Komilov Abdulloh

ALFRAGANUS UNIVERSITY ,Kiberxavfsizlik injiniringi yo'nalishi , 1-bosqich talabasi

Mavzu : Ikkilik sanoq tizimi va uning kiberxavfsizlikdagi o'rni

Kirish

Ikkilik (binary) sanoq tizimi — zamonaviy elektron hisoblashning poydevori. U faqat ikkita raqam — 0 va 1 — bilan ishlaydi va har bir bit (binary digit) axborotning eng kichik birlik hisoblanadi. Bu maqolada ikkilik tizimning asoslari, kompyuterda qanday ishlashi va ayniqsa kiberxavfsizlik (cybersecurity) sohasida qanday muhim rol o'ynashi tushuntiriladi.

Ikkilik tizimning asoslari

1. Ta'rif: Ikkilik sanoq tizimida har bir raqamning o'zi bitta bitni ifodalaydi: 0 yoki 1. Masalan, ikkilikda 1011 bu — $1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$ (o'nlikda).
2. Bit va bayt: Bit — eng kichik birlik, 8 bit esa 1 bayt (byte). Baytlar yozuv, son, belgi va boshqalarni kodlash uchun ishlatiladi.
3. Ikkiylichdan yuqori darajali kodlashgacha: Belgilarni (masalan ASCII yoki Unicode), surat va audio ma'lumotlarni saqlash — bularning hammasi ikkilik shaklida kodlanadi.

IIkkilik arifmetika va operatsiyalar

Ikkilik ustida qo'shimcha, ayirish, ko'paytirish kabi arifmetik amallar bajariladi. Bundan tashqari, bitwise operatsiyalar (AND, OR, XOR, NOT, shift) kiberxavfsizlikda keng qo'llanadi — ular xavfsizlik algoritmlarining asosi bo'lgan past darajali manipulyatsiyalarni osonlashtiradi.

Kiberxavfsizlikda ikkilik tizimning funksional rollari

1. Kriptografiya va shifrlash
- Asosiy qiymat: Shifrlash algoritmlari (symmetric va asymmetric) ikkilik ma’lumotlar ustida matematik operatsiyalar bilan ishlaydi. Masalan, blok shifrlash (AES) va oqim shifrlashlar barcha bitlar va baytlar bilan ishlaydi.
- Bit maniplulyatsiyasi: XOR kabi bitwise operatsiyalar shifrlash va tekshirish raqamlarini (MAC) yaratishda ishlatiladi.
- Kalitlar va tasodifiylik: Kriptografik kalitlar bitlar ketma-ketligidan iborat. Ularning tasodifiyligi va yetarli entropiyasi tizim xavfsizligini belgilaydi.

2. Hash funksiyalari va integritet

- Hash (SHA-256 kabi) ma’lumotni ikkilik ko‘rinishga o‘tkazib, deterministik “barcod” hosil qiladi. Bu integritetni tekshirish, parollarni saqlash va raqamli imzo kabi jarayonlarda muhim.

2. Hash funksiyalari va integritet

- Hash (SHA-256 kabi) ma’lumotni ikkilik ko‘rinishga o‘tkazib, deterministik “barcod” hosil qiladi. Bu integritetni tekshirish, parollarni saqlash va raqamli imzo kabi jarayonlarda muhim.

3. Avtorizatsiya va autentifikatsiya

- Parollar, tokenlar, HMAC va PKI (Public Key Infrastructure) — barchasi ikkilik ko‘rinishda ishlaydi. Masalan, parolni serverga yuborishdan oldin uni hash qilish va solishtirish jarayonida bitlar bilan operatsiyalar amalga oshiriladi.

4. Tarmoqli protokollar va ma’lumot uzatish

- TCP/IP, TLS kabi protokollar ma’lumotlarni paketlarga bo‘lib, ustiga boshqaruv bitlari, bayroqlar (flags) va tekshiruv yig‘indilarini (checksums) qo‘yadi. Paketlarda bit darajasidagi o‘zgartirishlar uzatuvchi va qabul qiluvchi o‘rtasidagi muloqot xavfsizligini ta’minlashda markaziy rol o‘ynaydi.

5. Xatolikni aniqlash va tuzatish (error detection and correction)

- CRC, parity bit va ECC (Error-Correcting Code) kabi usullar ma’lumot uzatishda yoki saqlashda bit darajasidagi xatoliklarni aniqlash va ba’zan to‘g‘rilashga yordam beradi. Bu tizimlar ma’lumotning yaxlitligini ta’minlashda kiberxavfsizlik uchun zarur — zararli o‘zgartirishlarni aniqlash imkonini beradi.

Amaliy misollar

- Parol saqlash: Parollar oddiy matn ko‘rinishda emas, hash(q) — ikkilik/kodlangan qiymat sifatida saqlanadi; server foydalanuvchi kiritgan parolni qayta hash qilib solishtiradi.
- TLS sessiyasi: Brauzer va server o‘rtasida xavfsiz kanal yaratishda ikkilikda olingan kalitlar va sertifikatlar ishlatiladi.
- Disk shifrlash: F whole-disk encryption tizimlari (masalan LUKS, BitLocker) ma’lumotlarni baytlarda shifrlaydi — hammasi ikkilik darajada.

Xavf va cheklovlar

- Entropiya yetishmasligi: Tasodifiy sonlarning yomonligi kalitlarni zaif qiladi.
- Yon-kanal hujumlari: Bit darajasidagi signallarni tahlil qilib shaxsiy kalitlar o‘g‘irlanishi mumkin.
- LSB steganografiya noto‘g‘ri qo‘llanilganda ma’lumotlar oshkor bo‘lishi yoki fayl buzilishi mumkin.
- Sof bit manipulyatsiya bilan hujumlar: Masalan, paketdagi bitlarni o‘zgartirish orqali paketni noto‘g‘ri yo‘naltirish yoki xatolik yaratish mumkin — shuning uchun autentifikatsiya va integritet tekshiruvlari muhim.

Kelajak va rivojlanish yo‘nalishlari

- Kvaнтt hisoblash kelajakda ayrim kriptografik algoritmlarga (RSA, ECC) tahdid solishi mumkin; lekin yangi post-kvant kriptografiya ham oxir-oqibat ikkilik darajadagi operatsiyalar bilan ifodalanadi — faqat matematik asoslari boshqacha bo‘ladi.
- Xavfsiz apparat (secure enclaves, TPM) va bit darajasida himoya qilish usullari yanada dolzarb bo‘ladi.
- Kuzatuv va mitigatsiya: Yon-kanal hujumlarini aniqlash va kamaytirish usullari kuchaytiriladi.

Kelajak va rivojlanish yo‘nalishlari

- Kvaнтt hisoblash kelajakda ayrim kriptografik algoritmlarga (RSA, ECC) tahdid solishi mumkin; lekin yangi post-kvant kriptografiya ham oxir-oqibat ikkilik darajadagi operatsiyalar bilan ifodalanadi — faqat matematik asoslari boshqacha bo‘ladi.
- Xavfsiz apparat (secure enclaves, TPM) va bit darajasida himoya qilish usullari yanada dolzarb bo‘ladi.
- Kuzatuv va mitigatsiya: Yon-kanal hujumlarini aniqlash va kamaytirish usullari kuchaytiriladi.

Xulosa

Ikkilik sanoq tizimi — kompyuterlarning "tili". Kiberxavfsizlik esa shu til asosida o‘zgarishlarni aniqlash, ma’lumotni himoya qilish va tizimlarni xavfsiz saqlash bilan bog‘liq. Ikkilik darajasidagi tushuncha va bit manipulyatsiyalarni chuqur bilish — kriptografiya, tarmoq xavfsizligi, apparat xavfsizligi va ma’lumot integriteti sohalarida muvaffaqiyat uchun zarur. Shu sababdan kiberxavfsizlik mutaxassislari doimo bitlar, baytlar, entropiya va past darajali operatsiyalarni chuqur tushunishlari kerak.
Agar xohlasangiz, men ushbu maqolani qisqartirilgan prezentatsiya, akademik referat shaklida yoki misollar (kodli minibeloglar — masalan XOR misoli) bilan kengaytirib bera olaman. Qaysi variantni xohlaysiz?