MAN-IN-THE-MIDDLE ATTACK

DESCRIPTION

Adversary replace or intercept the certificate and encryption parameter with its own and fake their identity by using a certificate signed by rogue authorities which the user wrongly assume it is coming from legitimate service, allowing the adversary to observe all information transfer between the user and the legitimate service

IMPACT

Steal data encrypted by parameter sent with the rogue certificate

a_A1