УДК 621.382

ОЦІНКА БЕЗПЕКИ ТА АНАЛІЗ ВРАЗЛИВОСТІ IP MULTIMEDIA SUBSYSTEM (IMS)

Полуденний О. М., Цуканов О. Ф.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: alexpoludenniy@gmail.com

IP MULTIMEDIA SUBSYSTEM (IMS) SECURITY ASSESSMENT. VULNERABILITY ANALYSIS OF IMS.

NGN introduces the concept of fix-mobile convergence (FMC). NGN provides the IP multimedia subsystem (IMS) as platform to converge the wire and wireless networks. It is open and distributed architecture that can enable easy access to services, information and resources. But the same time there is lot of risks in such approach. Potential hackers can access IMS architecture to lunch some attacks on IMS network. IMS security is vital important and it is beneficial to be aware of possible vulnerabilities. This paper investigates current situation in IMS security regulations, potential threats and attacks facing to IMS deployment. We also provide vulnerability discovering and analysis method with Open Source IMS Core.

Оцінка безпеки IMS проводиться на основі двох підходів:

1. eTVRA.
2. Архітектура безпеки ITU-T. 805.

Подібності в архітектурній структурі можуть бути знайдені між IMS і ITU-T X. 805, який є рекомендаціями MCE-T для наскрізних комунікацій. У цих рекомендаціях серії X. 800 загрози визначаються, як знищення інформації і ресурсів, пошкодження або зміну інформації, крадіжка або видалення даних, розкриття інформації та переривання роботи служб. Вони були запропоновані в якості основи для архітектури NGN для досягнення наскрізної безпеки в розподілених додатках (Atay and Masera, 2011). X. 805 складається з 3 архітектурних частин: розміри безпеки, рівні безпеки і площини безпеки, як показано на рис. 1.

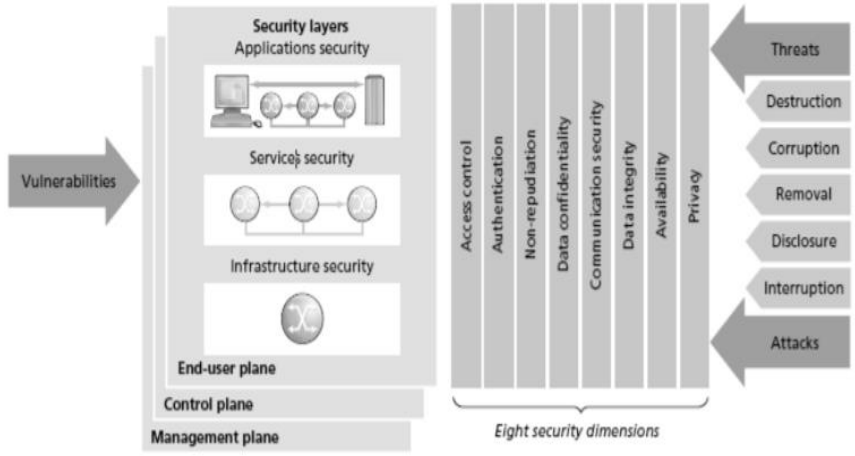

Рис. 1. ITU-T X. 805.

Рівні безпеки також складаються з 3 – х рівнів, рівень інфраструктури, рівень безпеки сервісу, рівень безпеки сервісу. Площина безпеки показує дії, які відбуваються на площині безпеки мережевого управління, площині безпеки управління і площині безпеки кінцевого користувача.

Безпека вимірювання - це методи забезпечення безпеки, спрямовані на захист: контроль доступу, аутентифікацію, відмова від анулювання, конфіденційність даних, безпека потоку зв'язку, цілісність даних, доступність та конфіденційність. Кожен рівень пов'язаний з унікальними вразливостями, погрозами та заходами щодо їх усунення.

Одним із стандартів оцінки безпеки є стандарт ISO 15408: 2009 загальні критерії оцінки безпеки інформаційних технологій, але цей стандарт є дорогим по часу і ресурсам. З цієї причини програма конвергенції телекомунікаційних послуг та протоколів для передових мереж (TISPAN) в Європейському інституті стандартів телекомунікацій (ETSI), найбільшої європейської організації по стандартизації телекомунікацій (Telco) з світовим впливом, розробила метод аналізу загроз, вразливостей і ризиків (eTVRA) для підтримки телекомунікаційних компаній у загальній оцінці критеріїв безпеки.

Оцінка уразливості в eTVRA складається з 7 етапів, показаних на рис.2. (Morali et al., 2009). Процес починається з визначення цілей безпеки системи або системного компонента, з яких вилучаються вимоги безпеки.

Надалі складається опис активів в системі. Мета використання eTVRA полягає в тому, щоб мати можливість ідентифікувати проблеми, які існують в системі. Тому після ідентифікації активів, визначаються проблеми, загрози, які використовують ці уразливості і викликають інциденти. Вимоги безпеки і загрози розширюються у відповідності з погрозами і вразливостями. Потім проводиться аналіз і кількісна оцінка ймовірності виникнення загроз і їх впливу. Це використовується в наступному кроці для розрахунку ризику. Отже, визначені контрзаходи для обробки ризику. Цей процес застосовується ітеративно, до тих пір, поки ризик небажаних інцидентів не буде знижено до прийнятного рівня, або всякий раз, коли відбуваються зміни в навколишньому середовищі (Rosseb et al., 2006).

В ході дослідження використаємо X. 805 модульні перспективи безпеки, які показані на РИС. 3. (Anon, 2011.) для аналізу основних вразливостей IMS, який показано з допомогою eTVRA.

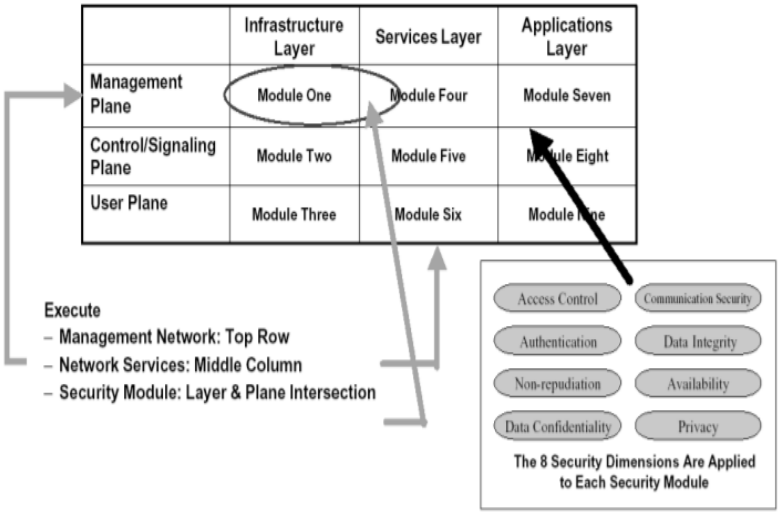

Рис. 3. Модульні перспективи безпеки з X. 805.

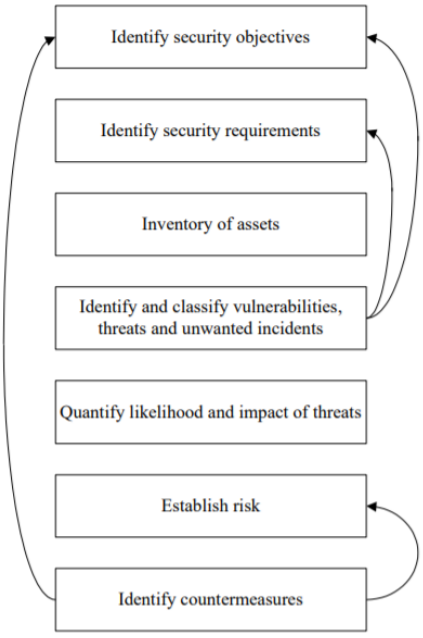

Рис. 2. Основні етапи роботи eTVRA.

Існує 9 точок зору або модулів безпеки, де необхідно ідентифікувати програмні та апаратні засоби. В кожній точці зору, в якості третього фактору в аналізі уразливості повинен бути включений людський фактор, який означає, що повинні бути оцінені всі види діяльності, а також таке рішення повинно забезпечувати не тільки аналіз вразливостей, але і кращу реалізацію та поліпшення безпеки, оскільки така модель дозволяє оновлювати безпеку при виявленні вразливостей.

Стандарти та протоколи постійно змінюються. IMS є досить новою архітектурою в мережах і знаходиться в процесі дослідження, вона буде змінюватись, виправлятись, розвиватись, і будуть інтегруватися нові функції. Це означає, що аналіз вразливостей

повинен постійно оновлюватися і контролюватися з кожною зміною в системі.

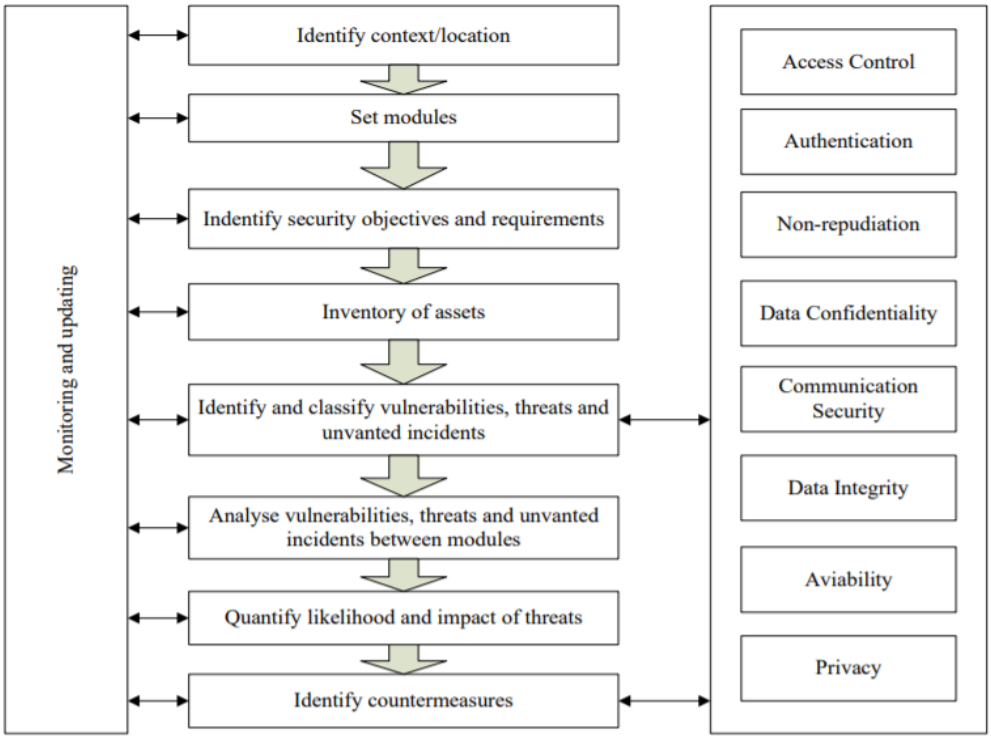

Рис.4. Розширена модель тестування вразливостей IMS.

Процес дослідження показав, що не всі аспекти безпеки можуть бути адресовані кожному модулю, але в будь-якому випадку вони повинні бути проаналізовані в контексті інфраструктури та основних елементів. Будь-який об'єкт з певною функціональною цінністю в цій архітектурі може бути проаналізований як основний елемент, який повинен бути згрупований у відповідності з його конкретним рівнем безпеки і площиною, що показано в таблиці 1. Аналіз вразливості IMS був проведений згідно з категоризацією основних елементів.

Таблиця 1. Основні елементи концепції IMS.

IMS assets by modules

	Infrastructure Layer	**Service Layer**	**Application Layer**
Management plane	CTF, CDF, CGF, PDF	Diameter (Rf, Rx, Ro) COPS (Go)	HTTP (Ut)
Control plane	CSCF, MGCF, MRFC, BGCF, IBCF, SLF, AS, DNS, ENUM	SIP/SDP(Gm, Mw, Mg, Mi, Mj,Mk, Mr), Diameter(Ch, Dx), H248 (Mp, Mn)	SIP(ISC), Diameter(Sh, Dh)
End-user plane	IM-MGW, MRFP, HSS, UE	RTP/RTCP(Mb), User profile	Voice, IM, VIDeo, State(XCAP)

Аналіз вразливостей IMS показав, що IMS може піддаватися різним типам атак. Тестування уразливості проводилося на відкритому тестовому стенді IMS. Це ядро вихідного коду проекту є відкритою частиною платформи IMS і використовується для налаштування тест-стенду для практичного моделювання сценарію. В таблиці 2 наведено результати поточного дослідження різних вразливостей системи безпеки.

Більшість заходів безпеки виявляються стандартними механізмами, такими як IPSec і TLS або аутентифікація і авторизація. Але такі атаки, як SQL-запити, не можуть бути захищені і вимагають додаткового інструменту реалізації найбільш ефективного захисту, метод захисту повинен мати інструмент виявлення і запобігання вторгнень. Це допомогло б покращити захист від загроз пов'язаних з людським фактором.

Висновки. Отже, розглянуто реалізацію моделі eTVRA в аналізі вразливостей IMS, яка доповнюється рекомендаціями ITU-T X. 805 безпеки. Пропонується метод для повного покриття тестування вразливостей. У роботі були показані основні загрози і майбутня

кількісна оцінка вразливостей та її аналіз. Також, як перспективна технологія для захисту може бути впровадження системи виявлення та запобігання вторгнень. Дослідження показують, що найбільша вразливість пов'язана з рівнем додатків і площиною управління, що означає, що цим частинам потрібно приділяти додаткову увагу для захисту.

Таблиця 1. Результати поточного дослідження різних вразливостей системи безпеки.

IMS vulnerability list

Vulnerability	Weakness	Security dimension	Asset module	Impact
Message spoofing	IMS has absence of IPsec protection between user equipment and P-CSCF	Authentication	Service layer Control plane	Fraud of trust
SIP SQL injection	SIP authentication controllability is unsecure	Availability	Service layer User plane	Deniel of service
Media theft	Not enough control on media streems	Non-repudiation	Infrastructure layer Management plane	Theft of sercices
SIP flooding	Unable effectively prevent REGISTER and INVITE message flooding	Availability	Infrastructure layer Control plane	Loss of QoS for users
RTP data sniffing	No default confidentiality from data streem	Confidentiality	Application layer User plane	Theft of information
CANCEL attack	Possibility to fake SIP CANCEL request	Integrity	Service layer Control plane	Session disruption
RTP injection	RTP protocol missing media integrity protection mechanisms	Integrity	Service layer User plane	Session disruption
Man in the Middle P-CSCF attack	Authentication using SIP must be improved	Authentication	Service Layer Control plane	Impersonation of a server
Dictionary attack	Inadequate identity protection and AKA chipper algorithm use	Authentication	Application layer Control plane	Identity theft
BYE attack	Possibility to fake SIP BYE request/ not enough confidentiality protection	Integrity	Service layer Control plane	Disruption of session
DNS Cache Poisoning	Not enough connection integrity protection	Integrity	Infrastructure plane Control plane	Loss of service
Network topology disclosure	Not protected SIP messages	Confidentiality	Infrastructure layer Control plane	Leak of network topology
HTTP Parse Attack	Improperly data ContentLenght regulation	Availability	Infrastructure layer Control plane	Loss of services
User equipment configuration tampering	Probability lack of user education in security questions	Availability	Infrastructure layer Control plane	Denial of services

Література

1. IP Multimedia Subsystem - IP Multimedia Subsystem [Електронний ресурс] – Режим доступу до ресурсу: https://ru.qwe.wiki/wiki/IP_Multimedia_Subsystem#Charging.
2. IP Multimedia Subsystem (IMS) Handbook / Ahson S.A., Ilyas M.., 2009. – 562 с.
3. Developing SIP and IP Multimedia Subsystem (IMS) Applications.. – 690 с.
4. F. Galán. Design and Implementation of an IP Multimedia Subsystem (IMS) Emulator Using Virtualization Techniques : дис. канд. техн. наук / F. Galán.. – 12 с.