

Project 2: SSL MiTM

Botao Hu (botaohu@stanford.edu), Borui Wang (borui@stanford.edu)

March 16, 2013

1 Design

This project implements a man-in-the-middle attack on SSL by implementing a SSL proxy server. Using keytool, we first created a keystore.

2 Steps to run

1. Create a private key in a keystore by running

```
1 keytool -genkeypair -dname "CN=Very Secure Software, OU=Very Secure Software Group,  
2   O=Very Secure Inc, L=Cupertino, S=California, C=US" -alias mykey -keypass foobar  
3   -keystore ./keystore -storepass foobar -validity 365 -keyalg RSA
```

The password for keystore is foobar, which is specified in password.txt as requested by the project assignment.

2. Run the SSL proxy server with the command

```
1 java -classpath ${CLASSPATH}::iaik_jce.jar mitm.MITMProxyServer  
2   -keyStore keystore -keyStorePassword foobar -pwdFile pwdFile
```

3. Set the SSL proxy of your browser to localhost:8001.
4. Visit a https site with the browser.

3 Short Answers

- (1) Q: Suppose an attacker controls the network hardware and can intercept or redirect messages. Show how such an attacker can control the admin server just as well as a legitimate admin client elsewhere on the network. Give a complete and specific description of the changes you would make to fix this vulnerability.

A:

- (2) Q: Suppose an attacker is trying to gain unauthorized access to your MITM server by making its own queries to the admin interface. Consider the security of your implementation against an attacker who (a) can read the admin server's password file, but cannot write to it; (b) can read and/or write to the password file between invocations of the admin server. For each threat model, either show that your implementation is secure, or give an attack. (N.B.: For full credit, your implementation should at least be secure under (a).) What, if anything, would you need to change in order to make it secure under (b)? If your answer requires any additional cryptographic tools, you should fully specify them (including the names of any algorithms, cryptosystems, and/or modes of operation that you would use.)

- (3) Q: How would you change a web browser to make it less likely that an end user would be fooled by a MITM attack like the one you have implemented? (This is an important question to ask because when dealing with security, we never just build attacks: we also need to think of ways to prevent them.)

A: