Jonathan Nguy

1. EAVESDROPPING

1. The data that's being transmitted in cleartext seems to be http GET requests.

It seems like the data is being transmitted via the HTTP protocol on port 80.

There also seems to be telnet communications in cleartext via port 23.

There is a lot of html being transferred to Bob.

Alice also updates Bob's stocks via stocks.cgi. (She updates it using something like GET /cgi-bin/stock.cgi?symbol=DNGL&new=76&hash=e96448d96721224ae48d0fa7baf53b0d.. and this seems to update the DNGL stock to "76")

Also, Bob tries to access the html by using the access1.cgi file.

2. Some sort of authentication would be user: jumbo, password: donald78 | jambo, password minnie77 | jimbo, password goofy76

3. The encrypted communication seems to be on port 443. (This is the HTTPS/ "secure" parts of the data)

2. REPLAY ATTACK

1. To execute this attack, I had to look through the things I sniffed, and I noticed that the stocks are updated by using an RPC like:

GET /cgi-bin/stock.cgi?symbol=FZCO&new=17&hash=5482d9afd8bdfb055114f449b5b67698

In this example, the stock FZCO would update to the 'new' value of 17. The hash is there to prevent a change in the number or symbol.

(I tried to change the symbol name to another name, and the new number to a different number, but I got the following error:

PROTOCOL ERROR! Cryptographic stamp incorrect. Stock price update ([symbol]; [number]) rejected. Basically, the encrypting hash did not match.)

2. To determine this worked, I attempted to replay the RPC by typing this into my browser:

- To get FZCO to be low:

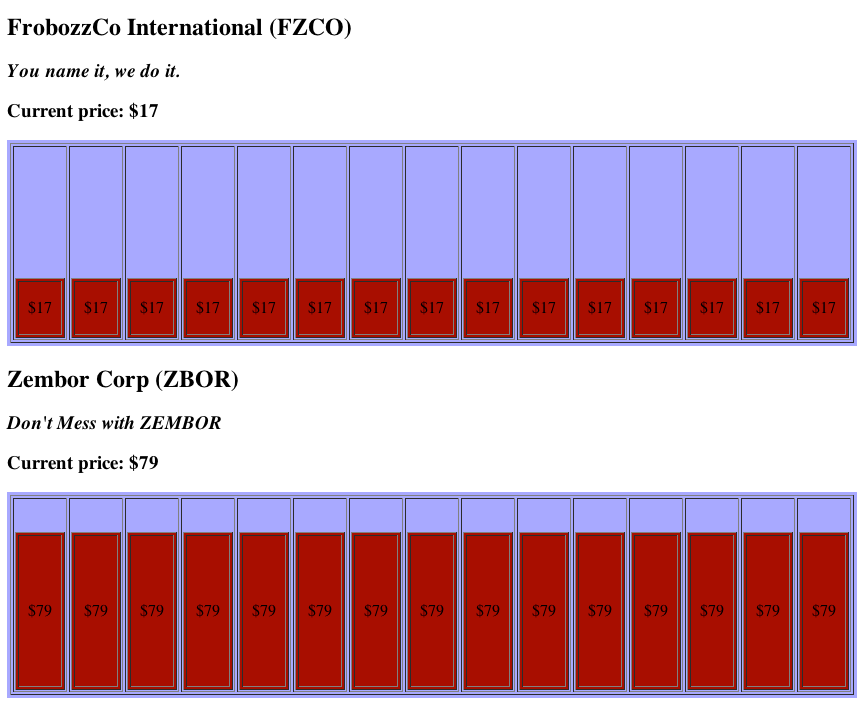
http://localhost:8118/cgi-bin/stock.cgi?symbol=FZCO&new=17&hash=5482d9afd8bdfb055114f449b5b67698

- To get ZBOR to be high:

http://localhost:8118/cgi-bin/stock.cgi?symbol=ZBOR&new=79&hash=5f70f9a4e87efd4e2a76b45389ed685e

I determined these were the right ones because I looked through all the data I sniffed and found the ones that matched the symbol of the stock, and either a high/low number.

3. Here’s a screenshot for proof:



3. INSERTION ATTACK

3. Here is my filter:

#it's using TCP protocol from soruce 80 (bob's port)

if (ip.proto == TCP && tcp.src == 80) {

# replace FZCO with OWND

replace("FZCO", "OWND");

# replace $ with $300

replace("$", "$300");

}

This filter basically replaces FZCO and OWND. It also replaces any $ with $300, so anyone would see the number $x as $300x.

1. I think that etterfilter can do something similar to the pathname attacks/injections that we did in the previous lab. It can put its own malicious code to “replace” and then execute it.
2. I think there would be a way to do some sort of pathname attack using these protocols. If we knew how to create a good hash, we could change the stocks to anything we wanted.

4. MITM & ENCRYPTION

1. The part of the configuration that I changed was this part:

# if you use iptables:

redir\_command\_on = “iptables -t nat -A PREROUTING -i %iface -p tcp –dport %port -j REDIRECT –to-port %rport”

redir\_command\_off = “iptables -t nat -D PREROUTING -i %iface -p tcp –dport %port -j REDIRECT –to-port %rport”

I uncommented those parts that were previously commented out.

I also changed this part:

ec\_uid = 65534 # nobody is the default

ec\_gid = 65534 # nobody is the default

to:

ec\_uid = 0

ec\_gid = 0

2. Some of the data I found was:

564 INT. INNER CHAMBER OF MCP

Over Dumont's shoulder, with a view of the MCP. Zoom IN on MCP face.

MCP

Welcome!

565 EXT. CARRIER BRIDGE

Flynn and Yori race into view. We can see two of the memory guards

in a de-rezzed, two dimensional state, disappearing completely in

the course of this scene. Flynn runs to Sark's position, looking out the window

3. Tcpdump doesn't capture the decrypted data because it isn't compiled with cryptography enabled. (From tcpdump man page)

4. If the users don't "click OK", it wont allow the user to access those webpages/ share the certificates.

If that happens, the data will not be sent over and the hacker wont be able to steal the information.

5. After Google'ing the data I found, I know that the information they're hiding is the Tron screenplay.