IP телефония

Дәріс 9: IP телефонияның қауіпсіздігі

ДӘРІСКЕР: PhD, доцент м.а.
Сқабылов Әлішер Әлиұлы

Дәрістің мақсаты:

IP-телефонияның активтері мен қауіптеріне сәйкес қорғаныс және қалпына келтіру шараларын таңдауды үйрету.

Оқу нәтижелері және дәріс жоспары

Оқу нәтижелері

1. Студент қауіптерді қорғалатын актив пен ықтимал салдарға байланыстырады.
2. Студент TLS, SRTP, SRTCP және IPsec қорғанысының шекарасын ажыратады.
3. Студент IP-АТС үшін қолжетімділік, мониторинг және инцидентке жауап беру жоспарын ұсынады.

Дәріс жоспары

1. Қорғалатын активтер және қауіп моделі
2. SIP сигнализациясын қорғау
3. Медиа және кілттер
4. IPsec және желіні сегментациялау
5. Қолданбалық және пайдалану шаралары
6. Инцидентке жауап берудің талданған сценарийі
7. Қауіпті актив пен сенім шекарасы арқылы талдау
8. Сәйкестендіру аутентификация және авторизация
9. TLS сертификатын тексерудің мағынасы
10. SRTP кілттерінің өмірлік циклі
11. Алаяқтық пен ресурс таусылуын шектеу
12. Инцидентті оқшаулау және дәлелді сақтау
13. Оқу жағдайына арналған тәуекелді бағалау
14. Терминдерді жүйелеу.

Алғышарттар: Алдыңғы 8 дәрістегі негізгі ұғымдарды білу.

Қорғалатын активтер және қауіп моделі

IP-телефонияда сигнализация, медиа, тіркелгі деректері, нөмірлеу жоспары, конфигурация, CDR және дыбыс жазбалары қорғалады. Қауіпсіздік құпиялылық, тұтастық және қолжетімділік мақсаттарын қатар қарастырады.

Құпиялылық

Мазмұнға рұқсатсыз қолжетімділікті шектеу.

Тұтастық

Конфигурация мен деректердің рұқсатсыз өзгеруінен қорғау.

Қолжетімділік

Телефон қызметін қажетті кезде пайдалануға мүмкіндік беру.

IP желісі міндетті түрде ашық интернет емес. Тәуекел жариялануға, сегментацияға, тіркелгі құқықтарына және қызмет көрсетуге тәуелді.

Негізгі қауіптер және қорғаныс шаралары

Қауіп	Ықтимал салдар	Негізгі шара
Медианы тыңдау	Сөйлесу құпиясының ашылуы	SRTP және қауіпсіз кілт келісу
Тіркелгіні басып алу	Шақыруды бөтен мекенжайға бағыттау	Күшті аутентификация және Contact өзгерісін бақылау
Toll fraud	Ұйым есебінен рұқсатсыз ақылы қоңырау	Бағыт құқықтары, лимит және CDR дабылы
DoS немесе ресурс таусылуы	Тіркелу не қоңырау қызметінің үзілуі	Кіріс шектеу, SBC, ресурс бақылауы
Басқару интерфейсінің бұзылуы	Конфигурация мен құқықтардың өзгеруі	Басқару сегменті, MFA, жаңарту және аудит
Vishing және жалған Caller ID	Пайдаланушының алдануы	Бөлек растау рәсімі және оқыту

SIP сигнализациясын қорғау

SIP Digest

Клиенттің құпияны білетінін тексереді, бірақ бүкіл SIP хабарламасын шифрламайды. Әлсіз пароль мен артық құқық TLS қосылғанда да қауіпті.

TLS

SIP тасымалдау арнасындағы құпиялылық пен тұтастықты қорғайды; сертификат тізбегі, атауы және мерзімі тексеріледі.

Hop-by-hop шекарасы

Аралық proxy немесе SBC хабарламаны өңдесе, TLS сол түйінде аяқталып, келесі қорғалған арна қайта орнатылады.

5061 портын пайдалану TLS-ті автоматты қоспайды. TLS саясаты, сертификат тексеруі және барлық тиісті бағыттардың қорғалуы бөлек бапталады.

Медиа және кілттер

Механизм	Қорғаныс міндеті
RTP	Медиа деректерді тасымалдайды, бірақ әдетте мазмұнды шифрламайды.
SRTP	Медиа құпиялылығын, аутентификациясын, тұтастығын және қайта ойнатудан қорғанысын қамтамасыз ете алады.
SRTCP	RTCP басқару/есеп ақпаратын қорғайды.
SDES	Кілт материалын SDP арқылы жеткізеді; SDP тасымалдайтын жол мен аралықтарға сенім қажет.
DTLS-SRTP	Медиақатысушылар арасында кілт алмасуын ұйымдастырады. Қолдау өнімге байланысты.

SRTP SIP аутентификациясының орнына жүрмейді. Серверде жазу, транскодтау немесе конференция болса, медиа өңдейтін түйін де қорғаныс шекарасына кіреді.

IPsec және желіні сегментациялау

IPsec

IP деңгейінде саясатқа кіретін трафикті қорғайды. ESP transport режимінде IP жүктемесін, tunnel режимінде бастапқы IP пакетін қорғайды. AH тұтастық пен аутентификацияға арналған, бірақ шифрламайды.

VPN және Voice VLAN

VPN қашықтағы қызметкерлер мен филиалдарға бақыланатын жол береді. Voice VLAN дауыс пен деректерді логикалық бөледі, бірақ өздігінен шифрламайды.

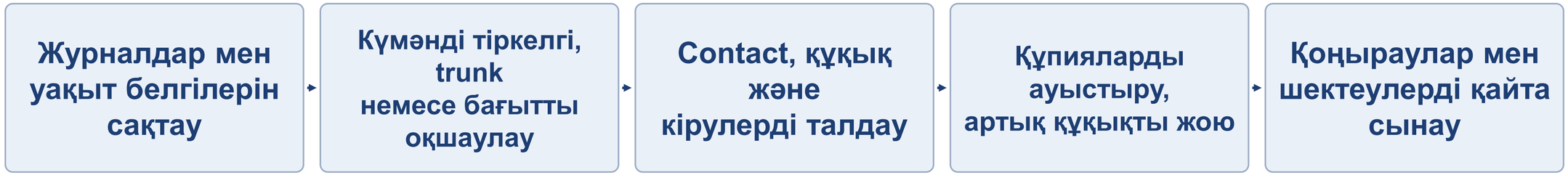
Firewall / ACL

Басқару интерфейстерін бөлек сегментте ұстап, SIP және RTP үшін нақты қажет бағыттарға ғана рұқсат береді.

Қолданбалық және пайдалану шаралары

- SBC хабарламаларды тексеру, қолжетімділікті шектеу, медиа жолын басқару және сұраныс жиілігін шектеу қызметтерін ұсына алады.
- Ақылы бағыттарды рөл бойынша шектеу, түнгі аномалияны бақылау, бірмезгілдегі қоңырау лимиті және шығын дабылы toll fraud тәуекелін төмендетеді.
- Жаңартулар сынақтан кейін жоспармен енгізіледі; басқару әрекеттері журналданады.
- Резервтік көшірмені қалпына келтіру тексеріледі және пайдаланушыларға жалған Caller ID-ді тану рәсімі түсіндіріледі.

Инцидентке жауап берудің талданған сценарийі



- Түнде белгісіз сыртқы бағыттарға қоңырау көбейсе, SIP оқиғалары, CDR және конфигурация өзгерістері сақталады.
- Қызметті толық өшірудің орнына күмәнді тіркелгі, trunk немесе маршрут мақсатты түрде оқшауланады.
- TLS арнасын қосу ұрланған парольді немесе ашық dialplan-ды өздігінен түземейді.

Қауіп активтері және сенім шекаралары



TLS аралық түйінде аяқталуы мүмкін

SRTP жолы мен кілт келісімі бөлек бағаланады

Абоненттік аймақ, басқарылатын қызмет, қорғалған сақтау және операторлық шекара

Сәйкестендіру, аутентификация және авторизация

Кезең	Сұрақ	Мәні
Сәйкестендіру	Кім әрекет ететінін мәлімдейді?	SIP username немесе пайдаланушы идентификаторы.
Аутентификация	Мәлімдеме қалай тексеріледі?	Пароль, сертификат немесе басқа қолдау көрсетілген дәлел.
Авторизация	Қандай әрекетке рұқсат бар?	Нөмірлеу бағыты, әкімшілік құқық, ресурс лимиті.

Caller ID пайдаланушы көретін шақырушы белгісі ғана; ол жеке өзі сенімді аутентификация құралы емес. Жеке тіркелгі мен ең аз құқық принципі журналдағы әрекетті нақты субъектпен байланыстыруға көмектеседі.

TLS сертификатын тексеру

Сенімді тізбек

Сертификат сенімді түбірге дейін расталуы керек.

Атау сәйкестігі

Сертификаттағы сервер атауы қосылатын сервермен сәйкес болуы керек.

Мерзім және уақыт

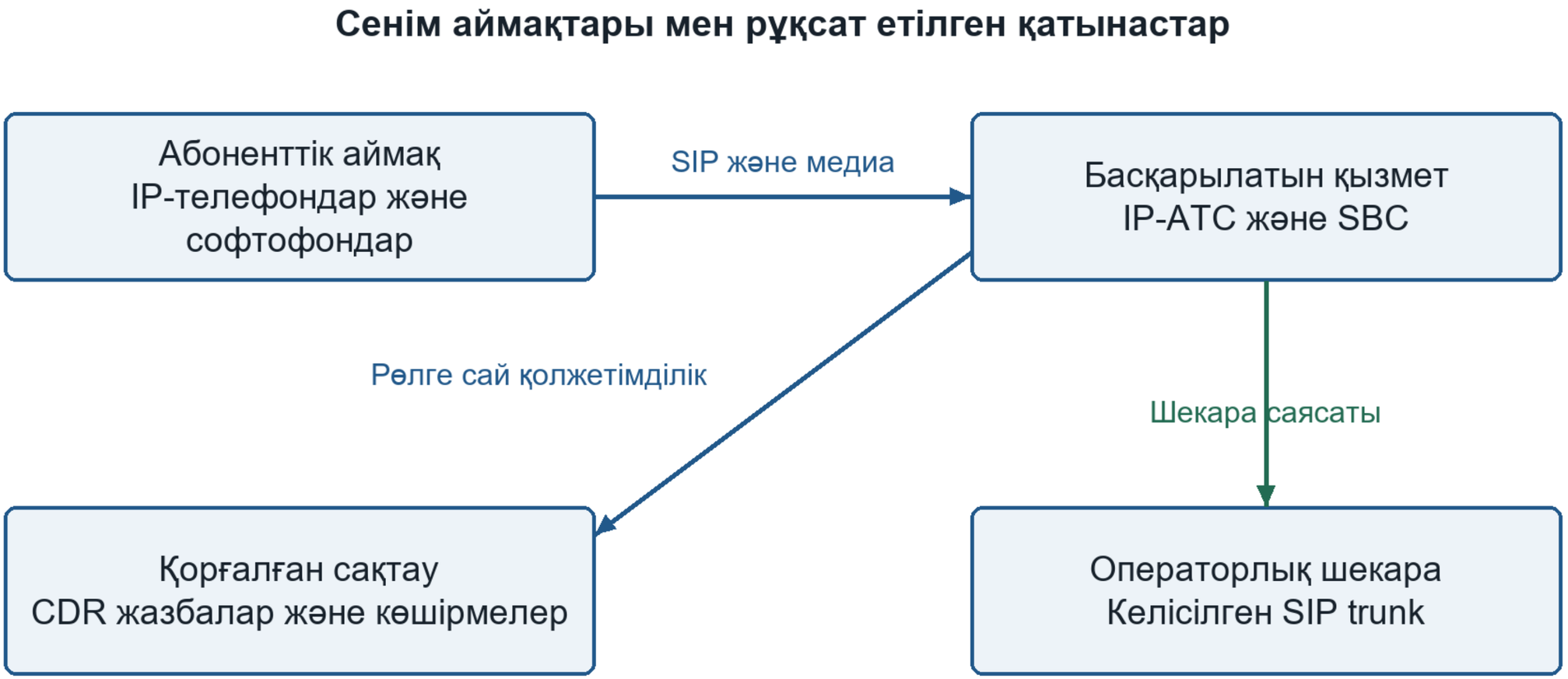
Жарамдылық мерзімі мен жүйелік уақыт дұрыс тексеріледі.

Қате сертификат

Пилотта клиенттің қате сертификаттан бас тартуы сынақтан өткізіледі.

TLS терминалдан SBC-ге дейін ғана қорғаса, SBC-ден операторға дейінгі бөлік бөлек бағаланады. Толық жолдың нақты қорғаныс шекаралары көрсетілуі тиіс.

SIP үшін TLS және медиа үшін SRTP қорғанысының шекаралары



Бір желіге қосылу барлық қызметке бірдей құқық бермейді

Сигнализация арнасы мен медиа ағынының қорғанысы бөлек келісіліп, бөлек тексеріледі

SRTP кілттерінің өмірлік циклі

- Кілтті алғашқы келісу, сақтау, пайдалану және ауыстыру кезінде қорғау қажет.
- Кілт материалын журналға немесе жалпыға ашық конфигурацияға шығару шифрлаудың тиімділігін жояды.
- SDES кілтті SDP арқылы береді; DTLS-SRTP басқа кілт алмасу тәсілін қолданады. Қолдау мен сәйкестік нақты тексеріледі.
- SRTP бар болуы соңғы құрылғыдағы malware-ді, әкімшілік рұқсатсыз кіруді немесе серверде сақталған жазбаның ашықтығын жоймайды.

Алаяқтық пен ресурс таусылуын шектеу

Toll fraud

Ақылы бағыттарды рөл бойынша шектеу; қоңырау ұзақтығы мен бірмезгілдегі сеанс лимиті; шығын дабылы; кіріс trunk-тан сыртқы ақылы маршрутқа еркін өтуге тыйым салу.

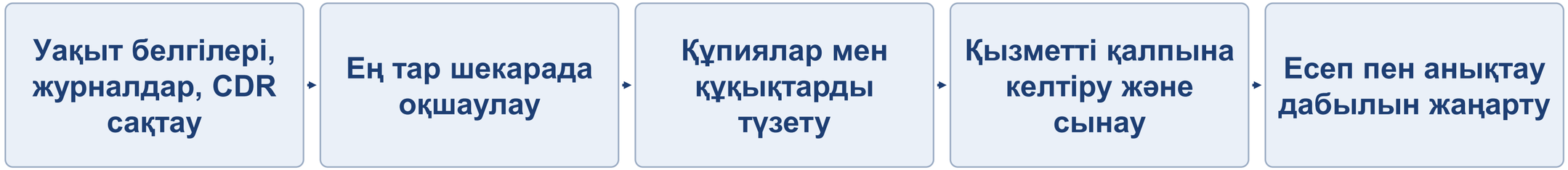
Rate limiting

Автоматты тіркелу сұраныстарын азайтады, бірақ шек тым төмен болса қорек қалпына келгеннен кейін қатар қайта тіркелетін заңды телефондарды бұғаттауы мүмкін.

DDoS тәуекелі

Желілік арнаны толтыратын көлемді шабуыл firewall-ға жеткенше қызметті тоқтатуы мүмкін; провайдермен келісілген шекаралық шаралар қажет.

Инцидентті оқшаулау және дәлелді сақтау



- Барлық құрылғыны бірден қайта іске қосу уақытша дәлелдерді жоғалтуы мүмкін.
- Әр әрекет кім, қашан және не үшін жасағаны көрсетіліп тіркеледі.
- Қалпына келтіру кезінде ішкі/сыртқы қоңырау, шифрлау келісімі, тыйым салынған маршрут және резервтік көшірме тексеріледі.

Оқу жағдайына арналған тәуекелді бағалау

IP-АТС басқару беті жалпы интернеттен ашық, әкімшілер ортақ құпия сөз қолданады және сыртқы бағыттар шектелмеген делік. TLS қосу пайдалы болғанымен, осы ұйымдастырушылық кемшіліктерді өздігінен жоймайды.

Тәуекел	Шара	Тексеру дәлелі
Басқару интерфейсі ашық	Басқаруға рұқсат аймағын тарылту; жеке әкімшілік тіркелгі енгізу.	Қонақ желісінен басқару бетіне қосылу өтпеуі.
Сыртқы бағыттар шектелмеген	Рөлдер мен бағыт құқықтарын шектеу; аномалия дабылын қосу.	Рұқсаты жоқ тіркелгі ақылы қоңырау жасай алмауы.

Қауіпсіздік терминдері

Термин	Мағынасы
Аутентификация	Мәлімделген сәйкестіктің дұрыстығын тексеру.
Авторизация	Тексерілген субъект орындай алатын әрекеттерді анықтау.
Сенім тізбегі	Сертификатты сенімді түбірге байланыстыратын растау тізбегі.
Оқшаулау	Инциденттің таралуын не зиянын шектеуге арналған мақсатты әрекет.
Ең аз құқық	Субъектіге міндетін орындауға жеткілікті рұқсатты ғана беру принципі.

Қорытынды

Қорғаныс активтер мен қауіптерді анықтаудан басталады. TLS сигнализация арнасын, SRTP медианы, ал IPsec саясатқа кіретін IP трафигін қорғайды. Қауіпсіздік аутентификацияны, құқықтарды шектеуді, жаңартуды, журналдарды және қалпына келтіруді бірге ұйымдастыруды қажет етеді.

Білімді бекітуге арналған сұрақтар:

1. Тыңдау, тіркелуді басып алу және toll fraud қауіптері қандай активтерге әсер етеді?
2. TLS қосылса да, RTP трафигі неліктен ашық қалуы мүмкін?
3. SIP TLS қорғанысы аралық proxy немесе SBC болғанда қай жерде аяқталуы мүмкін?
4. SRTP үшін кілттерді қауіпсіз келісу неге бөлек қажет?
5. VLAN мен firewall қандай әртүрлі қорғаныс міндетін атқарады?
6. Рұқсатсыз сыртқы қоңыраулар байқалғанда қандай ретпен әрекет етесіз?
7. Сәйкестендіру, аутентификация және авторизация айырмасын көрсетіңіз.
8. Caller ID неге жеке өзі сенімді сәйкестік дәлелі емес?
9. Қате сертификатқа клиенттің бас тартуын не үшін сынау керек?
10. SRTP кілті журналға түссе, шифрланған тасымалдаудың қаупі қалай өзгереді?
11. Көп телефон қатар қайта тіркелгенде rate limiting қандай заңды қызметке әсер етуі мүмкін?
12. Инцидент кезінде дәлел сақтау мен оқшаулауды қалай қатар ұйымдастырасыз?

Практикалық тапсырма

Университеттің IP-АТС журналында түнде көптеген сәтсіз REGISTER әрекеті және күтпеген сыртқы қоңыраулар байқалды. Қандай деректерді сақтайтыныңызды, қандай есептік жазбалар мен бағыттарды уақытша шектейтініңізді, кілттер мен құпия сөздерді қалай ауыстыратыныңызды және қалпына келтіруді қалай тексеретініңізді жазыңыз. TLS қосу бұл оқиғаның барлық себебін өздігінен жоймайтынын түсіндіріңіз.

Орындау критерийлері

- Инцидент белгілері мен ықтимал салдар ажыратылған — 2 балл.
- Оқшаулау және дәлелдерді сақтау реті орынды — 3 балл.
- Құқықтар, аутентификация және шифрлау шаралары байланысты берілген — 3 балл.
- Қалпына келтіру және қайта тексеру жоспары бар — 2 балл.

Әдебиеттер тізімі:

1. RFC 3261 SIP Session Initiation Protocol
2. RFC 3711 The Secure Real time Transport Protocol
3. RFC 9325 Recommendations for Secure Use of TLS and DTLS
4. RFC 4301 Security Architecture for the Internet Protocol