Jordan Bayles
June 6, 2014

Homework 5
ECE 478: Network Security

0. Disclaimer

This submission reflects my own understanding of the homework and solutions. All of the ideas are my own, unless I explicitly acknowledge otherwise.

1 Eavesdropping Tasks

1.1 What kind of data is being transmitted in cleartext?

1.2 What ports, what protocols?

1.3 Can you extract identify any meaningful information from the data? e.g., if a telnet session is active, what is happening in the sesion? If a file is being transferred, can you identify the data in the file?

1.4 Is any authentication information being sent over the wire? e.g., usernames and passwords. If so, what are they? What usernames and passwords can you discover?

1.5 Is any communication encrypted? What ports?

2 Replay Attack against the Stock Ticker

2.1 Explain exactly how to execute the attack, including the specific RPCs you replayed.

2.2 Explain how you determined that this strategy would work.

2.3 Execute your replay attack and show the results of your attack with a screen capture, text dump, etc. showing that you are controlling the prices on the stock ticker.

3 Insertion Attack

3.1 You can change the symbols a viewer of the ticker sees by intercepting the HTML bound for their browser. Write a filter to change the symbol FZCO to OWND.

3.2 Write a filter to affect the prices a user of the stock ticker sees. Include your filter sources with your submission materials.

3.3 Given the power of etterfilter and the kinds of traffic on this network, you can actually make significant changes to a machine or machines that you're not even logged in to. How?

3.4 Of the cleartext protocols in use, can you perform any other dirty tricks using insertion attacks? The more nasty and clever they are, the better.

4 MITM vs. Encryption

4.1 What configuration elements did you have to change?

4.2 Why doesn't it work to use tcpdump to capture this "decrypted" data?

4.3 For this exploit to work, it is necessary for users to blindly "click OK" without investigating the certificate issues. Why is this necessary?

4.4 What is the encrypted data they're hiding?