SIMSIZ TARMOQLAR XAVFSIZLIGINI TA’MINLASHDA EAP (EXTENSIBLE AUTHENTICATION PROTOCOL) PROTOKOLINING QO’LLANILISHI

Shermuxammedov Jasurbek Abobakir o'g'li
O'zbekiston Respublikasi Madaniyat vazirligi Raqamlashtirish va axborot xavfsizligi bo'limi boshlig'i
Xammuallif Odilov Ilhom Isoq o'g'li
O'zbekiston Respublikasi Madaniyat vazirligi Raqamlashtirish va axborot xavfsizligi bo'limi bosh mutaxassisi

Annotatsiya: *Hozirgi kunda axborot texnologiyalari jadal tarzda rivojlanib borayotgan bir vaqtda aloqa, axborot almashinuvi ham juda katta tezlik bilan rivojlanib bormoqda. Aloqalarning qulayligi oshirishda aloqa vositalarini ham o’rni beqiyosdir. Chunki aloqaning sifatliligi aloqa vositalariga chambarchas bog’liq. Dastlab aloqalarni faqat sim ulagichlar orqali amalga oshirilar edi.*

Kalit soz’lar: *Wi-Fi, WLAN(Wireless Local AreaNetwork — Simsiz Lokal Tarmoq), ESSID*

KIRISH

So'nggi bir necha yil ichida simsiz tarmoqlarning mashhurligi sezilarli darajada oshdi. Simsiz ulanishning mashhurligining o'sishiga asosan zamonaviy noutbuklarga simsiz ulanish kartalarining integratsiyasi, pda qurilmalari, telefonlar va boshqalarning paydo bo'lishi kabi omillar ta'sir qiladi.turli xil tarmoq xizmatlariga (masalan, Internet) simsiz ulanish nuqtalari kafelarda, resto - yaralarda va boshqa jamoat joylarida tashkil etilgan. Kompaniyalar tarmoq kabel tizimlarini tashkil etishning iloji bo'lmagan yoki maqsadga muvofiq bo'lmagan taqdirda o'z tarmoqlarining tarqoq segmentlarini simsiz uskunalar bilan birlashtiradilar. 802.11 standartlariga asoslangan katta tarmoq qamrovi xavfsizlik bilan bog'liq muammolarning asosiy sabablaridan biridir, chunki tajovuzkor tarmoqning jismoniy joylashuvi joyidan sezilarli masofada joylashgan bo'lishi mumkin.

Simsiz xavfsizlik muammolari

Simsiz tarmoqlarning xavfsizligini ta'minlash uchun turli xil protokollar va usullar qo'llaniladi.

ESSID TRANSLYATSIYASINI O'CHIRIB QO'YISH.

Essid parametri simsiz tarmoq identifikatoridir. U simsiz tarmoq foydalanuvchilarini mantiqiy guruhlarga ajratish uchun ishlatiladi. ESSID foydalanuvchini kerakli simsiz tarmoqqa ulanishga chaqiradi va agar kerak bo'lsa, uni virtual mahalliy tarmoq identifikatori (VLAN) bilan taqqoslash mumkin. Bunday taqqoslash simli foydalanuvchilarning korporativ infratuzilma resurslariga kirish darajasini farqlashni tashkil qilish uchun zarurdir.

Simsiz tarmoqni loyihalashda essid xavfsizlik vositalaridan biri ekanligi haqida noto'g'ri tushuncha mavjud va translyatsiya paytida ESSID qiymatini o'chirib qo'yish tarmoq xavfsizligini kuchaytiradi. Aslida, ESSID qiymati qayta autentifikatsiya qilish va qayta ulanish so'rovlari bilan boshqaruv paketlarida mavjud bo'lishda davom etmoqda.

2. MAC manzili yordamida autentifikatsiya.

Autentifikatsiya - bu mijozning shaxsini ularga berilgan ma'lumotlar, masalan, ism va parol bilan aniqlash jarayoni. Ko'pgina simsiz uskunalar ishlab chiqaruvchilari foydalanuvchi qurilmalarini MAC manzillari bo'yicha autentifikatsiyani qo'llab - quvvatlaydilar, ammo IEEE standarti (elektr va elektron muhandislar instituti)

802.11 ushbu turdagi autentifikatsiya ta'minlanmaydi.

Qo'shimcha xavfsizlik usullaridan foydalanmasdan MAC manzili orqali autentifikatsiya qilish samarasiz. Faqatgina MAC - manzil orqali autentifikatsiya o'rnatilgan simsiz tarmoqqa kirish tajovuzkor uchun juda oson. Buning uchun siz radio kirish nuqtasi mijozlar bilan ishlaydigan radiokanalni tahlil qilishingiz va tarmoqqa kirish ochiq bo'lgan qurilmalarning MAC manzillari ro'yxatini olishingiz kerak. Simsiz tarmoq resurslariga kirish uchun tarmoq simsiz kartangizning MAC manzilini taniqli bilan almashtirishi kerak

MIJOZNING MAC MANZILI.

3. Statik wep kalitlari yordamida shifrlash.

WEP (Wired Equivalent Privacy) – radio kirish nuqtasi va uning foydalanuvchilari o'rtasidagi trafikni shifrlash uchun mo'ljallangan protokol. Osno-Vano WEP shifrlash etarli darajada kriptoga chidamli rc4 shifrlash algoritmida. Wep kalitining uzunligi 40 yoki 104 bitni tashkil qiladi. 24 bitli orqa tarafdagi signalni muvaffaqiyatli dekodlash uchun kalitga shifrlanmagan belgilar ketma - ketligi (boshlash vektori) qo'shiladi. Shunday qilib, 64 va 128 bitli kalit uzunliklari haqida gapirish odatiy holdir, ammo kalitning samarali qismi atigi 40 va 104 bitni tashkil qiladi.

Wep-ga passiv va faol hujumlar mavjud. Passivlarga quyidagilar kiradi:

* to'liq qo'pol hujum;

* FMS hujumi-2001 yilda mol Flurer, itzik Mantin va adi Shamir tomonidan taklif qilingan [1];

* yaxshilangan FMS hujumi [2].

Ushbu hujumlar ushlangan simsiz tarmoq paketlarini tahlil qilishga asoslangan va ularning ishlashining EF - fektivligi to'plangan ma'lumotlar miqdoriga bog'liq. Wep Second key-ni olish nazariy jihatdan 6000000 ta paketni ushlab turishni talab qiladi, bu 3-4 soat davom etishi mumkin [3].

Faol hujumlarning mohiyati ma'lumotlarni nurlantirish uchun simsiz tarmoqqa ta'sir qilishdan iborat bo'lib, ular qayta ishlangandan so'ng radio tarmoq resurslariga kirish huquqiga ega bo'ladi. Bularga quyidagilar kiradi:

* boshlash vektorini qayta ishlatish. Hujumchi bir xil ma'lumotni (oldindan ma'lum bo'lgan tarkibni) tashqi tarmoq orqali hujum qilingan simsiz segmentda ishlaydigan foydalanuvchiga qayta-qayta yuboradi. Har doim tajovuzkor foydalanuvchiga ma'lumot yuborar ekan, u radiokanalni (foydalanuvchi va hujum qilingan radio post nuqtasi o'rtasidagi kanal) tinglaydi va o'zi yuborgan ma'lumotni o'z ichiga olgan shifrlangan ma'lumotlarni to'playdi. Keyin tajovuzkor asosiy ketma - ketlikni nurli shifrlangan ma'lumotlar va ma'lum shifrlanmagan ma'lumotlar yordamida hisoblab chiqadi;

* bitlarni manipulyatsiya qilish. Hujum butunlikni boshqarish vektorining zaifligiga asoslangan. Masalan, tajovuzkor uchinchi darajali ma'lumotni buzish uchun ramka ichidagi

foydalanuvchi ma'lumotlarining bitlarini boshqaradi. Ramka kanal darajasida o'zgartirilmadi, radio kirish nuqtasida yaxlitlikni tekshirish muvaffaqiyatli o'tdi va ramka yanada uzatildi. Router, ramkani ra - diodga kirish nuqtasidan olib, uni ochadi va tarmoq qatlami paketining nazorat summasini tekshiradi, paketning nazorat summasi noto'g'ri bo'ladi. Router xato xabarini yaratadi va ramkani radio kirish nuqtasiga qaytaradi. Radio kirish nuqtasi paketni shifrlaydi va mijozga yuboradi. Hujumchi shifrlangan paketni oldindan ma'lum bo'lgan xato xabari bilan ushlaydi, shundan so'ng siz asosiy ketma - ketlikni hisoblaysiz.

4. WPA protokolini qo'llash (Wi-Fi himoyalangan kirish).

Wep protokolining ko'plab zaifliklari tufayli 2003 yilda yangi WPA xavfsiz simsiz ulanish protokoli ishlab chiqildi va qabul qilindi [4]. Shifrlash uchun WPA 128 bit uzunlikdagi dinamik ravishda ishlab chiqarilgan kalitlarga ega Temporal Key Integrity Protocol (tkip) dan foydalanadi. Autentifikatsiyani kuchaytirish uchun IEEE 802.1 x standarti va Extensible Authentification Protocol (EAP) qo'llaniladi.

Agar autentifikatsiya 802.1 x protokoli va RADIUS serveri yordamida amalga oshirilmasa, oldindan ajratilgan kalit (Preshared Key – PSK) ishlatiladi. Garchi har bir mijoz kompyuterida o'z PSK-i bo'li hi mumkin bo'lsada, vaqt barcha dasturlarda WEP protokolida bo'lgani kabi har bir ESSID uchun bitta PSK ishlatiladi. Shuning uchun, agar siz PSK - dan foydalansangiz, tkip-ga muvaffaqiyatli hujumlar amalga oshirilishi mumkin, bu esa autentifikatsiya jarayonida ushlangan paketlarni olish va tahlil qilish orqali amalga oshiriladi.

Ikkinchi avlod WPA2 simsiz ulanish standarti 2004 yilda taqdim etilgan [5]. O'zidan oldingi WPA - dan farqli o'laroq, u butunlay IEEE 802.11 i standartining orqa kalit versiyasiga asoslangan va shifrlash protokoli sifatida 128 bit uzunlikdagi AES (Advanced Encryption Protocol) dan foydalanadi.

Shuni ta'kidlash kerakki, simsiz tarmoqlar DoS (Deny of Service) hujumlariga ham duch kelishi mumkin, buning natijasida simli tarmoq mijozlariga xizmat ko'rsatilmaydi. Ushbu hujumlarning mohiyati suvsiz tarmoq ishini falaj qilishdir.

Kvinslend texnologiya universiteti mutaxassislari ra - diokanalning spektrni to'g'ridan - to'g'ri tarqatish ketma-ketligi (dsss) texnologiyasida mavjudligini baholash bilan bog'liq aniqlangan zaiflik haqida ma'lumot e'lon qilishdi. Ushbu texnologiya asosida keng tarqalgan 802.11 b standarti amalga oshirildi. tajovuzkor zaiflikdan foydalanib, simsiz tarmoqning doimiy bandligini taqlid qiladi. Bunday hujum natijasida hujum sodir bo'lgan radio kirish nuqtasi bilan ishlaydigan barcha foydalanuvchilar o'chirib qo'yiladi.

Shuni ta'kidlash kerakki, ushbu hujum nafaqat 802.11 b standartida ishlaydigan konlarga, balki 802.11 g standartidagi uskunalarga ham tegishli bo'lishi mumkin, garchi u dsss texnologiyasidan foydalanmasa ham. Bu 802.11 g standartida ishlaydigan radio post-Pa nuqtasi 802.11 b Stan-dart bilan orqaga qarab muvofiqlikni saqlab turganda mumkin.

Bugungi kunda 802.11 b standartidagi uskunalar uchun DoS hujumlaridan himoya mavjud emas, ammo bunday hujumni oldini olish uchun 802.11 g standartidagi uskunalardan foydalanish tavsiya etiladi (802.11 b bilan orqaga qarab mos kelmasdan).

Zamonaviy axborot texnologiyalarining taraqqiyoti kompyuter jinoyatchiligi, konfedensial ma’lumotlarga ruxsatsiz kirish, o‘zgartirish, yo‘qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda. Simsiz aloqa tarmoqlari bundan mustasno emas, uning xavfsizligini

ta’minlash bo‘yicha ko‘pgina muzokarali qarashlar gobal tarmoq orqali keng tarqalmoqda. Qanday qilib, tarmog‘ingiz xavfsizligini yuqori darajaga ko‘tarish mumkin?

Har qanday tarmoq kirish nuqtasi va simsiz mijoz aloqasi quyidagicha qurilgan:

• Autentifikatsiya — mijoz va kirish nuqtasi bir — birlariga qanday tanishtirilishi va o‘zaro aloqa qilishga huquqini tasdiqlaydi;

• Shifrlash — uzatiluvchi ma’lumotlarda qanday shifrlash algoritmlari qo‘llanilishi, qanday qilib shifrlash kaliti shakllantirilishi va u qachon o‘zgartirilishi.

Simsiz aloqa tarmog‘i ko‘rsatkichlari, birinchi navbatda uning nomi, tarmoq paketlari yordamida bog‘lanish nuqtasi bilan doim aloqada bo‘ladi. Kutilgan xavfsizlik sozlamalaridan tashqari, xohishga ko‘ra bir necha ko‘rsatkichlar uzatilishi mumkin: QoS (xizmat ko‘rsatish sifati) va 802.11n (simsiz aloqa standarti) ma’lumot almashish tezligi hamda boshqa qo‘shnilar haqida axborot beradi. Autentifikatsiya mijozni kirish nuqtasiga o‘zini tanishtirishni aniqlab beradi.

Yuz berishi mumkin bo‘lgan variantlar:

• Open — ochiq tarmoq, barcha ulanuvchi qurilmalar oldindan avtorizatsiya qilingan;

• Shared — ulanuvchi qurilma haqiqiyligi kalit yoki parol bilan tekshirilishi lozim;

• EAP — ulanuvchi qurilma haqiqiyligi tashqi server EAP protokoli bilan tekshirilishi lozim.

EAP protokollaridan ixtiyoriy bittasini qo‘llash tarmoq ma’muri tomonidan bajarilishi zarur. Windows XPGVistaG7, iOS, Android OTga o‘rnatilgan standartlar kamida EAP-TLS va EAP-MSCHAPv2 protokollarini ishlata oladi. Windows osti Intel mijoz adarterlarini ProSet utilitasini (mavjud ro‘yxatni kengaytira oluvchi) taqdim etadi. Buni Cisco Any Connect Client amalga oshiradi. Open Authentication va No Encryption uchun hech narsa kerak emas, tarmoqqa ulanishni o‘zi kifoya. Radio muhit ochiqligi sababli signal barcha yo‘nalishlarda tarqaladi va uni to‘sib qolish qiyin masala. Ulanishga qo‘shilish mumkinligi mos mijoz adapterlari tufayli tarmoq trafigi hujum qiluvchiga o‘zini xuddi simli aloqa tarmog‘ida, NUV da, SPAN-port kommutatoridagidek xis qiladi. WEP protokoliga asoslangan shifrlash uchun TKIP yoki AES asoslangan shifrlash uchun to‘g‘ridan — to‘g‘ri deshifrlash nazariyada iloji bor, ammo amaliyotda buzish xolati uchramagan. Albatta, PSK kalit uchun yoki EAP protokolidan biriga parol tanlashni sinab ko‘rish mumkin. Berilgan hujumlarning qo‘llanilishi noma’lum. Bu jarayonda ijtimoiy injeneriya yoki kriptoanaliz usullaridan foydalanish mumkin.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. Kuralov, Y. A., (2020). Development Of Geometric Creativity Of Secondary Scholl Students By Computer. International Journal of Scientific & Technology Research - (IJSTR) Volume-9 Issue-2, February 2020 Edition, 4572-4576.

2. Kuralov, Y. A., Makhmudova, D. M., (2020). METHODOLOGY OF DEVELOPING CREATIVE COMPETENCE IN STUDENTS WITH PROBLEMATIC EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol. 8 No. 4, 2020, Part IIISSN 2056-5852, 142-146.

3. Akhmedov, B. A., Majidov, J. M., Narimbetova, Z. A., Kuralov, Yu. A. (2020). Active interactive and distance forms of the cluster method of learning in development of higher education. Экономика и социум, 12(79), 805-808.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001. - 376 с.