Design Document

for

Covert Channels

<Assignment 1>

Version 1.0

Prepared by Wesley Yue

September 24, 2012

Table of Contents

1. Introduction

1.1 Abstract

This assignment analyses and modifies the covert channel program, covert_tcp.c, which is designed and developed by Craig H. Rowland.

A covert channel, as described by Craig H. Rowland, means “any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy.” In this assignment, it demonstrates that an alternative file transfer technique, other than Rowland’s technique methods, can be transferred over a covert channel.

1.2 Analysis and Improvements

One of the weaknesses in Rowland’s program was the timing between sent packets. In the covert_tcp file, every packet was sent after a one second pause. Thus, it is vulnerable to anyone looking for this IDS signature. To avoid the detection of anyone looking for this signature, randomized seconds was used. In this assignment, the covert_channel file uses a range of 1-10 seconds that are randomized to insert between each sent packet.

A second weakness of Rowland’s program is the bounce server that is used in the covert_tcp file. If a stateful firewall is in place, then the firewall from the server rejects the covert channel. The reason is because the bounce server sends a SYN-ACK to the server, which is neither a new nor an established connection. Thus, the stateful firewall drops that particular packet. In this assignment, the covert_channel uses a direct connection to the server, but with a spoofed IP address. The use of this method avoids the detection of the stateful firewall, plus it hides the original IP address of the client.

The third weakness of Rowland’s program was stated in his article. The article mentioned that the embedded file content character in either the IP identification field or the TCP sequence number could be identified in the file transfer. In this assignment, the covert_channel forges the embedded file content in the IP time to live field. The reason why the embedded file content is in that field is because this field is mostly overlooked. Moreover, the time to live field will not be zero because that indicates null, which likely will not be used.

It should be mentioned that they were a couple weaknesses in Rowland’s covert_tcp file, but they were not fixed for this assignment. One other weakness is the use of spoofed IP addresses, which triggered the actually IP address to send RST packets to the server. Another weakness that was not fixed is the lack of ability to communicate with the server to determine the file size and estimation time of completion.

2. Design

2.1. Pseudo-Code

covert channel pseudo-code

```
Define function prototypes;
Define global variables;
Main() function {
    Initialize parameters and set defaults;
    Validate if user is root (else fail);
    Validate command-line parameters (else fail);
    Forgepacket() function;
    Exit;
}

Forgepacket() function {
    Define local variables;
    If (running as client) {
        Open file to be transferred (else fail);
        Sleep for 1-10 seconds;
        Forge IP and TCP header;
        Open raw socket (else fail);
        Calculate packet checksums;
        Send TCP packet;
        Increment IP address variable;
        Restartincrement() function;
        Close socket;
    }
    Close file input;
    Else (running as server){
        Create new file to be transferred (else fail);
        While(true){
            Open receive socket (else fail);
            Read TCP packet;
            If(Receive packet's syn = 1 && Receive packet's saddr = ipAddress){
                Decode TTL field and print it to file output
            }
            else(Receive packet's syn = 1 && Receive packet's dest = sPort){
                Decode TTL field and print it to file output
            }
```

```
                    Increment IP address variable;
                    Restartincrement() function;;
                    Close receive socket;
                }
                Close file output;
        }
}

Restartincrement() function {
        If (n=254)
                n = 0;
        return n;
}
```

2.2. Command-Line Parameters

-dest dest_ip	- Host to send data to. In server mode this is the server IP address.
-source_port port	- IP source port you want data to appear from.
-dest_port port	- IP source port you want data to go to. In server mode this is the port data will be coming on.
-file filename	- Name of the file to encode and transfer.
-server	- Server mode to allow receiving of data.

3. Summary

The Rowland's covert_tcp program for implementing covert channels has been improved and modified through the use of IP TTL packets. However, there are couples of remaining issues to be fixed in the covert_tcp program.

In this assignment, a few weaknesses in the covert_tcp program were analyzed and fixed. The timing between each packet sent has been fixed with randomizing to 1-10 seconds instead of the constant 1 second interval. Also, a direct connection to the server with a spoofed IP address fixed the problem with stateful firewall. Lastly, the covert_channel forges the embedded file content to the IP time to live field, which reduces the problem with the content being identified in the file transfer. It reduces the problem because the TTL field is overlooked.

The accompanying DVD will include the complete source code, and pcaps files for confirmation of design and evidence of test results. Also, the DVD will include this and testing document.

4. Appendix

/root directory:	
client.pcap	(client's Wireshark packet capture file)
server.pcap	(server's Wireshark packet capture file)
/documents/ directory:	
WY_DesignDocument_Assignment1.docx	(this file)
WY_DesignDocument_Assignment1.pdf	(pdf version of this file)
WY_Testing_Assignment1.docx	(docx version of the testing file for the covert channel)
WY_Testing_Assignment1.pdf	(pdf version of the testing file for the covert channel)
/src/ directory:	
covert_channel	(c executable file for this assignment)
covert_channel.c	(c main source file for this assignment)
covert_channel.h	(c header file for this assignment)
hello_world	(file used for transfer)