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: Selfsigned Root CA cert.: [7] Client public key:

Client private key:

Client hello Server hello	Client and server negotiate protocol Version	Szenario 1: Client and Server are non mallicios	Szenario 2: Mallory pretends to be the Server	Szenario 3: Mallory pretends to be the Client	Szenario 4: Mallory observes the connection
3. Certificate 4. request Client Cert.	Server sends its certificate which is checked agains public CA	Client Crt Server	Client Crt Mallory	Mallroy Crt Server	Client Mallroy Crt Server
5. Server hello done 6. Certificate	Client sends its certificate which is checked against own root CA	Client Server	Client Crt Mallory	Mallroy Crt Server	Client Crt Mallroy Server
7. ClientKey- Exchange	Client sends pre- master key signed with servers public key	Client Server	Client 1* Mallory	Mallroy Server	Client Mallroy Server
8.Certificate- Verify	Client sends previos messages signed with its private key	Client Server	Client Mallory	Mallroy 2* Server	Client Mallroy Server
the clients public be the owner of		Server	Mallory	Server	Mallroy Server
9.Change s CipherSpec d	Client and Server end finished msg lecrypted using the naster key	Server	Mallory Mallory	1 	Maliroy Server
if both msg could b properly the hands An authenticated e co <u>nnection has bee</u>	hake is completed. ncrypted		Pagent	 	Mallroy 31

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