



SMART HOME IOT TIZIMLARIDA AXBOROT XAVFSIZLIGI: TAHDIDLAR, ZAIFLIKLAR VA HIMOYA USULLARINING TAHLILI

<https://doi.org/10.5281/zenodo.23198405>

Habibjonova G.M.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada Smart Home IoT tizimlarining axborot xavfsizligi holati tizimli ravishda tahlil qilinadi. Tadqiqotning asosiy manbasi sifatida Smart Home xavfsizligiga bag'ishlangan ilmiy survey olinib, unda xavfsizlik muammolari platforma, qurilma va kommunikatsiya qatlamlariga ajratilgani asos qilib olindi. Smart Home arxitekturasi doirasida aqlli qurilmalar, gateway, bulut platformalari, aloqa kanallari va foydalanuvchi o'rtasidagi o'zaro bog'liqlik ko'rib chiqildi. Platforma qatlamida dasturlash, ilovalararo bog'lanish, autentifikatsiya, avtorizatsiya, ovozli yordamchilar va maxfiylik; qurilma qatlamida firmware zaifliklari, sensorlararo bog'lanish, side-channel hujumlari, autentifikatsiya, avtorizatsiya va maxfiylik; kommunikatsiya qatlamida esa Zigbee, BLE, Bluetooth, Wi-Fi va MQTT bilan bog'liq xavflar tahlil qilindi. Tahlil natijasida Smart Home xavfsizligidagi asosiy tizimli sabablar komponentlarning heterojenligi, ishlab chiqaruvchi va platformalarning maxsus moslashtirilgan yechimlari, mas'uliyat chegaralarining noaniqligi hamda yagona standartlashtirishning yetarli emasligi ekanligi ko'rsatildi. Shuningdek, avtomatlashtirilgan zaifliklarni aniqlash, qat'iy xavfsizlik tekshiruvlari va ma'lumotlarga asoslangan tahlil kelajakdagi muhim yo'nalishlar sifatida umumlashtirildi.

Аннотация. В статье системно анализируется информационная безопасность систем Smart Home на основе IoT. В качестве основной научной базы использован обзор исследований по безопасности Smart Home, в котором проблемы классифицируются на безопасность платформ, устройств и коммуникаций. Рассматривается архитектура, включающая интеллектуальные устройства, шлюз, облачную платформу, каналы связи и конечного пользователя. Для платформенного уровня анализируются безопасность программирования, межплатформенное взаимодействие, аутентификация, авторизация, безопасность голосовых помощников и защита конфиденциальности. Для уровня устройств рассматриваются уязвимости прошивки, взаимосвязи сенсоров, побочные каналы, аутентификация, авторизация и защита приватности. На коммуникационном уровне исследуются уязвимости Zigbee, BLE, Bluetooth, Wi-Fi и MQTT. Показано, что системными причинами рисков являются неоднородность компонентов, специализированные и модифицированные решения производителей, неясность границ ответственности и отсутствие унифицированных требований



безопасности. Обобщены перспективные направления, включая автоматизированное обнаружение уязвимостей, строгую проверку безопасности и анализ данных, генерируемых Smart Home системами.

Abstract. *This paper provides a structured analysis of information security in Smart Home IoT systems based on a comprehensive survey of Smart Home security research. The analysis follows a three-layer classification covering platform security, device security, and communication security. The Smart Home architecture is considered as an interaction of smart devices, gateways, cloud platforms, communication channels, and end users. Platform-level risks include programming and application linkage problems, authentication, authorization, voice-assistant security, and privacy protection. Device-level risks include firmware vulnerabilities, sensor-linkage problems, side-channel attacks, authentication, authorization, and device privacy. Communication-level risks are analyzed for Zigbee, BLE, Bluetooth, Wi-Fi, and MQTT. The analysis identifies heterogeneity, vendor-specific customization, unclear responsibility boundaries, and insufficient standardization as major systemic causes of Smart Home security weaknesses. Automated vulnerability discovery, rigorous security checking, and data-driven analysis are summarized as important directions for further research.*

Kalit so'zlar: *Smart Home, IoT, axborot xavfsizligi, platforma xavfsizligi, qurilma xavfsizligi, kommunikatsiya xavfsizligi, autentifikatsiya, avtorizatsiya, maxfiylik, zaifliklar.*

Internet of Things (IoT) texnologiyalarining jadal rivojlanishi natijasida raqamli qurilmalar kundalik hayotning turli sohalariga chuqur kirib bordi. Smart Home ushbu ekotizimning eng ko'p qo'llanayotgan yo'nalishlaridan biri bo'lib, u masofadan boshqarish, avtomatlashtirish va turli maishiy jarayonlarni o'zaro bog'lash imkonini beradi. Smart Home tizimlarining amaliy qiymati shundaki, foydalanuvchi uyga qaytishidan oldin haroratni sozlashi, qurilmalarni masofadan boshqarishi yoki sensor hodisalariga asoslangan avtomatik qoidalarini ishga tushirishi mumkin [1].

Biroq funksional imkoniyatlarning kengayishi xavfsizlik yuzasini ham kengaytiradi. Manbada keng qo'llaniladigan IoT qurilmalarining katta

qismida jiddiy zaifliklar uchrashi, bunday zaifliklar nafaqat qurilmaning o'ziga, balki foydalanuvchi maxfiyligi, jismoniy xavfsizligi va mulk xavfsizligiga ham ta'sir qilishi qayd etilgan [1]. Masalan, Smart Home qurilmalari orqali kamera, eshik qulfi, isitish tizimi yoki boshqa fizik muhit elementlari boshqarilishi mumkinligi sababli kiberhujumning oqibati oddiy axborot yo'qotilishidan tashqari jismoniy xavfga ham aylanishi mumkin.

Smart Home xavfsizligi alohida bitta qurilmaning himoyasi bilan cheklanmaydi. Tizim tarkibida turli ishlab chiqaruvchilarga tegishli qurilmalar, gatewaylar, bulut servislar, mobil ilovalar, avtomatlashtirish qoidalari va turli aloqa protokollari birgalikda ishlaydi. Shu



sababli bir komponentdagi zaiflik boshqa komponentlarga ham tarqalishi mumkin [1]. Tadqiqot manbasida Smart Home xavfsizlik muammolari platforma, qurilma va kommunikatsiya xavfsizligi sifatida tizimlashtirilgan [1].

Mazkur maqolaning maqsadi — berilgan ilmiy manbadagi Smart Home xavfsizligi bo'yicha yondashuvlarni yagona analitik tuzilma asosida qayta tizimlashtirish, asosiy tahdid va zaifliklarni ularning himoya usullari bilan bog'lash hamda kelgusidagi tadqiqotlar uchun istiqbolli yo'nalishlarni aniqlashdan iborat. Maqola yangi eksperimental ma'lumotlarni da'vo qilmaydi; natijalar manbadagi ilmiy kuzatuvlar va ularning tizimli sinteziga asoslanadi.

Tadqiqot materiali va tahlil doirasi

Tadqiqotning asosiy materiali — Bin Yuan, Jun Wan, Yu-Han Wu, De-Qing Zou va Hai Jin tomonidan 2023-yilda Journal of Computer Science and Technology jurnalida e'lon qilingan "On the Security of Smart Home Systems: A Survey" maqolasi [1]. Ushbu manbada Smart Home xavfsizligi bo'yicha mavjud tadqiqotlar tizimli ko'rib chiqilib, xavfsizlik masalalari uchta asosiy yo'nalishga ajratilgan: platforma xavfsizligi, qurilma xavfsizligi va kommunikatsiya xavfsizligi [1].

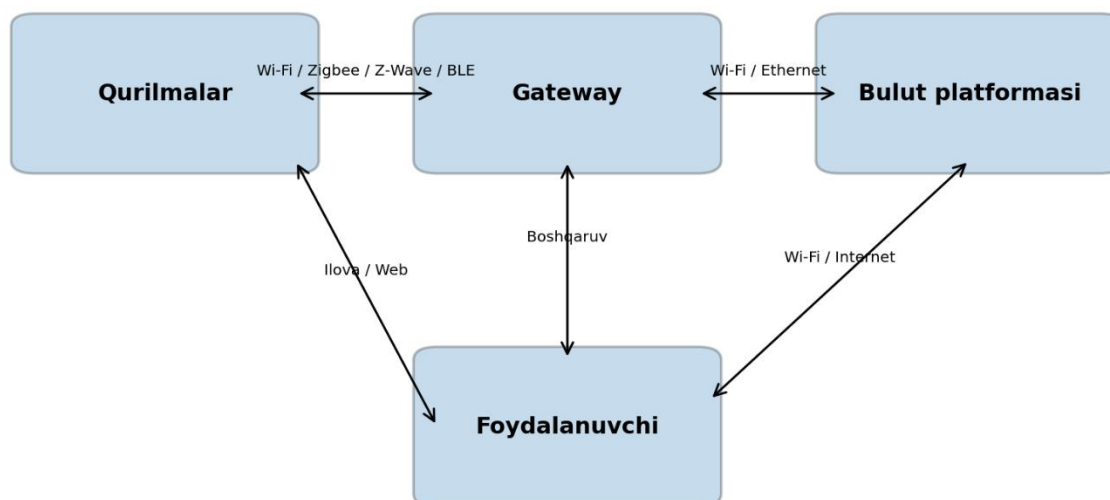
Tahlil usuli sifatida strukturaviy kontent tahlili va tahdid–himoya mosligi usuli tanlandi. Bunda avvalo Smart Home arxitekturasining asosiy komponentlari ajratildi, keyin har bir komponentga ta'sir qiluvchi tahdidlar, mavjud mitigatsiyalar va tadqiqot cheklovlari guruhlandi. Yakuniy bosqichda manbada ko'rsatilgan xavflarning ildiz sabablari va kelajakdagi tadqiqot yo'nalishlari birlashtirildi.

Smart Home arxitekturasini

Manbada mainstream Smart Home tizimlari beshta asosiy komponent orqali ifodalanadi: smart qurilmalar, gateway qurilmalar, IoT cloud platformalari, kommunikatsiya kanallari va oxirgi foydalanuvchi [1]. Smart qurilmalar sensorlar orqali atrof-muhit ma'lumotlarini yig'adi va boshqaruv buyruqlarini bajaradi. Gateway turli qurilmalarni birlashtirib, sensor ma'lumotlarini platforma yoki foydalanuvchiga uzatadi. Bulut platformasi sertifikatlarni boshqarish, avtomatlashtirish qoidalarini bajarish va boshqa servislarni taqdim etadi. Kommunikatsiya kanallari esa Wi-Fi, Zigbee, Z-Wave, Bluetooth va boshqa texnologiyalar orqali komponentlar o'rtasidagi ma'lumot almashinuvini ta'minlaydi [1].



Smart Home IoT tizimining umumlashtirilgan arxitekturası



1-rasm. Smart Home IoT tizimining umumlashtirilgan arxitekturası (asosiy manbadagi arxitektura tavsifi asosida qayta chizilgan).

1-jadval.

Smart Home IoT tizimi komponentlari va ularning asosiy xavfsizlik yuzalari

Komponent	Asosiy vazifa	Asosiy xavfsizlik yuzasi
Smart qurilmalar	Sensor ma'lumotlarini yig'ish va fizik harakatlarni bajarish	Firmware, sensorlar, autentifikatsiya, maxfiylik
Gateway	Qurilmalarni tarmoq va bulut bilan bog'lash	Kirish nazorati, sessiyalar, ma'lumotlar oqimi
Bulut platformasi	Avtomatlashtirish, sertifikat va servislarni boshqarish	API, avtorizatsiya, ilovalararo bog'lanish, maxfiylik
Kommunikatsiya kanallari	Komponentlar o'rtasida ma'lumot uzatish	Protokol zaifliklari, trafik, kuzatuv
Foydalanuvchi	Ilova yoki web orqali boshqarish	Autentifikatsiya, ovozli buyruqlar, vakolatlar

Tahdid modeli

Tahlil doirasida hujumchi Smart Home tizimining bir yoki bir nechta komponentidan foydalanib, maxfiy ma'lumotni qo'lga kiritishi, qurilma

boshqaruvini egallashi, avtomatlashtirish qoidalarini buzishi yoki kommunikatsiya jarayonini kuzatishi mumkin deb qaraladi. Manba bo'yicha tizimning bir komponenti



buzilganda uning boshqa komponentlar bilan o'zaro bog'liqligi sababli butun Smart Home xavfsizligiga ta'sir yuzaga kelishi mumkin [1].

Tahdidlarni tahlil qilishda uchta asosiy mezon ajratiladi: (1) ta'sir qilinayotgan qatlam; (2) hujumning asosiy mexanizmi; (3) hujum oqibatining turi. Oqibatlar maxfiylikning buzilishi, yaxlitlikning buzilishi, mavjudlikning pasayishi, foydalanuvchi vakolatlarining suiiste'mol qilinishi yoki fizik muhitga zarar yetkazish ko'rinishida namoyon bo'lishi mumkin.

Platforma xavfsizligi

Platforma xavfsizligi butun Smart Home tizimiga ta'sir qiluvchi yuqori qatlamdir. Manbada platforma xavfsizligi dasturlash, linkage, autentifikatsiya, avtorizatsiya, ovozi yordamchilar va maxfiylikni himoya qilish kabi oltita yo'nalishga ajratilgan [1]. Platformadagi nuqson butun platformaga ulangan qurilmalar va foydalanuvchilarga ta'sir qilishi mumkin.

Dasturlash va avtomatlashtirish xavfsizligi

Smart Home platformalarida foydalanuvchilarga avtomatlashtirish ilovalari, SmartApps yoki virtual yordamchi ko'nikmalarini yaratish imkonini beruvchi dasturlash muhitlari mavjud. Bunday moslashuvchanlik xavfsizlikka yangi xavflarni ham keltirib chiqaradi. Manbada noto'g'ri yoki ortiqcha ruxsatlar, xavfsiz bo'lmagan API interfeyslari va zararli avtomatlashtirish ilovalari asosiy muammolar qatorida ko'rsatilgan [1].

Himoya nuqtai nazaridan avtomatlashtirish ilovalarini audit qilish, xatti-harakatlarni kutilgan holat bilan taqqoslash va xavfsiz bo'lmagan APIlarni qayta loyihalash muhimdir. Manbada HoMonit kabi yondashuvlar kutilgan xatti-harakatlar bilan kuzatilgan xatti-harakatlarni taqqoslashga, skill-name scanner esa virtual yordamchi ko'nikmalarini tekshirishga yo'naltirilgani qayd etilgan [1].

Ilovalararo bog'lanish va qoida konfliktlari

Smart Home platformalarida bir nechta avtomatlashtirish qoidalari o'zaro ta'sirlashadi. Bitta qoida boshqa qoidani kutilmagan tarzda ishga tushirishi natijasida xavfsizlik yoki fizik xavfsizlik muammosi yuzaga kelishi mumkin. Masalan, bir sensor hodisasi derazani ochish qoidasini faollashtirib, boshqa xavfli harakat uchun sharoit yaratishi mumkin [1].

Manbada bunday muammolarni aniqlash uchun tabiiy tilni qayta ishlash (NLP), statik dastur tahlili, dinamik yo'naltirilgan graflar va finite-state machine (FSM) asosidagi modellash kabi usullar ko'rib chiqilgan. Ayrim ishlarda statik tahlil va NLP orqali trigger-action qoidalari orasidagi konfliktlar aniqlangan, boshqa yondashuvlarda esa real bajarilish grafigi kutilgan siyosat bilan solishtirilgan [1].

Autentifikatsiya va avtorizatsiya

Autentifikatsiya foydalanuvchi yoki boshqa subyektning haqiqiylikni aniqlashga xizmat qiladi. Platformadagi autentifikatsiya zaifligi tajovuzkorga



qonuniy foydalanuvchi nomidan buyruqlar yuborish imkonini berishi mumkin. Avtorizatsiya muammosida esa foydalanuvchi yoki ilovaga kerakli darajadan ortiq huquq berilishi xavfi mavjud [1].

Manbada ovoz orqali biometrik xususiyatlardan foydalanish, credential-less autentifikatsiya, kontekstga sezgir avtorizatsiya va OAuth asosidagi cross-cloud delegation xavfsizligini kuchaytirish kabi yondashuvlar tahlil qilingan. Umumiy xulosa shuki, ruxsatlarni faqat statik rolga emas, balki muhit, soʻralayotgan funksiya va foydalanuvchi kontekstiga ham bogʻlash xavfsizlikni oshirishi mumkin [1].

Ovozli yordamchilar va maxfiylik

Ovozli yordamchilar oʻziga xos hujum yuzasiga ega. Manbada inaudible voice attacks, qoʻshiq yoki boshqa audio ichiga yashirilgan buyruqlar, akustik uzatish xususiyatlaridan foydalanadigan hujumlar hamda voice squatting kabi tahdidlar koʻrsatilgan [1]. Bunday hujumlarda foydalanuvchi odatiy audio eshitayotgan boʻlsa-da, tizim yashirin buyruqni qabul qilishi mumkin.

Maxfiylik masalasida esa ovozli maʼlumotlarning bulutga yuborilishi, foydalanuvchi fotosuratlar va joylashuv maʼlumotlarining zararli ilovalar orqali sizib chiqishi muhim xavf sifatida koʻrsatiladi. FlowIT va FlowFence kabi yondashuvlar maʼlumot oqimini kuzatish va ruxsat etilgan oqimdan chetga chiqishni cheklashga qaratilgan [1].

Qurilma xavfsizligi

Qurilma qatlamidagi zaifliklar foydalanuvchining shaxsiy hayoti va fizik muhitiga bevosita taʼsir qilishi mumkin. Manbada qurilma xavfsizligi olti yoʻnalishga ajratilgan: qurilma zaifliklari, sensorlararo bogʻlanish, side-channel hujumlari, autentifikatsiya, avtorizatsiya va qurilma maxfiyligi [1].

Firmware zaifliklari

Smart Home qurilmalari firmware darajasida xotira buzilishi, autentifikatsiyani chetlab oʻtish va boshqa dasturiy mantiq nuqsonlariga ega boʻlishi mumkin. Insecure default password va yetarli xavfsizlik dizaynining yoʻqligi botnetga qoʻshilish xavfini oshiradi. Manbada Mirai botneti va uning hosilalari Smart Home qurilmalari xavfsizligi uchun muhim misol sifatida koʻrib chiqilgan [1].

Zaifliklarni aniqlash uchun fuzzing, full-system simulation, grey-box fuzzing, statik binary analysis, symbolic execution va companion application tahliliga asoslangan usullar koʻrib chiqilgan. FIRMADYNE, Firm-AFL va Firmalice kabi yondashuvlar turli afzallik va cheklovlarga ega: ayrimlari yuqori hisoblash resursini talab qiladi, ayrimlari esa qurilma yoki xavfsizlik siyosatini qoʻlda tavsiflashni talab qiladi [1].

Sensorlararo bogʻlanish va side-channel tahdidlar

Smart Home avtomatlashtirishida sensor hodisalari boshqa qurilmalarning ishga tushishiga sabab boʻladi. Shu sababli sensor maʼlumotining notoʻgʻri yoki zararli oʻzgartirilishi butun tizimning xatti-harakatini oʻzgartirishi mumkin. Manbada sensorlarning aktivatsiya ketma-



ketligini tahlil qilish, kontekstga sezgir intrusion detection va sensor ma'lumotlari asosida foydalanuvchi xatti-harakatlarini modellashtirish usullari ko'rsatilgan [1].

Side-channel xavflari esa elektromagnit nurlanish, fizik tebranishlar, sensor signallari va boshqa yordamchi belgilar orqali ma'lumot olish bilan bog'liq. Manbada harorat sensorini aldash, accelerometer ma'lumotidan klaviatura kiritmalarini taxmin qilish va LiDAR orqali fizik tebranishlardan tovush izlarini tiklashga oid misollar keltirilgan [1].

Qurilma autentifikatsiyasi, avtorizatsiyasi va maxfiyligi

Smart Home qurilmalarining ko'pchiligida an'anaviy klaviatura yoki ekran mavjud emasligi sababli oddiy

login-parol modeli har doim ham qulay emas. Shu sababli biometrik xususiyatlar, kalit kelishuvi, protokol asosidagi autentifikatsiya, gateway orqali autentifikatsiya va boshqa yengil mexanizmlar tadqiq qilingan [1].

Qurilma avtorizatsiyasida bir nechta Device Management Channel mavjud bo'lishi va ularning xavfsizlik siyosatlari bir xil bo'lmasligi xavf tug'diradi. CGuard kabi yondashuvlar turli boshqaruv kanallarining kirish huquqlarini qurilmaning mantiqiy boshqaruv qatlami orqali muvofiqlashtirishga qaratilgan [1]. Maxfiylikni himoyalashda esa surveillance camera, gateway va boshqa qurilmalar alohida xavfsizlik talablarini yuzaga keltiradi.

Smart Home xavfsizlik muammolarining uch qatlamli ko'lami

Platforma xavfsizligi	Autentifikatsiya	Avtorizatsiya	Maxfiylik
Qurilma xavfsizligi	Firmware	Sensorlar	Side-channel
Kommunikatsiya xavfsizligi	Wi-Fi	BLE/BT	Zigbee/MQTT

2-rasm. Smart Home xavfsizlik muammolarining uch qatlamli ko'lami (manbadagi tasnif asosida).

Kommunikatsiya xavfsizligi

Kommunikatsiya Smart Home tizimining barcha komponentlarini bog'lovchi qatlam bo'lib, Zigbee, BLE, Bluetooth, Wi-Fi va MQTT kabi protokollar turli vazifalarni bajaradi.



Biroq protokollarning dizayn yoki amalga oshirishdagi zaifliklari hujumchiga qurilmalarni kuzatish, ma'lumotni olish yoki boshqaruvni egallash imkonini berishi mumkin [1].

2-jadval.

Smart Home kommunikatsiya protokollari va ularga xos xavfsizlik muammolari

Protokol/kanal	Manbada qayd etilgan xavf	Asosiy himoya yo'nalishi
Zigbee	Firmware yangilanishidagi umumiy va oson buziladigan kalit; worm hujumi xavfi	Firmware yangilanishi va kalit boshqaruvini kuchaytirish
BLE	UUID orqali qurilmani aniqlash; secure connection talabining yetarli emasligi	O'zaro autentifikatsiya va xavfsiz ulanish rejimi
Bluetooth	Qurilma manzilini kuzatish orqali foydalanuvchini tracking qilish	Anonimlikni kuchaytirish va standartni takomillashtirish
Wi-Fi	Radio signallari orqali harakat va faoliyatni aniqlash	Trafikni maskalash/obfuscation va maxfiylikni himoyalash
MQTT	Autentifikatsiya va avtorizatsiyaning yetarli emasligi; DoS va ruxsatsiz buyruqlar	Kirish modeli, autentifikatsiya va vakolatlarni qat'iy boshqarish

Kommunikatsiya oqimini tahlil qilish

Tarmoq trafigi qurilma, foydalanuvchi va ilova faoliyati haqida bilvosita ma'lumot beradi. Manbada trafik xususiyatlari orqali qurilmalarni tasniflash, foydalanuvchi xatti-harakatlarini aniqlash va hatto fizik muhitga kirish bilan bog'liq xavflarni tahlil qiluvchi tadqiqotlar keltirilgan. Paket darajasidagi hodisa imzolarini avtomatik ajratish va broadcast/multicast trafikdan qurilmani aniqlash kabi usullar ma'lumotlarga asoslangan xavfsizlik

tahlilining istiqbolli yo'nalishi sifatida ko'rsatilgan.

Tahdid va himoya mosligi

Manbadagi tadqiqotlarni birlashtirish natijasida Smart Home xavfsizligida bitta universal himoya mexanizmi yetarli emasligi ko'rinadi. Platforma darajasida kod va ruxsatlar tahlili, qurilma darajasida firmware va sensor xatti-harakatlarini tekshirish, kommunikatsiya darajasida esa protokol va trafik tahlili birgalikda qo'llanishi zarur.

3-jadval.



Smart Home tahdidlari va ularni aniqlash hamda himoyalash yondashuvlari

Tahdid	Ta'sir qiluvchi qatlam	Aniqlash/himoya yondashuvi
Zararli avtomatlashtirish ilovasi	Platforma	Ilova auditi, statik tahlil, xatti-harakat monitoringi
Qoida konfliktlari	Platforma	NLP, statik/dinamik grafik tahlil, FSM
Soxta foydalanuvchi/ovozli buyruq	Platforma	Biometrik va signalga asoslangan autentifikatsiya
Ortiqcha vakolat	Platforma/qurilma	Kontekstga sezgir avtorizatsiya, access control
Firmware zaifligi	Qurilma	Fuzzing, symbolic execution, binary analysis
Sensorni aldash	Qurilma	Sensor ketma-ketligi va fizik muhitga asoslangan anomaly detection
Side-channel hujumi	Qurilma	Signal xususiyatlarini tahlil qilish, foydalanuvchi xabardorligi
Protokol zaifligi	Kommunikatsiya	Protokolni standartlashtirish, secure mode, autentifikatsiya
Trafik orqali maxfiylik buzilishi	Kommunikatsiya	Trafik xususiyatlarini tahlil qilish va maxfiylikni himoyalash

Xavflarning ildiz sabablari

Manbada Smart Home xavfsizligining tizimli sabablarini to'rtta asosiy guruhga ajratadi. Birinchisi — heterojenlik. Smart Home tizimida Wi-Fi, Bluetooth, Zigbee, Z-Wave kabi turli protokollar, cloud/mobile/third-party boshqaruv usullari, MQTT/OAuth/HTTP(S) kabi application-layer protokollar, turli autentifikatsiya va access-control mexanizmlari birgalikda

ishlaydi. Bu esa yagona himoya siyosatini joriy etishni murakkablashtiradi [1].

Ikkinchi sabab — customization, ya'ni mavjud yoki eski protokollarning Smart Home uchun maxsus moslashtirilishi. Bunday o'zgartirishlar har doim ham yetarli darajadagi xavfsizlik tahlilidan o'tmasligi mumkin. Uchinchi sabab — mas'uliyat chegaralarining noaniqligi: foydalanuvchi, ishlab chiqaruvchi, cloud provider va protokol



tashkilotchilari o'rtasidagi vazifalar aniq belgilanmagan bo'lsa, xavfsizlik nazorati bo'sh qolishi mumkin. To'rtinchi sabab — standartlashtirishning yetishmasligi; turli platformalar o'rtasidagi integratsiya yangi xavflarni yuzaga keltirishi mumkin [1].

Kelajakdagi tadqiqot yo'nalishlari

Manba uchta asosiy istiqbolli yo'nalishni ajratadi: avtomatlashtirilgan zaifliklarni aniqlash, qat'iy xavfsizlik tekshiruvlari va ma'lumotlarga asoslangan tahlil [1]. Avtomatlashtirishning maqsadi turli qurilma va platformalar uchun qo'lda xavfsizlik qoidalarini kiritish zaruratini kamaytirish hamda keng ko'lamda ishlay oladigan umumiy usullarni yaratishdir.

Qat'iy xavfsizlik tekshiruvlarida formal verification, fuzzing va differential testing kabi usullarni chuqurroq qo'llash

taklif qilinadi. Ayniqsa, Smart Home ekotizimini FSM sifatida modellashtirish va model checking imkoniyatlari kelajakdagi izlanishlar uchun muhim deb ko'rsatilgan [1].

Ma'lumotlarga asoslangan tahlil esa tizim loglari, qurilma holati, sensor ma'lumotlari va tarmoq trafikidan foydalanadi. Bunday ma'lumotlar anomal xatti-harakatlarni aniqlash, qurilma faoliyatini tasniflash va zararli hodisaning ildiz sababini tahlil qilish uchun ishlatilishi mumkin [1]. Shu jihatdan Smart Home xavfsizligi kelajakda faqat oldindan belgilangan qoidalar bilan emas, balki tizimdan hosil bo'ladigan ma'lumotlarning o'zidan ham foydalanadigan adaptiv tahlilga tomon rivojlanishi mumkin.

Tahliliy integratsiya modeli (manbadagi yo'nalishlar sintezi)



loglar • qurilma holati • sensorlar • tarmoq trafiklari • platforma hodisalari

3-rasm. Manbada ko'rsatilgan istiqbolli yo'nalishlarni yagona tahliliy jarayonda birlashtirish konsepsiyasi.

Muhokama

O'rganilgan manba Smart Home xavfsizligini alohida qurilma yoki protokol muammosi sifatida emas, balki

o'zaro bog'langan ekotizim sifatida ko'rishga imkon beradi. Masalan, firmware zaifligi qurilma boshqaruviga



olib kelishi, qurilma esa gateway yoki cloud platforma bilan bog'langan bo'lsa, keyingi qatlamlarga ta'sir ko'rsatishi mumkin. Shu sababli xavfsizlik siyosati qatlamlararo bo'lishi kerak.

Tahlil shuni ko'rsatadiki, platforma xavfsizligidagi muammolar ko'proq dasturiy abstraksiyalar, avtomatlashtirish qoidalari va ruxsatlar bilan bog'liq; qurilma xavfsizligida firmware, sensorlar va fizik muhit bilan bog'liq xavflar ustun; kommunikatsiya xavfsizligida esa protokol dizayni va trafikdan hosil bo'ladigan bilvosita ma'lumotlar muhim ahamiyat kasb etadi. Bu uch qatlam bir-biridan mustaqil emas, balki yagona hujum zanjirining ketma-ket bosqichlari bo'lishi mumkin.

Shu bilan birga, manbada keltirilgan ko'plab himoya mexanizmlari muayyan platforma yoki qurilma uchun ishlab chiqilgan. Ayrim usullar yuqori hisoblash resursini talab qiladi, ayrimlari qo'lda xavfsizlik siyosatini kiritishni talab etadi, ayrimlari esa faqat bitta foydalanuvchi yoki ma'lum turdagi qurilmalar uchun mos keladi [1]. Demak, umumlashtiriladigan, heterojen muhitda ishlaydigan va ma'lumotlardan foydalanib xavfni aniqlay oladigan yondashuvlarni ishlab chiqish ilmiy jihatdan muhim vazifa bo'lib qolmoqda.

Ushbu maqolada 3-rasmda berilgan integratsion sxema alohida yangi eksperimental algoritmi sifatida emas, balki manbada ko'rsatilgan uch istiqbolli yo'nalishni — avtomatlashtirilgan zaifliklarni aniqlash, qat'iy tekshiruv va data-driven analysis — bitta tahliliy

jarayonda ifodalovchi konseptual sintez sifatida qaraladi. Uni amaliy modelga aylantirish uchun real Smart Home trafiklari, qurilma loglari va tajriba stendi asosida alohida eksperimental tadqiqot talab etiladi.

Xulosa

Maqolada Smart Home IoT tizimlarining axborot xavfsizligi bo'yicha ilmiy survey asosida tizimli tahlil amalga oshirildi. Smart Home arxitekturasini smart qurilmalar, gateway, cloud platforma, kommunikatsiya kanallari va foydalanuvchidan tashkil topgan o'zaro bog'langan ekotizim sifatida ko'rib chiqildi. Xavfsizlik masalalari platforma, qurilma va kommunikatsiya qatlamlari bo'yicha guruhlandi.

Platforma qatlamida dasturlash va avtomatlashtirish, ilovalararo bog'lanish, autentifikatsiya, avtorizatsiya, ovozli yordamchilar va maxfiylik muammolari; qurilma qatlamida firmware zaifliklari, sensorlararo bog'lanish, side-channel hujumlari, autentifikatsiya, avtorizatsiya va maxfiylik; kommunikatsiya qatlamida esa Zigbee, BLE, Bluetooth, Wi-Fi va MQTT xavflari aniqlandi. Har bir yo'nalish bo'yicha mavjud himoya mexanizmlari va ularning cheklovlari umumlashtirildi.

Tizimli nuqtai nazardan Smart Home xavfsizlik muammolarining asosiy ildiz sabablari heterojen komponentlar, maxsus moslashtirilgan yechimlar, mas'uliyat chegaralarining noaniqligi va yagona standartlashtirishning yetishmasligi bilan bog'liq. Kelajakdagi tadqiqotlarda avtomatlashtirilgan zaifliklarni aniqlash,



formal va qat'iy xavfsizlik tekshiruvlari, fuzzing va differential testing, shuningdek loglar, sensor ma'lumotlari va tarmoq trafiklariga asoslangan data-driven tahlilni rivojlantirish muhimdir.

Natijada Smart Home xavfsizligini faqat alohida qurilmani himoyalash orqali emas, balki platforma–qurilma–

kommunikatsiya o'zaro ta'sirini birgalikda nazorat qiladigan qatlamlararo yondashuv orqali ta'minlash zarurligi asoslandi. Mazkur xulosa kelgusida intellektual aniqlash va adaptiv himoyalash modelini ishlab chiqish uchun nazariy asos bo'lib xizmat qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. B. Yuan, J. Wan, Y.-H. Wu, D.-Q. Zou, H. Jin. On the Security of Smart Home Systems: A Survey. *Journal of Computer Science and Technology*, 2023, 38(2): 228–247. DOI: 10.1007/s11390-023-2488-3.
2. P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, P. H. Ha. Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security*, 2017, 12(4): 968–979. DOI: 10.1109/TIFS.2016.2647225.
3. M. Antonakakis et al. Understanding the Mirai Botnet. In: *Proc. 26th USENIX Security Symposium*, 2017, pp. 1093–1110.
4. E. Fernandes, J. Jung, A. Prakash. Security Analysis of Emerging Smart Home Applications. *IEEE Symposium on Security and Privacy*, 2016, pp. 636–654. DOI: 10.1109/SP.2016.44.
5. N. Zhang et al. Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. *IEEE Symposium on Security and Privacy*, 2019, pp. 1381–1396. DOI: 10.1109/SP.2019.00016.
6. Y. D. Dong, Y. D. Yao. Secure mmWave-Radar-Based Speaker Verification for IoT Smart Home. *IEEE Internet of Things Journal*, 2021, 8(5): 3500–3511. DOI: 10.1109/JIOT.2020.3023105.
7. C. Celik et al. IOTGUARD: Dynamic analysis and policy enforcement for IoT applications. Mazkur manbada Smart Home avtomatlashtirish xavfsizligi kontekstida tahlil qilingan.
8. F. Shoshitaishvili et al. Firmalice: Automatic Detection of Authentication Bypass Vulnerabilities in Firmware. Mazkur manbada firmware xavfsizligi bo'yicha usul sifatida tahlil qilingan.
9. National Institute of Standards and Technology. Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.
10. W3C. PROV-DM: The PROV Data Model. W3C Recommendation, 2013.