Node ECP Server - Security Model (SSL)

Filename: SM-0200.svg

Project (in-dev): NodeECPtest1 Snapshot: alpha 0.2.4-0200 Content Type: Security Model

Date: Jan 31 2017 Author: dsalex1

Legend

Https Client: Client Https Server: Server Attacker: Mallory Symetric Key: Server public Key: Server private Key: Client cert.: Cert signed by trus. CA: Crt Selfsigned Root CA cert.: [54] Client public key: Client private key:

Szenario 1: Szenario 2: Szenario 3: Szenario 4: Client and Server Mallory pretends Mallory pretends Mallory observes the are non mallicios to be the Server to be the Client connection Client and server negotiate protocol 1. Client hello Version 2. Server hello Server sends its Mallory Mallroy Client Client Client Server Crt Mallrov Server certificate which is Certificate checked agains public CA 4. request Client Cert. 5. Server hello done Client sends its Client Mallroy Server certificate which is Crt Mallory Client Mallroy Server Server Crt 6. Certificate Cit checked against Crt Crt own root CA Client sends pre-7. ClientKev-Mallroy master kev signed Client Server Mallory Mallroy Server Client Client Server with servers public Exchange Crt Crt key 8. Certificate-Client sends previos Client Server Mallory Mallroy Server Mallroy Client Client Server VIa... messages signed ≅□□ Verify with its private key Mallroy If the msgs can be decrypted with the clients public key it is trusted to be the owner of the certificate. Mallory Server Client Client Mallroy Server Client Server □ Cr Ct Ct be the owner of the certificate. Client and Server 9.Change Trusted CipherSpec send finished msg decrypted using the Mallory Client Mallroy ok Server ok ok master key if both msg could be decrypted Trusted Trusted Mallory Client Mallroy Client properly the handshake is completed. Client Server An authenticated encrypted connection has been etablished

- 1*: Due to the llack of the Server's private key the 2*: Due to the lack of the Client's private key the encrypted pre-master key couldn't be decrypted
 - Certificate Verify msg couldn't be signed properly
- 3*: All information ratherd is non sensetive nor useful to hijack the connection