## 15 -MA’RUZA

## MAVZU: NGN TARMOQLARIDA AXBOROT XAVFSIZLIGI.

REJA

15.1 NGN tarmoqlarida axborot xavfsizligi arxitekturasi;

15.2. NGN uchun xavfsizlik mexanizmlari.

***Kalit so'zlar:*** *NGN, PSTN, Xavfsizlik*

### 15.1 NGN tarmoqlarida axborot xavfsizligi arxitekturasi.

Ushbu ma’ruzada yangi avlod tarmoqlarining (NGN) to'g'ri ishlashi uchun xavfsizlik choralarini ta'minlash va foydalanuvchilarning telekommunikatsiya xizmatlaridan to'g'ri foydalanishini himoya qilish bo'yicha amaliy ko'rsatmalar beradi. Buni NGN (ob'ektga asoslangan operatorlar) boshqaradigan yoki boshqalar tomonidan taqdim etilgan (NGN) dan foydalangan holda xizmatlar ko'rsatadigan (xizmatga asoslangan operatorlar) barcha operatorlar kuzatishi kerak. Xavfsizlik choralariga qo'shimcha ravishda, operatorlar xavfsizlik buzilishi to'g'risida xabar berish uchun ushbu hujjatda belgilangan ishga tushirish mezonlari va hisobot berish tartib-qoidalariga rioya qilishlari kerak. Shuningdek, ushbu ma’ruzada biz mavjud tizimda topilgan turli xil xavfsizlik zaifliklari haqida qayg'uramiz va ularni bartaraf etishning mumkin bo'lgan yechimlarini beramiz.

Operatorlar o'z tarmog'ini qurishda va xizmatlarini ko'rsatishda quyidagi xavfsizlik maqsadlarini, ya'ni maxfiylik, yaxlitlik va mavjudlikni hisobga olishlari kerak:

- Maxfiylik tarmoq va foydalanuvchi ma'lumotlarini ruxsatsiz kirish, ko'rish, yo'naltirish yoki ushlab qolishdan himoya qilishni anglatadi.

- yaxlitlik tarmoq va foydalanuvchi ma'lumotlarini ruxsatsiz o'zgartirish, o'chirish, yaratish va takrorlashdan himoya qilishni anglatadi.

- Mavjudlik, agar mavjud bo'lsa, xakerlar tomonidan xavfsizlik hujumlari tufayli to'xtab qolish vaqtini minimallashtirish uchun tarmoq va xizmatlarni taqdim etishni nazarda tutadi.

Ushbu maqsadlar tarmoq xavfsizligi imkoniyatlarini loyihalash, ishlab chiqish va amalga oshirishda yanada izchil va tizimli yondashuvni yaratish uchun asos yaratadi.

### 15.2 NGN xavfsizlik mexanizmlari

NGN xavfsizlik talablarini qondirish uchun maxsus xavfsizlik mexanizmlari ITU-T Y.secMechanisms (NGN Security Mechanisms) Tavsiya loyihasida yoritilgan. Misol uchun, Tavsiyada foydalanuvchilar va obunachilarni autentifikatsiya qilishning bir nechta sxemalari, jumladan ITU-T tomonidan tavsiya etilgan X.509 sertifikatlari, umumiy kalitlar va tarmoq manzillari asosidagi sxemalar ko'rib chiqiladi.

Signalizatsiya va boshqaruv tizimlarining xavfsizligi transport qatlami xavfsizligi (TLS - transport layer security) va Internet protokoli (IPsec) uchun xavfsizlik arxitekturasi asosida shifrlash orqali ta'minlanadigan holatlar o'rganilmoqda. Media xavfsizligi uchun vosita real vaqt rejimida xavfsiz transport protokoli (SRTP - secure real-time transport protocol) bilan shifrlangan bir nechta sxemalar ko'rib chiqilmoqda. Audit izlari va jurnal fayllarini saqlash bilan bog'liq holda, turli xil masalalar, ju mladan, boshqaruv tizimiga kirish yozuvlarini saqlash, jurnal serveridan foydalanish, boshqarish va boshqa masalalar ko'rib chiqilmoqda.

#### NGN autentifikatsiyasi va avtorizatsiya talablari

NGNda autentifikatsiya va avtorizatsiya talab qilinadigan turli xil vaziyatlar mavjud, masalan, transport va xizmat ko'rsatish qatlamlari ajratilgan holatlar va xizmatlar uchinchi shaxslar tomonidan taklif qilingan holatlar. ITU-T tavsiyasi loyihasi Y.NGN Authentication (NGN autentifikatsiya va avtorizatsiya) 15.1-rasmda keltirilgan autentifikatsiya va avtorizatsiya modeli asosida quyidagi autentifikatsiya namunalari va ularning talablarini belgilaydi.

(1) Tarmoqqa kirish uchun foydalanuvchining autentifikatsiyasi va avtorizatsiyasi

(2) Xizmat ko'rsatuvchi provayderning autentifikatsiyasi va xizmatga/ilovaga kirish uchun foydalanuvchining avtorizatsiyasi

(3) Xizmat ko'rsatuvchi provayderning autentifikatsiyasi va foydalanuvchining muayyan xizmatga/ilovaga kirish uchun avtorizatsiyasi

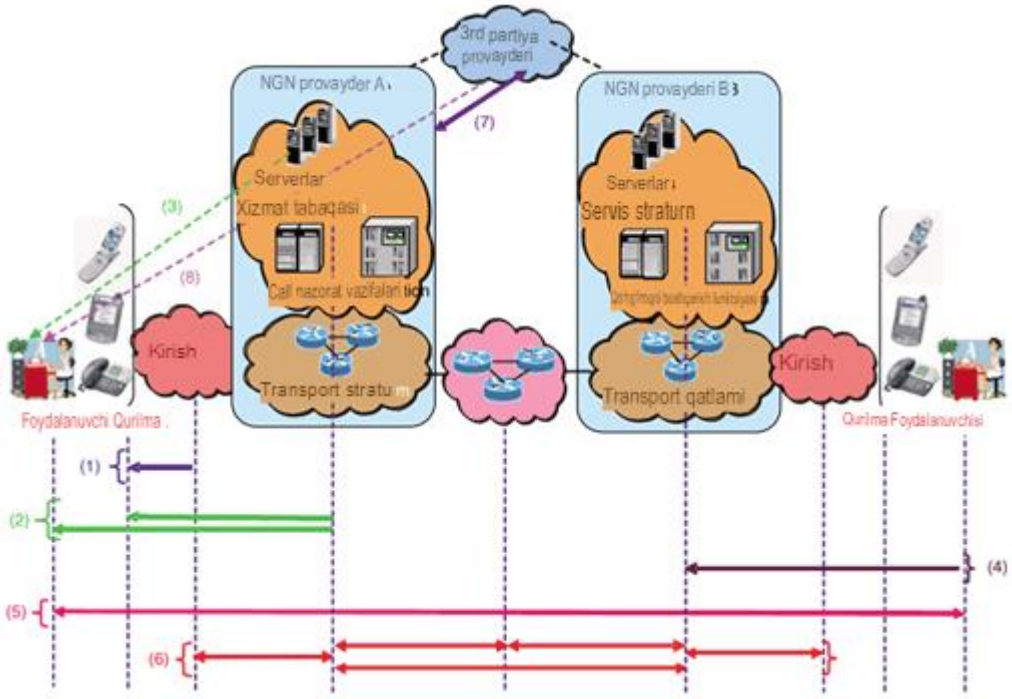
(4) Foydalanuvchi autentifikatsiyasi va tarmoqni avtorizatsiya qilish

(5) Foydalanuvchining tengdoshli autentifikatsiyasi va avtorizatsiyasi

(6) O'zaro tarmoq autentifikatsiyasi va avtorizatsiyasi

(7) autentifikatsiya va uchinchi tomon xizmat/ilova provayderining avtorizatsiyasi

(8) Uchinchi tomon autentifikatsiya xizmatidan foydalanish




**15.1-rasm. NGN autentifikatsiya va avtorizatsiya modeli.**

**NGN sertifikatini boshqarish**

---

Ochiq kalitlar infratuzilmasi (PKI) eski axborot texnologiyalari va aloqa tizimlarida autentifikatsiya, shifrlash va boshqa xavfsizlik mexanizmlarini amalga oshirishda muhim rol o'ynaydi va NGNda ham xuddi shunday muhim rol o'ynaydi. ITU-T Tavsiya loyihasi *Y.NGN Sertifikatlarni boshqarish* (NGN sertifikatlarini boshqarish) NGNda ochiq kalit sertifikatlaridan qanday foydalanishni ko‘rsatuvchi hujjatdir. U birinchi navbatda sertifikatlar formati va mazmuniga hamda sertifikatlarni boshqarishga qaratilgan.

Birinchidan, NGN da qo‘llaniladigan sertifikatlar formati X.509 3-versiyasiga asoslangan bo‘lib, u allaqachon keng tarqalgan sertifikat formatidir. Sertifikat formatidagi har bir maydonning mazmuniga (masalan, mavzu maydoni va kengaytma maydonlari) kelsak, batafsil foydalanish holatlari sertifikatni saqlaydigan qurilmalar turiga qarab tavsiflanadi.

Sertifikatlarni boshqarish uchun Tavsiya birinchi navbatda sertifikatlarni berish va tarqatish usullari, ularning haqiqiyligini tekshirish va ular haqida bekor qilish ma'lumotlarini saqlash bilan bog'liq. Sertifikat berish tartib-qoidalari ayniqsa batafsil tavsiflangan: Sertifikatlarning uchta turi egalik nuqtai nazaridan aniqlanadi — NGN provayderining tarmoq elementi sertifikatlari, NGN abonent sertifikatlari va NGN oxirgi foydalanuvchi sertifikatlari — hamda kalit juftligini yaratish, sertifikat berish va sertifikat tarqatish uchun tavsiya etilgan usullar. sertifikatning har bir turi uchun belgilanadi.

NGN identifikatorini boshqarish xavfsizligi

---

2007 yil iyul yig'ilishidan so'ng, NGNda identifikatsiyani boshqarish NGN xavfsizligi nuqtai nazaridan asosiy muammo sifatida paydo bo'ldi. Identifikatsiyani boshqarish texnologiyasi sohasi Internetning mashhurligi bilan juda kengaydi. OASIS [2], ixtiyoriy standartlashtirish organlari va biznes alyanslar texnik spetsifikatsiyalarni ishlab chiqishda, uning spetsifikatsiyalarini amalga oshirish uchun muvofiqlik tadbirlarini tashkil etishda va shuningdek, o'zaro muvofiqlikda yo'l ochib berdi. Ushbu ajoyib tadbirlarni hisobga olgan holda, 15/13-q.da ITU-T *Y.IdMsec Tavsiya loyihasini yaratish kelishuviga erishildi.*(NGN Identity Management Security) NGNda xavfsizlik nuqtai nazaridan va ko'plab tegishli manfaatlarni jamlagan. Ko'p sonli hissalar asosida Tavsiyani tahrirlash ishi 2006 yil oktabrdagi yig'ilishdan boshlangan. Tavsiya loyihasining joriy doirasi quyidagi oltita banddan iborat:

1. NGN identifikatorini boshqarish bilan bog'liq asosiy tushunchalarni aniqlang.

2. NGN funktsional talablari va arxitekturasi asosida identifikatsiyani boshqarish tizimini aniqlang (ramka barcha NGN ob'ektlari uchun qo'llanilishi kerak).

3. NGN muhitida identifikatsiyani boshqarish bilan bog'liq xavfsizlik tahdidlari va zaifliklarni baholang.

4. NGN muhitida identifikatsiyani boshqarish uchun ishonchlilik modelini ishlab chiqish.

5. NGN identifikatorini boshqarish uchun kafolat maqsadlari va shartlarini belgilang.

6. Taqdim etilgan ko'plab hissalarni muhokama qiling va kiberxavfsizlik va muhim infratuzilmani ta'minlash uchun zarur bo'lgan funksiyalarni aniqlang.

Mavjud identifikatsiyani boshqarish texnologiyasining uchta asosiy spetsifikatsiyasi ko'rib chiqildi:

(1) ITU-T X.1141 tavsiyasi (OASIS SAML v2.0) bir martalik kirish texnologiyasini o‘z ichiga oladi, (2) Liberty Alliance tomonidan ishlab chiqilgan foydalanuvchi o‘zi tasdiqlagan identifikator va atribut almashish texnologiyasi spetsifikatsiyalari va (3 ) ) OpenID, u ko‘plab veb-saytlarga kirish uchun yagona kirish identifikatori sifatida yagona resurs identifikatoridan (URI) foydalanadi.

Identifikatsiyani boshqarish bo'yicha fokus-guruh ITU-T diqqatni jamlash va ayniqsa muhim mavzularni muhokama qilishni tezlashtirish uchun maxsus fokus-guruhlarni (FG) shakllantirishga ruxsat beradi. Masalan, NGN shunday muhim mavzulardan biri bo'lib, FG NGNni o'rganish davrida yaqindan o'rganilgan. Xuddi shunday, FG IPTV hozirda Internet protokoli televideniesini o'rganmoqda. Identity Management (FG IdM) bo'yicha fokus-guruh 2006 yil dekabr oyida SG17 (xavfsizlik, til va telekommunikatsiya dasturlari bilan bog'liq masalalarni ko'rib chiqish bilan shug'ullangan tadqiqot guruhi) doirasida tuzilgan. Identifikatorni boshqarishning maqsadli diapazoni shunchalik kengki, qamrovni chegaralash juda muhim. Masalan, tarmoqni qanday aniqlashiga qarab (NGN, Internet, mobil tarmoqlar yoki ushbu tarmoqlarning kombinatsiyasi) yoki ID boshqaruv diapazoni

(tarmoq abonentlarini, veb-xizmat hisoblarini, RFID (radiochastota identifikatsiyasi) va boshqalar?), Qo'llanish doirasini chegaralashda juda ko'p muammoli muammolar bo'lishi mumkin. Shunday qilib, FG IdM ITU-T doirasidagi tegishli masalalar bo'yicha ishlaydigan guruhlar va ITU-Tdan tashqaridagi mavjud standartlashtirish guruhlari bilan fikr almashish, eski texnologiyalar bilan taqqoslash, kamchiliklarni tahlil qilish va foydalanish holatlari va talablar hujjatlarini tuzish bilan band.

Ushbu ma’ruzada NGN-ning 1-versiyasidagi xavfsizlikka oid hujjatlarga e'tibor qaratish va identifikatsiyani boshqarish bo'yicha so'nggi tashabbuslarni ko'rib chiqish orqali so'nggi NGN xavfsizligi bilan bog'liq standartlashtirish ishlarini jamladi.

## NAZORAT SAVOLLARI

1. NGN tarmoqlari xavfsizligi bizga nima uchun zarur?
2. NGN xavfsizlik mexanizmlari nimalar?
3. NGN autentifikatsiyasi va avtorizatsiya talablari qanday?
4. NGN identifikatorini boshqarish xavfsizligi nima?