CSEP564 : Computer Security : Reading 4

Karuna Sagar Krishna

October 23, 2024

Paper Title

Four Attacks and a Proof for Telegram

Paper Authors

Martin R. Albrecht, Lenka Marekova, Kenneth G. Paterson, Igors Stepanovs

Problem

Telegram is a popular messaging/chat platform among high risk users (activists, protest participants, etc) due to its claim to be a "encrypted messenger". It uses non-standard protocols to offer this security. However, very little attention is paid to the security analysis of this bespoke cryptographic protocol called MTProto. The authors want to address this by providing a comprehensive study of MTProto. In this paper, the authors specifically study the symmetric cryptography used in MTProto.

Approach

The authors have approached this problem by defining formal model to represent MTProto and proving security properties on it. The security model defines what it means to offer confidentiality (secrecy) and integrity (tamper detect). The authors use security game framework, where the main players are an adversary and challenger, both modelled as algorithms. The challenger algorithm represents MTProto protocol. Three separate game types are defined - correctness, confidentiality and integrity. Each of game types is defined by separate sets of game rules where the adversary can call oracles and chose plain/cipher text. The winner of the game is identified by calculating the advantage of the attacker as probability of winning as defined by the game rules.

A formal model of the MTProto is needed to verify the security as defined by the games above. Unfortunately, there is no official formal spec/model for MTProto. So, the authors define their own formal model while making critical decisions on what aspects need to be modelled. The authors justify various modelling differences mainly due to existing flaws in the protocol, inconsistencies in documentation and its various implementations and various details about the client/server role and message encoding.

The authors evaluate the formal model (MTP-CH) using the security games defined above. The formal model uses various building blocks like MTP-Hash, MTP-KDF, MTP-MAC and MTP-ME. For each primitive, the authors list and discuss various security requirements and assumptions needed to be satisfied. Finally, all of this comes together where the authors prove correctness, indistinguishably and integrity of MTP-CH.

It seems that while the authors were defining the formal model, security model and proving security properties, they also identified 4 concrete attacks - reordering and deletion attacks, timing side channel attack and key exchange attack.

Conclusions

On one hand, the authors show that Telegram's MTProto offers security (along with the suggested fixes) thus assuring Telegram users of confidentiality and integrity offering from MTProto. The authors do note, that there are various assumptions that were made on the underlying primitives used by MTProto and that their analysis so far is limited to only the symmetric cryptography part of MTProto. Also, the paper notes that more refined analysis is required to improve the tightness of their proofs. In short, MTProto offers comparable level of security to TLS which is an industry standard protocol.

On the other hand, the authors show the brittleness of MTProto and the various concerns with rolling out custom crypto solutions. The brittleness comes in various forms - various assumptions made by MTProto about underlying primitives which are anti-patterns, use of little known features like IGE block cipher mode and that there are wide variety of client implementations making it hard to maintain security across all of them.

New Ideas

The idea of defining and using support transcript and support functions was critical to model the correctness, confidentiality and integrity of CH and MTP-CH. To me, this sounded like a good way to define the games.

The separation of channel and protocol was as interesting new idea to me. This allowed me to think about the security at various abstractions particularly what does correctness, confidentiality and integrity mean for a channel and for a protocol operating over this channel.

Improvements

The paper can be improved by providing a short overview of the motivation on the origins of MTProto and why Telegram did not use TLS.

I would have improved this paper further by using illustrations/diagrams to explain the games used to prove security. The intent is to help novice readers assimilate this highly technical paper.

New Directions

As noted in the paper, formal model deviate from implementations/intent of the protocol. Telegram could address this by providing a formal spec/model. Further, there should be some language (similar to TLA+) and tooling to derive a formal model from implementation and/or vice versa. This would help defining the protocol, implementing it and assuring security guarantees. If we have a standardized formal model language, we could have tools to verify the security properties.

Given the GenAI trend at the moment, would GenAI be able to train on the implementations, derive a formal model and determine attacks and mitigation. This would be an interesting direction.