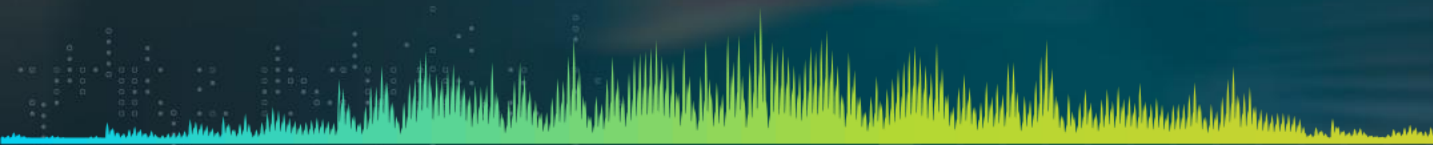
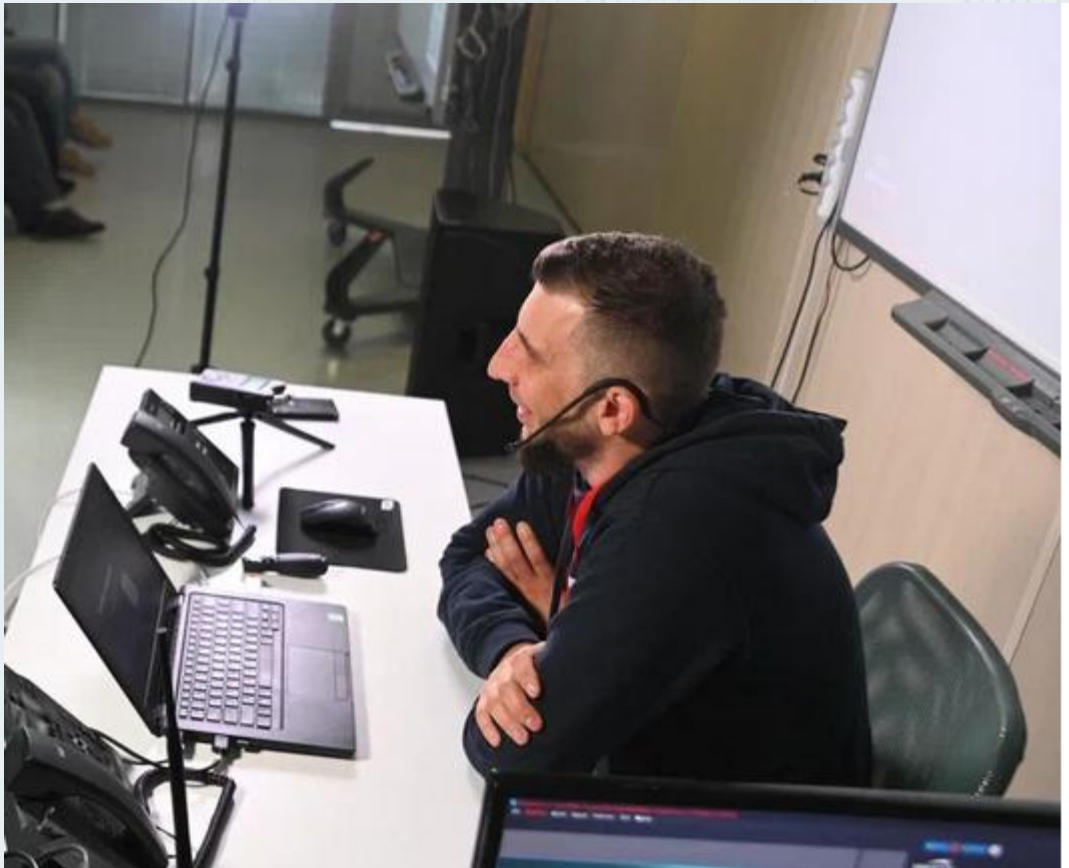


История об одном проекте, где неудачный выпуск мобильного приложения привел к ддосу



Обо мне:



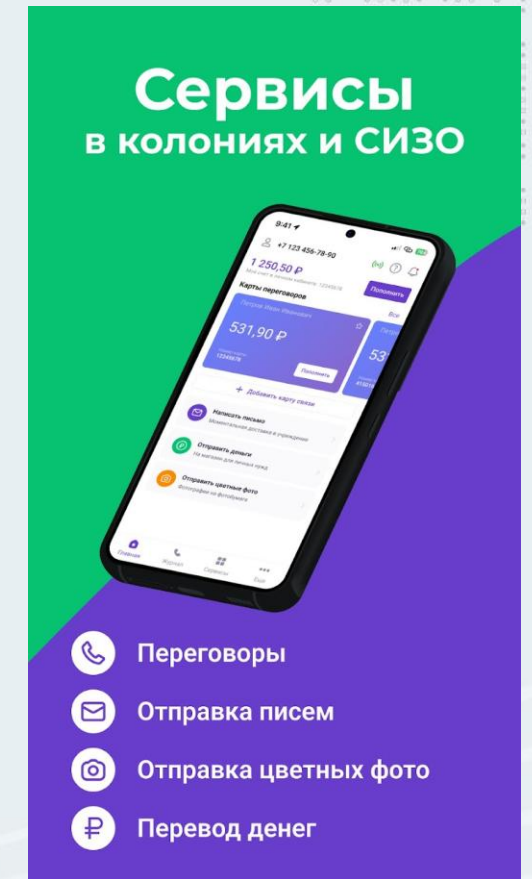
- Более 13 лет занимаюсь VoIP
- OpenSips фанат
-

О чем доклад

- Как ошибки в собственном мобильном приложении могут привести к DDoS-атаке на инфраструктуру.
- Влияние на сервисы и последствия для компании.
- Подумаем как предотвратить DDoS-атаки, вызванные собственными приложениями
- Важность взаимодействия между разработчиками и администраторами для предотвращения проблем.
- Создание процесса для выявления и устранения уязвимостей до выпуска приложения.

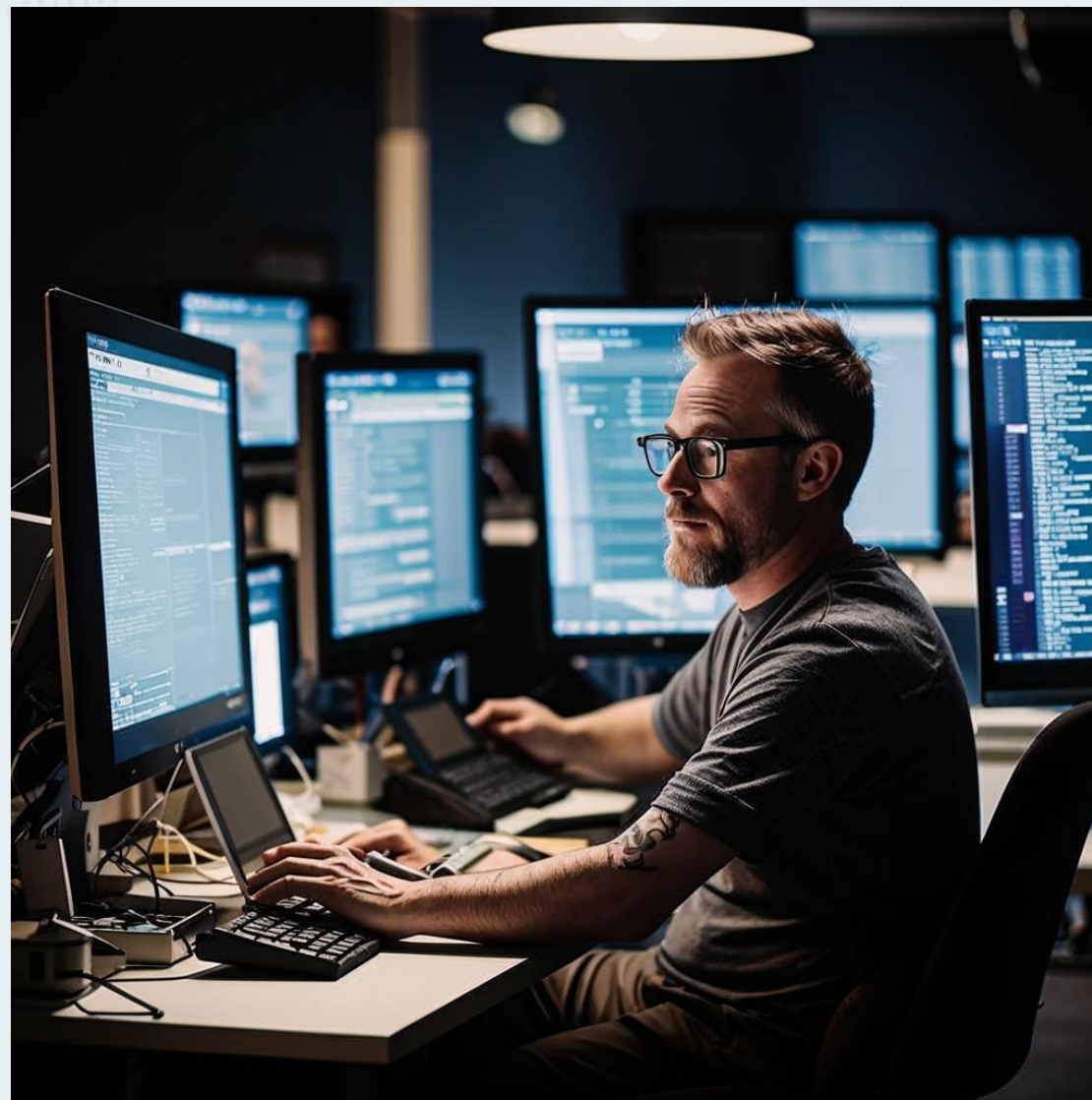
Мобильное приложение что под капотом

- linphone sdk
- WebView
- Чего то написали там программисты
- Да у нас регистрация постоянна...
-



История....

- Давайте откажемся от постоянных регистраций и будем будить по push
- Поддержка нового API google
- Поддержка новых версий Android
- Тестирование....



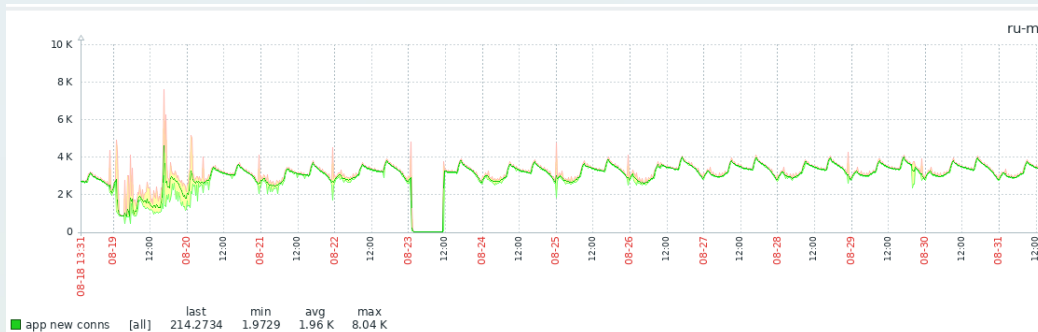
И Что же было далее

- Внезапный рост кол-ва регистраций
- Рост количества новых коннектов
- Нагрузка на OpenSips выросла в разы
- Что случилось?



Разбор...

- А собственно почему так...
- Что же было проблемного в МП — tls, webview
- Проблема ясна, закрыть новой версией быстро не можем.
-



```
2024-08-28 15:53:45.770 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Trying to connect to [TLS://:ffff:185.149.161.53:5061] 1
2024-08-28 15:53:46.269 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: Connected at TCP level, now doing TLS handshake with cname=video-ce.zonatelecom.ru
2024-08-28 15:53:47.777 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I ext key usage : TLS Web Server Authentication, TLS Web Client Authentication
2024-08-28 15:53:48.272 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: SSL handshake finished, SSL version is [TLSv1.2], selected ciphersuite is [TLS-RSA-WITH-AES-128-CBC
2024-08-28 15:53:48.295 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: message sent to [TLS://video-ce.zonatelecom.ru:5061], size: [669] bytes 2
2024-08-28 15:53:48.295 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44250;alias=branch-z9h04ok.ke99WYhav;rport
2024-08-28 15:53:48.276 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: *79890476509* <sip:79890476509@192.168.0.103:44250;transport=tls>;*sip.instance*=urn:uuid:39caad88-1af8-4d71-a2c7-b2509
2024-08-28 15:53:48.776 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: received [459] new bytes from [TLS://video-ce.zonatelecom.ru:5061]:
2024-08-28 15:53:48.776 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44250;received=178.120.66.166;alias=branch-z9h04ok.ke99WYhav;rport=6139
2024-08-28 15:53:48.776 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: <sip:79890476509@178.120.66.166:6139;transport=tls>;expires=3600
2024-08-28 15:53:48.803 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: message sent to [TLS://video-ce.zonatelecom.ru:5061], size: [669] bytes
2024-08-28 15:53:48.804 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: *79890476509* <sip:79890476509@178.120.66.166:6139;transport=tls>;*sip.instance*=urn:uuid:39caad88-1af8-4d71-a2c7-b2509
2024-08-28 15:53:49.274 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: received [459] new bytes from [TLS://video-ce.zonatelecom.ru:5061]:
2024-08-28 15:53:49.274 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44250;received=178.120.66.166;alias=branch-z9h04ok.ePvN8jgCH;rport=6139
2024-08-28 15:53:49.274 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: <sip:79890476509@178.120.66.166:6139;transport=tls>;expires=3600
2024-08-28 15:53:49.279 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Register refresher [200] reason [OK] for proxy [<sip:video-ce.zonatelecom.ru;transport=tls>] 3
2024-08-28 15:54:18.788 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: keep alive sent to [TLS://video-ce.zonatelecom.ru:5061]
2024-08-28 15:54:23.294 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Register refresher [503] reason [io error] for proxy [<sip:video-ce.zonatelecom.ru;transport=tls>] 4
2024-08-28 15:54:24.790 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Trying to connect to [TLS://:ffff:185.149.161.53:5061] 1
2024-08-28 15:54:32.294 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: Connected at TCP level, now doing TLS handshake with cname=video-ce.zonatelecom.ru
2024-08-28 15:54:35.295 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I ext key usage : TLS Web Server Authentication, TLS Web Client Authentication
2024-08-28 15:54:35.794 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: SSL handshake finished, SSL version is [TLSv1.2], selected ciphersuite is [TLS-RSA-WITH-AES-128-CBC
2024-08-28 15:54:35.795 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: message sent to [TLS://video-ce.zonatelecom.ru:5061], size: [669] bytes 2
2024-08-28 15:54:35.795 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44260;alias=branch-z9h04ok.ePvN8jgCH;rport
2024-08-28 15:54:35.795 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: *79890476509* <sip:79890476509@192.168.0.103:44260;transport=tls>;*sip.instance*=urn:uuid:39caad88-1af8-4d71-a2c7-b2509
2024-08-28 15:54:36.296 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: received [461] new bytes from [TLS://video-ce.zonatelecom.ru:5061]:
2024-08-28 15:54:36.296 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44260;received=178.120.66.166;alias=branch-z9h04ok.Fix020AZL;rport=54091
2024-08-28 15:54:36.296 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Contact: <sip:79890476509@178.120.66.166:5409;transport=tls>;expires=3600
2024-08-28 15:54:36.301 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Register refresher [200] reason [OK] for proxy [<sip:video-ce.zonatelecom.ru;transport=tls>] 3
2024-08-28 15:54:39.359 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Register refresher [503] reason [io error] for proxy [<sip:video-ce.zonatelecom.ru;transport=tls>] 4
2024-08-28 15:54:39.359 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Trying to connect to [TLS://:ffff:185.149.161.53:5061] 1
2024-08-28 15:54:41.366 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: Connected at TCP level, now doing TLS handshake with cname=video-ce.zonatelecom.ru
2024-08-28 15:54:41.860 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I ext key usage : TLS Web Server Authentication, TLS Web Client Authentication
2024-08-28 15:54:41.860 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Channel [0xb4000070bf2ee200]: SSL handshake finished, SSL version is [TLSv1.2], selected ciphersuite is [TLS-RSA-WITH-AES-128-CBC
2024-08-28 15:54:41.862 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I channel [0xb4000070bf2ee200]: message sent to [TLS://video-ce.zonatelecom.ru:5061], size: [669] bytes
2024-08-28 15:54:41.862 15179-15179 ZT_LIN_LOGGER: org.zonatelecom.mobileclient.purple I Via: SIP/2.0/TLS 192.168.0.103:44284;alias=branch-z9h04ok.naVj0vZr3;rport
```

работа инженеров. Как сейчас

- Одна нода opensips на двух ногах
- Что смотрит во внутрь нашей сети - принимает INVITE по udp и шлёт их в сторону МП
- Что смотрит наружу - принимает SIP-over-TLS от МП
- Rtp engine
- Так же в сторону мобильного апи посылается пуш-запрос
- Если в данный момент регистрации от МП нет, то ждём некоторое время их появления
- При появлении коннекта к МП и регистрации посылает на МП вызов
-

Когда тестировщик нашел баг в день релиза



Проблематика

- Нода только одна, а клиентов с МП много - единая точка отказа (со всеми вытекающими неприятными последствиями и эффектами)
- Есть проблема с IO Reactor, что приводит к отказу сервиса при большом рейте подключений
- Так как МП работает по SIP over TLS, то хост держит до каждого активного МП tcp соединение



Про osips

- Несколько нод opensips к которым цепляется МП
- Несколько A записей для имени domain.ru (именно сюда коннектится МП)
- Клиент согласно RFC случайно выбирает одну из существующих A-записей (по сути публичных адресов), к которым будет подключаться
- Инфра может посылать INVITE на любую из нод - всё должно быть ок
- Пуш в мобильное апи должен быть только один, вне зависимости от кол-ва нод
- INVITE должен в конечном счёте приземляться на ноду, к которой подключилось МП

Что под капотом 1



- По факту это схема [full sharing топология + SBC](#), только с той лишь разницей, что каждая нода является одновременно и SBC, и нодой кластера
- Из механизма кластеризации нам нужна лишь работа с location db, чтобы знать, на какой из нод приземляется МП (так как регистрации у нас свободно влезают в память)
- Так как МП не звонит друг другу, то это даёт возможность максимально всё упростить
- Переход на wolfssl

- если INVITE пришёл на anycast ip, то
 - послать пуш
 - установить хук на регистрацию и ждать
 - проверить БД location
 - если пир найден, то проверить home-node
 - если home-node == self
 - то послать INVITE в приложение
 - если home-node != self
 - то послать INVITE на target node на int ip
- если INVITE пришёл на int ip, то
 - проверить БД location
 - если пир найден, то послать INVITE в приложение
 - если пир не найден, то ответить 404

Что под капотом 2

- Перешли на схему с одним центральным main registrar (им стал тот прежний osips-app-proxy) и кучей (11 штук наклепал) mid registrar-ов. Mid Registrar принимает tls коннект от МП и передаёт его на main registrar через udp транспорт.

Как глубоко можно копать

Так же надо переключиться на использование библиотеки wolfssl вместо openssl.

Дело в том, что при работе с openssl используется глобальный лок на уровне модуля. Таким образом, а значит в каждый момент времени вызов `SSL_Accept` выполняется только одним воркером. Эта функция по какой-то причине возвращает ошибку (The TLS/SSL handshake was not successful but was shut down controlled and by the specifications of the TLS/SSL protocol. Call `SSL_get_error()` with the return value `ret` to find out the reason.), в спецификации ошибки (`SSL_get_error`) у нас, внезапно, строка "`SSL_ERROR_SYSCALL: Success(0)`". (Я когда-то даже пробовал искать её истоки в коде openssl, но там всё очень грустно - эта ошибка выводится в одной из default веток в switch case и она возникает при самых разных обстоятельствах).

В коде модуля работы с wolfssl глобальных локов нет.

Анализ дампа показал, из-за чего такая ошибка возникает - это когда сервер очень долго отвечает на Client Hello в TLS Handshake, а клиент уже начал закрывать соединение через FIN, и не получает подтверждение на эти FIN.

Ошибки

- Быстро делаем схему mid register
- Быстро делаем еще что-то
- Нагрузка на людей
- Взаимодействие между командами...

Тесты

- Тестирование важный процесс
- Твое приложение может тебе же и убить
- Где грань и ЗО

Выводы

- Холодная голова, важная часть
- Определение ЗО и кто что релизит, эффект лавины
- Повышение квалификации сотрудников.

Спасибо за внимание!

KAMAILIO
CONF'24

Буду рад ответить на все ваши вопросы сейчас
или свяжитесь со мной в будущем:



Замятин Михаил

