TLS MITM attack on the Ripple XRP Ledger

Research Project (CSE3000) by Wolfgang Bubberman
Supervised by Stefanie Roos & Satwik Prabhu Kumble / 25 June 2020

1. PROBLEM

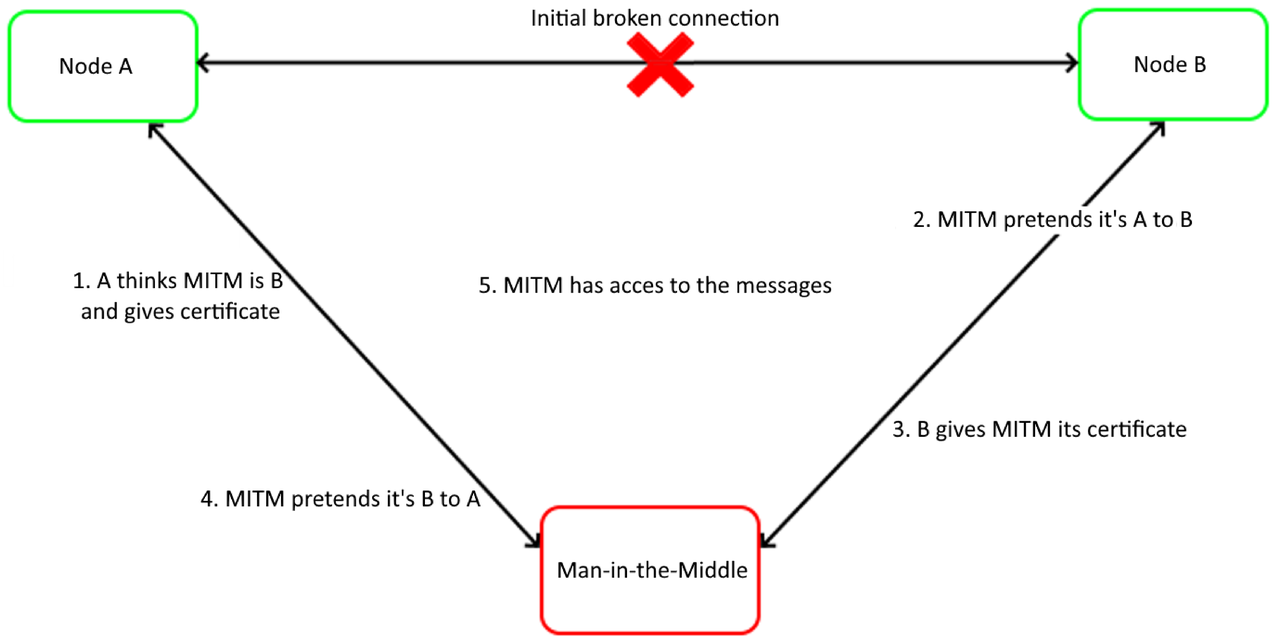
- Decentralized networks, cryptos and blockchains growing in popularity
- Security is important
- Man-in-the-Middle attacks pose a threat

2. RIPPLE

- Decentralized money transfer network
- XRP Ledger Consensus Protocol

3. MAN-IN-THE-MIDDLE ATTACKS

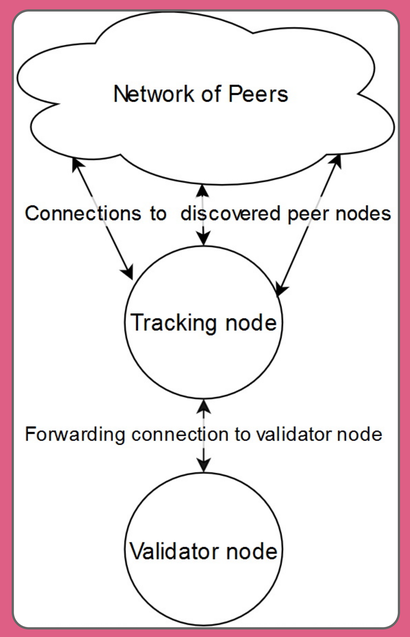
- Between client and server
- Active attack
- Operates as proxy
- Certificates and the Certificate Authority (CA)



High-level showcase of the TLS MITM attack in the situation where A wants to send B a message

4. SETUP

- Test-bed environment
- One tracking node, one validator node
- Connection between two nodes attacked by MITM



5. RESULTS

- It is possible to conduct a TLS MITM attack on the XRP Ledger
- Hard to quantify impact on performance
- Added delay in tested environment 69.2%

6. FUTURE WORK

- Message content not manipulable, could be done
- Flakiness in capturing of responses to proxied messages
- Anti-MITM measures by Ripple

TU Delft