμα 17 παρουσιάζονται τα επιμέρους δίκτυα που σχηματίζουν τελικά το 4G δίκτυο. Το σχήμα περιλαμβάνει και όλα τα στοιχεία που περιγράφηκαν στις προηγούμενες παραγράφους καθώς και τις συνδέσεις που υλοποιούνται μεταξύ τους.



Σχήμα 17 Αρχιτεκτονική στο 4G δίκτυο

4. Ανάλυση ρίσκου στο 4G δίκτυο

Η ανάλυση ρίσκου είναι η μεθοδική διαδικασία κατά την οποία αναλύονται οι ευπάθειες, οι απειλές και οι συνέπειες της εκδήλωσης των απειλών σε συγκεκριμένα αγαθά με σκοπό την αποτίμηση του ρίσκου. Στα πλαίσια του ASMONIA, οι συγγραφείς πραγματοποιούν μία ανάλυση ρίσκου για το 4G δίκτυο στο [8]. Τόσο η μέθοδος που ακολουθήθηκε όσο και η ανάλυση που πραγματοποιήθηκε παρατίθενται στις ακόλουθες παραγράφους.

4.1 Μεθοδολογία

Οι δημοσιεύσεις προτύπων από διαφορετικούς οργανισμούς σχετικά με τις απειλές και το ρίσκο είναι αρκετές. Στο [8] αναφέρονται η σειρά προτύπων ISO 27000, οι δημοσιεύσεις του 3GPP (TS 33.120, 21.133 και TR 33.821), του ETSI (TS 102 165-1), του NIST (SP800-30) και της ένωσης ITU (X.805 και E.408).

Οι ορισμοί που υιοθετούνται από το ASMONIA στηρίζονται στους ορισμούς που προκύπτουν από το ISO 31000 και ISO/IEC 27005. Κατά τα πρότυπα αυτά το ρίσκο ορίζεται ως «η επίδραση της αβεβαιότητας στους στόχους» («*effect of uncertainty on objectives*»). Ο όρος αβεβαιότητα ακολουθεί τον ορισμό «*the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood*» που ερμηνεύεται ως η κατάσταση κατά την οποία η σχετική πληροφορία είναι ελλιπής και εμποδίζεται έτσι η κατανόηση ή η γνώση ενός γεγονότος, των συνεπειών του ή της πιθανότητας εμφάνισής του.

Η μέθοδος που ακολουθήθηκε στο ASMONIA δεν είναι μία εκ των προτύπων. Αντίθετα είναι μία μέθοδος που συνδυάζει στοιχεία από διάφορες πρότυπες μεθόδους. Τα στοιχεία αυτά επιλέχθηκαν με βάση προηγούμενη εμπειρία από τις σχετικές μεθόδους. Τελικά πρόκειται για μία απλή μέθοδο η οποία προϋποθέτει την εξής παραδοχή: *η αβεβαιότητα (uncertainty) αποτελεί το κύριο συστατικό του ρίσκου*.

Οι έννοιες και οι ορισμοί που χρησιμοποιούνται στη μέθοδο είναι οι εξής:

- Αγαθό (asset)
- Απειλή (threat), η πιθανή αιτία ενός περιστατικού που ενδέχεται να βλάψει το αγαθό ή το σύστημα ή τον οργανισμό
- Ευπάθεια (vulnerability), η αδυναμία ενός αγαθού ή ομάδας αγαθών την οποία μπορεί να εκμεταλλευτεί μία ή περισσότερες απειλές

- Παράγοντας ευπάθειας (vulnerability factor), ο όρος περιγράφει την γενική κατάσταση ως προς τις ευπάθειες

Για την αναγνώριση των απειλών που θα εξεταστούν από το ASMONIA, προτιμήθηκε το να υιοθετηθούν συγκεκριμένες απειλές με κριτήριο το περιεχόμενο (context) έναντι της εναλλακτικής της χρήσης καταλόγου απειλών που είναι διαθέσιμοι συνήθως από οργανισμούς. Ο στόχος της συγκεκριμένης εναλλακτικής είναι να τελεστεί η αναγνώριση των απειλών όσο το δυνατόν ακριβέστερα και με το μικρότερο κόστος. Οι απειλές που αναγνωρίστηκαν είναι οι:

- T1 Flooding an Interface
    - T1a Flooding the radio interface
    - T1b Flooding the backhauling interfaces
- T2 Crashing a network element via a protocol or application implementation flaw
- T3 Eavesdropping
    - T3a Eavesdropping on the radio interface
    - T3b Eavesdropping on the backhauling interfaces
- T4 Unauthorized access to sensitive data on a network element via leakage
- T5 Traffic modification
    - T5a Traffic modification on the radio interface
    - T5b Traffic modification on the backhauling link
- T6 Data modification on a network element
- T7 Compromise of a network element via a protocol or application implementation flaw
- T8 Compromise of a network element via a management interface
- T9 Malicious insider
- T10 Theft of service

Οι απειλές T3 και T5 διακρίνονται σε δύο επιπλέον κατηγορίες βάσει του επιπέδου στο οποίο πραγματοποιείται η κίνηση. Έτσι οι T3.1 και T5.1 αναφέρονται στο επίπεδο ελέγχου (control plane), ενώ οι T3.2 και T5.2 αναφέρονται στο επίπεδο χρήστη (user plane).

Από τις κατηγορίες των απειλών εξαιρούνται από το ASMONIA οι φυσικές απειλές όπως είναι μία φυσική καταστροφή. Εξαιρούνται επίσης και οι αποτυχίες του συστήματος που προκαλούνται από άλλους παράγοντες όπου οι αποτυχίες δεν είναι το αποτέλεσμα της εκδήλωσης μιας απειλής.

Οι αναγνωρισθείσες απειλές ακολουθούν μία λογική κατηγοριοποίηση ως προς το χαρακτηριστικό ασφάλειας στο οποίο εκδηλώνονται. Οι κατηγορίες που προκύπτουν είναι *loss of availability* {T1, T2}, *loss of confidentiality* {T3, T4}, *loss of integrity* {T5, T6},

loss of control (compromise/abuse of network elements) {T7, T8, T9} και *theft of service* {T10}.

Κάθε μία από τις παραπάνω απειλές διαμορφώνει κάποιο βαθμό ρίσκου. Το διαμορφούμενο ρίσκο ως προς μία απειλή προκύπτει ως αποτέλεσμα των ακόλουθων παραγόντων:

- Δυνητικότητα απειλής (threat's potential) ή πιθανότητα (likelihood)
- Εκμετάλλευση ευπαθειών (vulnerabilities to be exploited) ή vulnerability factor ή vulnerability
- Πρόκληση βλάβης (harm caused) ή impact

Στα πλαίσια του ASMONIA ο παράγοντας impact εξετάζεται ως οι επιπτώσεις ή οι συνέπειες στο δίκτυο από την σκοπιά του παρόχου.

Οι μέθοδοι εκτίμησης ρίσκου μπορεί να βασίζονται είτε σε μία ποιοτική προσέγγιση (qualitative) είτε σε μία ποσοτική προσέγγιση (quantitative). Στην ποιοτική προσέγγιση η εκτίμηση ρίσκου γίνεται χρησιμοποιώντας συγκεκριμένα ποιοτικά χαρακτηριστικά (low, medium, high) για την περιγραφή της αποτίμησης ρίσκου. Στην ποσοτική χρησιμοποιείται μία κλίμακα αριθμών, λόγου χάρη 1 έως 10, για τον χαρακτηρισμό της πιθανότητας (likelihood), του βαθμού ευπάθειας (vulnerability factor) και των επιπτώσεων (impact). Η μέθοδος που επιλέχθηκε ως καταλληλότερη για το ASMONIA είναι μία ποσοτική μέθοδος.

Η κλίμακα που χρησιμοποιήθηκε είναι μία κλίμακα από το 1 έως το 5. Η ερμηνεία της κάθε τιμής διαμορφώνεται διαφορετικά ανάλογα με τον παράγοντα στον οποίο αποδίδεται. Στους πίνακες Πίνακας 1 και Πίνακας 2 παρουσιάζονται οι ερμηνείες που αντιστοιχούν στις παραπάνω έννοιες:

Likelihood	Ερμηνεία
1	< 1 φορά σε 5 χρόνια
2	< 1 φορά σε 1 χρόνο
3	< 1 φορά σε 1 μήνα
4	< 1 φορά σε 1 εβδομάδα
5	> 1 φορά σε 1 εβδομάδα

Πίνακας 1 Ερμηνεία likelihood

Vulnerability Factor	Ερμηνεία
1	Εκτενείς έλεγχοι. Θα πρέπει να αποτύχουν πολλοί ώστε να εκδηλωθεί η απειλή
2	Πολλοί έλεγχοι. Μπορεί να προσπελαστούν από υψηλά καταρτισμένους επιτιθέμενους
3	Μερικοί έλεγχοι. Θα προσπελαστούν από υψηλά καταρτισμένους επιτιθέμενους
4	Περιορισμένοι έλεγχοι. Θα προσπελαστούν

	από μέτριας κατάρτισης επιτιθέμενους ή/και λόγω υψηλής έκθεσης
5	Ελάχιστοι έλεγχοι, θα προσπελαστούν

Πίνακας 2 Ερμηνεία Vulnerability factor

Για τον παράγοντα impact δεν ακολουθείται συγκεκριμένη ερμηνεία από το ASMONIA. Η αποτίμησή του είναι γενική και όχι τμηματική ως προς το κάθε χαρακτηριστικό ασφάλειας και πραγματοποιείται με υποκειμενικά κριτήρια και λαμβάνοντας ως δεδομένο ότι οι αρμόδιοι για την αποτίμησή του αντιλαμβάνονται τον συγκεκριμένο παράγοντα με όμοιο τρόπο. Χαρακτηριστικά αναφέρεται ότι «…there was a joint understanding of the experts involved…». Ως συνέπεια αυτής της επιλογής για τις απειλές που αναφέρονται στο user plane traffic T3.2 και T5.2 το impact αποτιμάται από 1 έως 3 και αυτό είναι κάτι που θεωρείται δεδομένο για το ASMONIA.

Το επιχείρημα στο οποίο οι συγγραφείς στηρίζουν την συγκεκριμένη τους επιλογή είναι η απουσία συγκεκριμένου περιβάλλοντος με συγκεκριμένες τιμές ως προς τις συνέπειες και ενδεικτικά αναφέρουν τις οικονομικές συνέπειες ως παράδειγμα.

Οι συγγραφείς αντιλαμβάνονται ότι η υποκειμενική αποτίμηση του παράγοντα impact αποτελεί το αδύναμο σημείο της μεθόδου. Το γεγονός αυτό τους οδηγεί στην παραδοχή ότι η συγκεκριμένη εκτίμηση υστερεί ως προς την τεκμηρίωση της ορθότητάς της.

Το επιχείρημα για την συγκεκριμένη επιλογή δεν είναι αρκετά ισχυρό. Η μη ύπαρξη ερμηνείας για κάθε μία από τις τιμές της κλίμακας για τον παράγοντα impact καταργεί την αντικειμενικότητα της εκτίμησης. Θα έπρεπε να είχε ακολουθηθεί συγκεκριμένη ερμηνεία ώστε να εξαλειφτεί κάθε υποκειμενικό κριτήριο.

Μία ενδεικτική ερμηνεία για την κάθε τιμή βασισμένη στον οικονομικό παράγοντα και στον παράγοντα της φήμης (reputation) θα μπορούσε να είναι η ακόλουθη που παρουσιάζεται στον Πίνακας 3.

Impact	**Ερμηνεία**
1	Καθόλου οικονομικές συνέπειες, βλάβη στη φήμη
2	Μικρές οικονομικές συνέπειες
3	Μικρές οικονομικές συνέπειες, βλάβη στη φήμη
4	Μεγάλες οικονομικές συνέπειες
5	Μεγάλες οικονομικές συνέπειες και βλάβη στη φήμη

Πίνακας 3 Ερμηνεία Impact

Η παραπάνω πρόταση αποτελεί μία πρώτη και αρκετά απλοϊκή προσέγγιση ωστόσο θα μπορούσε να σταθεί ως μία αντικειμενική ερμηνεία. Με τον τρόπο αυτό η μέθοδος θα ήταν πιο ολοκληρωμένη και κατά συνέπεια περισσότερο ορθή.

Τελικά, η εκτίμηση του ρίσκου θα προκύπτει ως το γινόμενο των τιμών που αποδόθηκαν σε κάθε παράγοντα.

4.2 Ανάλυση ρίσκου

Για την ανάλυση ρίσκου οι συγγραφείς του ASMONIA διαχωρίζουν το δίκτυο και το εξετάζουν τμηματικά στα ακόλουθα μέρη:

- Τις τερματικές συσκευές
- Το δίκτυο πρόσβασης
- Το δίκτυο κορμού
- Το δίκτυο υπηρεσιών
- Το δίκτυο υποδομής

Στο [8] αναλύουν διεξοδικά καθένα από τα παραπάνω μέρη. Στην παρούσα εργασία το βάρος δίνεται στο δίκτυο πρόσβασης και το δίκτυο κορμού που σχηματίζουν ένα 4G δίκτυο, επομένως αυτά είναι και τα μέρη που παρουσιάζονται στις ακόλουθες ενότητες. Μια σύντομη αναφορά στα υπόλοιπα μέρη του δικτύου γίνεται στο τέλος του τρέχοντος κεφαλαίου ενώ η ανάλυση ρίσκου για τις τερματικές συσκευές σκόπιμα δεν περιέχεται στην εργασία λόγω της διαφορετικής φύσης των απειλών οι οποίες εμπεριέχονται στον τομέα των λειτουργικών συστημάτων και όχι στο 4G δίκτυο.

4.2.1 Δίκτυο πρόσβασης

Όπως παρουσιάστηκε στο κεφάλαιο της αρχιτεκτονικής του δικτύου, το δίκτυο πρόσβασης αποτελείται από τα εξής στοιχεία: eNodeB, Relay Nodes, HeNBs, HeNB-GW και HeMS. Η ανάλυση ρίσκου που παρουσιάζεται αφορά στα eNodeB, RN, HeNB και HeNB-GW.

4.2.1.1 eNodeB

Το eNB είναι το στοιχείο που αποτελεί το κεντρικό στοιχείο στο δίκτυο πρόσβασης και είναι αυτό που υλοποιεί και τα περισσότερα interfaces σε σχέση με τα υπόλοιπα στοιχεία αυτής της κατηγορίας. Επίσης είναι και το στοιχείο στο οποίο ο χρήστης έχει άμεση πρόσβαση μέσω της συσκευής του. Ο Πίνακας 4 περιέχει τα αποτελέσματα της ανάλυσης.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1a (radio)	3	5	2	30
T1b (backhauling)	2	2	2	8
T2	2 - 3	3	2	12 - 18
T3.1a (radio, control)	4	2	3	24
T3.1b (backhauling, control)	3	2	4	24
T3.2a (radio, user)	4	2	1 - 3	8 - 24
T3.2b (backhauling, user)	3	2	1 - 3	6 - 18
T4	2	2	4	16
T5.1a (radio, control)	3	2	4	24
T5.1b (backhauling, control)	2	2	5	20
T5.2a (radio, user)	3	2	1 - 3	6 - 18
T5.2b (backhauling, user)	2	2	1 - 3	4 - 12
T6	2	2	4	16
T7	3	2	5	30
T8	3	2	5	30
T9	1	4	5	20
T10	2	2	5	20

Πίνακας 4 Ανάλυση ρίσκου στο eNB

Η απειλή T1 Flooding an Interface παρατηρείται στο radio interface (a) και στο interface προς το δίκτυο (backhauling interface, (b)). Για την πρώτη περίπτωση, οι συγγραφείς θεωρούν πιθανή την εκδήλωση μιας επίθεσης τύπου DoS που θα επηρεάσει τους νόμιμους χρήστες οι οποίοι δεν θα μπορούν να εξυπηρετηθούν. Το interface θα πλημμυρίσει από μηνύματα και όλοι οι διαθέσιμοι πόροι του eNB θα καταναλωθούν από τη συσκευή η οποία ευθύνεται για την επίθεση. Η φύση του eNB είναι τέτοια ώστε οφείλει να δέχεται μηνύματα σηματοδοσίας από οποιαδήποτε συσκευή. Επίσης το λογισμικό που επιτρέπει την υλοποίηση μιας τέτοιας επίθεσης είναι εύκολα διαθέσιμο ως ανοιχτό λογισμικό. Στη δεύτερη περίπτωση, δηλαδή στην περίπτωση του backhauling interface, το εκτιμώμενο ρίσκο είναι σαφώς μικρότερο κυρίως λόγω του ότι το eNB θα δέχεται μηνύματα από συγκεκριμένα στοιχεία του δικτύου κορμού. Επιπλέον στα συγκεκριμένα interfaces είναι δυνατή η χρήση IPSec, γεγονός που καθιστά τα interfaces λιγότερο ευπαθή. Έτσι το τελικώς εκτιμώμενο ρίσκο που προκύπτει είναι 30 στην πρώτη περίπτωση και 8 στη δεύτερη.

Η απειλή T2 crashing a NE via a protocol or application implementation flaw, θεωρείται πιθανό να εκδηλωθεί δεδομένου ότι στο eNB υλοποιούνται interfaces που βασίζονται σε αρκετά καινούρια πρωτόκολλα. Η υλοποίηση των πρωτοκόλλων λοιπόν είναι πιθανό να κρύβει κάποιες αδυναμίες τις οποίες μπορούν αν εκμεταλλευθούν οι επιτιθέμενοι και να εκδηλωθεί η επίθεση. Ωστόσο αναμένεται ότι ορισμένος μόνο αριθμός των χρηστών του δικτύου θα έχει πρόσβαση στο δίκτυο μέσω του eNB στο οποίο εκδηλώνεται η επίθεση. Επομένως και οι συνέπειες της εκδηλωμένης απειλής επηρεάζουν μικρό μέρος επί του συνολικού αριθμού των χρηστών. Τελικά το ρίσκο εκτιμάται ότι θα κυμαίνεται μεταξύ 12 και 18.

Όμοια με την απειλή T1, έτσι και για την απειλή T3 Eavesdropping γίνεται ο διαχωρισμός ως προς το interface για το οποίο αναλύεται. Ένας επιπλέον διαχωρισμός γίνεται και ως προς το είδος της κίνησης το οποίο επηρεάζεται, δηλαδή control-plane traffic ή user-plane traffic.Το είδος της κίνησης είναι αυτό που θα καθορίσει και την εκτίμηση των συνεπειών με την έννοια ότι οι συνέπειες θα είναι χειρότερες για τον πάροχο στην περίπτωση του control-plane καθώς ενδέχεται να αποκαλυφθούν πληροφορίες που αφορούν και άλλα interfaces και κατά συνέπεια να εκτεθεί σε κίνδυνο όλο το δίκτυο. Τόσο για το radio interface όσο και για το backhauling προτείνεται η χρήση IPSec από τα standards όπως αναφέρεται στο [25] χωρίς όμως να επιβάλλεται. Αυτό σημαίνει ότι στην περίπτωση που δεν εφαρμόζεται IPSec στο backhauling interface, ευαίσθητες πληροφορίες όπως είναι πληροφορίες σχετικές με τα κλειδιά ενδέχεται να αποκαλυφθούν κατά την εκδήλωση μίας τέτοιας επίθεσης. Τελικά το ρίσκο εκτιμάται ως εξής για κάθε μία περίπτωση:

- Radio interface με control-plane traffic:24
- Backhauling interface με control-plane traffic: 24
- Radio interface user-plane traffic: 8 - 24
- Backhauling interface με control traffic: 6 - 18

Η απειλή T4 Unauthorized access to sensitive data on a network element via leakage αφορά κυρίως τις ευαίσθητες για τον πάροχο πληροφορίες που βρίσκονται αποθηκευμένες στο eNB, όπως είναι παραδείγματος χάρη τα κλειδιά κρυπτογράφησης. Εάν κάποιος αποκτήσει πρόσβαση στα κλειδιά αυτά ενδέχεται να εκδηλωθούν επιθέσεις όπως ψευδής ή παραποιημένη κίνηση του χρήστη και δημιουργία πληθώρας μηνυμάτων προς το δίκτυο κορμού. Εάν εκδηλωθούν τέτοιου είδους επιθέσεις, οι συνέπειες είναι πολύ σημαντικές για τον πάροχο, οι πιθανότητες όμως να εκδηλωθούν δεν θεωρούνται πολλές. Συνολικά το ρίσκο εκτιμάται με τιμή 16.

Η απειλή T5 Traffic modification κατηγοριοποιείται όπως και η T3 σε radio και backhauling interface αλλά οι συνέπειες εκτιμώνται διαφορετικά ως προς το είδος της κίνησης που επηρεάζεται. Γενικά στο radio interface υλοποιούνται μηχανισμοί για την

προστασία της ακεραιότητας και το ίδιο αναμένεται να ισχύει και για το backhauling interface. Το εκτιμώμενο ρίσκο για τις επιμέρους περιπτώσεις είναι

- Radio interface με control-plane traffic:24
- Backhauling interface με control-plane traffic: 20
- Radio interface user-plane traffic: 6 - 18
- Backhauling interface με control traffic: 4 - 12

Για την απειλή T6 Data modification on a network element αναφέρεται ως περισσότερο πιθανό ότι αυτή επηρεάζει τα δεδομένα παραμετροποίησης (configuration data) και τα δεδομένα σχετικά με τα κλειδιά του κρυπτογράφησης. Μια ενδεχόμενη εκδήλωση τέτοιας επίθεσης θα είχε πολύ σοβαρές συνέπειες. Η πιθανότητα όμως να εκδηλωθεί δεν θεωρείται μεγάλη καθώς αναμένεται να εφαρμόζονται μηχανισμοί ασφάλειας όπως καθορίζονται από τον οργανισμό 3GPP. Έτσι το εκτιμώμενο ρίσκο που προκύπτει είναι 16.

Η απειλή T7 Compromise of a network element via a protocol or application implementation flaw θεωρείται δύσκολο να εκδηλωθεί χωρίς να προκαλέσει την ολική παύση λειτουργίας του eNB. Σε περίπτωση όμως που εκδηλωθεί μία τέτοια επίθεση, οι συνέπειες θα είναι καταστροφικές. Εύλογα λοιπόν το εκτιμώμενο ρίσκο είναι 30.

Όμοιος συλλογισμός γίνεται και για την απειλή T8 Compromise of a network element via a management interface. Η διαφορά είναι ότι ένα τέτοιο interface δεν είναι αυστηρώς καθορισμένο από τον οργανισμό 3GPP, είναι όμως το interface στο οποίο εκδηλώνονται πολύ συχνά επιθέσεις και επομένως θεωρείται πολύ πιθανό να εκδηλωθούν και στην περίπτωση του eNB. Οι συνέπειες μιας τέτοια επίθεσης είναι όμοιες με αυτές στην περίπτωση της απειλής T7, επομένως το εκτιμώμενο ρίσκο είναι 30.

Η απειλή T9 Malicious insider δεν θεωρείται ιδιαίτερα πιθανή καθώς αναμένεται τέτοιου είδους επιθέσεις να στοχεύουν κυρίως στο δίκτυο κορμού και όχι στο δίκτυο πρόσβασης. Εάν όμως αυτή η απειλή εκδηλωθεί, οι συνέπειες θα είναι καταστροφικές. Το ρίσκο που εκτιμάται για την απειλή αυτή είναι 20.

Για την απειλή T10 Theft of service αναφέρεται ότι είναι μάλλον απίθανο να εκδηλωθεί στο συγκεκριμένο στοιχείο καθώς οι υπηρεσίες που υλοποιούνται σε αυτό δεν είναι ιδιαίτερα ελκυστικές για τους επιτιθέμενους. Το ρίσκο σε αυτή την περίπτωση εκτιμάται να είναι 20.

Το eNB είναι το στοιχείο με την εξής ιδιαιτερότητα: υλοποιεί radio και backhauling interface. Προκειμένου λοιπόν η ανάλυση του eNB να είναι συγκρίσιμη με την ανάλυση άλλων στοιχείων, οι συγγραφείς προχωρούν στην ενοποίηση αυτών των περιπτώσεων. Με βάση αυτά τα δεδομένα, προκύπτει ο Πίνακας 5

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	3	5	2	30
T2	3	3	2	18
T3.1	3	2	4	24
T3.2	3 – 4	2	1 – 3	6 – 24
T4	2	2	4	16
T5.1	2 – 3	2	4	16 – 24
T5.2	2 – 3	2	1 – 3	4 – 18
T6	2	2	4	16
T7	3	2	5	30
T8	3	2	5	30
T9	1	4	5	20
T10	2	2	5	20

Πίνακας 5 Ενοποιημένη ανάλυση ρίσκου στο eNB

4.2.1.2 Relay Node

Το RN χρησιμοποιείται για την μεγαλύτερη κάλυψη ραδιοσήματος όπως παρουσιάστηκε και στην αντίστοιχη παράγραφο. Οι λειτουργίες του είναι όμοιες με αυτές του eNB όσον αφορά το interface προς τους χρήστες. Και για το RN ακολουθείται ο διαχωρισμός σε user plane traffic και control plane traffic στις απειλές T3 και T5.

Τα interfaces του RN είναι αποκλειστικά radio interfaces και η απειλή T1 είναι πιθανή όπως και για το αντίστοιχο interface του eNB. Η διαφορά είναι ότι το RN εμφανίζει μεγαλύτερη ευπάθεια, οι συνέπειες όμως μιας τέτοιας επίθεσης είναι μικρότερες. Το εκτιμώμενο ρίσκο είναι ίδιο με το αντίστοιχο του eNB, δηλαδή 30.

Για τις απειλές T2, T5, T8 και T9 ισχύουν ακριβώς τα ίδια που αναφέρθηκαν για το eNB και τα ρίσκα είναι ακριβώς τα ίδια, δηλαδή 18, 16 – 24 (T5.1), 4 – 18 (T5.2), 30 και 20 αντίστοιχα.

Αναφορικά με την απειλή T3, το διαφορετικό χαρακτηριστικό του RN είναι το Un interface το οποίο δεν υλοποιεί IPSec για την προστασία της εμπιστευτικότητας, αλλά το συγκεκριμένο χαρακτηριστικό ασφάλειας επιτυγχάνεται μέσω των μηχανισμών ασφάλειας που εφαρμόζονται κατά τη μετάδοση του LTE ραδιοσήματος. Λόγω της μικρότερης έκτασης που καλύπτει το RN, οι συνέπειες από μία τέτοια απειλή αναμένεται να είναι μικρότερες. Το εκτιμώμενο ρίσκο κυμαίνεται τελικά από 18 έως 32 για το control plane traffic και από 6 έως 24 για το user plane traffic.

Το RN θεωρείται περισσότερο ευάλωτο στην απειλή T4 δεδομένου ότι η φυσική προστασία του στοιχείου θα είναι δυσκολότερη. Ωστόσο η εκδήλωση μιας επίθεσης τέτοιου είδους στο RN ενδεχομένως να μην επηρεάζει το δίκτυο στον ίδιο βαθμό που θα

επηρέαζε η ίδια απειλή στην περίπτωση του eNB. Το εκτιμώμενο ρίσκο που προκύπτει είναι 36. Το ίδιο ρίσκο εκτιμάται και για την απειλή T6 καθώς η ανάλυση για την απειλή T4 εφαρμόζεται και στην περίπτωση της απειλής T6.

Η φυσική ασφάλεια του RN είναι ο παράγοντας που αυξάνει το βαθμό ευπάθειας και στην περίπτωση της απειλής T7. Έτσι το εκτιμώμενο ρίσκο και σε αυτή την περίπτωση είναι μεγαλύτερο από το αντίστοιχο του eNB, και η τιμή του είναι 45. Ο βαθμός ευπάθειας είναι το στοιχείο που αυξάνει το ρίσκο και στην περίπτωση της απειλής T10, όπου το εκτιμώμενο ρίσκο είναι 30.

Ο Πίνακας 6 παρουσιάζει το εκτιμώμενο ρίσκο για το RN για κάθε μία από τις απειλές. Με κόκκινο απεικονίζονται οι τιμές οι οποίες είναι μεγαλύτερες από τις αντίστοιχες του eNB.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	3	5	2	30
T2	3	3	2	18
T3.1	3 – 4	2	3 – 4	18 – 32
T3.2	3 – 4	2	1 – 3	6 – 24
T4	3	3	4	36
T5.1	2 – 3	2	4	16 – 24
T5.2	2 – 3	2	1 – 3	4 – 18
T6	3	3	4	36
T7	3	3	5	45
T8	3	2	5	30
T9	1	4	5	20
T10	2	3	5	30

Πίνακας 6 Ανάλυση ρίσκου στο RN

Προκύπτει λοιπόν ότι για πέντε απειλές το εκτιμώμενο ρίσκο του RN είναι μεγαλύτερο από το αντίστοιχο του eNB και αυτό οφείλεται κυρίως στη μικρότερη φυσική ασφάλεια που μπορεί να εφαρμοστεί στο RN.

4.2.1.3 Home eNodeB

Το HeNB προσομοιάζει τη λειτουργία του eNB όπως περιγράφηκε στις προηγούμενες ενότητες, επομένως ισχύουν τα ίδια πράγματα ως προς την ασφάλεια του όπως ισχύουν και για το eNB. Επιπλέον, το HeNB υλοποιεί interface προς το Διαδίκτυο, ενώ είναι περισσότερο ευάλωτο ως προς την φυσική έκθεση σε απειλές καθώς είναι εγκατεστημένο σε περιοχές που δεν ελέγχονται από τον πάροχο.

Η ανάλυση που παρουσιάζεται στο [8] βασίζεται σε αποτελέσματα πειραμάτων που πραγματοποιήθηκαν στα πλαίσια του ASMONIA αλλά και σε πειράματα που έχουν δημοσιοποιηθεί στην πανεπιστημιακή κοινότητα [26], [27] και [28]. Ο Πίνακας 7 περιλαμβάνει τα αποτελέσματα της ανάλυσης. Με κόκκινο απεικονίζονται οι τιμές οι οποίες είναι μεγαλύτερες συγκριτικά με τις αντίστοιχες τιμές του eNB.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	5	1	10
T2	2	4	1	8
T3.1	3	3	3	27
T3.2	3	3	1 – 3	9 – 27
T4	4	4	3	48
T5.1	3	3	4	36
T5.2	3	3	1 – 3	9 – 27
T6	4	4	3	48
T7	4	4	4	64
T8	4	4	4	64
T9	1	4	4	16
T10	2	4	4	32

Πίνακας 7 Ανάλυση ρίσκου στο HeNB

Εύκολα γίνεται αντιληπτό ότι το HeNB παρουσιάζει μεγαλύτερο ρίσκο για τις περισσότερες από τις απειλές που αναλύονται. Αυτό οφείλεται κυρίως στην ευκολότερη φυσική πρόσβαση που μπορούν να αποκτήσουν οι επιτιθέμενοι αλλά και στην πιθανότητα να υπάρχουν αρκετές ατέλειες στο ασφαλές περιβάλλον που χρειάζεται για την σύνδεση του HeNB στο δίκτυο, τις οποίες οι επιτιθέμενοι μπορούν εύκολα να εκμεταλλευθούν. Για τις περισσότερες από τις απειλές όμως, οι συνέπειες αξιολογούνται ως λιγότερο σημαντικές από τις αντίστοιχες για το eNB, λόγω του περιορισμένου αριθμού των χρηστών που θα επηρεαστούν από την εκδήλωση της απειλής.

4.2.1.4 Home eNodeB-Gateway

Το HeNB-GW, αν και αποτελεί στοιχείο του δικτύου πρόσβασης, αναμένεται να τοποθετείται στο δίκτυο κορμού, όπως φαίνεται και από την αρχιτεκτονική που απεικονίζεται στο Σχήμα 9. Ως εκ τούτου, θεωρείται ότι εκτίθεται σε μικρότερο βαθμό σε ενδεχόμενες επιθέσεις. Είναι επομένως λογικό να εμφανίζει και μικρότερο ρίσκο για τις απειλές που αναλύονται. Στον Πίνακας 8 παρουσιάζονται οι τιμές του εκτιμώμενου ρίσκου, όπου και σε αυτή την περίπτωση με κόκκινο εμφανίζονται οι τιμές όπου το εκτιμώμενο ρίσκο για το eNB είναι μικρότερο.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2 – 3	2	4	16 – 24

T2	2 – 3	2	4	16 – 24
T3.1	2	1	4	8
T3.2	2	1	1 – 3	2 – 6
T4	2	1	4	8
T5.1	1	1	4	4
T5.2	1	1	1 – 3	1 – 3
T6	1	1	4	4
T7	2	2	5	20
T8	2	2 – 3	5	20 – 30
T9	1 – 2	4	5	20 – 40
T10	1	1	5	5

Πίνακας 8 Ανάλυση ρίσκου στο HeNB-GW

Οι απειλές για τις οποίες το ρίσκο εκτιμάται ότι είναι μεγαλύτερο είναι οι T2 και T9. Στην περίπτωση της απειλής T2 αυτό οφείλεται στο γεγονός ότι μία επιτυχημένη DoS επίθεση στο HeNB-GW θα θέσει εκτός δικτύου όλα τα HeNBs με τα οποία είναι συνδεδεμένο, επομένως οι συνέπειες αναμένεται να είναι μεγαλύτερες. Στην περίπτωση της απειλής T9, το εκτιμώμενο ρίσκο είναι μεγαλύτερο γιατί ενδέχεται να αυξηθεί και η πιθανότητα εκδήλωσης της συγκεκριμένης απειλής.

4.2.2 Δίκτυο κορμού

Το δίκτυο κορμού όπως παρουσιάστηκε και στο προηγούμενο κεφάλαιο, αποτελείται κυρίως από τα SAE-GW, MME, ePDG, HSS, EIR και AAA. Το κοινό χαρακτηριστικό όλων αυτών είναι ότι βρίσκονται στο εσωτερικό δίκτυο του παρόχου και θεωρούνται αρκετά καλά προστατευμένα ως προς τη φυσική ασφάλεια. Στις ενότητες που ακολουθούν περιγράφεται η ανάλυση που παρουσιάζεται για τα στοιχεία του 4G δικτύου κορμού στο [8].

4.2.2.1 SAE-GW

Το SAE-GW μπορεί να λειτουργεί είτε ως S-GW είτε ως PDN-GW (αναφέρεται και ως P-GW). Στην ανάλυση ρίσκου που παρουσιάζεται δεν ακολουθείται αυτός ο διαχωρισμός αλλά η ανάλυση γίνεται για το SAE-GW συνολικά.

Αυτό που χαρακτηρίζει το SAE-GW είναι τα πολλά interfaces που υλοποιούνται σε αυτό αλλά και η πληθώρα πρωτοκόλλων πάνω στα οποία βασίζονται αυτά τα interfaces. Τα περισσότερα όμως από τα interfaces είναι προς το εσωτερικό δίκτυο, προς τα άλλα στοιχεία του δικτύου κορμού. Από την άλλη βέβαια το SAE-GW είναι το στοιχείο που

υλοποιεί το interface προς το Διαδίκτυο, γεγονός που αυξάνει τον βαθμό έκθεσης του στοιχείου σε απειλές.

Με δεδομένα τα παραπάνω, η απειλή T1 εκτιμάται ως αρκετά πιθανή ενώ οι συνέπειες εκδήλωσης της συγκεκριμένης απειλής είναι καταστροφικές καθώς μπορεί να οδηγήσει σε επιτυχημένη DoS επίθεση, όπου η κατάσταση αυτή μπορεί να διαρκέσει μεγάλο χρονικό διάστημα και το πλήθος των χρηστών που θα επηρεαστούν αναμένεται να είναι μεγάλο. Έτσι το ρίσκο που προκύπτει είναι 40.

Λόγω της πληθώρας των πρωτοκόλλων που υλοποιούνται στο SAE-GW, η απειλή T2 θεωρείται πολύ πιθανή ενώ και οι συνέπειες εκδήλωσης μιας τέτοιας απειλής είναι πολύ σοβαρές καθώς το SAE-GW θα σταματήσει να είναι λειτουργικό επηρεάζοντας πλήθος χρηστών. Επιπλέον, από τη στιγμή που ο επιτιθέμενος κατορθώσει να εκμεταλλευθεί την συγκεκριμένη ευπάθεια, θα είναι σε θέση να το επαναλαμβάνει μέχρις ότου αναβαθμιστεί το SAE-GW με λογισμικό που θα διορθώνει το συγκεκριμένο πρόβλημα. Τελικά το ρίσκο που εκτιμάται για την συγκεκριμένη απειλή είναι 48.

Για την απειλή T3 η ανάλυση που γίνεται συνεκτιμά τον μεγάλο αριθμό των interfaces ωστόσο θεωρείται ότι θα πρέπει να λαμβάνονται τα κατάλληλα τεχνικά μέτρα για την διασφάλιση τους. Έτσι αναμένεται ότι στα interfaces του δικτύου κορμού θα εφαρμόζεται IPSec που θα εξασφαλίζει τον επιθυμητό βαθμό ασφάλειας. Ωστόσο, για την περίπτωση του control-plane traffic θεωρείται αρκετά πιθανό τα μέτρα ασφάλειας να μην εστιάζουν τόσο στην προστασία της εμπιστευτικότητας όσο στην προστασία της ακεραιότητας. Ως προς το user-plane traffic, το SAE-GW δεν θεωρείται το κατάλληλο στοιχείο για την εκδήλωση μιας τέτοιας επίθεσης. Επιπλέον, στα πλαίσια τις ανάλυσης αναμένεται ότι για τα ευαίσθητα δεδομένα χρήστη θα έχουν ληφθεί και τα αντίστοιχα τεχνικά μέσα, επομένως τυχόν αποκάλυψη του user-plane traffic δεν θα προσφέρει πληροφορίες στους επιτιθέμενους καθώς τα δεδομένα θα είναι κρυπτογραφημένα, γεγονός που περιορίζει και τις συνέπειες από την εκδήλωση τέτοιων επιθέσεων. Το ρίσκο που προκύπτει για το control-plane και το user-plane εκτιμάται να είναι 6 και από 4 έως 12 αντίστοιχα.

Στο SAE-GW δεν αποθηκεύονται τα δεδομένα χρήστη ενώ τα δεδομένα παραμετροποίησης του συστήματος που είναι αποθηκευμένα δεν προσφέρουν κάποια χρήσιμη πληροφορία προς τους επιτιθέμενους. Έτσι ο βαθμός ευπάθειας για την απειλή T4 εκτιμάται να είναι πολύ μικρός όπως και οι συνέπειες της συγκεκριμένης απειλής. Συνεπώς, το ρίσκο εκτιμάται να είναι αντίστοιχα μικρό και είναι 6.

Για την απειλή T5 ακολουθείται όμοια ανάλυση με αυτή που παρουσιάστηκε για την απειλή T3. Ωστόσο για αυτή την περίπτωση μία επιτυχής επίθεση μπορεί να οδηγήσει σε επιτυχημένη DoS επίθεση γεγονός που θα επηρεάσει σημαντικό αριθμό χρηστών.

Το ρίσκο σε αυτή την απειλή εκτιμάται να είναι 5 και από 2 έως 6 για την περίπτωση του control-plane traffic και user-plane traffic αντίστοιχα.

Όμοια με την απειλή T4, η απειλή T6 ακολουθεί την ίδια ανάλυση καθώς δεν αποθηκεύονται στο SAE-GW δεδομένα χρήστη. Πιθανή τροποποίηση όμως των δεδομένων ελέγχου μπορεί να οδηγήσει σε DoS ή και theft of service επομένως οι συνέπειες μπορεί να είναι καταστροφικές. Έτσι, το ρίσκο που προκύπτει για αυτή την απειλή είναι 10.

Η απειλή T7 θεωρείται αρκετά πιθανή λόγω των πολλών πρωτοκόλλων που υλοποιούνται στο SAE-GW. Φυσικά οι συνέπειες από την εκδήλωση μιας τέτοιας απειλής μπορεί να είναι καταστροφικές. Το ρίσκο εκτιμάται να είναι 45 για την συγκεκριμένη απειλή.

Μία από τις πιο συνηθισμένες επιθέσεις είναι προς το management interface. Επομένως η απειλή T8 θεωρείται αρκετά πιθανό να εκδηλωθεί. Ο βαθμός ευπάθειας του SAE-GW διαφέρει και εξαρτάται στα μέτρα ασφάλειας που θα έχει λάβει ο εκάστοτε πάροχος για την διασφάλιση του συγκεκριμένου interface. Και σε αυτή την περίπτωση οι συνέπειες αναμένεται να είναι καταστροφικές. Τελικά το ρίσκο που εκτιμάται κυμαίνεται από 30 έως 60.

Η απειλή T9 δεν θεωρείται αρκετά πιθανή καθώς η πρόσβαση στο SAE-GW αναμένεται να ελέγχεται αυστηρά και οι ενέργειες να καταγράφονται. Ωστόσο ο βαθμός ασφάλειας και τα κίνητρα για μία τέτοια επίθεση ποικίλουν από χώρα σε χώρα και έχουν να κάνουν με την οικονομική κατάσταση, την κουλτούρα της χώρας και άλλους κοινωνικοπολιτικούς παράγοντες. Σε περίπτωση εκδήλωσης τέτοιου είδους επίθεσης όμως, οι συνέπειες αναμένεται να είναι καταστροφικές. Το ρίσκο που προκύπτει από την ανάλυση κυμαίνεται από 10 έως 40.

Η ανάλυση για την απειλή T10 εστιάζει στις υπηρεσίες χρέωσης καθώς αυτές αναμένεται να προσελκύσουν το ενδιαφέρον των επιτιθέμενων. Οι συνέπειες εκδήλωσης μιας τέτοιας επίθεσης αναμένεται αν είναι καταστροφικές για τον πάροχο. Το ρίσκο που προκύπτει από τη συγκεκριμένη ανάλυση κυμαίνεται από 30 έως 45.

Στον Πίνακας 9 παρουσιάζονται οι τιμές για το εκτιμώμενο ρίσκο της κάθε απειλής.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	4	2	5	40
T2	4	3	4	48
T3.1	2	1	3	6
T3.2	2	2	1 – 3	4 – 12
T4	3	1	2	6
T5.1	1	1	5	5
T5.2	1	2	1 – 3	2 – 6
T6	2	1	5	10

T7	3	3	5	45
T8	3	2 – 4	5	30 – 60
T9	1 – 2	2 – 4	5	10 – 40
T10	3	2 – 3	5	30 – 45

Πίνακας 9 Ανάλυση ρίσκου στο SAE-GW

4.2.2.2 Mobility Management Entity

Η ανάλυση που γίνεται για το MME θεωρεί ότι ισχύουν σε γενικές γραμμές τα όσα ίσχυουν και στην ανάλυση του SAE-GW αναφορικά με τα interfaces και την υλοποίηση των πρωτοκόλλων. Για το λόγο αυτό η ανάλυση δεν γίνεται σε λεπτομέρεια για κάθε μία από τις απειλές αλλά γίνεται μία ενιαία ανάλυση που καλύπτει τα γενικά σημεία. Επίσης το MME χειρίζεται μόνο control-plane traffic επομένως δεν ακολουθείται ο διαχωρισμός σε user-plane και control-plane traffic για τις απειλές T3 και T5.

Τα interfaces που υλοποιούνται στο MME είναι εσωτερικά προς άλλα στοιχεία που βρίσκονται στο δίκτυο κορμού εκτός από το interface προς το δίκτυο πρόσβασης που υλοποιεί το NAS signaling. Στην ανάλυση εκτιμάται ότι η υλοποίηση του MME θα είναι τέτοια ώστε το συγκεκριμένο interface θα χειριστεί με την απαιτούμενη προσοχή ως προς το θέμα της ασφάλειας.

Αναμένεται επίσης ότι όλα τα interfaces θα είναι ασφαλή μέσω της χρήσης IPSec όπως ορίζεται και από τα πρότυπα 3GPP. Οι συνέπειες όμως από την εκδήλωση απειλών αναμένεται να είναι σημαντικές και σε ορισμένες από αυτές, καταστροφικές.

Στον Πίνακας 10 συνοψίζονται οι τιμές που αντιστοιχούν στους παράγοντες καθορισμού του ρίσκου αλλά και το τελικό εκτιμώμενο ρίσκο όπως προκύπτει από την ανάλυση.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	2	3	12
T2	2	2	3	12
T3	2	1	4	8
T4	2	1	4	8
T5	1	1	4	4
T6	1	1	4	4
T7	2	2	5	20
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40
T10	2	1	5	10

Πίνακας 10 Ανάλυση ρίσκου στο MME

Στον παραπάνω πίνακα με κόκκινο χρώμα απεικονίζεται η τιμή του ρίσκου για την απειλή T4. Σε αυτή μόνο την περίπτωση το ρίσκο προκύπτει να είναι μεγαλύτερο από

το αντίστοιχο ρίσκο στην περίπτωση του SAE-GW. Το γεγονός αυτό οφείλεται στα κλειδιά κρυπτογράφησης στα οποία ενδέχεται να αποκτήσει πρόσβαση ο επιτιθέμενος μέσω του MME.

4.2.2.3 ePDG

Όπως και για το MME, έτσι και για το ePDG η ανάλυση δεν είναι λεπτομερής ως προς κάθε απειλή ξεχωριστά αλλά ενιαία και γενική. Οι παραδοχές που αναφέρθηκαν στις προηγούμενες παραγράφους ισχύουν και σε αυτή την περίπτωση.

Το ePDG είναι το στοιχείο που υλοποιεί το interface προς κάποιο μη έμπιστο δίκτυο πρόσβασης επομένως είναι εκτεθειμένο σε επιθέσεις προερχόμενες από ένα τέτοιο δίκτυο. Η χρήση IKE/IPSec συνίσταται για το συγκεκριμένο interface και στα πλαίσια της ανάλυσης εκτιμάται ότι το ePDG θα είναι σε θέση να απορρίψει οποιαδήποτε κίνηση δεν προέρχεται από κάποιο IPSec tunnel. Τα υπόλοιπα interfaces είναι εσωτερικά και εφαρμόζεται παρόμοια ανάλυση με αυτή των άλλων στοιχείων. Επιπλέον στο ePDG δεν αποθηκεύονται δεδομένα χρήστη. Οι συνέπειες από επιτυχημένες επιθέσεις στο ePDG αναμένεται να είναι ιδιαίτερα σημαντικές έως και καταστροφικές για ορισμένες απειλές καθώς μπορεί τα τεθεί σε κίνδυνο η όλη ασφάλεια του δικτύου κορμού.

Στον Πίνακας 11 παρουσιάζονται συνοπτικά οι τιμές που αντιστοιχούν στην πιθανότητα, στο βαθμό ευπάθειας, στις συνέπειες και στο ρίσκο που προκύπτει για κάθε μία από τις απειλές. Με κόκκινο χρώμα απεικονίζεται το ρίσκο που λαμβάνει μεγαλύτερη τιμή από το αντίστοιχο ρίσκο του SAE-GW.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	4	3	4	48
T2	4	2	4	32
T3.1	2	1	3	6
T3.2	2	2	1 – 3	4 – 12
T4	3	1	3	9
T5.1	1	1	4	4
T5.2	1	2	1 – 3	2 – 6
T6	2	1	5	10
T7	3	2	5	30
T8	3	2 – 4	5	30 – 60
T9	1 – 2	2 – 4	5	10 – 40
T10	1	1	5	5

Πίνακας 11 Ανάλυση ρίσκου στο ePDG

4.2.2.4 3GPP AAA-Server or –Proxy

Και ο 3GPP AAA-Server εμπίπτει στις παραδοχές που έχουν ήδη αναφερθεί για το δίκτυο κορμού. Η ανάλυση που παρουσιάζεται στο [8] είναι και σε αυτή την περίπτωση ενιαία ενώ δεν γίνεται διαχωρισμός εάν πρόκειται για AAA-Server ή AAA-Proxy.

Ο 3GPP AAA-Sever επικοινωνεί μόνο με έμπιστα στοιχεία του δικτύου ή με έναν 3GPP AAA-Proxy σε περιπτώσεις περιαγωγής όπως αναφέρθηκε και στην παράγραφο της αρχιτεκτονικής του δικτύου. Τα πρωτόκολλα που υλοποιούνται σε έναν AAA περιορίζονται σε πρωτόκολλα Diameter. Επιπλέον από τον AAA δεν διέρχεται καθόλου user-plane traffic ενώ το control-plane traffic εκτιμάται ότι θα προστατεύεται μέσω IPSec.

Σε έναν AAA-Server όμως βρίσκονται αποθηκευμένες κρίσιμες πληροφορίες, όπως είναι τα δεδομένα αυθεντικοποίησης του χρήστη ή δεδομένα συνδρομητή που σχηματίζουν το προφίλ του. Επομένως οι συνέπειες από μία επιτυχημένη επίθεση ενδέχεται να είναι αρκετά σημαντικές έως και καταστροφικές για κάποιες απειλές όπως είναι παραδείγματος χάρη η πλήρης κατάληψη του AAA από κάποιον επιτιθέμενο.

Οι εκτιμήσεις για τους παράγοντες ρίσκου και το υπολογιζόμενο ρίσκο παρουσιάζονται στον Πίνακας 12.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	2	4	8
T2	1	2	3	6
T3	2	1	4	8
T4	2	1	4	8
T5	1	1	3	3
T6	1	1	3	3
T7	1	2	5	10
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40
T10	2	1	5	10

Πίνακας 12 Ανάλυση ρίσκου στο AAA

Στον παραπάνω πίνακα με κόκκινο χρώμα απεικονίζονται οι τιμές ρίσκου για τις απειλές για τις οποίες το ρίσκο εκτιμάται μεγαλύτερο από το αντίστοιχο στο SAE-GW. Αυτό παρατηρείται για τις απειλές T4 και T9 και οφείλεται στα ευαίσθητα δεδομένα που διατηρούνται σε έναν AAA.

4.2.2.5 Home Subscriber Server

Μία γενική ανάλυση παρουσιάζεται για το HSS. Όπως και για τα προηγούμενα στοιχεία, θεωρείται ότι βρίσκεται σε ασφαλές σημείο στο εσωτερικό δίκτυο και δεν χειρίζεται καθόλου user-plane traffic.

Στο HSS υλοποιούνται δύο κρίσιμες λειτουργίες για το δίκτυο: το AuC και το HLR. Για την εκτέλεση αυτών των λειτουργιών στο HSS αποθηκεύονται ιδιαίτερα κρίσιμες πληροφορίες όπως είναι τα μυστικά κλειδιά αυθεντικοποίησης. Σε αντίθεση όμως με τα στοιχεία που αναλύθηκαν στις παραπάνω παραγράφους, στο HSS υλοποιείται περιορισμένος αριθμός πρωτοκόλλων όπως Diameter και η στοίβα πρωτοκόλλων SS7. Επίσης, αναμένεται να γίνεται χρήση IPSec στα interfaces του HSS προκειμένου να διασφαλιστεί η προστασία της ακεραιότητας.

Η πιθανότητα εκδήλωσης επιθέσεων εκτιμάται να είναι αρκετά μικρή δεδομένου ότι το HSS τοποθετείται «πίσω» από άλλα στοιχεία του δικτύου κορμού όπως το MME. Ωστόσο μία επιτυχημένη επίθεση στο HSS θα έχει καταστροφικές συνέπειες.

Στον Πίνακας 13 παρουσιάζονται οι εκτιμήσεις όπως προκύπτουν από την ανάλυση.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	2	5	10
T2	1	2	5	10
T3	2	2	5	20
T4	2	1	5	10
T5	1	2	5	10
T6	1	1	5	5
T7	1	2	5	10
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40
T10	1	1	5	5

Πίνακας 13 Ανάλυση ρίσκου στο HSS

Με κόκκινο χρώμα απεικονίζονται οι τιμές του ρίσκου οι οποίες εκτιμώνται να είναι μεγαλύτερες από τις τιμές του SAE-GW για την αντίστοιχη απειλή. Οι απειλές για τις οποίες ισχύει αυτό είναι οι T3, T4 και T5 και οφείλεται κυρίως στη συνέπειες οι οποίες θα είναι καταστροφικές για το HSS αλλά και στα ευαίσθητα δεδομένα που βρίσκονται αποθηκευμένα στο HSS.

4.2.2.6 Equipment Identity Register

Το EIR είναι ένα προαιρετικό στοιχείο στο δίκτυο κορμού. Τα interfaces που υλοποιούνται σε αυτό είναι εσωτερικά μόνο προς άλλα στοιχεία του δικτύου. Η ανάλυση που παρουσιάζεται στο [8] είναι γενική και καλύπτει όλες τις απειλές.

Στα πλαίσια της ανάλυσης και καθώς το EIR υλοποιεί παρόμοιες λειτουργίες με αυτές του HSS, θεωρείται ότι αντιμετωπίζει τον ίδιο βαθμό πιθανότητας και ευπάθειας με αυτούς που εκτιμήθηκαν και για το HSS. Δεδομένου όμως ότι πρόκειται για ένα προαιρετικό στοιχείο του δικτύου το οποίο εμφανίζεται να είναι ένα όχι και τόσο ελκυστικό στοιχείο για τους επιτιθέμενους, οι συνέπειες εκτιμώνται να είναι αρκετά μικρότερες για ορισμένες από τις επιθέσεις.

Στον Πίνακας 14 παρουσιάζονται οι απειλές και το εκτιμώμενο ρίσκο όπως προκύπτει από την ανάλυση.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	2	4	8
T2	1	2	4	8
T3	2	2	3	12
T4	2	1	3	6
T5	1	2	4	8
T6	1	1	4	4
T7	1	2	5	10
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40
T10	1	1	5	5

Πίνακας 14 Ανάλυση ρίσκου στο EIR

4.2.2.7 2G/3G στο 4G

Όπως παρουσιάστηκε στο προηγούμενο κεφάλαιο, το 4G δίκτυο θα συμπληρώνεται από την συνύπαρξη των 2G/3G στοιχείων όπως το SGSN και το GGSN, αλλά και το CS και IMS δίκτυο. Για την πληρέστερη εικόνα της ανάλυσης που πραγματοποιήθηκε στα πλαίσια του ASMONIA, οι πίνακεςΠίνακας 15, Πίνακας 16,Πίνακας 17 καιΠίνακας 18 παρουσιάζουν τις εκτιμώμενες τιμές για τους παράγοντες ρίσκου και το υπολογιζόμενο ρίσκο όπως αυτές προκύπτουν από την ανάλυση.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	2	4	16
T2	2	2	4	16
T3.1	2	1	4	8
T3.2	2	1	1 – 3	2 – 6
T4	2	1	4	8
T5.1	1	1	4	4
T5.2	1	1	1 – 3	1 – 3
T6	1	1	4	4
T7	2	2	5	20
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40

T10	2	2	5	20

Πίνακας 15 Ανάλυση ρίσκου στο SGSN

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	2	5	40
T2	4	2	4	32
T3.1	2	1	3	6
T3.2	2	2	1 – 3	4 – 12
T4	3	1	2	6
T5.1	1	1	5	5
T5.2	1	2	1 – 3	2 – 6
T6	2	1	5	10
T7	3	2	5	30
T8	3	2 – 4	5	30 – 60
T9	1 – 2	2 – 4	5	10 – 40
T10	3	2 – 3	5	30 – 45

Πίνακας 16 Ανάλυση ρίσκου στο GGSN

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	2	4	16
T2	2	2	4	16
T3.1	2	2	3	12
T3.2	2	2	1 – 3	4 – 12
T4	1	1	2	2
T5.1	1	2	5	10
T5.2	1	2	1 – 3	2 – 6
T6	1	1	5	5
T7	2	3	5	30
T8	2	2 – 4	5	20 – 40
T9	1 – 2	2 – 4	5	10 – 40
T10	2	2	5	20

Πίνακας 17 Ανάλυση ρίσκου στο CS

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	3	2	4	24
T2	2	2	4	16
T3.1	3	2	3	18
T3.2	3	3	1 – 3	9 – 27
T4	2	1	3	6
T5.1	2	2	4	16
T5.2	1	2	1 – 3	2 – 6
T6	1	1	4	4
T7	2	3	5	30
T8	3	2 – 4	5	30 – 60
T9	1 – 2	2 – 4	5	10 – 40
T10	3	2	5	30

Πίνακας 18 Ανάλυση ρίσκου στο IMS

4.2.3 Δίκτυο υπηρεσιών και δίκτυο υποδομής

Στο [8] παρουσιάζεται επίσης η ανάλυση ρίσκου και για τα Charging Systems, PCRF, Security Gateway, αλλά και για συγκεκριμένες υπηρεσίες που υλοποιούνται στο δίκτυο, όπως είναι οι Location Services και Short Message Services. Οι πίνακες που περιέχουν τις εκτιμώμενες τιμές ρίσκου για τα παραπάνω βρίσκονται στο παράρτημα Β καθώς θεωρείται ότι τα παραπάνω συναντώνται και σε δίκτυα 2G/3G και η συγκεκριμένη εργασία εστιάζει στο 4G δίκτυο.

Στο ίδιο παράρτημα βρίσκονται και ο αντίστοιχοι πίνακες που περιέχουν το εκτιμώμενο ρίσκο για τους OAM Servers και Application Servers που ανήκουν στο δίκτυο κορμού αλλά είναι ανεξάρτητοι από το 4G δίκτυο. Ως παράδειγμα Application Server αναφέρονται οι Web Proxies.

Στο δίκτυο υποδομής εντάσσονται τα στοιχεία εκείνα που συντελούν στην ολοκλήρωση της σύνδεση των στοιχείων του δικτύου κορμού. Ως πιο σημαντικά, αυτά που εξετάζονται είναι οι δρομολογητές του δικτύου κορμού (backbone routers) και οι DNS Servers. Οι αντίστοιχοι πίνακες για αυτά τα στοιχεία βρίσκονται και αυτοί στο παράρτημα Β.

5. Η προτεινόμενη αρχιτεκτονική

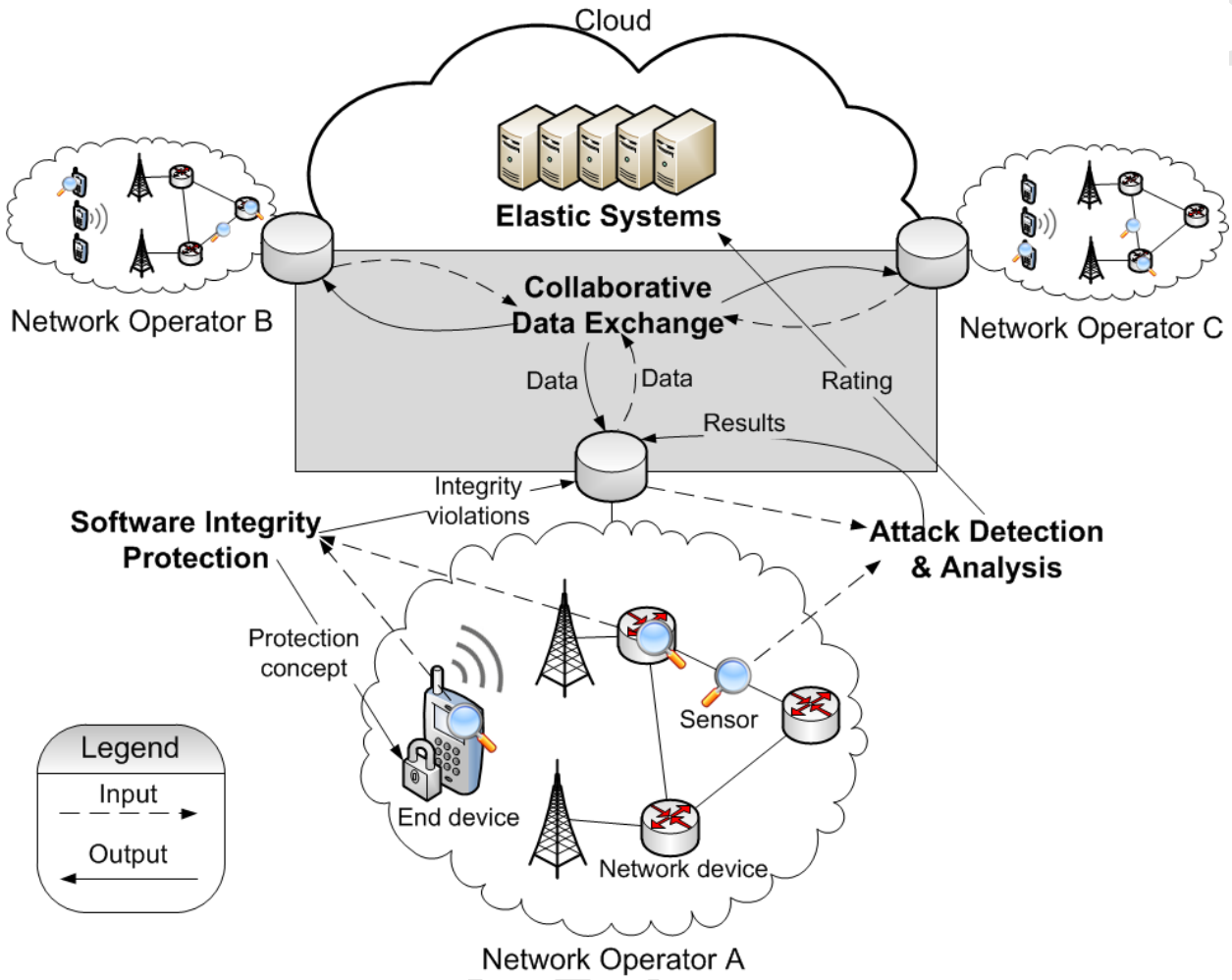
Στο Σχήμα 18 απεικονίζεται η γενική ιδέα της προτεινόμενης αρχιτεκτονικής όπως παρουσιάζεται στο [1]. Στην ιδέα αυτή εμφανίζονται τέσσερα βασικά στοιχεία:

- Προστασία της ακεραιότητας του λογισμικού (Software Integrity Protection)
- Ανίχνευση επιθέσεων και ανάλυση (Attack detection and Analysis)
- Ελαστικά συστήματα/Υπολογιστική νέφους (Elastic Systems/Cloud Computing)
- Ανταλλαγή δεδομένων σε καθεστώς συνεργασίας (Collaborative Data Exchange)

Στο δίκτυο του παρόχου υπάρχουν σένσορες οι οποίοι συγκεντρώνουν στοιχεία που τους επιτρέπουν να ανιχνεύουν επιθέσεις, παραβιάσεις ακεραιότητας (integrity violations) και γενικά μη φυσιολογική συμπεριφορά στο δίκτυο. Οι σένσορες μεταφέρουν τα στοιχεία αυτά στις λειτουργικές μονάδες του δικτύου οι οποίες αναλαμβάνουν να τα αναλύσουν και να προβούν στην εκτίμησή τους. Τα αποτελέσματα αυτά αποθηκεύονται στην τοπική βάση δεδομένων που διαθέτει ο κάθε πάροχος και μπορούν να χρησιμοποιηθούν ως γνώση για τη μελλοντική αποφυγή ίδιων επιθέσεων. Τα δεδομένα αυτά μπορούν να μεταφερθούν μέσα από το cloud και στους υπόλοιπους παρόχους προκειμένου να ενημερωθούν και αυτοί για το περιστατικό ασφάλειας που σημειώθηκε.

Μέσα από τη συγκεκριμένη αρχιτεκτονική σχηματίζεται ένα πλαίσιο (ASMONIA framework), στο οποίο ορίζονται μια σειρά από ιδέες, διαδικασίες (procedures), πρωτόκολλα, διεπαφές (Interfaces), λειτουργικές δομές (Functional Components) και απεικονίσεις δεδομένων, τα οποία αποτελούν το τεχνολογικό υπόβαθρο για την διαμοίραση τόσο πληροφοριών όσο και πόρων στους συμμετέχοντες στο δίκτυο ASMONIA.

Στις παρακάτω ενότητες παρουσιάζονται αναλυτικά τα συστατικά μέρη της προτεινόμενης αρχιτεκτονικής (Components), λειτουργικές μονάδες (Functional Clusters), sensors, interfaces και τα ASMONIA modules.



Σχήμα 18 Η προτεινόμενη αρχιτεκτονική

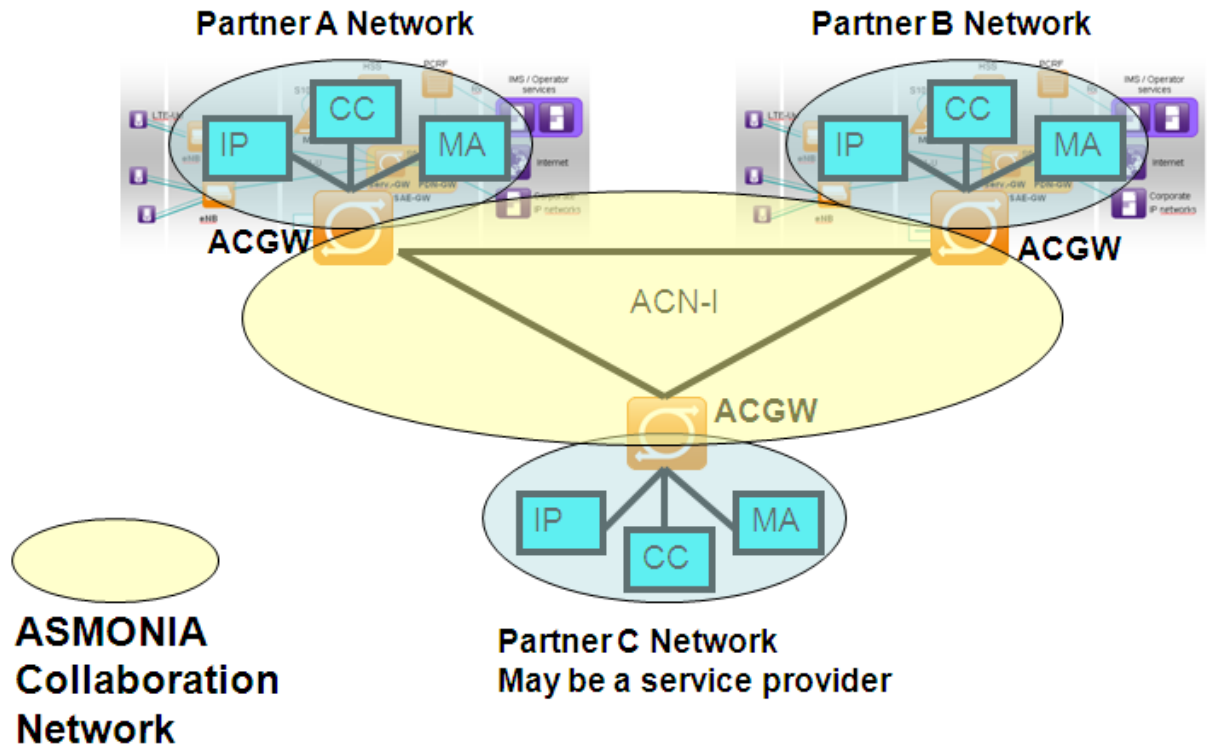
5.1 Συστατικά στοιχεία

Τα κύρια στοιχεία της αρχιτεκτονικής είναι το δίκτυο του παρόχου (Operator Network, ON), το cloud και το συνεργαζόμενο δίκτυο που σχηματίζουν οι συμμετέχοντες στο ASMONIA. Προκειμένου να επιτελούνται οι τέσσερις βασικές λειτουργίες του ASMONIA, πρέπει να ενσωματωθούν στο δίκτυο τα ακόλουθα functional clusters, τα οποία θα παρουσιαστούν αναλυτικά στη συνέχεια :

- Functional Cluster Integrity Protection (FC IP)
- Functional Cluster Collaborative Cloud (FC CC)
- Functional Cluster Monitoring & Analysis (FC MA)

Για να συμμετάσχει κάποιος στο ASMONIA θα πρέπει να ενσωματώσει στο δίκτυό του έναν επιπλέον κόμβο, ο οποίος καλείται ASMONIA Collaboration Gateway (ACGW). Μέσω του κόμβου αυτού καθίσταται δυνατή η επικοινωνία των συμμετεχόντων και αποτελεί τον συνδετικό κρίκο ανάμεσα στο ιδιωτικό δίκτυο του παρόχου και το δίκτυο που σχηματίζεται από τους συμμετέχοντες. Το δίκτυο αυτό που δημιουργείται με τη συμμετοχή δύο ή περισσότερων ACGWs, ονομάζεται Δίκτυο Συνεργασίας ASMONIA (ASMONIA Collaboration Network, ACN).

Στο Σχήμα 19 διακρίνονται τα κύρια συστατικά μέρη της αρχιτεκτονικής που προαναφέρθηκαν καθώς και άλλα τα οποία θα περιγραφούν στις παραγράφους που ακολουθούν στη συνέχεια του κεφαλαίου.



Σχήμα 19 Το Asmonia Collaboration Network

5.2 Functional Clusters

Ο κάθε συμμετέχοντας θα πρέπει να περιλαμβάνει στο ιδιωτικό του δίκτυο τουλάχιστον ένα από τα functional clusters. Κάθε functional cluster υλοποιεί συγκεκριμένες λειτουργίες και interfaces, τα οποία είναι απαραίτητα για την ολοκλήρωση

συγκεκριμένων δυνατοτήτων του ASMONIA. Έτσι προκύπτουν τα ακόλουθα functional clusters:

- FC IP: υλοποιεί τις αναγκαίες λειτουργίες για συνεργασία ως προς το κομμάτι της προστασίας της ακεραιότητας
- FC CC: υλοποιεί τις αναγκαίες λειτουργίες για την διαμοίραση πόρων, όπως είναι ο αποθηκευτικός χώρος αλλά και οι υπολογιστικοί πόροι
- FC MA: υλοποιεί τις αναγκαίες λειτουργίες για την πρόσβαση, συγκέντρωση, επεξεργασία και προώθηση των συλλεγόμενων πληροφοριών

Να σημειωθεί ότι δεν είναι απαραίτητο για κάθε συμμετέχοντα να χρησιμοποιεί όλα τα functional clusters, αλλά αρκεί η χρήση ενός εξ αυτών εάν ο τρόπος συμμετοχής του στο ASMONIA δεν επιβάλει την χρήση των υπολοίπων. Παραδείγματος χάρη η περίπτωση όπου ένας συμμετέχων παρέχει απλώς την υποδομή cloud στο ASMONIA. Στην περίπτωση αυτή ο συμμετέχων καλείται να ενσωματώσει μόνο το FC CC.

Τα functional clusters μπορούν να θεωρηθούν ως το επιπλέον επίπεδο το οποίο εισάγει το απαιτούμενο λογικό επίπεδο αφαίρεσης που χρειάζεται προκειμένου να ενσωματωθεί στο ιδιωτικό δίκτυο του εκάστοτε συμμετέχοντα ο κόμβος ACGW.

5.3 Sensors

Οι sensors είναι μονάδες εγκατεστημένες στο ON και είναι υπεύθυνες για την συλλογή πληροφοριών για τους σκοπούς του ASMONIA. Στο [1] δίνονται οι ακόλουθοι ορισμοί:

Sensor: οποιαδήποτε πηγή πληροφορίας

Local sensor: οι sensors που λειτουργούν στο τοπικό ON

Visible sensor: ένας sensor ορατός στο MA functional cluster και προσπελάσιμος από αυτό

Shared sensor: ένας sensor ορατός και προσπελάσιμος σε όλους τους συμμετέχοντες μέσω του κατάλληλου interface (ACN-I)

External sensor: από τη σκοπιά του ON, πρόκειται για έναν visible sensor ο οποίος όμως δεν είναι local sensor

5.4 Interfaces

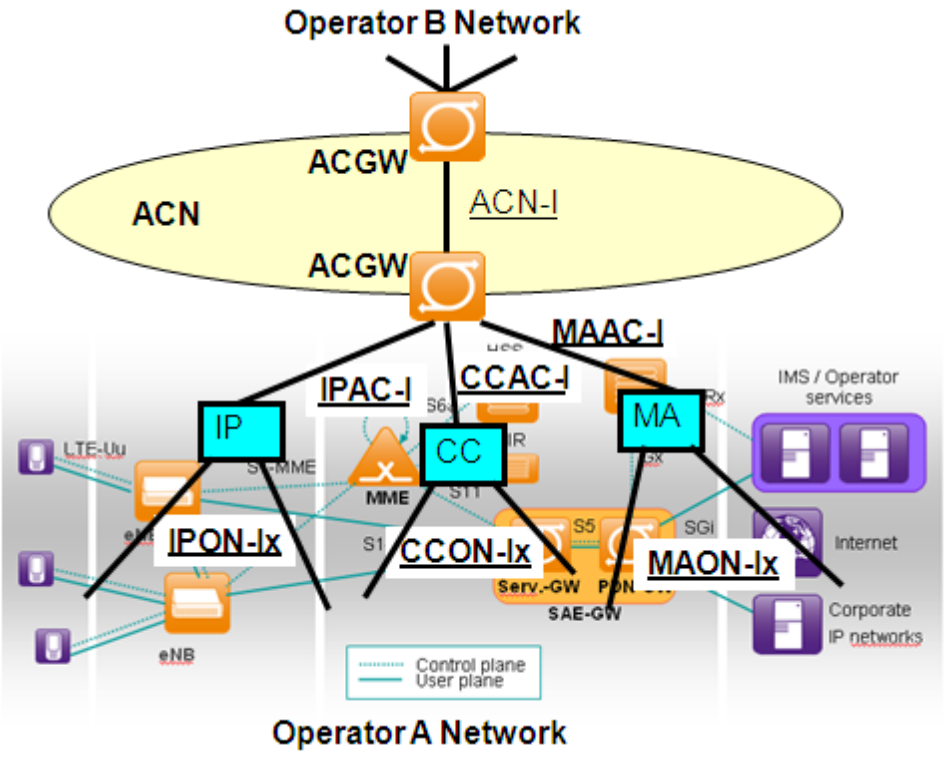
Τα interfaces χρησιμοποιούνται για την επικοινωνία των κόμβων μεταξύ τους, των κόμβων με τα functional clusters, των functional clusters με τα ιδιωτικά δίκτυα των συμμετεχόντων, αλλά και όλων των επιμέρους μερών όπου αυτό χρειάζεται. Διακρίνονται σε εσωτερικά και εξωτερικά ανάλογα με το ποιες μονάδες ενώνουν. Έτσι εξωτερικό interface θεωρείται το ACN-I, που είναι το interface που ενώνει δύο ACGWs μεταξύ τους, ενώ εσωτερικά θεωρούνται τα ακόλουθα, τα οποία ενώνουν τα αντίστοιχα functional clusters με τον κόμβο ACGW:

- IPAC-I
- CCAC-I
- MAAC-I

Εσωτερικά όμως θεωρούνται και τα interfaces που ενώνουν τα functional clusters με τα ιδιωτικά δίκτυα. Έτσι προστίθενται και αυτά στην κατηγορία των εσωτερικών:

- IPON-Ix
- CCON-Ix
- MAON-Ix

Στο Σχήμα 20 παρουσιάζονται τα interfaces και το πως διαμορφώνεται το δίκτυο επικοινωνίας σύμφωνα με αυτά.



Σχήμα 20 ASMONIA interfaces

5.4.1 ACN-I

Το ACN-I ενώνει τα ACGW που σχηματίζουν το ACN επιτρέποντας στους συμμετέχοντες να αλληλεπιδρούν μεταξύ τους. Μέσω αυτού κάθε ACGW μπορεί να αναγνωρίσει τους υπόλοιπους συμμετέχοντες. Επίσης καθίσταται δυνατός ο έλεγχος της πολιτικής ασφάλειας και απορρήτου του δικτύου. Το ACN-I καθιστά δυνατό για ένα ACGW να αποκτήσει πρόσβαση και να διαχειριστεί τις δυνατότητες συνεργασίας όπως αυτές παρέχονται από τα functional clusters. Τέλος, το ACGW λαμβάνει συγκεκριμένα αιτήματα (requests) μέσω του ACN-I τα οποία και μετατρέπει στα αντίστοιχα αιτήματα προς τα functional clusters.

5.4.2 xxAC-I interfaces

Όπως ήδη αναφέρθηκε, πρόκειται για εσωτερικά interfaces που καθιστούν δυνατή την επικοινωνία μεταξύ του ACGW και των functional clusters. Έτσι, οι λειτουργίες που υλοποιούνται μέσα από αυτά, καθορίζονται από το functional cluster το οποίο

συνδέουν. Συγκεκριμένα το IPAC-I παρέχει τις αναγκαίες λειτουργίες για την ανταλλαγή πληροφοριών ως προς την προστασία της ακεραιότητας. Αντιστοίχως το CCAC-I παρέχει τις λειτουργίες που χρειάζονται για την κοινή χρήση του cloud. Οι λειτουργίες αυτές περιλαμβάνουν την πρόσβαση και διαχείριση του κοινού αποθηκευτικού χώρου και των κοινών υπολογιστικών πόρων. Τέλος το MAAC-I παρέχει τις λειτουργίες για την πρόσβαση και διαχείριση των πληροφοριών που διαμοιράζονται στους συμμετέχοντες.

Στο [1] αναφέρεται ότι είναι δυνατή η χρήση των παραπάνω interfaces και για την επικοινωνία μεταξύ διαφόρων οντοτήτων του ON, που δεν αποτελούν όμως συστατικά στοιχεία του ASMONIA, με τα functional clusters. Ωστόσο κάτι τέτοιο θεωρώ ότι δεν είναι εφικτό και δεν εμπίπτει στην λειτουργικότητα που καλούνται να υλοποιήσουν τα συγκεκριμένα interfaces, αλλά και οι ίδιοι οι συγγραφείς δεν τεκμηριώνουν αυτή τους την πρόταση. Αυτό που επίσης παρατηρούν είναι ότι θα πρέπει να εξεταστεί η δυνατότητα χρήσης των interfaces για την εσωτερική επικοινωνία σε ένα ιδιωτικό δίκτυο, λειτουργώντας ουσιαστικά ένα ACN αυτή τη φορά όμως τοπικά, χωρίς ωστόσο να αναμένουν θετικά αποτελέσματα.

5.4.3 xxON-Ix Interfaces

Πρόκειται για τα interfaces μεταξύ των functional clusters και των ASMONIA sensors που έχουν εγκατασταθεί στο ON. Έτσι, με βάση το functional cluster το οποίο συνδέουν προκύπτουν τα IPON-Ix, CCON-Ix και MAON-Ix.

Το IPON-Ix είναι το interface μέσω του οποίου μεταφέρονται οι πληροφορίες σχετικά με την ακεραιότητα των τερματικών συσκευών και άλλων μερών του ON προς το IP cluster. Πρόκειται για αμφίδρομο interface καθώς μέσω αυτού μεταφέρονται και πληροφορίες από το IP προς τα στοιχεία του δικτύου προκειμένου να επανέρθουν στην αρχική κατάσταση ύστερα από την εκδήλωση μιας επίθεσης.

Το CCON-Ix είναι το interface μέσω του οποίου καθίσταται δυνατή η επικοινωνία των στοιχείων του ON με το CC cluster. Οι λειτουργίες που ολοκληρώνονται μέσω αυτού είναι

- η μεταφορά πληροφοριών σχετικά με τη διαχείριση των πόρων από το cluster προς το ON
- η μεταφορά προειδοποιητικών μηνυμάτων (warnings) που έλαβε το CC cluster από το ACN
- η μεταφορά δεδομένων που είναι προϊόντα ανάλυσης είτε από το ON προς το CC cluster είτε από το MA cluster προς το CC cluster, με σκοπό την προώθησή τους στο ACN

- η δημιουργία backup και αποθήκευσή του στο cloud

Το MAON-Ix είναι το interface που ενώνει το MA cluster με τα διάφορα στοιχεία του ON. Ουσιαστικά, μέσω αυτού επικοινωνούν οι ASMONIA sensors με το MA cluster, επομένως οι λειτουργίες που το interface παρέχει, έχουν να κάνουν με την διαχείριση των sensors και την πρόσβαση σε πληροφορίες που προέρχονται από το ON και προορίζονται για το MA cluster. Επίσης μέσω του interface αυτού φτάνουν στο ON πληροφορίες από το ACN σχετικά με αντίμετρα που αφορούν συγκεκριμένες επιθέσεις. Η εφαρμογή των αντίμετρων ωστόσο, δεν εμπίπτει στους σκοπούς την συγκεκριμένης έρευνας που πραγματοποιείται από το ASMONIA.

5.5 ASMONIA modules

Πέρα από τα συστατικά μέρη που περιγράφηκαν μέχρι τώρα, υπάρχουν και κάποιες πιο μικρές μονάδες (modules), οι οποίες υλοποιούν βασικές λειτουργίες για το ASMONIA, οι οποίες όμως δεν συνδέονται άμεσα με ένα συγκεκριμένο cluster. Οι μονάδες αυτές λειτουργούν βοηθητικά στα xxON-Ix και xxAC-I interfaces προκειμένου να επικοινωνήσουν σωστά τα functional clusters με το ON και το ACN. Τα modules που παρουσιάζονται είναι τα TM, APM, NFM και RMM.

Το TM (Translation module) υποστηρίζει κυρίως τα IPON-Ix και MAON-Ix interfaces και μετατρέπει τις πληροφορίες που συλλέγουν οι sensors σε μία ενιαία μορφή, κατάλληλη να την επεξεργαστούν τα clusters, ώστε να επιτευχθεί καλύτερη και ταχύτερη ανάλυση. Το TM μπορεί να υλοποιηθεί είτε ως ξεχωριστός κόμβος είτε ως μέρος ενός cluster.

Το APM (Anonymization and Privacy module) αναλαμβάνει να αφαιρέσει ολόκληρη ή μέρος της ευαίσθητης πληροφορίας που πρόκειται να εξέρθει από το ON προς το ACN. Η πληροφορία αυτή αφορά τα στοιχεία εκείνα που συνδέονται με περιστατικά ασφάλειας, τα οποία όμως σχετίζονται αποκλειστικά με το ON και δεν θα πρέπει να αποκαλυφθούν στους συμμετέχοντες, καθώς κάτι τέτοιο θα έβλαπτε την φήμη του ON. Καθώς πρόκειται για ένα ιδιαίτερα σημαντικό module, προτείνεται να υλοποιείται είτε ως ξεχωριστός κόμβος πριν το ACGW ώστε οι εξερχόμενες πληροφορίες να διέρχονται πρώτα από το APM, είτε ως μέρος του ACGW. Για την πρώτη περίπτωση όμως δεν ορίζονται καινούρια interfaces σε κάποια από τις δημοσιεύσεις του ASMONIA.

Το NFM (Normalization and Format module) εκτελεί λειτουργία αντίστοιχη με αυτή του TM, μετατρέποντας τις πληροφορίες από τους sensors σε μία μορφή κατάλληλη για την επικοινωνία μεταξύ των clusters. Αυτό που προτείνεται για την υλοποίησή του, είναι αυτή να γίνει ως μέρος του ACGW ούτως ώστε να είναι διαθέσιμο για όλα τα clusters μέσω των XXAC-I interfaces.

Το RMM (Reputation Monitoring module) είναι ένα module το οποίο διατηρεί ιστορικό των αναφερθέντων συμβάντων τα οποία ελήφθησαν μέσω του ACN, ώστε στην περίπτωση που κάποιο αποδειχθεί μη ακριβές, το RMM να μπορεί να καταγράψει την πληροφορία αυτή καθώς και ποιος είναι ο αποστολέας του. Στην περίπτωση που η αποστολή ψευδών πληροφοριών συμβαίνει συστηματικά από κάποιον συμμετέχοντα, μέσω του RMM θα είναι δυνατό να μειωθεί ο βαθμός εμπιστοσύνης προς αυτόν. Η προτεινόμενη θέση του στην όλη αρχιτεκτονική είναι ανάμεσα στο cloud cluster και το cloud του ON. Ωστόσο με αυτό τον τρόπο δίνεται η συγκεκριμένη δυνατότητα μόνο σε όσους διαθέτουν στο δίκτυο τους cloud. Εναλλακτικά θεωρώ ότι θα ήταν καλύτερα να υλοποιηθεί ως μέρος του ACGW, προσφέροντας τη συγκεκριμένη δυνατότητα σε όλους τους συμμετέχοντες. Επιπλέον θα μπορούσε να εξελιχθεί περαιτέρω και οι συμμετέχοντες να ανταλλάζουν και πληροφορίες σχετικά με την ακρίβεια των πληροφοριών που έλαβαν.

6. Τεχνικά μέσα και πολιτική χρήσης για την εκπλήρωση των απαιτήσεων συστήματος

Στο [1] γίνεται αναφορά στις διάφορες απαιτήσεις συστήματος (requirements) τις οποίες πρέπει να ικανοποιεί το ASMONIA. Στο [5] παρουσιάζονται τα τεχνικά μέσα και η προτεινόμενη πολιτική χρήσης για την εκπλήρωση των συγκεκριμένων απαιτήσεων. Στις ενότητες που ακολουθούν περιγράφονται οι απαιτήσεις, τα τεχνικά μέσα και η πολιτική χρήσης.

6.1 Απαιτήσεις συστήματος

Η βασική απαίτηση που καλείται να εκπληρώσει το ASMONIA είναι η ακόλουθη :

«the economic payoff should be maximized for interaction carried out in 4G mobile networks, including transparent and traceable associated security risks for participating agents»,

το οποίο σημαίνει ότι το σύστημα θα πρέπει να λειτουργεί με τέτοιο τρόπο, ώστε να μεγιστοποιείται το οικονομικό όφελος για τους συμμετέχοντες μέσω αλληλεπιδράσεων που συντελούνται σε 4G δίκτυα προκειμένου να επιτευχθεί η συνεργασία στον τομέα της ασφάλειας.

Η γενική αυτή απαίτηση μπορεί να διασπαστεί σε επιμέρους απαιτήσεις οι οποίες ορίζουν με περισσότερη ακρίβεια μικρότερα τμηματικά μέρη αυτής. Με την υλοποίηση όλων των επιμέρους απαιτήσεων, υλοποιείται και η γενική απαίτηση.

Οι επιμέρους απαιτήσεις διακρίνονται σε λειτουργικές και σε μη λειτουργικές. Οι μη λειτουργικές απαιτήσεις αναφέρονται σε γενικά χαρακτηριστικά που πρέπει να έχει το σύστημα κυρίως λόγω της φύσης του. Οι λειτουργικές απαιτήσεις περιγράφουν χαρακτηριστικά του συστήματος που σχετίζονται με συγκεκριμένες λειτουργίες που καλείται να πραγματοποιήσει.

Μια άλλη κατηγοριοποίηση που ακολουθείται από τους συγγραφείς έχει να κάνει με τον τομέα εφαρμογής των απαιτήσεων. Έτσι υπάρχουν οι απαιτήσεις για τα συστατικά μέρη της αρχιτεκτονικής, οι απαιτήσεις ως προς την ασφάλεια του συστήματος και οι απαιτήσεις για την εκπλήρωση της συνεχόμενης μείωσης του ρίσκου μέσω του ASMONIA.

Στις ενότητες που ακολουθούν περιγράφονται σύντομα οι πιο βασικές απαιτήσεις όπως προκύπτει από το [1]. Όλες οι απαιτήσεις καταγράφονται στο παράρτημα Γ.

6.1.1 Απαιτήσεις συνεχόμενης μείωσης ρίσκου

Οι συγκεκριμένες απαιτήσεις διακρίνονται σε λειτουργικές και μη λειτουργικές. Οι λειτουργικές περιγράφουν ιδιότητες του συστήματος προκειμένου να επιτευχθεί η μείωση του ρίσκου μέσω της συνεργασίας των συμμετεχόντων. Οι απαιτήσεις αυτές σχετίζονται με οικονομικά και επιχειρηματικά χαρακτηριστικά του συστήματος με γνώμονα την συνεργασία και πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό του συστήματος.

Οι μη λειτουργικές απαιτήσεις περιγράφουν τα γενικά χαρακτηριστικά που πρέπει να διαθέτει ένα σύστημα, όπως αυτά προκύπτουν από τις τελευταίες τάσεις της βιομηχανίας. Η πιο σημαντική ανάμεσα σε αυτές, είναι η απαίτηση για δια-λειτουργικότητα. Αυτό προκύπτει αν ληφθεί υπόψη μία από τις βασικές λειτουργίες του συστήματος που περιλαμβάνει την διαμοίραση των πληροφοριών μεταξύ των συμμετεχόντων. Άλλη μία σημαντική απαίτηση είναι αυτή της ασφάλειας η οποία όμως εξετάζεται και αντιμετωπίζεται ως διαφορετική κατηγορία απαιτήσεων.

6.1.2 Απαιτήσεις συστατικών μερών

Τα συστατικά μέρη του ASMONIA πρέπει να υλοποιούν συγκεκριμένες λειτουργίες και ως εκ τούτου οι απαιτήσεις που ορίζονται για τα συστατικά μέρη είναι μόνο λειτουργικές. Περιγράφουν την ανάγκη ύπαρξης ενός interface προκειμένου να επικοινωνούν οι συμμετέχοντες μέσω αυτού αλλά η επικοινωνία αυτή θα πρέπει να γίνεται με τρόπο ώστε να διασφαλίζεται η ανωνυμία και το απόρρητο ευαίσθητων δεδομένων του κάθε συμμετέχοντα, αλλά θα πρέπει επίσης να μπορεί να αναγνωριστεί η «ταυτότητα» κάποιου υπό συνθήκες. Δεδομένου ότι οι πληροφορίες που ανταλλάσσονται προέρχονται από διαφορετικά σημεία του ιδιωτικού δικτύου, θα πρέπει να έχουν μία ενιαία μορφή ώστε να μπορούν να χρησιμοποιηθούν από οποιοδήποτε άλλη μονάδα. Θα πρέπει επίσης να υπάρχει ένας τρόπος αποθήκευσης των δεδομένων αλλά και πληροφοριών σχετικών με αναφορές για επιθέσεις που εκδηλώθηκαν, ώστε να εξασφαλίζεται ότι δεν θα μεταδίδονται εσκεμμένα ψευδείς αναφορές.

Ορισμένες από τις προαναφερθείσες απαιτήσεις ωστόσο, όπως φαίνεται και στο παράρτημα Γ, δεν καταγράφονται από τους συγγραφείς ξεκάθαρα ως απαιτήσεις

συστήματος, αλλά περιγράφονται περιφραστικά στο [1]. Η πρακτική αυτή ενδέχεται να οδηγήσει στην παράληψη ελέγχου πληρότητας ορισμένων απαιτήσεων με αποτέλεσμα το σύστημα να μην υλοποιεί ολοκληρωτικά την λειτουργία για την οποία σχεδιάστηκε.

Τα συστατικά μέρη θα πρέπει να υλοποιηθούν με τέτοιο τρόπο ώστε να καλύπτουν τις απαιτήσεις με τεχνικά μέσα. Οι συγγραφείς αναγνωρίζουν ότι τα τεχνικά μέσα ίσως δεν επαρκούν οπότε για τα κενά που προκύπτουν, προτείνεται η πολιτική χρήσης ως το μέσο που θα τα καλύψει. Έτσι προκύπτει ότι και η πολιτική χρήσης θα πρέπει να οριστεί ως απαίτηση και να ακολουθείται από όλους τους συμμετέχοντες.

6.1.3 Απαιτήσεις ασφάλειας

Πρώτα από όλα οι συμμετέχοντες θα πρέπει να έχουν εξασφαλίσει ένα επίπεδο ασφάλειας για το ιδιωτικό τους δίκτυο το οποίο καλούνται να επιτύχουν ακολουθώντας προδιαγραφές όπως το BSI Standards.

Οι απαιτήσεις ασφάλειας που ορίζονται για το ASMONIA είναι κυρίως οι απαιτήσεις ασφάλειας που ορίζονται και για οποιοδήποτε σύστημα. Επομένως προτείνεται η δημιουργία ενός δικτύου στο οποίο οι συμμετέχοντες θα εισέρχονται αφού πρώτα αυθεντικοποιηθούν. Επίσης, δεδομένου ότι πρόκειται για ένα δίκτυο αποτελούμενο από συνδέσεις μεταξύ των συμμετεχόντων, θα πρέπει οι συνδέσεις να πραγματοποιούνται με ασφαλή τρόπο και τα δεδομένα που ανταλλάσσονται να είναι κρυπτογραφημένα.

Ασφαλώς τα βασικά χαρακτηριστικά της ασφάλειας πληροφοριών για προστασία της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας θα πρέπει να ακολουθούνται όπως επίσης και της ανωνυμίας, της ιδιωτικότητας και της μη αποποίησης για τους συμμετέχοντες. Ούτε οι απαιτήσεις αυτές αναφέρονται όλες ρητά στην λίστα με τις απαιτήσεις ασφάλειας, επομένως ορισμένες από τις απαιτήσεις ασφάλειας ενδέχεται να μην ικανοποιηθούν πλήρως κατά την υλοποίηση.

6.2 Τεχνικά μέσα

Προκειμένου να ικανοποιηθούν οι απαιτήσεις, η αρχιτεκτονική του ASMONIA εισάγει modules που διεκπεραιώνουν μέρος των απαιτούμενων λειτουργιών. Τέτοιο είναι το APM το οποίο αναλαμβάνει να αποκρύψει την ταυτότητα ή να την αφαιρέσει τελείως από δεδομένα που πρόκειται να αποσταλούν πριν όμως αυτά εξέρθουν από το ιδιωτικό δίκτυο των συμμετεχόντων. Για να επιτευχθεί όμως η πλήρης ανωνυμία για τον κάθε

συμμετέχοντα θα πρέπει να παραμένει κρυφή η ταυτότητα του και αφού τα δεδομένα εξέρθουν από το δίκτυο του. Κυρίως για το λόγο αυτό, οι συγγραφείς προτείνουν την χρήση των TACs (Traceable Anonymous Certificates), των peer-to-peer overlay networks και ασφαλών τεχνικών MPCs (Multiparty Computation).

Δεδομένου ότι όλοι οι συμμετέχοντες θα ανταλλάσσουν πληροφορίες, πρέπει να υιοθετηθεί μία ενιαία μορφή αυτών (Common data exchange format). Για να είναι ασφαλής η επικοινωνία μεταξύ των συμμετεχόντων προτείνεται η χρήση ασφαλών τεχνικών όπως είναι τα VPN, TLS και IPSec.

Οι περισσότερες από τις τεχνικές έχουν κοινό στοιχείο την ανάγκη πιστοποιητικών τα οποία διαχειρίζονται από υποδομές δημόσιου κλειδιού, PKI (Public Key Infrastructure).

6.2.1 TACs

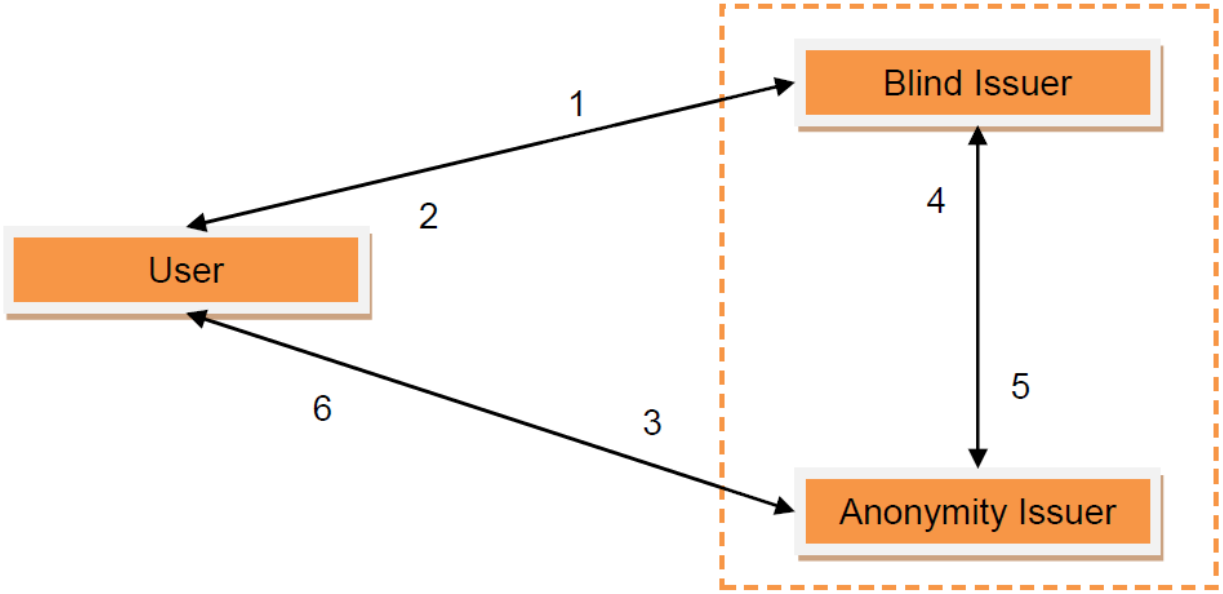
Η τεχνολογία TAC παρέχει στους χρήστες υπηρεσίες ενυπόγραφων πληροφοριών (signed information), εμπιστευτικότητας, μη αποποίησης και αυθεντικοποίησης, επιτρέποντάς τους όμως να διατηρούν κρυφή την ταυτότητά τους. Πρόκειται για ένα πιστοποιητικό που συμμορφώνεται με το πρότυπο X.509 το οποίο εκδίδεται μετά από αίτημα του χρήστη βασισμένο σε ψευδώνυμο που ο ίδιος έχει επιλέξει.

Για τη δημιουργία του πιστοποιητικού απαιτείται η συμβολή δύο μερών, των Blind Issuer (BI) και Anonymity Issuer (AI), τα οποία συνεργάζονται και συμπεριφέρονται ως μία ενιαία αρχή έκδοσης πιστοποιητικού. Επίσης, η συμβολή και των δύο μερών είναι αναγκαία προκειμένου να αποκαλυφθεί η πραγματική ταυτότητα ενός χρήστη όταν αυτό κριθεί απαραίτητο, όπως λόγου χάρη στην περίπτωση που παραβιαστεί το πιστοποιητικό του. Η διαδικασία παραγωγής του πιστοποιητικού παρουσιάζεται στο Σχήμα 21.

Ο χρήστης ζητά την έκδοση πιστοποιητικού από το BI (1). Το BI γνωρίζει την πραγματική ταυτότητα του χρήστη, και δημιουργεί ένα κλειδί που αντιστοιχεί στον χρήστη το οποίο και αποθηκεύει μαζί με την ταυτότητα του. Το BI επιστρέφει στο χρήστη ένα token το οποίο περιέχει το κλειδί και μία τιμή που αντιστοιχεί στο χρονικό διάστημα για το οποίο θα είναι έγκυρο το πιστοποιητικό. (2)

Στη συνέχεια ο χρήστης στέλνει το token που έλαβε από το BI, και ένα ψευδώνυμο της επιλογής του στο A, το οποίο και αποθηκεύει στην βάση του (3). Το AI δημιουργεί έναν σειριακό αριθμό που αντιστοιχεί στο πιστοποιητικό που ζητήθηκε. Ο σειριακός αυτός αριθμός και το ψευδώνυμο αποστέλλονται στο BI αφού εφαρμοστεί μία συνάρτηση Hash. Στο BI επίσης αποστέλλεται και το token αφού πρώτα κρυπτογραφηθούν (4).

Με βάση τα δεδομένα που έλαβε και μη γνωρίζοντας στην πραγματικότητα το ψευδώνυμο, το BI παράγει το μερικώς υπογεγραμμένο πιστοποιητικό το οποίο και στέλνει στο AI (5). Το AI ολοκληρώνει την διαδικασία παραγωγής του πιστοποιητικού υπογράφοντας και αυτό το μερικώς υπογεγραμμένο από το BI πιστοποιητικό που έλαβε. Το τελικό πιστοποιητικό αποθηκεύεται από το AI συσχετιζόμενο με το token και αποστέλλεται τελικά στο χρήστη (6).



Σχήμα 21 Διαδικασία παραγωγής πιστοποιητικού

Σε όλη τη διάρκεια της διαδικασίας παραγωγής του πιστοποιητικού το AI δεν γνωρίζει την πραγματική ταυτότητα του χρήστη ενώ το BI που γνωρίζει την πραγματική ταυτότητα δεν γνωρίζει τίποτα σχετικά με το πιστοποιητικό.

Η χρήση τεχνολογίας TAC παρουσιάζεται ως μία καλή εναλλακτική για το ASMONIA καθώς δεν αλληλεπιδρά με τα υπόλοιπα συστατικά μέρη ενώ μπορεί να καλύψει τις ανάγκες του ACN για εμπιστευτικότητα, ακεραιότητα, μη αποποίηση, ανωνυμία και αυθεντικότητα.

6.2.2 Peer-to-peer Overlay Networks

Τα overlay networks είναι δίκτυα τα οποία λειτουργούν πάνω από άλλα δίκτυα. Οι συγγραφείς προτείνουν τη χρήση ενός ιδιωτικού και ασφαλούς peer-to-peer δικτύου μέσω της χρήσης GNUnet. Το GNUnet είναι ένα σύνολο πρωτοκόλλων, προϊόν

ελεύθερου λογισμικού (open source framework), το οποίο παρέχει έμπιστες, μη κεντρικοποιημένες υπηρεσίες.

Όλοι οι χρήστες σε ένα GNUnet δίκτυο συμπεριφέρονται ως δρομολογητές (routers) και προωθούν τα μηνύματα που έλαβαν από τους άλλους χρήστες στο υπόλοιπο δίκτυο μέσω κρυπτογραφημένων ζεύξεων (link-encrypted connections). Η ανωνυμία εξασφαλίζεται με τη χρήση του πρωτοκόλλου GAP, το οποίο μετατρέπει τα μηνύματα σε μία μορφή η οποία είναι τέτοια ώστε να μην είναι δυνατόν να γίνει αντιληπτό εάν το μήνυμα προέρχεται από έναν συγκεκριμένο χρήστη ή εάν ο χρήστης το προωθεί στο υπόλοιπο δίκτυο.

Το GNUnet παρέχει λοιπόν ανωνυμία, εμπιστευτικότητα και ελαστικότητα (resilience) λόγω της φύσης του peer-to-peer δικτύου, ωστόσο δεν μπορεί να καλύψει την ανάγκη αποκάλυψης της ταυτότητας εφόσον αυτό ζητηθεί. Οι συγγραφείς προτείνουν για το λόγο αυτό τη χρήση των πιστοποιητικών TACs.

Ένας ακόμη αποθαρρυντικός λόγος ως προς τη χρήση της συγκεκριμένης τεχνικής είναι οι περιορισμοί που εισάγονται ως προς την πλατφόρμα που μπορεί να υποστηρίξει το GNUnet (Debian, Fedora, Ubuntu, Arch, FreeBSD, OS x και Windows 7) [29]. Αυτό σημαίνει ότι το ACGW θα πρέπει να είναι βασισμένο σε μία από τις συγκεκριμένες πλατφόρμες το οποίο μπορεί να είναι πράγματι εφικτό, ωστόσο στις μέχρι τώρα δημοσιεύσεις του ASMONIA δεν αναφέρεται.

6.2.3 Secure Multiparty Computation

Υπάρχουν πρωτόκολλα που υποστηρίζουν την τεχνολογία secure multiparty computation (MPC), τα οποία αποτελούν τεχνικές στον τομέα της κρυπτογραφίας που επιτρέπουν την από κοινού εξαγωγή αποτελέσματος βάση μίας συνάρτησης η οποία δέχεται ως είσοδο δεδομένα τα οποία όμως δεν αποκαλύπτονται.

Η μη αποκάλυψη των δεδομένων επιτυγχάνεται είτε με εφαρμογή κρυπτογραφικών αλγορίθμων στα δεδομένα (homomorphic encryption) ούτως ώστε να μην είναι δυνατόν να αποκαλυφθούν, είτε διασπώντας την πληροφορία ενός συμμετέχοντα σε πολλά μέρη τα οποία διαμοιράζονται στους συμμετέχοντες (secret sharing).

Στο [5] οι συγγραφείς προτείνουν την χρήση της μεθόδου secret sharing, όπως αυτή περιγράφεται στα [30] και [31]. Μια τέτοια υλοποίηση προσφέρει ευελιξία και διατηρεί την ανωνυμία όπως ορίζουν οι απαιτήσεις του ASMONIA. Ωστόσο, η απαίτηση για αποκάλυψη της ταυτότητας εφόσον αυτό ζητηθεί, δεν εξετάζεται καθόλου για την συγκεκριμένη εναλλακτική. Επιπλέον, η χρήση αυτής της τεχνικής προς το παρόν

απαιτεί αρκετό υπολογιστικό χρόνο [32]. Αυτό που οι συγγραφείς θα ήθελαν να εξετάσουν σε μελλοντική τους εργασία είναι το πώς οι τεχνικές MPC μπορούν να χρησιμοποιηθούν προκειμένου να αναγνωρίζουν επιθέσεις που συμβαίνουν στο δίκτυο των χρηστών.

6.2.4 Ενιαία μορφή δεδομένων

Η ανταλλαγή πληροφοριών αποτελεί τη βασική λειτουργία του ASMONIA. Οι πληροφορίες αυτές θα πρέπει να έχουν μία ενιαία μορφή προκειμένου να μπορούν να χρησιμοποιηθούν από όλους τους συμμετέχοντες χωρίς ή με μερική επιπρόσθετη προσπάθεια.

Στο [5] αναφέρεται η πιθανότητα να είναι περισσότερες από μία οι μορφές που θα πρέπει να χρησιμοποιηθούν. Η μία θα εφαρμόζεται στα δεδομένα που θα πρέπει να ανταλλάσσονται εσωτερικά στο δίκτυο κάθε συμμετέχοντα μεταξύ των clusters, και η άλλη στα δεδομένα που θα ανταλλάσουν οι συμμετέχοντες. Στην δεύτερη περίπτωση αυτό θα συμβαίνει για τις εξής κατηγορίες, στις οποίες και επικεντρώνονται οι συγγραφείς:

- Προειδοποιητικά μηνύματα (warnings)
- Δεδομένα ανίχνευσης και ανάλυσης (Collaborative detection and analysis)

Η μορφή που θα χρησιμοποιηθεί να πρέπει να είναι μία εκ των προτυποποιημένων (standardized) προκειμένου να υιοθετηθεί με σχετική ευκολία από όλους τους συμμετέχοντες. Οι προτεινόμενες μορφές είναι

- IODEF (Incident Object Description Exchange Format)
- FINE (Format for INcident Exchange)
- RID (Real-time Inter-network Defence)
- IDMEF, (Intrusion detection Message Exchange Format)
- EISPFormat (European Information Security Promotion Programme)
- CVRF (Common Vulnerability Reporting Framework)
- SCAP (Security Content Automation Protocol)
- CYBEX (Cybersecurity Information Exchange Techniques)

Οι παραπάνω μορφές συγκρίνονται και προκύπτει ότι οι δύο επικρατέστερες που θα ταιριάζουν καλύτερα στο ASMONIA είναι οι IODEF και CYBEX.

6.2.5 Εκπλήρωση απαιτήσεων

Στο Σχήμα 22 παρουσιάζονται οι απαιτήσεις όπως ορίζονται για τα τεχνικά μέσα. Επίσης καταδεικνύεται το ποιες από τις απαιτήσεις καλύπτονται από κάθε ένα από τα τεχνικά μέσα που αναφέρονται στις προηγούμενες παραγράφους.

Component / Requirement	TAC	P2P	MPC	Data format
Anonymity	X	X		
Privacy			X	
Non-repudiation	X			
Interoperability				X
Resilience		X		
Authentication	X			
Integrity	X			
Confidentiality	X			
Fairness		X	X	

Σχήμα 22 Βαθμός κάλυψης απαιτήσεων

6.3 Πολιτική χρήσης

Για την επιτυχή υλοποίηση του ASMONIA πρέπει να περιγραφούν ενέργειες που άπτονται στο οργανωτικό κομμάτι του δικτύου. Οι ενέργειες αυτές εμπίπτουν στην πολιτική χρήσης που ορίζεται για το ASMONIA.

Η πολιτική χρήσης αποτελείται από κανόνες οι οποίοι ορίζουν ενέργειες, διαδικασίες και συμπεριφορές, με τους οποίους οφείλουν να συμμορφώνονται όλοι οι συμμετέχοντες, και όλοι οι συμμετέχοντες έχουν συμφωνήσει για το περιεχόμενό τους.

Συνοπτικά, η πολιτική χρήσης περιγράφει τη διαδικασία που απαιτείται προκειμένου ένας συμμετέχων :

- Να συνδεθεί στο δίκτυο
- Να εγκαταλείψει το δίκτυο, είτε με δική του πρωτοβουλία είτε ως εφαρμογής ποινής, η οποία είναι συνέπεια παραβίασης της πολιτικής
- Να προμηθευτεί τα απαραίτητα πιστοποιητικά (TACs)
- Να διαμοιράσει πληροφορίες στο δίκτυο
- Να επεξεργαστεί δεδομένα που έλαβε από το δίκτυο

Επιπλέον, στην πολιτική χρήσης περιγράφονται οι συνέπειες από πιθανή παραβίαση της ίδιας της πολιτικής.

Αυτό που προκύπτει ωστόσο από την περιγραφή της πολιτικής χρήσης όπως αυτή παρουσιάζεται στο [5], είναι ότι εν τέλει γίνεται αποδεκτό ότι ανάμεσα στους συμμετέχοντες θα πρέπει να υπάρχει ένα επίπεδο εμπιστοσύνης το οποίο όμως δεν είναι άμεσα ελεγχόμενο από κάποια τεχνικά μέσα τα οποία θα εξασφάλιζαν το επίπεδο ασφάλειας που είναι απαραίτητο για τους σκοπούς του ASMONIA. Ως λύση για αυτό το ζητήματα εμφανίζεται ο κανόνας της πολιτικής που ορίζει την ανάγκη ύπαρξης φυσικού προσώπου ανά συμμετέχοντα, ο οποίος θα είναι υπεύθυνος για την διασφάλιση της πλήρωσης των απαιτήσεων ασφάλειας που ορίζονται από το ASMONIA. Για τους σκοπούς του ASMONIA όμως, αυτή η προσέγγιση ίσως να είναι ελλιπής καθώς για το επίπεδο ασφάλειας που απαιτείται από το συγκεκριμένο δίκτυο θα έπρεπε να υπάρχουν αξιόπιστα τεχνικά μέτρα που να διασφαλίζουν το επίπεδο εμπιστοσύνης που απαιτείται.

Επιπλέον δεν υπάρχουν τεχνικά μέσα που θα μπορούσαν να ανιχνεύσουν μία ενδεχόμενη παραβίασης της πολιτικής, και ούτε γίνεται ξεκάθαρο το πώς θα πραγματοποιείται η ανίχνευση. Άλλο ένα αδύναμο σημείο σχετικά με την παραβίαση της πολιτικής έχει να κάνει με τις συνέπειες για τους συμμετέχοντες. Υπάρχει η περίπτωση ο συμμετέχων Α είτε σκόπιμα είτε όχι να βλάψει κάποιον από τους συμμετέχοντες (ή και όλους) δεδομένου ότι οι συμμετέχοντες τις περισσότερες φορές θα είναι και εμπορικοί ανταγωνιστές. Στην περίπτωση αυτή, η ζημιά που θα προκληθεί ενδεχομένως να έχει μεγάλες συνέπειες από τις οποίες τελικά να επωφεληθεί ο συμμετέχων Α. Με βάση την πολιτική χρήσης, αλλά και τα τεχνικά μέσα που αναφέρθηκαν, δεν υπάρχει τρόπος να αποφευχθεί μία τέτοια κατάσταση. Αυτό που περιγράφεται είναι απλώς οι συνέπειες που μπορεί να υποστεί ο συμμετέχων Α, αφού ανιχνευθεί η παραβίαση.

7. Συμπεράσματα

Στα κεφάλαια που προηγήθηκαν παρουσιάστηκε η αρχιτεκτονική ενός 4G τηλεπικοινωνιακού δικτύου. Το 4G δίκτυο στηρίζεται αποκλειστικά στη μεταγωγή πακέτων. Για να επιτευχθεί αυτό αλλάζει το δίκτυο πρόσβασης και το δίκτυο κορμού σε σχέση με τα δίκτυα 2G και 3G. Τα σημαντικότερα στοιχεία που εισάγονται στο νέο δίκτυο είναι το eNB για το δίκτυο πρόσβασης και τα SAE-GW και MME στο δίκτυο κορμού.

Για τους σκοπούς του project ASMONIA πραγματοποιείται μία ανάλυση ρίσκου για το 4G δίκτυο. Η ανάλυση αυτή εξετάζει δέκα απειλές οι οποίες είναι οι εξής:

- T1 Flooding an Interface
- T2 Crashing a network element via a protocol or application implementation flaw
- T3 Eavesdropping
- T4 Unauthorized access to sensitive data on a network element via leakage
- T5 Traffic modification
- T6 Data modification on a network element
- T7 Compromise of a network element via a protocol or application implementation flaw
- T8 Compromise of a network element via a management interface
- T9 Malicious insider
- T10 Theft of service

Όπου κρίνεται απαραίτητο εξετάζονται χωριστά οι απειλές για user plane και control plane traffic. Η μέθοδος εκτίμησης ρίσκου βασίζεται σε μία ποσοτική μέθοδο με κλίμακα 1 έως 5. Το πρόβλημα που προκύπτει από την εφαρμογή της συγκεκριμένης μεθόδου είναι ότι για τον παράγοντα impact δεν ακολουθείται μία αυστηρή ερμηνεία για την κάθε τιμή της κλίμακας με αποτέλεσμα η μέθοδος να χάνει την αντικειμενικότητά της. Ο πίνακας 3 παρουσιάζει μία πιθανή ερμηνεία που θα μπορούσε να αποδοθεί στις τιμές.

Η εκτίμηση ρίσκου που παρουσιάζεται στο κεφάλαιο 4 αφορά το δίκτυο πρόσβασης και το δίκτυο κορμού. Παρατίθεται και μία ενδεικτική σύγκριση των τιμών όπου αυτό είναι εφικτό. Η ανάλυση όπως παρουσιάζεται στο [8] εμφανίζεται αρκετά γενική αναφορικά με το δίκτυο κορμού και το δίκτυο πρόσβασης. Σε αρκετές περιπτώσεις δεν είναι λεπτομερής, ενώ η ανάλυση που γίνεται για ορισμένα στοιχεία κρίνεται επισφαλής καθώς δεν είναι ξεκάθαρη η συλλογιστική που ακολουθήθηκε και οδήγησε στην συγκεκριμένη εκτίμηση όπως αυτή αποδόθηκε.

Η αρχιτεκτονική που προτείνεται από τους συντελεστές του ASMONIA στοχεύει στα ακόλουθα στοιχεία:

- Προστασία της ακεραιότητας του λογισμικού (Software Integrity Protection)
- Ανίχνευση επιθέσεων και ανάλυση (Attack detection and Analysis)
- Ελαστικά συστήματα/Υπολογιστική νέφους (Elastic Systems/Cloud Computing)
- Ανταλλαγή δεδομένων σε καθεστώς συνεργασίας (Collaborative Data Exchange)

Για να επιτευχθούν αυτά προτείνεται η χρήση συγκεκριμένων στοιχείων τα οποία θα ενσωματωθούν στο δίκτυο του κάθε συμμετέχοντα. Τα στοιχεία αυτά είναι το ACGW, τα IP, CC και MA functional clusters, sensors που θα συλλέγουν πληροφορίες από το ιδιωτικό δίκτυο των συμμετεχόντων, ενώ για την επίτευξη της μεταξύ τους επικοινωνίας θα αξιοποιείται η τεχνολογία cloud. Το σχηματιζόμενο δίκτυο που προκύπτει ονομάζεται ACN.

Για την υλοποίηση της συγκεκριμένης αρχιτεκτονικής είναι απαραίτητος ο ορισμός κάποιων απαιτήσεων, τις οποίες θα πρέπει να καλύπτει το νέο δίκτυο. Οι απαιτήσεις αυτές καλύπτουν τους τομείς της συνεχόμενης μείωσης ρίσκου, τα συστατικά μέρη και την ασφάλεια. Στα προτεινόμενα τεχνικά μέσα για την κάλυψη αυτών των απαιτήσεων συγκαταλέγονται η τεχνολογία TAC, τα peer-to-peer overlay networks και η τεχνολογία secure multiparty computation ενώ αναφέρεται και η ανάγκη ύπαρξης μίας ενιαίας μορφής που θα πρέπει να έχουν οι πληροφορίες που διακινούνται στο δίκτυο. Καμία από τις παραπάνω τεχνολογίες δεν καλύπτει ταυτόχρονα όλες τις απαιτήσεις οπότε ο συνδυασμός κάποιων από αυτές είναι απαραίτητος.

Για την επιτυχή λειτουργία του δικτύου είναι αναγκαίος και ο ορισμός μιας πολιτικής χρήσης. Ωστόσο προκύπτει ένα κενό. Θεωρείται δεδομένο ότι ανάμεσα στους συμμετέχοντες θα πρέπει να υπάρχει ένα επίπεδο εμπιστοσύνης το οποίο όμως δεν είναι άμεσα ελεγχόμενο από κάποια τεχνικά μέσα τα οποία θα εξασφάλιζαν το επίπεδο ασφάλειας που είναι απαραίτητο για τους σκοπούς του ASMONIA. Η έλλειψη αξιόπιστων τεχνικών μέσων παρατηρείται και ως προς την ανίχνευση παραβιάσεων της ίδιας της πολιτικής όπως επίσης και ως προς την άμυνα του ίδιου του δικτύου απέναντι σε τέτοιου είδους παραβιάσεις.

Η γενική ιδέα για σχηματισμό δικτύου που θα επιτρέπει τη συνεργασία για μεγαλύτερη ασφάλεια όπως παρουσιάζεται στο ASMONIA χαρακτηρίζεται εν γένει αρκετά ενδιαφέρουσα. Οι δημοσιεύσεις του project αποτελούν γενικά μία αρκετά καλή πρώτη προσπάθεια αποτύπωσης διάφορων ιδεών, καλύπτοντας πολλούς τομείς της ασφάλειας όπως είναι το 4G δίκτυο, η τεχνολογία cloud αλλά και τα λειτουργικά συστήματα, υστερούν όμως των αποδείξεων. Στην πράξη η εφαρμογή του project εκτιμάται να μην είναι σε μεγάλο βαθμό πιθανή καθώς προϋποθέτει επιπλέον εξοπλισμό για τον οποίο θα πρέπει να επενδύσουν οι συμμετέχοντες, άρα επιπρόσθετο κόστος για αυτούς, ενώ και οι ανταγωνιστικές σχέσεις μεταξύ των συμμετεχόντων καθιστούν ακόμη πιο δύσκολη την μεταξύ τους συνεργασία. Επομένως το project

ASMONIA αποτελεί μία πολύ καλή προσπάθεια στην θεωρία, η εφαρμογή του όμως φαντάζει απίθανη.

Παράρτημα Α

Authentication procedures: A3 Authentication and A8 Key Generator

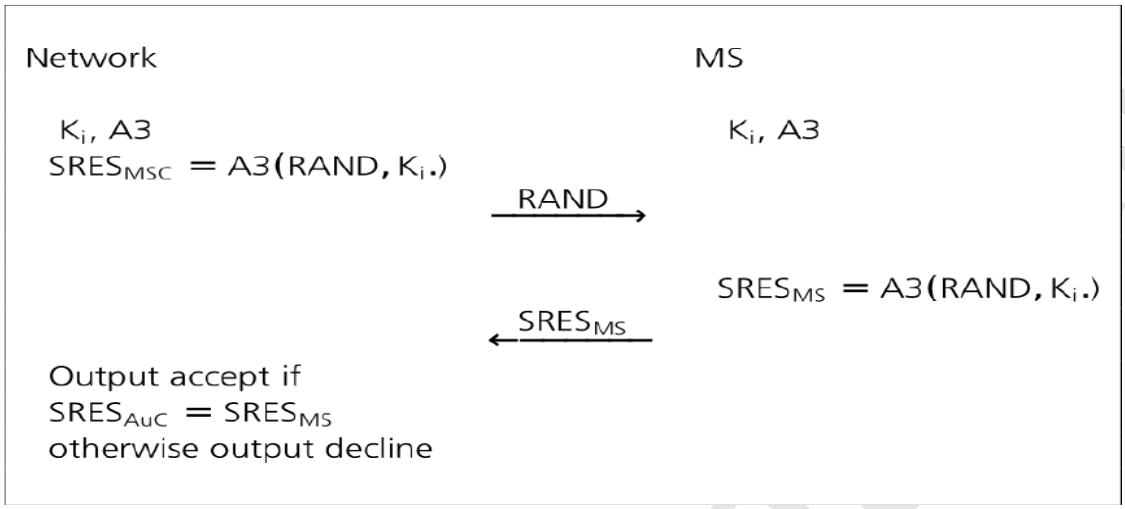
When a MS requests access to the network, the MSC/VLR will normally require the MS to authenticate. The MSC will forward the IMSI to the HLR and request authentication *Triplets*.

The network can have the MS authenticate whenever it wants and this can vary from network to network. The network can require the MS to authenticate every time an event is initiated (location update, mobile-originated call, mobile-terminated call, etc.), every so many events, or even after a certain time period has elapsed. The network will almost always require authentication whenever the MS moves into a new Location Area and does a Location Update.

When the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and belongs to the network. Once it has accomplished this, it will forward the IMSI and authentication request to the *Authentication Center* (AuC).

The AuC will use the IMSI to look up the Ki associated with that IMSI. The Ki is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. **The Ki is only stored on the SIM card and at the AuC.** The Auc will also generate a 128-bit random number called the RAND.

The RAND and the Ki are inputted into the A3 encryption algorithm. The output is the 32-bit *Signed Response* (SRES). The SRES is essentially the "challenge" sent to the MS when authentication is requested.



Σχήμα 23 A3 Authentication Procedure

The RAND and Ki are input into the A8 encryption algorithm. The output is the 64-bit Kc. The Kc is the ciphering key that is used in the A5 encryption algorithm to encipher and decipher the data that is being transmitted on the Um interface.

The RAND, SRES, and Kc are collectively known as the *Triplets*. The AuC may generate many sets of Triplets and send them to the requesting MSC/VLR. This is in order to reduce the signaling overhead that would result if the MSC/VLR requested one set of triplets every time it wanted to authenticate the MS. It should be noted that a set of triplets is unique to one IMSI and it cannot be used with any other IMSI.

Once the AuC has generated the triplets (or sets of triplets), it forwards them to the HLR. The HLR subsequently sends them to the requesting MSC/VLR.

The MSC stores the Kc and the SRES but forwards the RAND to the MS and orders it to authenticate.

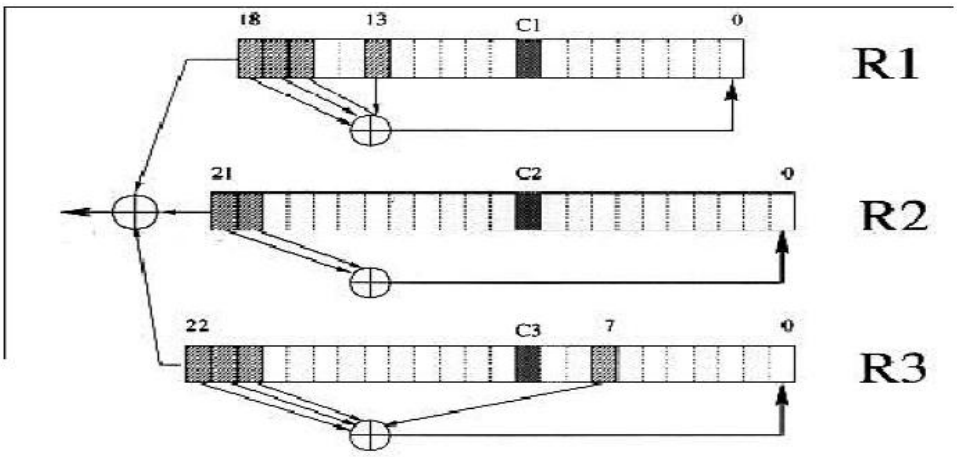
The MS has the Ki stored on the SIM card. The A3 and A8 algorithms also reside on the SIM card. The RAND and Ki are inputted into the A3 and A8 encryption algorithms to generate the SRES and the Kc respectively.

A5/1 encryption algorithm

A5/1 is built from three short linear feedback shift registers (LFSR) of lengths 19, 22, and 23 bits, which are denoted by *R*1; *R*2 and *R*3 respectively. The rightmost bit in each register is labeled as bit zero. The taps of *R*1 are at bit positions 13, 16, 17, 18; the taps

of *R*2 are at bit positions 20,21; and the taps of *R*3 are at bit positions 7, 20,21,22 (see Figure x).

When a register is clocked, its taps are XORed together, and the result is stored in the rightmost bit of the left-shifted register. The three registers are maximal length LFSR's with periods 2^{19} -1, 2^{22} - 1, and 2^{23} -1, respectively. They are clocked in a stop/go fashion using the following majority rule: Each register has a single "clocking" tap (bit 8 for *R*1, bit 10 for *R*2, and bit 10 for for *R*3); each clock cycle, the majority function of the clocking taps is calculated and only those registers whose clocking taps agree with the majority bit are actually clocked. Note that at each step either two or three registers are clocked, and that each register moves with probability 3/4 and stops with probability 1/4.



Σχήμα 24 A5/1 Encryption Algorithm

The process of generating pseudo random bits from the session key *K* and the frame counter F_n is carried out in four steps:

- The three registers are zeroed, and then clocked for 64 cycles (ignoring the stop/go clock control). During this period each bit of *K* (from lsb to msb) is XOR'ed in parallel into the lsb's of the three registers.
- The three registers are clocked for 22 additional cycles (ignoring the stop/go clock control). During this period the successive bits of F_n (from lsb to msb) are again XOR'ed in parallel into the lsb's of the three registers. The content of the three registers at the end of this step is called the initial state of the frame.
- The three registers are clocked for 100 additional clock cycles with the stop/go clock control but without producing any outputs.
- The three registers are clocked for 228 additional clock cycles with the stop/go clock control in order to produce the 228 output bits. At each clock cycle, one output bit is produced as the XOR of the msb's of the three registers.

A5/2 encryption algorithm

A5/2 consists of four maximal-length LFSRs: R1, R2, R3, and R4. These registers are of length 19-bit, 22-bit, 23-bit, and 17-bit respectively. Each register has taps and a feedback function. Their irreducible polynomials are: x^{19} xor x^5 xor x^2 xor x xor 1, x^{22} xor x xor 1, x^{23} xor x^{15} xor x^2 xor x xor 1, and x^{17} xor x^5 xor 1, respectively.

At each step of A5/2 R1, R2 and R3 are clocked according to a clocking mechanism. Then R4 is clocked. After the clocking is performed, one output bit is ready at the output of A5/2. The output bit is a non-linear function of the internal state of R1, R2, and R3.

After the initialization 99 bits of output are discarded, and the following 228 bits of output are used as the output key-stream.

Denote session key Kc and Kc[i] the i'th bit of the 64-bit session key, and the i'th bit of register j by Rj[i]. The initialization of the internal state with Kc and the frame number is done in the following way:

```
set all LFSRs to 0

for i:=0 to 63 do

1. clock all 4 LSFRs

2. R1[0]←R1[0]xorKc[i]

3. R2[0]←R2[0]xorKc[i]

4. R3[0]←R3[0]xorKc[i]

5. R4[0]←R4[0]xorKc[i]

for i:=0 to 21 do

1. clock all 4 LSFRs

2. R1[0]←R1[0] xor f[i]

3. R2[0]←R2[0] xor f[i]

4. R3[0]←R3[0] xor f[i]

5. R4[0]←R4[0] xor f[i]
```

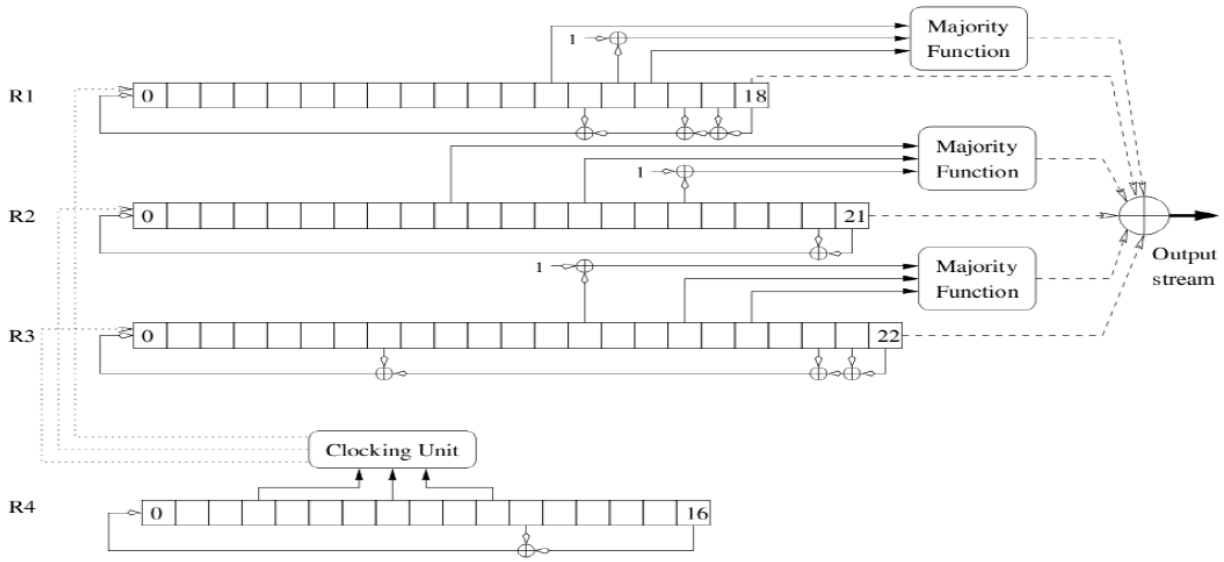
The key-stream generation is as follows:

1. initialize the internal state with Kc

2. force the bits R1[15], R2[16], R3[18] and R4[10] to be 1.

3. run A5/2 mfor 99 clocks and ignore the output

4. run A5/2 for 228 clocks and use the output as key-stream.



Σχήμα 25 A5/2 Internal Structure

The internal structure of A5/2 is shown in the figure above. The clocking mechanism works as follows: R4 controls the clocking of R1, R2, and R3. When clocking of R1, R2, and R3 is to be performed, bits R4[3], R4[7], and R4[10] are the input of the clocking unit. The clocking unit performs a majority function on the bits.

Once the clocking is performed, an output is bit is ready. The output bit is computed as follows: in each register the majority of two bits and the complement of a third bit is computed; the results of all the majorities and the rightmost bit from each register are XORed to form the output.

A5/2 is built on a similar framework with A5/1. The feedback functions of R1, R2 and R3 are the same as A5/1's feedback functions. The initialization process of A5/2 is also similar to that of A5/1. The difference is that A5/2 also initializes R4, and that one bit in each register is set to 1 after initialization. Also, A5/2 discards 99 bits whereas A5/1

discards 100 bits of output. Clocking mechanism is the same but the input bits are from R4 in case of A5/2, while in A5/1 they are from R1, R2, and R3.

The algorithm output is 228 bits of key-stream. The first block of 114 bits is used as a key-stream to encrypt the link from the network to the customer, and the second block of 114 bits is used to encrypt the link from the customer to the network. A5 is used to encrypt frames. The frames are sequentially numbered by a TDMA frame number.

Παράρτημα Β

Οι παρακάτω πίνακες απεικονίζουν το εκτιμώμενο ρίσκο για τα Charging Systems, PCRF, Security Gateway και τις υπηρεσίες Location services και Short Message Services. Ακολουθούν οι πίνακες για τους OAM Servers και τους Web Proxies. Τέλος από το δίκτυο υποδομής παρουσιάζονται οι πίνακες για τα backbone routers και DNS Servers.

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	2	4	8
T2	1	2	4	8
T3	1	3	4	12
T4	1	1	4	4
T5	1	3	5	15
T6	1	2	5	10
T7	1	2	5	10
T8	2	2 – 3	5	20 – 30
T9	1 – 2	2 – 4	5	10 – 40
T10	2	2	5	20

Πίνακας 19 Εκτίμηση ρίσκου για Charging Systems

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	3	4	12
T2	1	3	4	12
T3	1	3	4	12
T4	1	2	4	8
T5	1	3	5	15
T6	1	2	5	10
T7	1	3	5	15
T8	2	2 – 4	5	20 – 40
T9	1 – 2	2 – 4	5	10 – 40
T10	2	2	5	20

Πίνακας 20 Εκτίμηση ρίσκου για PCRF

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	4	2	4	32
T2	3	2	4	24
T3.1	2	1	3	6
T3.2	2	2	1 – 3	4 – 12
T4	2	1	3	6
T5.1	1	1	4	4
T5.2	1	2	1 – 3	2 – 6
T6	1	1	5	5
T7	3	2	5	30

T8	3	2 – 4	5	30 – 60
T9	1 – 2	2 – 4	5	10 – 40
T10	1	1	5	5

Πίνακας 21 Εκτίμηση ρίσκου για Security Gateway

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	4	3	24
T2	2	3	3	18
T3	3	2	3	18
T4	3	2	3	18
T5	1	1	3	3
T6	2	3	4	24
T7	2	3	4	24
T8	2	3	4	24
T9	1 – 2	2 – 4	4	8 – 32
T10	2	1	5	10

Πίνακας 22 Εκτίμηση ρίσκου για Location Services

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	3	4	3	36
T2	2	3	4	24
T3	3	2	1 – 3	6 – 18
T4	3	2	1 – 3	6 – 18
T5	1	2	1 – 3	2 – 6
T6	1	2	1 – 3	2 – 6
T7	3	3	5	45
T8	3	3	5	45
T9	1 – 2	2 – 4	5	10 – 40
T10	3	3	5	45

Πίνακας 23 Εκτίμηση ρίσκου για Short Message Services

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	1	2	4	8
T2	1	2	4	8
T3	3	2	3	18
T4	3	2	3	18
T5	1	2	5	10
T6	2	2	5	20
T7	3	2	5	30
T8	3	2 – 3	5	30 – 45
T9	1 – 2	2 – 4	5	10 – 40
T10	2	2	5	20

Πίνακας 24 Εκτίμηση ρίσκου για OAM Servers

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	2	2	2	8
T2	2	2	2	12
T3	2	2	2	8
T4	1	3	1	3
T5	3	3	4	36
T6	3	3	4	36
T7	3	3	4	36
T8	3	2	4	24
T9	1	4	4	16
T10	1	1	2	2

Πίνακας 25 Εκτίμηση ρίσκου για Web Proxies

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	4	2	3	24
T2	3	2	4	24
T3.1	2	4	4	32
T3.2	2	4	1 – 3	8 – 24
T4	3	2	2	12
T5.1	1	3	5	15
T5.2	1	3	1 – 3	3 – 9
T6	1	2	4	8
T7	3	2	5	30
T8	4	2	5	40
T9	1	4	5	20
T10	1	2	5	10

Πίνακας 26 Εκτίμηση ρίσκου για Backbone Routers

Threats	Likelihood	Vul. Factor	Impact	Risk
T1	3	2	3	18
T2	2	2	4	16
T3	1	5	2	10
T4	4	2	3	24
T5	2	3	4	24
T6	1	2	4	8
T7	2	2	5	20
T8	4	2	5	40
T9	1	4	5	20
T10	1	2	5	10

Πίνακας 27 Εκτίμηση ρίσκου για DNS Servers

Παράρτημα Γ

Στον πίνακα που ακολουθεί παρατίθενται οι απαιτήσεις συστήματος όπως παρουσιάζονται στο [1].

No	Title	Details
FReq. 1	Continuously monitoring	The system should be capable of continuously monitoring a 4G mobile network by means of deployed sensors
FReq. 2	Making measurements available	The system should be capable of making measurements available that allow concluding about the security characteristics (confidentiality, integrity, availability) and the imposed security risk for service invocations
FReq. 3	Inferring the security characteristics	The system should be capable of inferring the security characteristics (confidentiality, integrity, availability) for service based on measurements made with respect to a security model that allows concluding about the security
FReq. 4	Enhancing the security model	The system should be capable of enhancing the security model (e.g. by supervised learning) to improve precision, recall and accuracy of inferring the security characteristics. In the context of behavioral classification with respect to security characteristics, the terms true positives, true negatives, false positives and false negatives are used to compare the given classification of a service invocation with the desired correct classification. • Precision = tp/(tp+fp) • Recall = tp/(tp+fn) • Accuracy = (tp+tn)/(tp+tn+fp+fn)
FReq. 5	Identifying the economical impact	The system should be capable of identifying the economical impact of detected behavioral deviations in service invocations with respect to inferred security characteristics.
FReq. 6	Providing an interactive presentation	The system should be capable of providing an interactive presentation of the current and past security status for decision support allowing exploring root causes and predictive analytics and on-line analytical processing. [On-line analytical processing is an approach to swiftly answer analytical queries.]

FReq. 7	Ensuring true collaboration for increasing social welfare	The system should implement a mechanism design ensuring true collaboration for increasing social welfare in terms of ensured adequate security characteristics. • The mechanism design should perform a true and incentive compatible security risk assignment • The mechanism design should be capable to discover “conflicts resolution” between agents having different security needs or divergent intentions
FReq. 8	Effective collaboration	The system should be capable of enabling effective collaboration by exchanging models, measurements, inference and realized security risks
NFReq. 1	Flexibility	Flexibility, as the ability to adapt quickly to new security challenges and the ability to invoke innovative and standardized methods, technologies and resources.
NFReq. 2	Security	Security, as the ability to provide available, integer, and confidential services.
NFReq. 3	Extendibility	Extendibility, as the ability to easy and flexible integrates with evolving mobile network infra structures and the ability to integrate new measurements.
NFReq. 4	Maintainability	Maintainability, as the ability to easy and flexible change measurements and related components and the ability to integrate these measurements smoothly.
NFReq. 5	Interoperability	Interoperability, as the ability to share information and operate according to an agreed operational semantics.
NFReq. 6	Scalability	Scalability, (e.g., in the dimensions of service invocations, measurements and equipment) as the ability to store and process the emerging data volume.
NFReq. 7	Performance	Performance, as the ability to derive results timely.
NFReq. 8	Usability	Usability, as the quality of a user's experience in interacting with information or services.
FUNC.01	External interface for data communication	To enable the information exchange between participants of the ASMONIA collaboration network an external interface for bilateral communication is required at each site
FUNC.02	Generic internal interface between FCs (NFM)	Sensor data is collected from various sensors in different FCs. A common format for data exchange is needed
FUNC.03	Local database with Security	Information on security incidents received

	incident and reputation (RMM) information	from other participants of the collaboration network should be stored in a local knowledge base for efficient access
FUNC.04	External existing EWS needs an ACGW for communication with ACN	To enable the communication between the ACN and an existing EWS a generic interface is needed. This is provided by the ASMONIA ACGW and a TM, which has to be included in the EWS
FUNC.05	ASMONIA policy for data exchange	Each ASMONIA collaboration partner must fulfill the ASMONIA policy for data exchange
SEC.01	Protect external interface of ACGW	The location of the system offering this external interface depends on the existing network layout of participant. If a perimeter network approach is used, the node offering the external interface should be placed in the DMZ
SEC.02	Mechanism for anonymization and privacy preservation	A mechanism for anonymization and privacy preservation of the data is required when using the external interface for data communication between operators
SEC.03	Closed user group for CAN communication	To prevent falsified messages in the CAN a closed user group of CAN participants is needed. One possibility is to realize this via a VPN and certificates for each participant
SEC.04	Detection of disconnection from ACGW and ACN	To prevent attacks that try to disconnect ASMONIA components a mechanism is required that detects when essential ASMONIA components are disconnected from ACGW or ACN. Valid maintenance messages must be protected to prevent spoofing
SEC.05	Connection between ACGWs must be distributed and decentralized	To make it harder for an adversary to successfully carry out attacks on the connections between ACGWs we propose the usage of distributed and totally decentralized structures, namely Peer-to-Peer (P2P) overlay networks
SEC.06	Hardening of all ASMONIA components	To reduce the attack surface on host level we propose to harden ASMONIA components by techniques such as port knocking, CPP, IDS/IPS etc.
SEC.07	ACGW split into two physical nodes	To reduce the risk for the participant's network if an ACGW is successfully compromised, it may be split into two physical nodes which form one logical component: one node is responsible for offering an external interface to the other participants the other node may be separated from external node and integrate all modules which must not be compromised,

		to protect the participants internal data and infrastructure.
SEC.08	Mechanism for data encryption	To avoid wiretappers from getting details about an operator's network infrastructure or further details by eavesdropping the data, all data exchange between the ACGWs shall be encrypted. This is based on asymmetric cryptography for authentication and key management, which requires certificates and PKI infrastructure

Πίνακας 28 Απαιτήσεις συστήματος

Βιβλιογραφία

[1] M. Hoche, H. Hofinger, H. Kirsch and S. Kraemer, "Reference Architecture for Collaboration in Mobile Netwoeks," 2011.

[2] M. Schafer, S. Wessel, A. Egners and M. Hoche, "Evaluating Methods to assure System Integrity and Requirements For Future Protection Concepts," 2011.

[3] M. Gall, B. Jager, H. Kirsch and J. Luken, "Analysis of Requirements for the Deployment of Cloud Systems," 2011.

[4] M. Haustein, M. Hoche, P. Kirner and H. Kirsch, "Development of a Monitoring System for Security Risk Reduction," 2011.

[5] H. Hofinger, H. Kirsch, S. Kraemer and M. Montag, "Collaborative Procedures for Mobile Network Infrastructure Architectures," 2012.

[6] M. Schafer, S. Wessel, S. Wagner and A. Egners, "Protection Methods for Target Systems," 2012.

[7] M. Gall, B. Jager, R. Koch and M. Luft, "Architecture Concept for the Use of Cloud Systems," 2012.

[8] A. Egners, E. Rey, H. Schmidt and P. Schneider, "Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals," 2012.

[9] "3GPP," 3GPP Organization, [Online]. Available: www.3gpp.com.

[10] D. Forsberg, G. Horn, W. D. Moeller and V. Niemi, LTE Security, John Willey & Sons, 2010.

[11] I. Goldberg and M. Briceno, "GSM Clonning - Over the Air," 1998.

[12] I. Goldberh, D. Wagner and L. Green, "The (Real Time) Cryptanalysis of A5/2," in *Crypto'99*, 1999.

[13] C. Nohl, "Attacking Phone Privacy," in *Blackhat*, 2010.

[14] A. Biryukov, A. Shamir and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," *Lecture Notes in Computer Science,* pp. 37-44, 2003.

[15] "33.102 3G Security; Security Architecture," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/33102.htm.

[16] C. Xenakis and L. Merakos, "Security in third Generation Mobile Networks," *Computer Communications,* pp. 638-650, 2004.

[17] "3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/35202.htm.

[18] "3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/33908.htm.

[19] "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/35216.htm.

[20] C. Xenakis and L. Merakos, "Vulnerabilities and Possible Attacks Against the GPRS Backbone Network," *Lecture Notes in Computer Science,* pp. 262-272, 2006.

[21] "Security of Home Node B (HNB) / Home evolved Node B (HeNB)," [Online]. Available: www.3gpp.org/ftp/specs/html-info/33320.htm.

[22] "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/36300.htm.

[23] "Direct tunnel deployment guideline," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/23919.htm.

[24] "IP Multimedia Subsystem (IMS); Stage 2," [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/23228.htm.

[25] "3GPP System Architecture Evolution (SAE); Security architecture," [Online]. Available: www.3gpp.org/ftp/Specs/html-info/33401.htm.

[26] "The Hacker’s Choice," [Online]. Available: www.thc.org.

[27] "Google Code Project," [Online]. Available: http://code.google.com/p/samsung-femtocell.

[28] "T-Labs TU Berlin Project," [Online]. Available: http://femto.sec.tlabs.tu-berlin.de/bh2011.pdf.

[29] "GNU's Framework for Secure Peer-to-Peer Networking," [Online]. Available: https://gnunet.org/.

[30] M. Burkhart, M. Strasser, D. Many and X. A. Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," in *USENIX Security Symposium*, 2010.

[31] M. Burkhart, "Enabling Collaborative Network Security with Privacy-Preserving Data Aggregation," 2011. [Online]. Available: http://sepia.ee.ethz.ch/publications/dissertation-burkhart.pdf.

[32] C. Orlandi, "Is Multiparty Computation Any Good In Practice?," in *ICASSP*, 2011.