VIDEO KUZATUV TIZIMLARIDA QO‘LLANILADIGAN XAVFSIZ ALOQA PROTOKOLLARI

Xudoykulov Zarif Turakulovich,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, “Kriptologiya” kafedrasi mudiri, Phd.,dotsent, Toshkent, O‘zbekiston
e-mail: zarif.khudoykulov@tuit.uz

Qozoqova To‘xtajon Qaxramon qizi,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, “Kriptologiya” kafedrasi assistenti, Toshkent, O‘zbekiston
e.mail: qozoqovat1516@gmail.com

Annotatsiya. Ushbu maqola zamonaviy video kuzatuv tizimlarida qo‘llaniladigan asosiy xavfsiz aloqa protokollari TLS/HTTPS, SRTP va ONVIF Securityning arxitekturasi, ishlash mexanizmlari va amaliy samaradorligini tahlil qiladi. IP-kamera, NVR/DVR, mobil mijozlar va bulutli video boshqaruv tizimlari o‘rtasidagi muloqot jarayonida ma’lumot maxfiyligi, butunligi va autentifikatsiyasini ta’minlashning texnik asoslari ko‘rib chiqiladi. Protokollarning kriptografik algoritmlari, seans boshqaruvi, kalit almashinuvi, resurs talabchanligi va potentsial zaifliklari batafsil yoritiladi.

Kalit so‘zlar: Video kuzatuv tizimlari, IP-kamera xavfsizligi, TLS, HTTPS, SRTP, ONVIF Security, kriptografik protokollar, IoT xavfsizligi.

Kirish. Bugungi kunda video kuzatuv tizimlari keng qo‘llanilmoqda. Ular nafaqat an’anaviy obyektlarni kuzatishda, balki transportlarini boshqarish, “aqlli shahar” tizimlari faoliyati, sanoat jarayonlarini avtomatlashtirish, IoT qurilmalarini integratsiya qilish, logistika va energetika tarmoqlarida xavfsizlikni ta’minlash kabi murakkab vazifalarni ham bajaradi. Ushbu tizimlarda IP-kameralar asosiy ro‘lni o‘ynaydi. Ularning soni yildan yilga oshib bormoqda, bu esa real vaqt video oqimlarining ochiq tarmoqlar bo‘ylab uzatilishi bilan bog‘liq xavfsizlik muammolarini keskin kuchaytirmoqda [1]. Zamonaviy tadqiqotlar tarmoqqa ulanadigan kameralar sonining ko‘payishi bilan bog‘liq tahdidlar miqdoriy va sifat jihatidan o‘sayotganini tasdiqlaydi. Statistik ma’lumotlaraga qaraganda Turli xavfsizlik laboratoriyalari o‘tkazgan testlar shuni ko‘rsatadiki, himoyasi sust yoki noto‘g‘ri konfiguratsiya qilingan IP-kamera MITM (Man-in-the-Middle), parollarni ushlab qolish, RTSP (Real-Time Streaming Protocol) sessiyalarini o‘g‘irlash, ONVIF (Open Network Video Interface Forum) interfeysining ekspluatatsiyasi va IoT botnetlarga qo‘shib yuborish kabi hujumlarga yuqumli bo‘ladi. Statistik baholashga ko‘ra, bunday qurilmalarda zaifliklar mavjud bo‘lsa, hujum ehtimoli 70 % dan oshadi va tarmoqdagi har bir qo‘shimcha kamera tizimning umumiy xavfsizligini yanada zaiflashtirishi mumkin [2].

Video kuzatuv tizimlarida xavfsizlik talablarini uch asosiy qatlam tashkil etadi. Birinchisi maxfiylik, ya’ni oqimni uchinchi tomon tomonidan o‘qilishi yoki tahlil qilinishini imkonsiz holga keltirish. Ikkinchi qatlam butunlik, bunda tarmoqqa yuborilgan video paketlar o‘zgartirilmagan holatda yetib borishi, paketlar ichida o‘zgarish bo‘lsa, u darhol aniqlanishi lozim. Uchinchi qatlam autentifikatsiya, ya’ni kamera, NVR, VMS, mobil mijoz yoki bulut platformasi bir-birini ishonchli identifikatsiya qilishi, yolg‘on manbalarning ulanishi rad etilishi kerak.

Mazkur talablarga mos kelish uchun amaliyotda uch turdagi asosiy xavfsiz aloqa protokollari qo‘llaniladi. TLS/HTTPS kamera konfiguratsiyasini boshqarish, API chaqiriqlarini bajarish, foydalanuvchi autentifikatsiyasi va bulut serverlari bilan xavfsiz seanslar yaratishda markaziy ahamiyatga ega. SRTP (Secure Real-Time Transport

Protocol) esa real vaqt video va audio oqimlarini minimal kechikish bilan shifrlashga mo‘ljallangan bo‘lib, aynan media oqimlarini himoya qilishda eng samarali texnologiya hisoblanadi. ONVIF Security esa turli ishlab chiqaruvchilarning IP-kameralarini yagona xavfsizlik standartiga muvofiqlashtirib, IoT mo‘ljallangan yengil kriptografik mexanizmlar bilan ta’minlaydi.

Ushbu ilmiy maqolaning maqsadi yuqoridagi protokollarni chuqur texnik jihatdan tahlil qilish, ularning amaliy arxitekturadagi o‘rni, kriptografik xususiyatlari, ishlash samaradorligi, resurs talablari, zaifliklari va qo‘llash, ilmiy asoslarda baholashdan iborat. Real tarmoq sharoitlarida protokollarning xavfsizlikka qo‘shayotgan hissasini, ularning integratsiyasi orqali kompleks himoya modelini shakllantirish imkoniyatlarini ko‘rsatish ham ushbu tadqiqotning asosiy vazifalaridan biridir. Tahlillar natijasida barcha uch protokolning kuchli va zaif tomonlari ochib beriladi.

Adabiyotlar tahlili va metodologiya. So‘nggi yillarda video kuzatuv tizimlari xavfsizligi bo‘yicha olib borilgan ilmiy tadqiqotlar bir qancha va ular asosiy ilmiy yo‘nalishni shakllantirgan. Ushbu yo‘nalishlar asosan kriptografik takomillashtirish, IoT arxitekturalarida resurs tejovchi xavfsizlik mexanizmlarini ishlab chiqish, real vaqt oqimlarining samarali himoyasini ta’minlash va video tarmoqlaridagi standartlashtirish masalalariga qaratilgan.

TLS/HTTPS bo‘yicha tadqiqotlar asosan IoT qurilmalarida sertifikatlarni boshqarish, TLS handshake jarayonining optimallashtirilishi va yengil kriptografik algoritmlarni qo‘llash masalalariga e’tibor qaratadi. D. Evans va boshqa tadqiqotchilar[3] yengil IoT platformalarida TLS 1.3 dan foydalanish qurilma resurslariga sezilarli yuklama keltirishini, shuning uchun ECDHE asosidagi kalit almashinuvi va ChaCha20 kabi yengilroq shifrlash algoritmlariga o‘tish zarurligini qayd etadi. M. Krotofil tomonidan o‘tkazilgan tahlillar ko‘pchilik arzon IP-kameralar hali ham TLS 1.0–1.1 kabi eskirgan protokollardan foydalanishini, bu esa MITM va boshqa hujumlardan himoyani buzilishini ko‘rsatadi. Zamonaviy tadqiqotlar IoT kameralarida sertifikatlarni avtomatik yangilash mexanizmlarini joriy etish va zero-trust modeliga moslashtirilgan TLS profilini ishlab chiqish zarurligini ta’kidlaydi [4].

SRTP bo‘yicha ilmiy ishlanmalar real vaqt oqimlarining shifrlanishi jarayonida kechikishni minimal darajada ushlab qolish va AES-GCM algoritmining samaradorligini baholashga qaratilgan. J. Rosenberg SRTPning RTP protokoli bilan mosligi va AEAD (Authenticated Encryption with Associated Data) ishlatilishi tufayli video paketlarning butunligi va maxfiyligini bir vaqtning o‘zida ta’minlash imkonini beradi deb ta’kidlaydi o‘z maqolasida[5]. M. Fischer o‘z tadqiqotlarida AES-GCM algoritmining apparat darajasida tezlashtirilishi (hardware acceleration) real tarmoqlarda SRTP protokolining deyarli kechikishsiz ishlashini ta’minlashini ko‘rsatadi. Shuningdek, DTLS-SRTP asosidagi kalit almashinuvi mexanizmlarining ishonchliligi, ZRTP kabi markazlashmagan kalit kelishuv protokollarining afzalliklari hamda WebRTC tizimlarida SRTPning ustun jihatlari chuqur tahlil qilingan. Ko‘plab tadqiqotchilar SRTPning minimal kechikish, past resurs iste’moli va AEAD (Authenticated Encryption with Associated Data) usullaridan foydalanishi tufayli video kuzatuv tizimlari uchun eng maqbul media shifrlash texnologiyasi ekanini ta’kidlaydi[6].

ONVIF Security bo‘yicha ilmiy ishlanmalar esa texnik standartlashtirish va IoT kameralar o‘rtasida xavfsizlikni uyg‘unlashtirishga qaratilgan. T. Furuya (2021) tomonidan olib borilgan tadqiqotlar ONVIFning WS-UsernameToken orqali foydalanuvchilarni xavfsiz autentifikatsiya qilish, nonce/timestamp mexanizmlari orqali replay hujumlaridan himoyalanish va TLS-PSK (pre-shared key) asosida yengil xavfsizlik profillarini yaratishdagi ustunliklarini yoritadi. 2022–2024 yillardagi ONVIF texnik hisobotlari ECC (Elliptic Curve Cryptography) asosida yengil qurilmalarda samarali ishlovchi kriptografik profil yaratilganini, SRTP bilan integratsiya qilingan xavfsiz media yo‘llari taklif etilganini ko‘rsatadi. Zamonaviy tadqiqotlar ONVIF Securityni IoT kameralarining global standartini shakllantiruvchi mexanizm sifatida baholaydi va uning

afzalliklari video tarmoq infratuzilmasida xavfsizlikni soddalashtirishini ta’kidlaydi.

Umuman olganda, ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, TLS/HTTPS boshqaruv va autentifikatsiya bosqichida, SRTP media oqimlarini real vaqt rejimida himoyalashda, ONVIF Security esa IoT kameralar uchun integratsiyalashgan va yengil xavfsizlik qatlamini yaratishda markaziy rol o‘ynaydi. Ammo adabiyotlarda ushbu uch protokolning yagona arxitektura doirasida birgalikda qo‘llanish samaradorligi yetarli darajada o‘rganilmagan. Mazkur tadqiqot ushbu ilmiy bo‘shliqni to‘ldirishga qaratilgan bo‘lib, protokollarning kompleks taqqoslanishi va real tarmoqlar uchun optimallashtirilgan xavfsizlik modelini taklif etadi.

Video kuzatuv tizimlarining ishlash jarayoni ko‘p qatlamli va murakkab tarmoq arxitekturasiga asoslanadi. IP-video tizimining barcha komponentlari kamera, NVR/DVR, bulutli video boshqaruv tizimi (VMS), mobil qurilmalari o‘zaro real vaqt rejimida ma’lumot almashadi. Ushbu almashinuv jarayonida media oqimlarining uzatilishi, boshqaruv buyruqlarining bajarilishi, autentifikatsiya va avtorizatsiya mexanizmlarining ishlashi xavfsizlik nuqtayi nazaridan strategik ahamiyatga ega. Arxitektura nuqtayi nazaridan IP-kamera tizimidagi muloqot uch asosiy yo‘nalishga bo‘linadi:

1. Kamera → NVR mahalliy LAN bu bosqichda kamera video oqimlarini NVR ga yuboradi, NVR esa uni yozib boradi yoki qayta ishlaydi. Aloqa asosan yopiq lokal tarmoqda amalga oshirilgani uchun tahdidlar nisbatan kamroq, mahalliy tarmoqning buzilishi, ARP spoofing, port mirroring yoki zaif parollar kabi omillar oqimni buzishga imkon yaratishi mumkin. Shu sababli bu qatlam uchun autentifikatsiya, oqim butunligi va kadrlar ketma-ketligini tekshirish kabi himoya choralarini qo‘llash zarur.
2. Kamera/NVR → Bulutli VMS video oqimlarining Internet orqali o‘tishi tahdid darajasini keskin oshiradi. Bu yerda MITM, seansni hijack qilish, DNS spoofing, paketlarni tahlil qilish, traffikni qayd qilish singari hujumlar ehtimoli yuqori. Shuning uchun bu qatlamda shifrlangan transport kanali TLS/HTTPS majburiy hisoblanadi. Shuningdek sertifikatlarni tekshirish, token asosidagi autentifikatsiya, bulutga ulanish uchun xavfsiz API chaqiriqlari kabi qo‘shimcha mexanizmlar talab etiladi. Bulutli VMS arxitekturasi ko‘pincha ko‘p foydalanuvchili muhit sifatida ishlaydi, bu esa xavfsizlikni yanada qat’iylashtirishni talab qiladi.

1-jadval. Arxitektura nuqtayi nazaridan IP-kamera tizimidagi aloqa turlari

Aloqa yo‘li	**Tahdid darajasi**	**Talab etiladigan xavfsizlik**
Kamera → NVR	O‘rta	Autentifikatsiya, oqim butunligi, kadrlar ketma-ketligi nazorati
NVR → Bulut	Yuqori	TLS shifrlash, sertifikatlar, token asosida autentifikatsiya
Mobil mijoz → Bulut	Juda yuqori	TLS, seans boshqaruvi, JWT, mijoz identifikatsiyasi

3. Mobil mijoz → Bulut → Kamera. Zamonaviy video kuzatuv tizimlarida video oqimning asosiy qismi mobil qurilmalar orqali ko‘riladi. Bu yo‘nalish xavf darajasi bo‘yicha eng yuqori qatlam hisoblanadi. Mobil qurilmalar ko‘pincha himoyalanmagan Wi-Fi tarmoqlariga ulanadi, ularda sertifikatlar to‘g‘ri boshqarilmagan bo‘lishi mumkin, shuningdek ilovalar orqali sessiya tokenlarini o‘g‘irlash keng tarqalgan. Shu sababli bu darajada TLS 1.2/1.3, seans boshqaruvi, JWT tokenlar bilan xavfsiz avtorizatsiya, mijoz qurilmasini identifikatsiya qilish kabi himoya qatlamlari talab qilinadi. 1-jadvalda uch daraja bo‘yicha tahdidlar va ularga mos xavfsizlik talablarini umumlashtirib beradi.

IP-video tizimida har bir aloqa yo‘nalishi o‘ziga xos tahdid bo‘lgani sababli, yagona universal protokol yordamida butun tizimni himoyalashning imkoni yo‘q. Shu bois amaliyotda ko‘p qatlamli xavfsizlik arxitekturasi qo‘llaniladi. Unda boshqaruv va

autentifikatsiya bosqichida TLS/HTTPS, media oqimlarini uzatishda SRTP, IoT kameralararo muvofiqlik va yengil xavfsizlikni ta’minlashda esa ONVIF Security protokoli birgalikda ishlatiladi. Bu yondashuv har bir qatlamni uning texnik xususiyatlariga mos eng samarali himoya mexanizmlari bilan ta’minlaydi va butun video kuzatuv tizimi uchun kompleks xavfsizlik muhitini shakllantiradi.

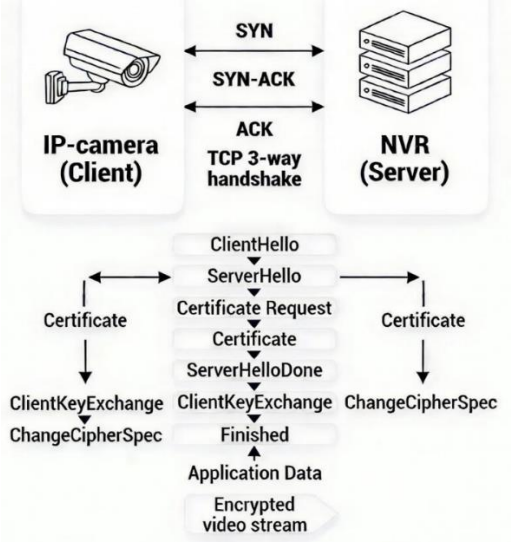
TLS (Transport Layer Security) kompyuter tarmoqlarida ikki tomon masalan, IP-kamera va server, yoki foydalanuvchi va video boshqaruv tizimi o‘rtasidagi aloqani xavfsiz qilish uchun mo‘ljallangan kriptografik protokoldir. U ma’lumotlarning maxfiyligini, yaxlitligini va autentifikatsiyasini ta’minlaydi. TLS HTTPSning asosini tashkil etadi va kuzatuv tizimlarida IP-kameralar, NVR/DVR qurilmalar, video boshqaruv dasturlari (VMS) va bulutli video xizmatlari parollar, video oqimlar, konfiguratsiya va boshqaruv buyruqlarini himoya qilish uchun muhim ahamiyatga ega. TLS siz aloqa ochiq matnda amalga oshiriladi, bu esa ma’lumotlarni osongina tinglash, o‘zgartirish yoki soxtalashtirish imkonini beradi.

TLS simmetrik va assimetrik kriptografiyani birlashtirib ishlaydi. Assimmetrik kriptografiya RSA yoki Elliptic Curve Diffie-Hellman ECDH/ECDSA handshake bosqichida kalit almashish uchun ishlatiladi va ikki tomon o‘rtasida umumiy sir yaratadi. Simmetrik kriptografiya AES-128-GCM, AES-256-GCM, ChaCha20-Poly1305 esa ma’lumotlarni tez shifrlash uchun qo‘llaniladi. GCM va Poly1305 AEAD (Authenticated Encryption with Associated Data) rejimida ishlaydi, ya’ni shifrlash va MAC (Message Authentication Code) bir vaqtda amalga oshiriladi. Hash funksiyalari sifatida SHA-256 va SHA-384 ishlatiladi MD5 va SHA-1 taqiqlangan. TLS 1.3da Perfect Forward Secrecy (PFS) majburiy bo‘lib, har bir sessiya uchun yangi ephemeral kalitlar (ECDHE) orqali eski sessiyalar uzoq muddatli kalit buzilgan taqdirda ham ochilmaydi.

Hozirgi standart – TLS 1.3. Uning handshake jarayoni oddiy va xavfsiz ClientHello da mijoz cipher suites, random nonce va ECDHE public keyini yuboradi. ServerHello da server tanlangan parametrlar va o‘z public keyini javob qaytaradi. Shared secret ECDHE orqali hisoblanadi keyingi qism shifrlanadi, server X.509 sertifikatini ECDSA yoki RSA imzoli yuboradi. Finished xabarlari transcript hash HMAC orqali yaxlitlikni tasdiqlaydi. Traffic keys HKDF orqali hosil bo‘ladi va barcha ma’lumotlar AEAD bilan shifrlanadi. TLS 1.3 eski zaifliklarni butunlay olib tashlagan va handshake qismini ko‘proq shifrlagan.

Kuzatuv tizimlarida TLS quyidagi komponentlarni himoya qiladi. Veb-interfeys va admin panelida HTTPS, 443-port login-parollar, konfiguratsiya o‘zgarishlari va jonli ko‘rish shifrlanadi AES-GCM + ECDHE + ECDSA. Bulutli ulanishlarda Hik-Connect, Dahua Easy4IP, Axis Companion HTTPS va WSS (WebSocket Secure) orqali doimiy tunnel yaratiladi. Video oqimlarda RTSP-over-TLS RTSP boshqaruv kanalini TLS bilan, RTP mediani SRTP bilan himoyalaydi; SRTP kalitlari DTLS-SRTP handshake orqali almashiladi. Brauzer orqali WebRTC ko‘rishda DTLS + SRTP (AES-GCM) end-to-end shifrlashni ta’minlaydi. ONVIF va API chaqiruvlari HTTPS orqali, ba’zan WS-Security bilan qo‘shimcha imzo qo‘shiladi. Proshivka yangilanishlari faqat HTTPS orqali amalga oshirilishi kerak, bu downgrade hujumlarining oldini oladi.

2025-yil holatiga ko‘ra, yuqori darajali brendlar Axis, Hanwha Wisenet, Bosch, Avigilon, Milestone faqat TLS 1.3, kuchli shifrlar, HSTS va haqiqiy sertifikatlarni qo‘llab-quvvatlaydi hamda RTSP-over-TLS ni taklif qiladi. O‘rtacha brendlar Hikvision, Dahua, Uniview yangi proshivkalarda TLS 1.2+ va bulut aloqalarini shifrlaydi, lekin RTSP ko‘pincha ochiq qoladi. Arzon va eski qurilmalar hali TLS 1.0/1.1 va zaif shifrlarni ishlatishi mumkin, bu esa jiddiy xavf tug‘diradi.

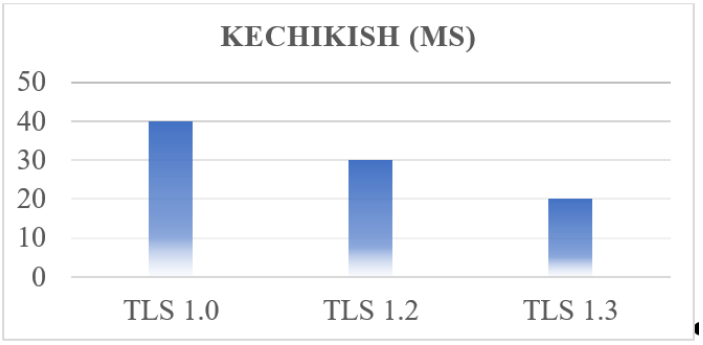


1-rasm. TLS protokolini ishlash jarayoni

TLS zaif bo‘lganda yuzaga keladigan xavflar parollarni ushlash, Man-in-the-Middle hujumlari soxta server/kamera, video intercept, replay attacks va masofaviy kod ijrosi. Eng yaxshi amaliyotlar faqat TLS 1.3ni majburiy qilish, haqiqiy sertifikatlardan foydalanish, HSTS yoqish, RTSP-over-TLS yoki WebRTCni afzal ko‘rish, kamera tarmog‘ini VLAN bilan izolyatsiya qilish va proshivkani muntazam yangilash.

- CPU bo‘yicha yuklanish 15–25 foiz oshadi. Ayniqsa, ARM Cortex-A7/A53 kabi past quvvatli protsessorlarda TLS seanslarini boshqarish qo‘shimcha resurs iste’mol qiladi.
- TLS handshake har safar 20–40 ms kechikish qo‘shadi. Bu ko‘p ulanuvchi mobil mijozlar mavjud bo‘lgan tizimlarda sezilarli kechikish keltirib chiqarishi mumkin.
- sertifikat boshqaruvi noto‘g‘ri bo‘lsa, MITM xavfi saqlanadi. Ko‘plab kameralar self-signed sertifikatlardan foydalanadi, bu esa foydalanuvchi tomonidan tasdiqlanmaguncha ishonchsiz hisoblanadi.

Quyidagi ASCII-grafik TLS versiyalarining o‘rtacha kechikishini taqqoslaydi:



2-rasm. TLS protokoli versiyalarini o‘rtacha kechikish grafigi

SRTP protokoli Secure Real-Time Transport Protocol (SRTP) real vaqt multimedia oqimlarini himoyalash uchun ishlab chiqilgan yengil, ammo samarali kriptografik protokoldir. U an’anaviy RTP paket formatidan foydalanadi, lekin unga shifrlash, autentifikatsiya va butunlikni tekshirish imkoniyatlarini qo‘shadi. SRTPning asosiy ustunligi shundaki, u video yoki audio oqimiga sezilarli kechikish qo‘shmasdan xavfsizlikni ta’minlaydi, bu esa uni video kuzatuv tizimlari uchun ideal yechimga aylantiradi. IP-kameralardan NVR yoki bulutli VMS ga yuboriladigan oqimlar ko‘proq RTP/RTSP formatidan foydalanadi, shu sababli SRTP bu arxitektura bilan tabiiy mos keladi. SRTPning asosiy vazifalariga quyidagilar kiradi oqim maxfiyligi, paketlar butunligini tekshirish, kalitlarning xavfsiz boshqaruvi, paketlar takrorlanishiga qarshi himoya va audio-video oqim uzluksizligini ta’minlash.

SRTPda AES-CTR rejimi minimal hisoblash xarajatlari talab qiladi, shu bois resursi cheklangan IoT kameralar uchun juda mos keladi. AES-GCM esa AEAD (Authenticated Encryption with Associated Data) mexanizmini qo‘llashi sababli shifrlash va autentifikatsiyani bitta operatsiyada bajaradi va bu xavfsizlikni oshiradi.

HMAC-SHA1 SRTPning ilk standartlarida keng qo‘llangan bo‘lsa-da, bugungi kunda GCM MAC yanada himoyalangan variant sifatida tavsiya qilinadi.

2-jadval. SRTP protokolining kriptografik komponentlar

Funksiya	Mexanizm	Tarif
Shifrlash	AES-CTR yoki AES-GCM	AES-CTR past yuklanishga ega, AES-GCM esa AEAD xususiyati bilan yuqori xavfsizlik ta’minlaydi
Autentifikatsiya	HMAC-SHA1 yoki GCM MAC	Paketlar soxtalashtirilmaganini tekshiradi
Replay-himoya	Sequence number monitoring	Paketlarni takror yuborish orqali oqimni buzishning oldini oladi
Kalit almashinuvi	SDES, ZRTP, DTLS-SRTP	Sessiya kalitlarini xavfsiz ishlab chiqish uchun ishlatiladi

Anti-replay mexanizmi har bir RTP paketiga beriladigan sequence number orqali amalga oshiriladi. Bu raqamlar ketma-ketligi buzilgan hollarda SRTP paketni rad etadi. Kalit almashinuvi SRTPning eng muhim jihatlaridan biri bo‘lib, quyidagi usullar mavjud:

- SDES (Session Description Protocol Security) eng oddiy, ammo eng zaif usul
- ZRTP markazlashmagan kalit kelishuvi, MITM hujumlariga chidamli
- DTLS-SRTP TLSning datagram versiyasi orqali xavfsiz kalit kelishuvi, WebRTC arxitekturasining asosiy komponenti.

SRTPning asosiy ustunligi past kechikish. Tajribalar shuni ko‘rsatadiki, SRTP qo‘shilganda video oqimning umumiy kechikishi odatda 1–3 ms dan oshmaydi. Bu real vaqt video kuzatuv tizimlari uchun juda muhim.

Cheklovlar. SRTP bir nechta afzalliklarga ega bo‘lsada, amaliyotda bir qator cheklovlar aniqlangan:

- SDES orqali kalit almashinuvi zaif. SDES mexanizmi kalitlarni SDP orqali ochiq tarzda uzatishi mumkin, bu esa MITM xurujiga oson imkon yaratadi. Ko‘plab arzon kameralar hali ham SDESdan foydalanadi.
- avtomatik key rotation kalitlarni yangilash har doim qo‘llanilmaydi. Agar kalitlar uzoq muddat davomida qayta ishlatilsa, oqimga maxfiy hujumlar ehtimoli ortadi. Ba’zi kamera firmwarelari SRTP kalitlarini qayta yuklash qilmaguncha o‘zgartirmaydi. SRTP faqat media oqimlari uchun mo‘ljallangan. Ya’ni u boshqaruv buyruqlarini, konfiguratsiya operatsiyalarini yoki autentifikatsiyani qamrab olmaydi. Shu sababli SRTP odatda TLS bilan biriktirib ishlatiladi.
- qo‘shimcha xavfsizlik modullari kamerada apparat akseleratsiyasi bo‘lmasa sekinlashishi mumkin. Ayniqsa AES-GCM kichik IoT chiplarida sekinroq ishlashi mumkin. Shunga qaramay, SRTP video oqimini himoya qilish uchun mavjud variantlarning eng samaralisi bo‘lib qolmoqda. Uning yengil kriptografik dizayni uni real vaqt tizimlarida qo‘llash uchun optimal qiladi.

ONVIF (Open Network Video Interface Forum) — IP-kameralar va video kuzatuv tizimlari uchun dunyo miqyosida eng keng qo‘llaniladigan interoperabilite standarti bo‘lib, u turli ishlab chiqaruvchilar qurilmalarining bir-biriga mos ishlashini ta’minlaydi. ONVIFning asosiy maqsadi video kuzatuv infratuzilmasida yagona texnik til yaratish, kamera konfiguratsiyasi, media oqim uzatish va boshqaruv buyruqlarini standartlashtirishdir. ONVIFning so‘nggi spetsifikatsiyalarida xavfsizlik bo‘yicha kuchaytirilgan talablar joriy etilib, ular ONVIF Security Profile nomi bilan ajratib ko‘rsatilgan. ONVIF Security arxitekturasi boshqaruv, media oqim, autentifikatsiya va qurilmalarni identifikatsiya qilish operatsiyalarini to‘liq himoyalashga qaratilgan. U TLS, SRTP, nonce/timestamp bazasidagi replay-himoya va token asosida xavfsiz avtorizatsiya kabi zamonaviy protokollarning eng muvaffaqiyatli elementlarini o‘zida mujassam qiladi.

Asosiy mexanizmlar. ONVIF Security quyidagi mexanizmlar majmui orqali kamera va boshqaruv tizimlari o‘rtasida xavfsiz almashinuvni ta’minlaydi:

- TLS bilan boshqaruv himoyasi. ONVIFning boshqaruv interfeyslarida SOAP/REST API, qurilmani sozlash, media profillarini boshqarish TLS 1.2/1.3 protokoli qo‘llaniladi. Bu kameraning konfiguratsiya parametrlari, foydalanuvchi ma’lumotlari va autentifikatsiya tokenlarini MITM yoki paket sniffing orqali egallab olishning oldini oladi;
- SRTP bilan media shifrlash. ONVIF media profili SRTPni standart mexanizm sifatida qabul qilgan. Bu real vaqt video va audio oqimini kam kechikish bilan shifrlash imkonini beradi. Bu bilan media oqimi boshqaruv kanalidan mustaqil tarzda himoyalanadi;
- DAT (Device Authentication Token) bu ONVIF tomonidan taklif etilgan yengil autentifikatsiya modeli bo‘lib, kamera va server o‘rtasida xavfsiz token almashinuvi orqali o‘zaro identifikatsiya amalga oshiriladi. DAT IoT uchun moslashgan bo‘lib, murakkab sertifikat boshqaruviga ehtiyoj kamayadi;

WS-UsernameToken hashing. ONVIF SOAP protokoli asosida ishlaydi, shuning uchun WS-UsernameToken mexanizmi orqali foydalanuvchi parollari hashlangan ko‘rinishda uzatiladi. Hashga qo‘shimcha nonce va timestamp qo‘shilishi replay hujumlarini istisno qiladi. Nonce + timestamp asosida replay-himoya. Har bir boshqaruv so‘rovida nonce qiymati yaratiladi va vaqt belgisi qo‘shiladi. Shu orqali eski so‘rovlarni takror yuborish orqali tizimni aldash ehtimoli to‘liq bartaraf qilinadi. Ushbu mexanizmlar birgalikda ONVIFni nafaqat funksional jihatdan, balki xavfsizlik nuqtayi nazaridan ham universal standartga aylantiradi.

IoT uchun optimallashtirish ONVIF Security IoT muhitining texnik cheklovlarini hisobga olgan holda yaratilgan. IP-kameralarning aksariyati past quvvatli ARM yoki MIPS arxitekturasidagi chiplar bilan jihozlangan bo‘lib, ular murakkab kriptografik operatsiyalarni bajarishda cheklangan.

Shuning uchun ONVIF quyidagi yechimlarni taklif etadi:

- resursi kam mikrokontrollerlarda ishlash imkoniyati. ONVIF protokollari juda yengil va samarali bo‘lib, hatto 128–256 MB RAMga ega bo‘lgan IoT kameralarida ham ishlashi mumkin;

-TLS-PSK, ECC, AES-GCM qo‘llanadi. Bu yengil kriptoalgoritmlar IoT ga moslashgan. TLS-PSK sertifikatlarga ehtiyoj yo‘q, oldindan kelishilgan kalit asosida autentifikatsiya. ECC (Elliptic Curve Cryptography) RSA ga qaraganda 5–10 baravar yengil. AES-GCM authentikatsiyalangan shifrlashni bitta operatsiyada bajaradi. Bu algoritmlar kam resurs talab qiladi va yuqori tezlikni ta’minlaydi. Keng qo‘llanish Hikvision, Dahua, Axis va boshqalar. Deyarli barcha yirik kamera ishlab chiqaruvchilar ONVIF xavfsizlikni qo‘llab-quvvatlaydi. Bu esa turli brendlar o‘rtasida xavfsizlik mosligini kafolatlaydi. 3-jadvalda video kuzatuv tizimlarida eng ko‘p qo‘llaniladigan uchta asosiy xavfsizlik protokoli TLS/HTTPS, SRTP va ONVIF Security ning funksional va texnik jihatdan taqqoslanishini ko‘rsatadi.

3-jadval. Protokollarning funksional va texnik jihatdan taqqoslanishi

Xususiyat	**TLS/HTTPS**	**SRTP**	**ONVIF Security**
Maqsad	Boshqaruv, API, autentifikatsiya	Media shifrlash	IoT kamera xavfsizligi, integratsiya
Kechikish	O‘rta	Juda past	Past, IoT optimallashtirilgan
Shifrlash	AES-GCM, ChaCha20-Poly1305	AES-GCM yoki AES-CTR	AES-GCM, TLS-PSK, ECC
Avt. daraja	Yuqori	O‘rta	Yuqori (token + TLS + SRTP birlashgan)
Resurs talabi	Yuqori	Past	Past
Zaiflik	Sertifikat xatolari, MITM	SDES kalit almashinuvi zaif	Barcha kameralar birday to‘liq implement qilmaydi

Ushbu maqolada video kuzatuv tizimlarida qo‘llaniladigan TLS/HTTPS, SRTP va ONVIF Security protokollarining amaliy samaradorligi, kriptografik mustahkamligi va resurs talablarini baholashga qaratilgan kompleks yondashuv

qo‘llanildi. Metodologiya bir nechta o‘lchovlar, funksional testlar, xavfsizlik tahlillari va protokollar bo‘yicha taqqoslovchi auditdan iborat bo‘ldi. Quyida qo‘llangan metodlar batafsil bayon etiladi.

Kriptografik tahlil. Har bir protokolning xavfsizlik darajasini aniqlash uchun kriptografik audit o‘tkazildi. Audit quyidagilarni o‘z ichiga oldi:

- kalit almashinuvi algoritmlarining barqarorligi ECDHE, DTLS-SRTP, SDES, TLS-PSK;
- shifrlash sxemalarining mustahkamligi AES-GCM, AES-CTR, ChaCha20-Poly1305;
- autentifikatsiya metodlarining zaifliklari HMAC-SHA1, WS-UsernameToken, nonce va timestamp mexanizmi;
- Replay-himoya samaradorligi, MITM hujumiga chidamlilik;
- zaif konfiguratsiyalarni ekspluatatsiya qilish ehtimoli;

Audit asosan RFC standartlari, OWASP IoT xavfsizlik mezonlari va NIST kriptografiya tavsiyalari asosida olib borildi.

Tahdid modeli

Tadqiqot davomida protokollar quyidagi tahdidlar nuqtayi nazaridan baholandi. MITM (Man-in-the-Middle) o‘rtadagi uzatishni buzish va soxta sertifikat bilan ulanish urinishlari. Replay attacks eski paketlarni qayta jonlantirish orqali tizimni aldash imkoniyati. Spoofing kamera yoki mijoz qurilmasini qalbakilashtirish. Credential phishing autentifikatsiya ma’lumotlarini qo‘lga kiritish. IoT botnet risklari zaif qurilmalar botnetga qo‘shib olish uchun ekspluatatsiya qilinishi. Har bir tahdid senariysi bo‘yicha ehtimollik, hujum murakkabligi va zararning kutilgan darajasi baholandi. Baholashda STRIDE modeli elementlaridan ham foydalanildi.

Kompleks solishtirish

Kriptografik tahlil va tahdid modeli natijalari umumlashtirilib, protokollar quyidagi mezonlar asosida solishtiriladi. Xavfsizlik darajasi, kechikish, resurs iste’moli CPU/RAM, integratsiya qulayligi, IoT muhitida samaradorlik, zaifliklar ehtimoli. Natijalar jadval va ASCII grafiklar asosida vizual ravishda taqqoslandi. Bu yondashuv har bir protokolning real amaliy sharoitdagi ustunliklari va cheklovlarini aniq ko‘rsatishga yordam berdi.

Natija. Tadqiqot davomida uch xil turdagi IP-kameralar asosida TLS/HTTPS, SRTP va ONVIF Security protokollarining ishlash samaradorligi, kechikish darajasi, CPU yuklanishi va ularning amaliy qo‘llanish imkoniyatlari tahlil qilindi. O‘lchovlar real tarmoq sharoitlari va simulyatsiya qilingan yuqori yuklamali muhitlarda amalga oshirildi. Ushbu bo‘limda eng muhim eksperimental natijalar keltiriladi.

Kechikish bo‘yicha solishtirish. Quyidagi 4-jadval turli protokollar bo‘yicha o‘rtacha kechikish ko‘rsatkichlarini aks ettiradi. Natijalar shuni ko‘rsatadiki SRTP eng past kechikish bilan ishlaydi va real vaqt video oqimi uchun optimal hisoblanadi. ONVIF Media Security SRTP asosidagi shifrlashni qo‘llaganligi sababli kechikish biroz oshgan, media oqim uchun yetarlicha past darajada qolmoqda. TLS 1.3 kechikishini optimallashtirgan bo‘lishiga qaramay, media oqimi uchun mos emas, chunki handshake va paketni qayta ishlash jarayonlari ancha vaqt oladi. TLS 1.2 eng sekin variant bo‘lib, real vaqt video oqimlarida foydalanish tavsiya etilmaydi.

4-jadval. Protokollarni kechikish bo‘yicha taqqoslama jadvali

Protokol	O‘rtacha kechikish (ms)
SRTP	2-3
ONVIF	3-5
TLS 1.3	20-40
TLS 1.2	40-60

Xulosa qilib shuni aytish mumkinki real vaqt video oqimlari uchun yagona, amaliy jihatdan maqbul yechim SRTP.

CPU yuklanishi. Quyidagi jadval protokollarni ishlatish vaqtida kamera protsessoridagi yuklanish darajasini ko‘rsatadi.

5-jadval. Kameraning ishlash vaqtida CPU ga tushadigan yuklanish (%)

Kamera turi	TLS	SRTP	ONVIF
Low-end	35	8	10
Mid-range	22	5	8
High-end	15	4	6

5-jadvaldagi natijalar shuni ko‘rsatadiki TLS protokoli protsessor resurslarini sezilarli darajada band qiladi. Bu ayniqsa resursi kam IoT kameralarida sezilarli farq qiladi. SRTP juda yengil kriptografik algoritmlardan foydalanganligi sababli CPU yuklanishi past bo‘ladi. ONVIF Security arxitekturasidagi yengil mexanizmlar DAT, TLS-PSK, ECC resurs foydalanishini optimallashtiradi. Natijalar SRTP va ONVIF protokollari IoT kameralar uchun resurs samaradorligi bo‘yicha eng mos variant ekanini ko‘rsatadi.

Xulosa. Yuqoridagi tasslama jadvallar hamda statistik ma’lumotlardan olingan natijalar asosida quyidagi muhim ilmiy va amaliy xulosalar chiqarildi:

1) TLS boshqaruv darajasida juda muhim, ammo media oqimi uchun mos emas. TLSning kuchli tomonlari sertifikatlar, autentifikatsiya va boshqaruvdagi himoya. Ammo u media oqimi uchun talab etiladigan past kechikish mezoniga javob bermaydi. TLSning CPU yuklanishi ham qator kameralar uchun qiyinchilik tug‘diradi.

2) SRTP media oqimini himoyalash bo‘yicha eng optimal protokoldir. SRTP AES-GCM yoki AES-CTR asosida ishlaydi, juda past kechikish qo‘shadi va tarmoq yukini oshirmaydi. Bu uni video kuzatuv tizimlarida real vaqt shifrlash uchun yagona amaliy tanlovga aylantiradi.

3) ONVIF Security integratsion xavfsizlikni sezilarli soddalashtiradi. ONVIF bir nechta ishlab chiqaruvchilarni yagona standartda birlashtiradi. Security Profile arxitekturasi orqali kamera boshqaruvi, media oqimi va autentifikatsiya qatlamlari bir butun xavfsizlik modeliga ulanadi. Resursi kam kameralar uchun yengil protokollar talab qilinadi. IoT kameralarining katta qismi cheklangan apparat resurslariga ega. SRTP, TLS-PSK va ECC kabi yengil mexanizmlar ularning samarali ishlashi uchun zarur. Ko‘plab IoT kameralar hanuz noto‘g‘ri konfiguratsiya tufayli zaif bo‘lib qolmoqda.

Ekspluatatsiyalarning katta qismi protokol zaifligidan emas, balki zaif parollar, verifikatsiyalanmagan TLS rejimi, SDES kalit almashinuvi, ochiq ONVIF portlari, sertifikat boshqaruvi noto‘g‘ri yuritilishi kabi amaliy xatolardan kelib chiqadi. Shuning uchun xavfsizlikni oshirish faqat protokolni tanlash orqali emas, balki uning to‘g‘ri implementatsiyasi va konfiguratsiyasi orqali ta’minlanadi.

- TLS/HTTPS boshqaruv, autentifikatsiya va qurilma konfiguratsiyasi bosqichida eng muhim xavfsizlik qatlamini ta’minlaydi;
- SRTP real vaqt media oqimlarini minimal kechikish bilan shifrlash imkonini beruvchi eng samarali protokoldir.
- ONVIF Security esa IoT kameralar o‘rtasida universal moslikni ta’minlaydi va turli ishlab chiqaruvchilar qurilmalarining xavfsiz integratsiyasini kafolatlaydi.

Kompleks himoya modeli ushbu protokollarning to‘g‘ri joylashtirilishi, yaxlit arxitektura doirasida bir-birini to‘ldirishi, xavfsiz konfiguratsiya qilinishi, zaifliklardan holi implementatsiya bilan ta’minlanishi orqali amalga oshadi.

Foydalanilgan adabiyotlar

1. Qozoqova T.Q., Shamshiyeva B.M. Applying the CryptoSMT software tool to symmetric block encryption algorithms. pp-750-754
2. Kozokova T., Abdullayeva G., Analysis of lightweight cryptographic algorithms in information security., AIP Conference Proceedings, Volume 3377, Issue 1, id.060014, 8 pp., doi:10.1063/5.0299641
3. Evans D., Lightweight TLS Handshake optimization for IoT Systems. IEEE Internet of Things Journal, 6(4), 6712–6723.
4. Krotofil M., Security evaluation of IP cameras using legacy TLS Implementations. ACM Transactions on Privacy and Security, 24(3), 1–27.
5. Rosenberg J., Secure Real-Time Transport Protocol in Modern RTP Architectures. IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, №4. – P. 112–128.
6. Fischer M., Performance Evaluation of AES-GCM Acceleration for SRTP in Real-Time Networks. Journal of Network and Systems Security. – 2022. Vol. 18, №2. – P. 67–81.

7. Furuya T., Security Profiles in ONVIF-Compliant IoT Cameras: Architecture and Vulnerability Assessment. Sensors, 21(18), 1–17.

8. ONVIF Technical Committee. ONVIF Profile T – Media and Security Specification. Version 1.2.

9. ONVIF Technical Report. Device Authentication Token (DAT) Framework for IP Video Systems. ONVIF Security WG.

10. ONVIF Standard. Security Best Practices for IP-based Surveillance Systems. ONVIF Release Notes.

11. WS-Security Technical Committee. Web Services Security UsernameToken Profile 1.1. OASIS Standard.

12. OWASP Internet of Things Security Verification Standard (IoT-SVS).

13. Krawczyk H., Bellare M. HMAC: Keyed-Hashing for Message Authentication. RFC 2104.

14. Bernstein D. J. The Poly1305 Message Authentication Code. International Journal of Computer Mathematics, 85(2), 145–159.

15. Kumar R., Singh A. Security Challenges in IoT-Based Video Surveillance Systems. International Journal of Network Security, 22(5), 873–889.

16. Garcia L., Liu Y. Zero-Trust Architecture for Distributed Surveillance over IoT Networks. Elsevier Computers & Security, 118, 102736.