امیر پادیار

1-MTProto که به عنوان پروتکل دسترسی به سرور API در تلگرام از طریق اپلیکیشن‌های در حال اجرا بر روی دستگاه‌های موبایل استفاده می‌شود به صورت مجازی به چند لایه تقسیم می شود؟آن ها را نام ببرید و وظایف هریک را بیان کنید.

الف)لایه سطح بالای فراخوانی‌های APIهای موجود: این لایه فراخوانی‌هاو پاسخ‌های APIها را به پیام‌های باینری تبدیل می‌کند.

ب)لایه رمزنگاری: این لایه وظیفه تعیین پارامترهای رمزنگاری و انجام آن را پیش از ارسال داده‌ها برعهده دارد.

پ)لایه انتقال: وظیفه تعیین پارامترها و روش‌های ارتباط کاربر و سرور بر اساس انتخاب‌های موجود برای پروتکل‌های شبکه(tcp، UDP، http و ..) را دارد.

%%

2-رمزنگاری پیام‌ها در MTProto (server-client) در تلگرام با استفاده از چه الگوریتم رمزنگاری ، چه طول کلیدی و در چه مدی انجام می گیرد؟کلید رمزنگاری چگونه بدست می‌آید؟

پیام‌ها در این ساختار با الگوریتم AES و کلید با طول 256 در مد CBC رمزگذاری می‌شوند.

AES Key=KDF(Pre-shared key,message key)=KDF(Pre-shared key,SHA1(Server Salt,Session id,payload))

%%

3-در MTProto (server-client)در دو مرحله سرآیندهایی بر روی داده‌ها اعمال می شود، سرآیندهای اعمال شده در دو مرحله را به صورت جداگانه ذکر کنید.

%%

4-در اپلیکیشن Telegram که از پروتکل MTProto جهت تضمین محرمانگی پیام‌ها استفاده می نماید نحوه تولید کلید مشترک با سرور Authorization Key (یا Shared key) و احراز اصالت پیام‌های سرور را ذکر نمائید.

در ابتدای راه‌اندازی نرم‌افزار باید یک کلید مشترک بین سرور و هرکاربر ایجاد شود این کار با استفاده از اجرای یک دیفی هلمن احراز اصالت شده اجرا میشود. کلید تولید شده به عنوان Authorization Key در نظر گرفته می‌شود. این دیفی هلمن احراز اصالت شده با استفاده از کلید2048 بیتی سرور که از ابتدا در اپلیکیشن قرار داده شده اس تحت الگوریتم RSA جهت امضای دیجیتال استفاده می‌شود.

%%

5- نحوه تضمین یکتایی کلید مشترک بین کاربر و سرور در MTProtoچگونه است؟

کلیدی تصادفی به طول 2048 بیت تولید شده و پس از اعمال چکیده‌ساز SHA1 بر روی آن 64 بیت کم ارزش آن را به عنوان Key Identifier در نظر گرفته می‌شود که این مقدار باید برای هر کاربر یکتا باشد. به همین شکل در صورتی که Key Identifier ایجاد شده تکراری باشد کلید دیگری تولید می‌شود.

%%

6- نحوه تعیین g به عنوان مولد گروه در دیفی هلمن بین کاربر و سرور در پروتکل MTProto به چه صورت است؟

برای آنکه از میزان رد و بدل پیام‌های فاش بین سرور و کاربر کم شود برای انتخاب g قاعده‌ایی ترتیب دیده شده است. به این صورت که پس از مشخص شده p کاربر g را بر اساس جدول زیر انتخاب خواهد نمود:

p mod 4g	g
P mod 8=7	2
P mod 3=2	3
No extra codition	4
P mod 5=1 or 4	5
P mod 24=19 or 23	6
P mod 7=3 or 5 or 6	7

%%

7-همان طور که می دانیم SHA1 از لحاظ امنیتی مشکلاتی دارد.دلیل طراحان پروتکل MTProto برای استفاده از این الگوریتم چیست؟و چرا یافتن تصادم در آن را مشکلی در پروتکل خود نمی دانند؟

الگوریتم مناسب نسبت به دیگر نسخه ها مانند SHA256 از لحاظ نیاز محاسباتی و توان مصرفی و پیاده سازی بهینه از عمده دلایلی است که طراحان جهت اجرای روان تر اپلیکیشن در تلفن‌های همراه قدیمی تر با توان محاسباتی پایین تر SHA1 را استفاده نموده اند. در عین حال از دید طراحان برای اختلال در کار پروتکل یافتن تصادم در SHA1 به تنهایی کافی نخواهد بود بلکه باید تصادمی مانند

SHA1 (AES Decrypt(key unknown to attacker, ciphertext))

را یافت.

%%

8-روش مقابله MTProto با حمله ایی که طی آن درخواست بسیار زیادی جهت ایجاد کلید دیفی هلمن داشته باشد چیست؟

MTProto برای مقابله با این نوع حملات تدبیری کرده است به این صورت که هر بار کاربری درخواست ایجاد Authorization Key کند نخست به آن یک n=pq بزرگ که در آن p و q اعدادی اول هستند می دهد تا کاربر ابتدا آن ها را تجزیه کند و با درست برگشت دادن p و q ، سرور p را به عنوان پارامتر عمومی سیستم دیفی-هلمن مورد استفاده قرار خواهد.

%%

9-رمزگذاری انتها به انتها در نرم فزار تلگرام چگونه انجام می گیرد؟ در این روش چگونه perfect forward secrecy تامین می شود؟

در حالتی که بخواهیم رمزگذاری انتها به انتها (Secret Chats) داشته باشیم با استفاده از اجرای الگوریتم دیفی هلمن بین دو کاربر از طریق سرور به جای استفاده از کلید Authorization Key در فرآیند تولید کلید AES جهت رمزگذاری داده ها از این کلید استفاده خواهد شد در نتیجه در این بین سرور امکان خواندن پیام‌ها را نخواهد داشت.

در این پروتکل علاوه بر این که بین دو کاربر رمزنگاری مستقیمی انجام می گیرد سرور جهت امنیت بیش تر و ایجاد forward secrecy پس از رد و بدل شدن 100 پیام کاربران را مجبور به تولید کلید جدید می نماید. زیرا داشتن پیام‌های بیشتر احتمال لو رفتن کلید را بیش‌تر خواهد نمود.

نکته: البته در هیچ کجای پروتکل ذکر نشده است که چرا سرور نمی تواند خود به عنوان مهاجم دیفی هلمن غیر احراز اصالت شده کاربران را مورد حمله MITM قرار دهد.

%%

10-می دانیم کاربر ممکن است به طور همزمان از چند دستگاه بخواهد به سرور متصل شود در MTProto این موضوع چگونه مدیریت می شود؟در عین حال پیام‌های هر نشست چگونه مشخص خواهند شد؟

در این پروتکل این مشکل با استفاده از تولید session id توسط کاربر برای هر نشست خود انجام می شود در این صورت کاربر می تواند نشست های متعددی را با کاربر ایجاد نماید و سرور از این جهت محدودیتی برای کاربر قائل نیست.

همچنین کاربر یک Message id نیز برای پیام‌های خود تولید می کند و یک Message sequence برای هر پیام. که در این صورت علاوه بر این که امکان جابه جایی پیام‌ها وجود نخواهد داشت درستی دنباله پیام‌ها در ارتباطات مختلف نیز حفظ خواهد شد.

%%