WLAN (WIRELESS LOCAL AREA NETWORK) TARMOQLARIDA XAVFSIZLIK

Babakulov Bekzod Mamatkulovich o‘g‘li
Assistant. Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
babakulov.bekzod23@gmail.ru
Norov Beksulton Botir o‘g‘li
Talaba. Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
norovbeksulton72@gmail.com
https://doi.org/10.5281/zenodo.14603098

Annotatsiya: Ushbu maqolada WLAN tarmoqlarining xavfsizlik masalalari batafsil ko‘rib chiqilgan. U shaxsiy hudud tarmoqlari (PAN) uchun Bluetooth standartiga va Simsiz LAN (WLAN) uchun IEEE 802.11 standarti. ning kuchli va zaif tomonlari ushbu echimlar muhokama qilinadi va kelgusidagi rivojlanish va takomillashtirish istiqbollari taqdim etiladi. Nihoyat, mobil maxsus tarmoqlar uchun xavfsizlik masalalari kiritiladi.

Kalit so‘zlar: Simsiz xavfsizlik, PAN, WAN, maxsus tarmoqlar.

Mobil qurilmalar va simsiz texnologiyalar tez sur'atlar bilan rivojlanmoqda. O'rtasidagi chiziqlar mobil telefonlar PDA-lar bilan birlashgani sababli qo'l qurilmalari xiralasha boshlaydi va kitoblar ish stoli quvvatini oladi. Haqiqiy mobil bo'lish uchun hamma bir yoki bir nechtasini o'z ichiga olishi kerak imsiz texnologiyalar, ularga tengdoshlar orasidagi shaxsiy hududni shakllantirish imkoniyatini taklif qiladi (PAN) va mahalliy (LAN) tarmoqlariga kiring. Shuni hisobga olib, simsiz radio chastotasi (RF) signallar devorlar va binolardan tashqariga tarqaladi, simsiz chastotali uzatishni ta'minlash vazifasi murakkabdir. Yaxshiyamki, bu xavfsizlik muammolari hal qilinmoqda va echimlar topildi standartlashtirilgan.

Simsiz tarmoqlar uchun xavfsizlik arxitekturasi

Xavfsizlik arxitekturasi ma'lum bir tizimni himoya qilish uchun qo'llaniladigan barcha xavfsizlik choralari va usullaridan iborat. Bunday arxitekturani qatlamli tuzilma sifatida ko'rish mumkin, unda yuqori darajadagi chora-tadbirlar quyi darajadagi xizmatlardan foydalanadi:

1. Kriptografik primitivlar barcha yuqori darajadagi xavfsizlik protokollari tomonidan qo'llaniladigan qurilish bloklaridir. Simmetrik kalit blokli shifrlar va raqamli imzolar yaxshi ma'lum misollardir.

2. Kalitlarni boshqarish va autentifikatsiya qilish, ehtimol, eng muhim xavfsizlik protokollaridir, chunki ular xavfsiz marshrutlash tizimlari kabi ilg'or protokollar uchun zarurdir. Kalitlarni boshqarish sxemasi tarmoqdagi turli tugunlar o'rtasida maxfiy kalitlarni xavfsiz taqsimlash uchun funksionallikni ta'minlashi kerak.

3. Xavfsizlik siyosati tugunlar bo'ysunishi kerak bo'lgan "qoidalarni" belgilaydi. Masalan, faqat vakolatli foydalanuvchilarga simsiz tarmoqqa kirishga ruxsat bering yoki faqat RSN bilan himoyalangan ulanishlarga ruxsat bering. Shubhasiz, siyosatni belgilash qiyin va uni doimiy ravishda ko'rib chiqish kerak bo'ladi.

BLUETOOTH XAVFSIZLIGI

1998 yil fevral oyida Bluetooth maxsus qiziqish guruhi (SIG) telekommunikatsiya sohasi yetakchilari tomonidan tashkil etilgan. Ushbu savdo assotsiatsiyasining asosiy vazifasi mobil telefonlar, kompyuterlar, PDA'lar, naushniklar va boshqa mobil qurilmalar bir-biri bilan simsiz aloqa qilishini tavsiflovchi Bluetooth spetsifikatsiyasini yaratish edi. 2000 yil iyun

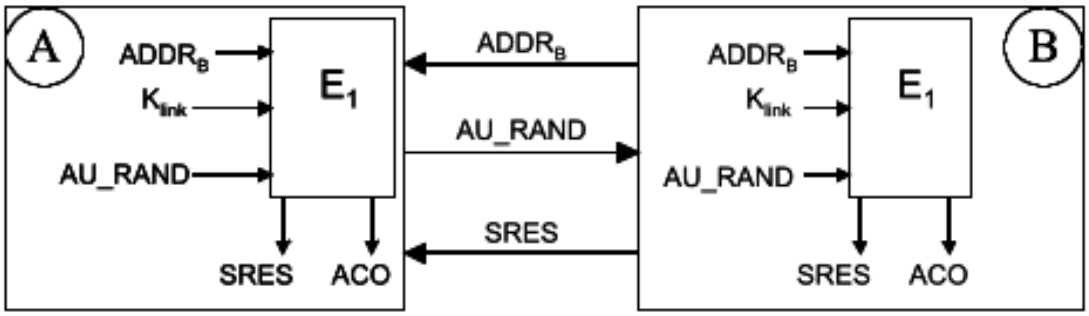
oyida Bluetooth standarti Simsiz shaxsiy tarmoq ishchi guruhiga kiritildi (IEEE 802.15). Bluetooth simsiz texnologiyasi radio tarqatish orqali arzon narxlardagi qisqa masofali simsiz ovoz va ma'lumotlar ulanishini amalga oshiradi. Endi biz Bluetooth-ning xavfsizlik arxitekturasini muhokama qilamiz va uning xavfsizlik zaif tomonlari haqida umumiy ma'lumot beramiz.

Xavfsizlik arxitekturasi

Xavfsizlik arxitekturasining ikkita eng muhim qismi bu asosiy o'rnatish protokoli va shifrlash algoritmidir. Aytaylik, ikkita Bluetooth qurilmasi (A va B deb ataladi) xavfsiz muloqot qilishni xohlaydi. Dastlab bu qurilmalar umumiy umumiy sirga ega emas. Shuning uchun ular quyidagi amallarni bajaradilar:

Birlik kalitini yaratish: Bluetooth qurilmasi birinchi marta yoqilganda, u birlik kaliti deb ataladigan narsani hisoblaydi. Bu har bir qurilma uchun noyob bo'lgan va deyarli hech qachon o'zgartirilmaydigan kalit. Bu tasodifiy raqam va Bluetooth manzilining funktsiyasidir (bu har bir qurilma uchun zavod tomonidan o'rnatilgan parametrdir).

Ishga tushirish kalitini yaratish: Bluetooth qurilmalari hali ham seansni kalitlarini baham ko'rmaydi. Bu turli bosqichlarda amalga oshiriladi. Birinchidan, ishga tushirish kaliti yaratiladi. Ushbu vaqtinchalik kalit tasodifiy raqam (muloqotni boshlagan qurilma tomonidan ishlab chiqariladi), umumiy shaxsiy identifikatsiya raqami (PIN) va PIN-kod uzunligi L funktsiyasidir. PIN-kod ikkala qurilmada ham kiritilishi kerak va uzunligi 8 va 128 bit orasida tanlanishi mumkin. Agar qurilmalardan birida kirish interfeysi bo'lmasa, qattiq PIN-kod ishlatiladi (ko'pincha standart qiymat 0000). Natijada vaqtinchalik umumiy kalit (insializatsiya kaliti).



1.O'zaro (mutual) autentifikatsiya protokoli

O'zaro (Mutual) autentifikatsiya: Endi ikkala qurilma ham kalitni baham ko'radi va o'zaro autentifikatsiyani amalga oshiradi chaqiruv-javob protokoliga asoslangan tekshirish protokoli. Ushbu protokol ikki marta amalga oshiriladi. Birinchidan, 1-rasmda ko'rsatilganidek, B o'zini A ga autentifikatsiya qiladi. Agar bu autentifikatsiya muvaffaqiyatli bo'lsa, rollar almashtiriladi (B tekshirgichga, A esa isbotlovchiga aylanadi). Autentifikatsiya quyidagicha davom etadi. A AU RAND tasodifiy sonini hosil qiladi va uni B ga yuboradi. Bu tasodifiy raqam chaqiruv deb ataladi. Endi ikkala qurilma ham SRES E_1 (ADDRB, Klink, AU RAND) javobini hisoblaydi. Autentifikatsiya funksiyasi E_1 SAFER+ shifrlash funksiyasiga asoslangan. Algoritm SAFER-SK128 mavjud 64 bitli blokli shifrning takomillashtirilgan versiyasidir [15]. Klunk - umumiy kalit (boshlash kaliti). Agar B javobi A hisoblagan qiymatga mos kelsa, autentifikatsiya muvaffaqiyatli bo'ladi. Biz protokol tafsilotlarini o'tkazib yuboramiz.

Bog'lanish kalitini yaratish: ikkala qurilma endi ishga tushirish kalitini baham ko'radi. Bu kalit yangi, yarim doimiy kalit (bog'lanish kaliti deb ataladi) bo'yicha kelishish uchun ishlatiladi. Bog'lanish kaliti ikkala qurilmada ham saqlanadi, shunda u kelajakdagi aloqa uchun ishlatilishi mumkin. Agar qurilmalardan birida kalitlarni saqlash uchun yetarli xotira bo‘lmasa, havola tugmasi xotirasi cheklangan qurilmaning birlik kaliti bo‘ladi. Ushbu birlik kaliti ishga tushirish kaliti bilan shifrlanadi va boshqa qurilmaga yuboriladi. Agar ikkala qurilmada ham yetarlicha xotira bo‘lsa, havola kaliti ikkala qurilmaning kiritilishidan va umumiy ishga tushirish kalitidan olingan kombinatsiyalangan kalit bo‘ladi.

O'zaro autentifikatsiya: havola kaliti yaratilgandan so'ng, eski vaqtinchalik ulanish kaliti butunlay o'chiriladi va almashtirilgan havola kaliti bilan o'zaro autentifikatsiya boshlanadi.

Shifrlash kalitini yaratish: havola kaliti muvaffaqiyatli ishlab chiqarilgandan so'ng, shifrlash kalitini yaratish mumkin. Ushbu shifrlash kaliti umumiy havola kalitiga, tasodifiy raqamga (muloqotni boshlagan qurilma tomonidan yaratilgan) va ACO qiymatiga (1-rasmda ko'rinib turganidek, o'zaro autentifikatsiya protokolining natijasi) bog'liq. Agar kerak bo'lsa, shifrlash kaliti uzunligi qisqartirilishi mumkin.

Kalit oqimini yaratish: shifrlash kaliti (yoki uzunligi qisqartirilgan kalit) oziqlanadi oqim shifriga E Bluetooth manzili va master soati bilan birga. Natijada shifrlanishi kerak bo'lgan ma'lumotlar bilan XORlangan kalit oqimi paydo bo'ladi. Asosiy soat kalit oqimini taxmin qilishni qiyinlashtirish uchun ishlatiladi.

Xavfsizlikning zaif tomonlari

Bluetooth standartida bir nechta xavfsizlik kamchiliklari mavjud (masalan, Jakobsson va Wetzel ga qarang). Ushbu muammolarning ba'zilari tajovuzkor tomonidan osonlikcha foydalaniladi, boshqa xavfsizlik zaif tomonlari esa nazariydir. Endi eng muhim muammolar haqida qisqacha ma'lumot beriladi.

Xavfsizlik PIN-kod xavfsizligiga bog'liq: ishga tushirish kaliti ishga tushirish funktsiyasidir dom raqami, umumiy PIN-kod va PIN-kod uzunligi. Tasodifiy raqam ishga tushirish bosqichida mavjud bo'lgan tajovuzkor tomonidan ma'lum. Bu shuni anglatadiki, agar tajovuzkor PIN-kodni olsa, u ishga tushirish kalitini biladi. Hatto yomonlashadi! Boshqa barcha kalitlar ishga tushirish kalitidan olinganligi sababli, ular tajovuzkor tomonidan ham ma'lum bo'ladi. Kalitlarning xavfsizligi PIN-kod xavfsizligiga bog'liq. Agar u juda qisqa yoki zaif bo'lsa (masalan, 0000), tajovuzkor PIN-kodni taxmin qilish juda oson. E'tibor bering, PIN-kodni tekshirish har doim ham mumkin. Buning sababi shundaki, o'zaro autentifikatsiya protokoli ishga tushirish kaliti yaratilgandan so'ng amalga oshiriladi. Agar tajovuzkor ushbu protokolga rioya qilsa, u chaqiruv va tegishli javobni oladi. Tajovuzkor PIN-kodning har bir taxmini uchun tegishli javobni hisoblab chiqadi va bu kuzatilgan javobga teng bo'lsa, to'g'ri PIN-kod ishlatilgan bo'lishi mumkin. PIN-kod qanchalik qisqa bo'lsa, bu brute-force hujumi tezroq amalga oshirilishi mumkin.

Birlik (unit) kaliti: Bluetooth qurilmalaridan birida seans kalitlarini saqlash uchun yetarli xotira bo'lmasa, birlik tugmasi ishlatiladi. Bu kalit doimiy xotirada saqlanadi; deyarli hech qachon o'zgarmaydi. Birlik kaliti boshqa qurilmaga shifrlangan (boshlash kaliti bilan) yuboriladi. Bu taqlid qilish hujumi uchun eshikni ochadi. Birlik tugmalaridan foydalanishdan qochish tavsiya etiladi.

Shifrlash algoritmi: Bluetooth E_0 shifrlash algoritmidan foydalanadi. Ushbu oqim shifrida ba'zi xavfsizlik kamchiliklari mavjud. E_0-ga bir nechta hujumlar nashr etilgan, ammo bu hujumlarning aksariyati E-ni Bluetooth-da amalga oshiradigan algoritmda ishlamaydi. Biroq, istisnolar mavjud. Golic 9 Bluetooth oqimi shifriga hujumni topdi, u 128 bitli maxfiy kalitni 45 ta ishga tushirishdan 270 ga yaqin murakkablik bilan qayta tiklay oladi. Oldindan hisoblash bosqichida taxminan 280 103 bitli so'zlardan iborat ma'lumotlar bazasini saralash kerak. Hujum taxminiy chiziqli tenglamalarning ikkilik tizimlarini echish uchun umumiy chiziqli iterativ kriptotahlil usulidan foydalanadi.

Xizmatni rad etish hujumlari: Mobil tarmoqlar xizmat ko‘rsatishni rad etish hujumlariga nisbatan zaif. Ular mobil qurilmalardan iborat va bu qurilmalar ko'pincha batareya bilan oziqlanadi. Bluetooth ham bundan mustasno emas. Buzg'unchi mobil qurilmaga soxta xabarlarni yuborishi mumkin. Ushbu qurilma xabar olganida, u biroz hisoblash (va batareya) quvvatini sarflaydi. Biroz vaqt o'tgach, barcha batareya quvvati sarflanadi. Batareya quvvatining bunday tugashi birinchi marta Stajano va Anderson tomonidan kiritilgan uyquni yo'qotish hujumi deb ataladi . Amalga oshirish qarorlari tufayli xizmat ko'rsatishni rad etish hujumlari ham mavjud. Yaxshi misol - o'zaro autentifikatsiya protokoli paytida ishlatiladigan qora ro'yxat. Qurilma autentifikatsiya protokolini qayta-qayta ishga tushirishiga yo'l qo'ymaslik uchun har bir qurilmada o'zini to'g'ri autentifikatsiya qila olmagan qurilmalarning Bluetooth manzillarining qora ro'yxati mavjud. Ushbu qurilmalar ma'lum vaqt davomida autentifikatsiya protokolini boshlay olmaydi. Ushbu mexanizmdan bir nechta xizmat ko'rsatishni rad etish hujumlarida foydalanish mumkin

Joylashuv maxfiyligi: Ikki yoki undan ortiq Bluetooth qurilmalari aloqa o'rnatayotganda, yuborilgan paketlar har doim jo'natuvchi va qabul qiluvchining Bluetooth manzillarini o'z ichiga oladi. Buzg'unchi uzatilgan ma'lumotlarni tinglaganida, u ikki qurilma aloqa qilgan joy va vaqtni kuzatishi mumkin. Bu foydalanuvchining maxfiyligini buzishdir. Joylashuv ma'lumotlari boshqa shaxslarga sotilishi va joylashuvga bog'liq tijorat reklamalari uchun ishlatilishi mumkin.

Bluesnarf hujumi: Yaqinda Bluesnarf hujumi topildi. Bu mumkin ba'zi mobil telefonlar, so'rov to'g'risida maqsadli qurilma egasini ogohlantirmasdan qurilmaga ulanish va telefonda saqlangan ma'lumotlarning cheklangan qismlariga, shu jumladan butun telefon kitobiga (va har qanday rasm yoki boshqa ma'lumotlarga kirishga) ruxsat olish. yozuvlar), taqvim, real vaqt soati, tashrif qog'ozi, xususiyatlar, o'zgartirish jurnali, IMEI (Xalqaro mobil uskuna identifikatori,) Bu odatda faqat qurilma ko'rish mumkin bo'lgan rejimda bo'lsa mumkin, lekin u erda asboblar mavjud ushbu xavfsizlik tarmog'ini chetlab o'tishga imkon beruvchi Internet.

Bluejacking: Ikkita Bluetooth qurilmasi ulanganda, ular o'zlarining "ismlarini" bir-biriga yuboradilar. Ushbu foydalanuvchi nomi 248 ta belgidan iborat bo'lishi mumkin va boshqa qurilmaning chiqish interfeysida ko'rsatiladi. Bluejacking hujumi ushbu nomdan Bluetooth qurilmalariga reklama yuborish uchun foydalanadi.

SIMSIZ LAN XAVFSIZLIGI

1997 yil iyun oyida dominant 802.3 Ethernet standartini belgilagan IEEE organi simsiz mahalliy tarmoq uchun 802.11 standartini chiqardi. IEEE 802.11 standarti litsenziyasiz 2,4 gigagertsli chastota diapazoni doirasida infraqizil yorug'lik va ikki turdagi radio uzatishni qo'llab-quvvatlaydi: Frequency Hopping Spread Spectrum (FHSS) va Direct Sequence Spread Spectrum (DSSS). Bugungi kunda bir nechta 802.11 standartlari mavjud. 802.11b - 11 Mbit / s

gacha uzatish tezligini ta'minlaydigan standartning kengayishi. Yangi 802.11a va 802.11g versiyalari 54 Mbit/s gacha tezlikni qo‘llab-quvvatlaydi.

Umumiy ko'rinish

IEEE 802.11 dizaynerlari simli va simsiz muhit o'rtasidagi o'ziga xos farqni, xususan, o'rtacha kirishda ekanligini tan oldilar. Transport vositasi umumiy bo'lganligi sababli, boshqa mijozning uzatish diapazonidagi har qanday mijoz ushbu xostdan kelgan paketlarni qayta ishlashi mumkin. WLAN kabi simsiz muhitda ma'lumotlar va xizmatlarga ruxsatsiz kirishning oldini olish uchun bajarilishi kerak bo'lgan uchta maqsad: (1) autentifikatsiya va avtorizatsiya, (2) maxfiylik va (3) yaxlitlik. 802.11 standarti ushbu maqsadlarga erishish uchun bir nechta o'zgarishlardan o'tdi.

2002 yilda sanoat 802.11 ratifikatsiyasini kuta olmasligini aytib, Wi-Fi Alliance sanoat konsorsiumi Wi-Fi himoyalangan kirishni (WPA) joriy qildi. Bu 802.11i imkoniyatlarining kichik to'plami bo'lib, yaxshi shifrlash, oldindan umumiy kalit yordamida oson sozlash va foydalanuvchilarning RADIUS asosidagi 802.1X autentifikatsiyasidan foydalanish qobiliyatidir. 2004 yil iyun oyida IEEE nihoyat 802.11i standartini ratifikatsiya qildi. 802.11i WPA-ning barcha imkoniyatlariga ega va ma'lumotlarni shifrlash uchun Advanced Encryption Standard (AES) dan foydalanish imkoniyatini qo'shadi. Salbiy tomoni shundaki, AES qo'llab-quvvatlashi ko'plab mavjud WLANlar uchun yangi uskunani talab qilishi mumkin, chunki u shifrlash va shifrni ochish uchun maxsus chipga muhtoj.

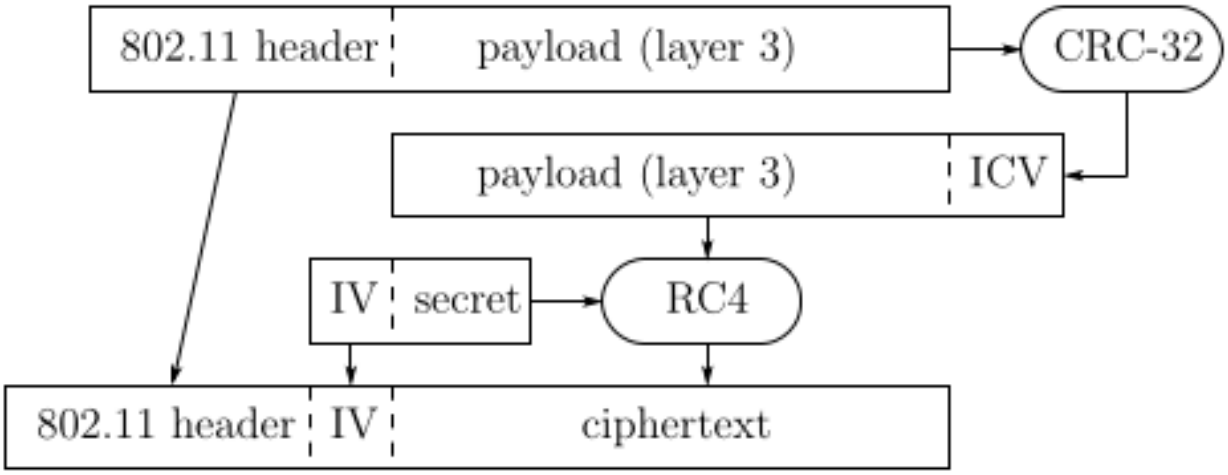
Simli ekvivalent maxfiylik (WEP) protokoli

Birinchi 802.11 uskunasi WEP protokolini o'z ichiga olgan bo'lib, u ixtiyoriy ravishda Mobil stantsiya (ST) va kirish nuqtasi (AP) o'rtasidagi ulanishni ta'minlash uchun ishlatilishi mumkin. Tavsiya etilgan xavfsizlik arxitekturasining birinchi kamchiligi - bu kalitlarni boshqarishning yo'qligi. Foydalanuvchilar o'z qurilmalariga (va AP) to'rttagacha maxfiy kalitlarni qo'lda kiritishlari kerak. Haqiqiy ishlatilgan kalit ham foydalanuvchi tomonidan qo'lda tanlanishi kerak. Agar WEP ishlatilsa, ST va AP o'rtasidagi barcha trafik shifrlanadi va WEP va tanlangan maxfiy kalit yordamida autentifikatsiya qilinadi. Standartda kirishni boshqarishning ikkita majburiy mexanizmi tasvirlangan. Sukut bo'yicha "ochiq tizim" yoki kirishni boshqarishning yo'qligi, ikkinchisi esa WEP-ga asoslangan chaqiruv-javob sxemasi. Ularning yonida bir nechta sotuvchiga xos sxemalar qo'shildi. 2-rasmda WEP shifrlash sxemasi ko'rsatilgan. Avval chiziqli CRC-32 nazorat summasi (Integrity Check Value yoki ICV) hisoblanadi va foydali yukga qo'shiladi. Keyinchalik ochiq matnni shifrlash uchun RC4 oqim shifridan foydalaniladi. RC4-ni ishga tushirish uchun ishlatiladigan kalit 24-bitli Boshlang'ich qiymat (IV) va maxfiy kalit (42 yoki 104 bit) birikmasidan iborat. Olingan shifrlangan matn IV bilan birga qabul qiluvchiga yuboriladi. IV har bir paket uchun o'zgartiriladi.

Yuqorida aytib o'tganimizdek, standart chiqarilgandan so'ng ko'p zaifliklar aniqlandi. Ushbu kamchiliklar sxemaning uchta asosiy muammosiga bog'liq edi:

1. Kichik IV bo'sh joy: 24 bit etarli emas. Tug'ilgan kun paradoksi shuni ko'rsatadiki, 5000 paketdan keyin (tasodifiy IV tanlovi bilan) birinchi to'qnashuv yuqori ehtimollik bilan sodir bo'ladi. IV-to'qnashuv sodir bo'lganda, ikkala natijada RC4 oqimlari Kamdan-kam teng. Buzg'unchi endi ikkita mos keladigan C_1 M_1R va C2 M2 R shifrlangan matnni XOR qilishi mumkin, natijada C_1C M_1M2 hosil bo'ladi. Ikkita shifrlangan matnning yig'indisi psevdo-tasodifiy R oqimini o'z ichiga olmaydi, chunki ularning yig'indisidan M_1 va M_2 olish uchun statistik hujumlar qo'llanilishi mumkin.

2. Chiziqli, kalitga bog'liq bo'lmagan CRC-32 nazorat summasidan oqim shifrlash bilan birgalikda foydalanish. CRC-32 hisoblash maxfiy kalit ma'lumotlarini o'z ichiga olmaydi va tasodifiy xatolarni aniqlash uchun mo'ljallangan (masalan, transport qatlami tomonidan kiritilgan). WEP-da CRC-32 ma'lumotlarni autentifikatsiya qilish uchun ishlatiladi va dizayn oqilona bo'lib, raqib to'g'ri CRC-32 nazorat summasini hisoblay olmaydi, chunki u RC4 shifrlash bilan himoyalangan. Amalda esa bunday emas. Raqib boshqa foydalanuvchilarning xabarlarini o'zgartirishi va maxfiy kalitni bilmasdan turib, o'z xabarlarini kiritishi mumkin. Bu shuni anglatadiki, WEP ma'lumotlar autentifikatsiyasini ta'minlay olmaydi.



2-rasm. WEB ma'lumotlarini shifrlash va inkapsulyatsiya qilish

3. RC4 kalit oqimini qayta ishlatish aniqlanmaydi. Tajovuzkor bitta oddiy matn shifrlangan matn juftligini va shuning uchun shifrlash uchun ishlatiladigan kalit oqimini qo'lga kiritgandan so'ng, maxfiy kalit o'zgartirilgunga qadar ushbu kalit oqimidan qayta foydalanish mumkin. Ayniqsa, agar qurilma autentifikatsiyasi uchun chaqiriq/javob ishlatilsa, tajovuzkor osonlikcha ochiq matn (chaqiriq) va shifrlangan matn (javob) juftligini olishi mumkin va natijada olingan kalit oqimidan qayta foydalanishi mumkin.

Kalit boshqaruvining etishmasligi hatto bu hujumlarni kuchaytiradi, chunki kalitni tez-tez o'zgartirish zerikarli va shuning uchun kalit ko'p holatlarda deyarli yangilanmaydi.

Nihoyat 2001 yil iyul oyida Fluhrer va boshqalar. WEP da qo'llanilganidek RC4 ga hujumni taqdim etdi. Ushbu hujum tajovuzkorga etarli miqdordagi kriptogrammalarni passiv ravishda qo'lga kiritgandan so'ng foydalaniladigan maxfiy kalitni hisoblash imkonini beradi (128 bitli WEP kaliti uchun 1,3 million; og'ir yuklangan APda bu 1 soatdan kamroq vaqtni oladi). Ushbu hujum kalit o'lchamiga nisbatan chiziqli, shuning uchun maxfiy kalitni kattalashtirish bu erda yordam bermaydi. Ushbu hujum turli xil vositalarda amalga oshirildi va 802.11 WEP-ga asoslangan xavfsizlik uchun haqiqiy tahdid deb hisoblanishi kerak.

Wi-Fi bilan himoyalangan kirish (WPA)

2002 yilda Wi-Fi Alliance sanoat konsortsiumi WLAN xavfsizligi uchun qisqa muddatli yechimni taqdim etish uchun Wi-Fi himoyalangan kirishni (WPA) joriy qildi. Wi-Fi Alliance WPA mavjud 802.11 uskunasiga mos kelishi kerakligini aytdi. Bu, shubhasiz, erishish mumkin bo'lgan yaxshilanishlarni cheklab qo'ydi, chunki WEP hali ham qo'llanilmoqda va Fluhrer va boshqalarning hujumi. hali ham amal qiladi. WEP atrofida uning xavfsizligini oshirish uchun yangi shifrlash/autentifikatsiya sxemasi "Vaqtinchalik kalit yaxlitligi protokoli" (TKIP)

qurilgan. TKIP ketma-ketlik qoidalariga ega bo'lgan kattaroq IV bo'sh joydan (48 bit) foydalanadi va vaqtinchalik maxfiy kalitdan, qurilmaning MAC manzilidan va paketlar tartib raqamidan har bir paket uchun WEP kalitlarini olish mexanizmini qo'shadi. Bu bir nechta ST bir xil maxfiy kalitni baham ko'rsa ham noyob kalitlarni ta'minlaydi. Vaqtinchalik kalitning o'zi tez-tez o'zgartiriladi (har 10000 paket) va AP va ST o'rtasida almashinadigan juft asosiy kalit (PMK) va noncesga asoslanadi. Buning yonida Maykl deb nomlangan yangi 64-bitli kalitli xabar yaxlitlik kodi (MAC) foydali yukni WEP bilan shifrlashdan oldin qo'llaniladi. Maykl juda samarali bo'lishi kerak edi (<5 ko'rsatmalar/bayt) va unchalik kuchli emas, lekin bu CRC-32 ga nisbatan sezilarli yaxshilanishdir. Ushbu yaxshilanishlar orqali TKIP WEP ning barcha ma'lum zaifliklarini ko'rib chiqadi.

Nihoyat, WPA foydalanuvchi yoki qurilma autentifikatsiyasi uchun IEEE 802.1X tizimidan foydalanishga ham imkon beradi. 802.1X himoyalangan tarmoqqa foydalanuvchi trafigini autentifikatsiya qilish va nazorat qilish, shuningdek dinamik ravishda o'zgaruvchan shifrlash kalitlari uchun samarali tizimni taklif etadi. 802.1X simli va simsiz LAN muhitiga EAP (kengaytirilgan autentifikatsiya protokoli) deb nomlangan protokolni bog'laydi va token kartalari, Kerberos, bir martalik parollar va ochiq kalit autentifikatsiyasi kabi bir nechta autentifikatsiya usullarini qo'llab-quvvatlaydi. EAP haqida batafsil ma'lumot olish uchun IETF ning RFC 2284 [4] ga qarang. Dastlabki 802.1X aloqasi autentifikatsiya qilinmagan so'rovchi (ST) autentifikator (AP) bilan ulanishga urinishidan boshlanadi. AP mijozdan kirish nuqtasining simli tomonida joylashgan autentifikatsiya serveriga faqat EAP paketlarini o'tkazish uchun portni yoqish orqali javob beradi. Kirish nuqtasi autentifikatsiya serveri (masalan, RADIUS) yoki oldindan o'rnatilgan umumiy kalit yordamida mijozning identifikatorini tekshirmaguncha kirish nuqtasi boshqa barcha trafikni bloklaydi. Autentifikatsiya qilingandan so'ng, kirish nuqtasi boshqa trafik turlari uchun mijozning portini ochadi. 802.1X dan PMKlarni xavfsiz almashish uchun ham foydalanish mumkin.

Dastlabki 802.11 standartida WEP-dan foydalanish ixtiyoriy bo'lsa, WPA-da TKIP va 802.1X-dan foydalanish majburiydir.

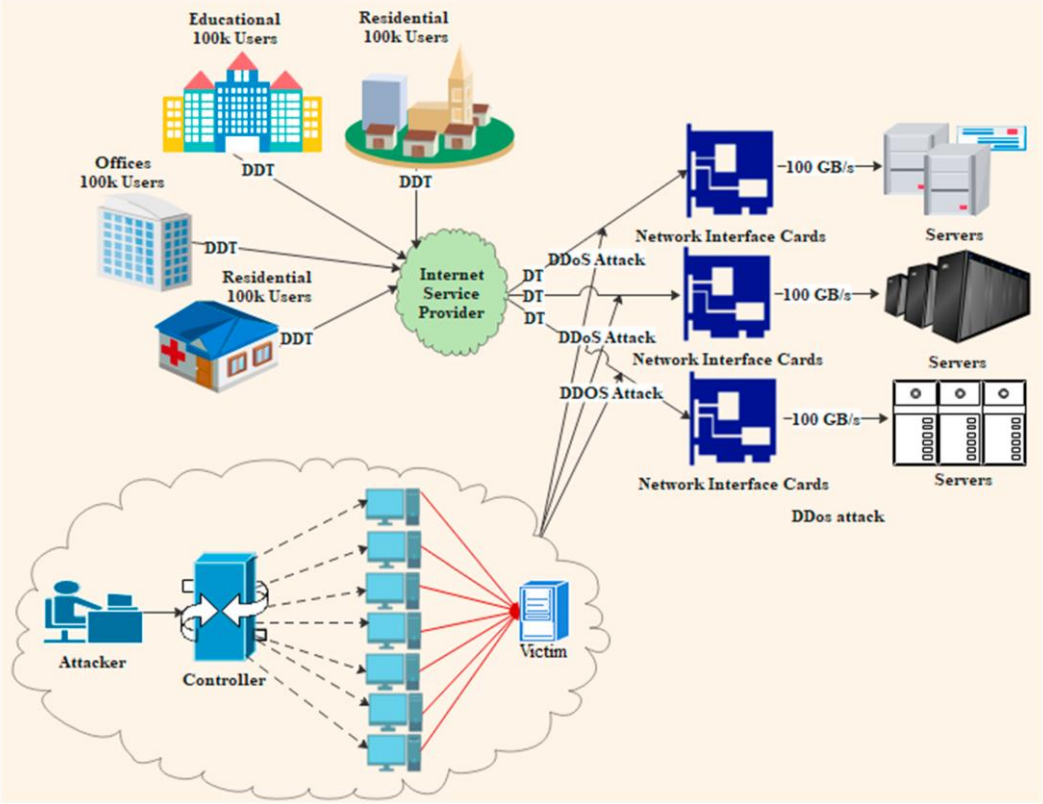
802.11i va mustahkam xavfsizlik tarmog‘i (RSN)

2004 yil iyun oyida IEEE 802.11i standartini ratifikatsiya qildi. IEEE 802.11i mustahkam xavfsizlik tarmog'i (RSN) deb ataladigan yangi simsiz tarmoq turini belgilaydi. RSN ga qo'shilish uchun simsiz qurilma oldingi bo'limda muhokama qilingan imkoniyatlarga ega bo'lishi kerak. Biroq, kengaytirilgan yangilanish davrini osonlashtirish uchun 802.11i RSN va WEP tizimlari parallel ravishda ishlashi mumkin bo'lgan o'tish davri xavfsizlik tarmog'ini belgilaydi. WPA va RSN umumiy arxitektura va yondashuvga ega. WPA xavfsiz tarmoqni amalga oshirishning bir usuliga qaratilgan bir qator imkoniyatlarga ega, RSN esa ko'proq moslashuvchanlikni ta'minlaydi. RSN TKIPdan tashqari AES algoritmini ham qo'llab-quvvatlaydi. Joriy uskuna to'liq 802.11i standartini qo'llab-quvvatlamaganligi sababli, WPA joriy WLAN foydalanuvchilarining ehtiyojlarini ta'minlaydi, uzoq muddatda to'liq RSN esa ko'proq moslashuvchanlikni ta'minlaydi.

WLAN xavfsizligiga asosiy tahdidlar

WLAN tarmoqlari ochiq havoda radio signallari orqali ishlagani sababli, ular ko‘pincha quyidagi xavflarga duch keladi:

- **Eavesdropping (Signalni kuzatish):** WLAN'ning radio signallarini ushlab olib, shifrlanmagan ma'lumotlarni o'qish imkonini beradi. Bu, ayniqsa, ochiq Wi-Fi tarmoqlarida keng tarqalgan.
- **Spoofing (Soxta tarmoq yaratish):** Hujumchi haqiqiy tarmoqqa o'xshash soxta tarmoq yaratib, foydalanuvchilarni ulanishga majbur qiladi.
- **Denial of Service (DDoS):** Hujumchi tarmoqni ortiqcha trafik bilan yuklab, uni ishdan chiqaradi.
- **Man-in-the-Middle (MITM):** Hujumchi signal uzatilayotgan qurilma va router o'rtasida vositachi sifatida qatnashib, ma'lumotlarni manipulyatsiya qiladi.
- **Parollarni buzish:** Zaif parollar yoki himoyasiz autentifikatsiya mexanizmlarini buzish orqali tarmoqqa kirish.



Xulosa

Bluetooth va IEEE 802.11 ga kiritilgan xavfsizlik texnikasi haqida umumiy ma'lumot berdik. Bundan tashqari, biz simsiz maxsus tarmoqlarning xavfsizlik masalalarini ham muhokama qildik. Ushbu munozaralardan ko'rinib turibdiki, simsiz tarmoqlar xavfsizligini ta'minlash qiyin va uni to'g'ri qabul qilish uchun mutaxassislar tomonidan katta e'tibor va baholash talab etiladi. WEP bilan bog'liq muammolar jiddiy va IEEE ushbu muammolarni tezda hal qilish uchun vazifa guruhini yaratganligi ajablanarli emas. Bluetooth xavfsizligi mukammal bo'lmasa-da, muammolar sanoat tomonidan xavfsizlik mexanizmlarini yaxshilash uchun Bluetooth SIG-ni surish uchun etarlicha jiddiy deb hisoblanmagan ko'rinadi.

References:

1. "History of Wireless". Johns Hopkins Bloomberg School of Public Health. Archived from the original on 2007-02-10. Retrieved 2007-02-17.

2. Wayne Caswell (November 17, 2010). "HomeRF Archives". Archived from the original on May 29, 2018. Retrieved July 16, 2011.
3. Wireless Mesh Routing Compared WDS, archived from the original on 2023-01-17, retrieved 2022-11-11
4. "Is this the same as Ad Hoc mode?". Archived from the original on 2013-08-30.
5. "Wireless Distribution System Linked Router Network". DD-WRT Wiki. Archived from the original on June 30, 2017. Retrieved December 31, 2006.
6. "How Wi-Fi Roaming Really Works". Archived from the original on 2019-02-23. Retrieved 2008-10-09.
7. https://www.geeksforgeeks.org/wlan-full-form/
8. https://en.wikipedia.org/wiki/Bluejacking
9. "Introduction and overview", Educational Leadership, Cambridge University Press, pp. 1–5, 2007-01-22, doi:10.1017/cbo9781139168564.001, ISBN 978-0-521-68512-2, retrieved 2024-02-16
10. L. Zhou and Z. Haas, "Securing ad hoc networks", IEEE Network Magazine Special Issue on Network Security vol. 13, no.6 Nov./Dec. 1999