

Workshop on Network Traffic Capturing and Analysis IITG, DIT, CERT-In, C-DAC

Host based Analysis

{Himanshu Pareek, himanshup@cdac.in}

{C-DAC Hyderabad, www.cdachyd.in}

Reference to previous lecture

- Bots use ICMP for passing commands
 - Covert channel hacking
- SYN flooding attacks
- Key logger attacks
- Current Patch Process
- Autorun.INF
- Runs as a DLL attached to svchost.exe

Outline

- Introduction
- Network monitoring tools
- Analysis for malicious activities
- Application level analysis
- Developer's Call
 - Implementing software packet capture

Prerequisites

- What is a socket
 - Socket is the interface between the application layer and transport layer within a host
- Three way TCP handshake
- ARP
- HTTP Headers for Request and Response
- TCP Segment and UDP Datagram

HTTP : Request

```
GET http://eleltech/ftrans/include/global.css HTTP/1.0
Accept: */*
Referer: http://eleltech/ftrans/file.asp
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 28 May 2002 14:00:16 GMT
If-None-Match: "0d864fe4f6c21:920"
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: eleltech
Connection: Keep-Alive
Cookie: ASPSESSIONIDGGGGQHUY=FNDDHOJAKBDGNILPFHDOHGMM
```

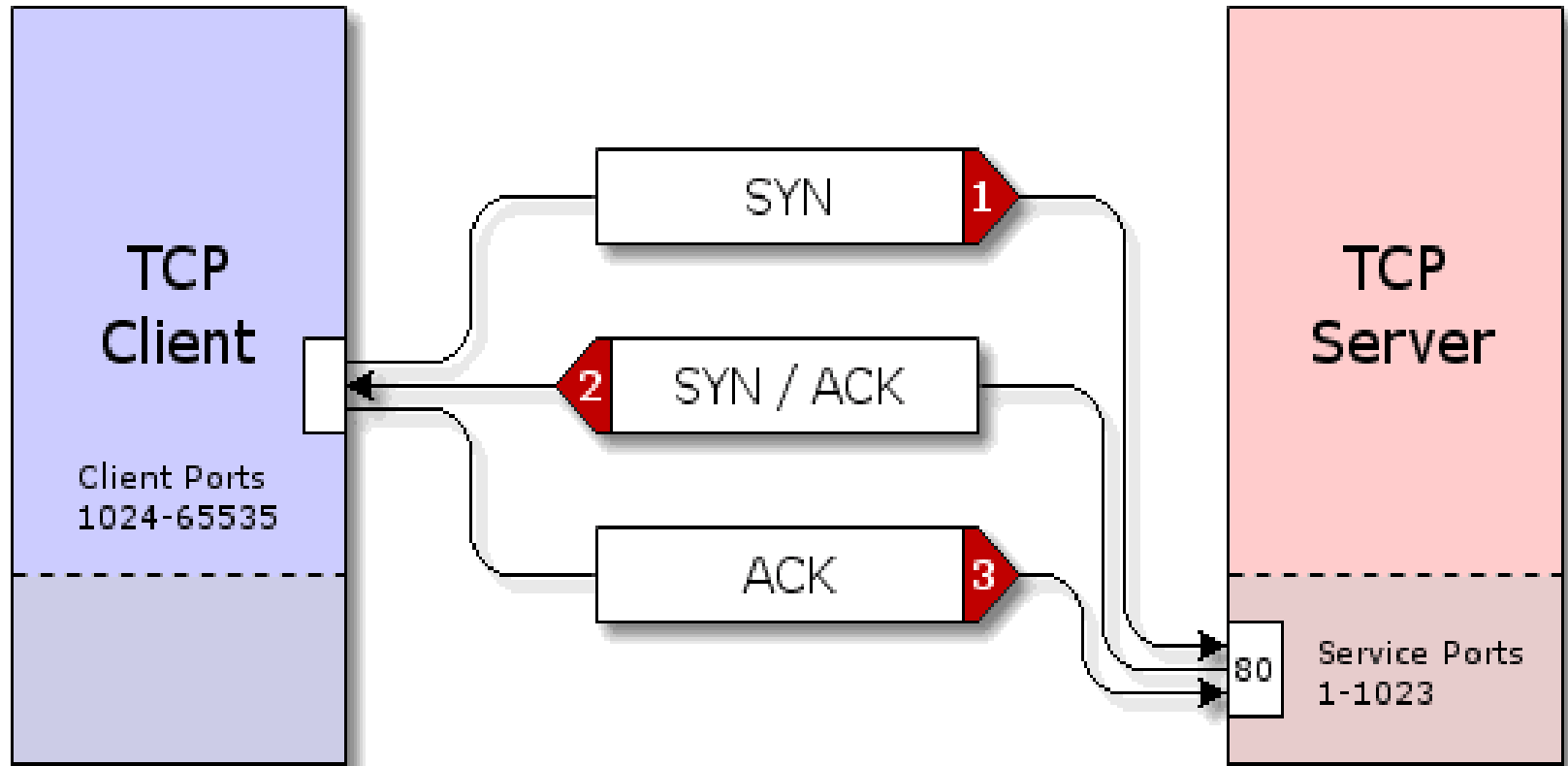
```
POST http://eleltech/ftrans/file_post.asp HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, */*
Referer: http://eleltech/ftrans/file.asp
Accept-Language: en-us
Content-Type: multipart/form-data; boundary=-----7d212843d0156
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: eleltech
Content-Length: 3359
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: ASPSESSIONIDGGGGQHUY=FNDDHOJAKBDGNILPFHDOHGMM
```

HTTP : Response

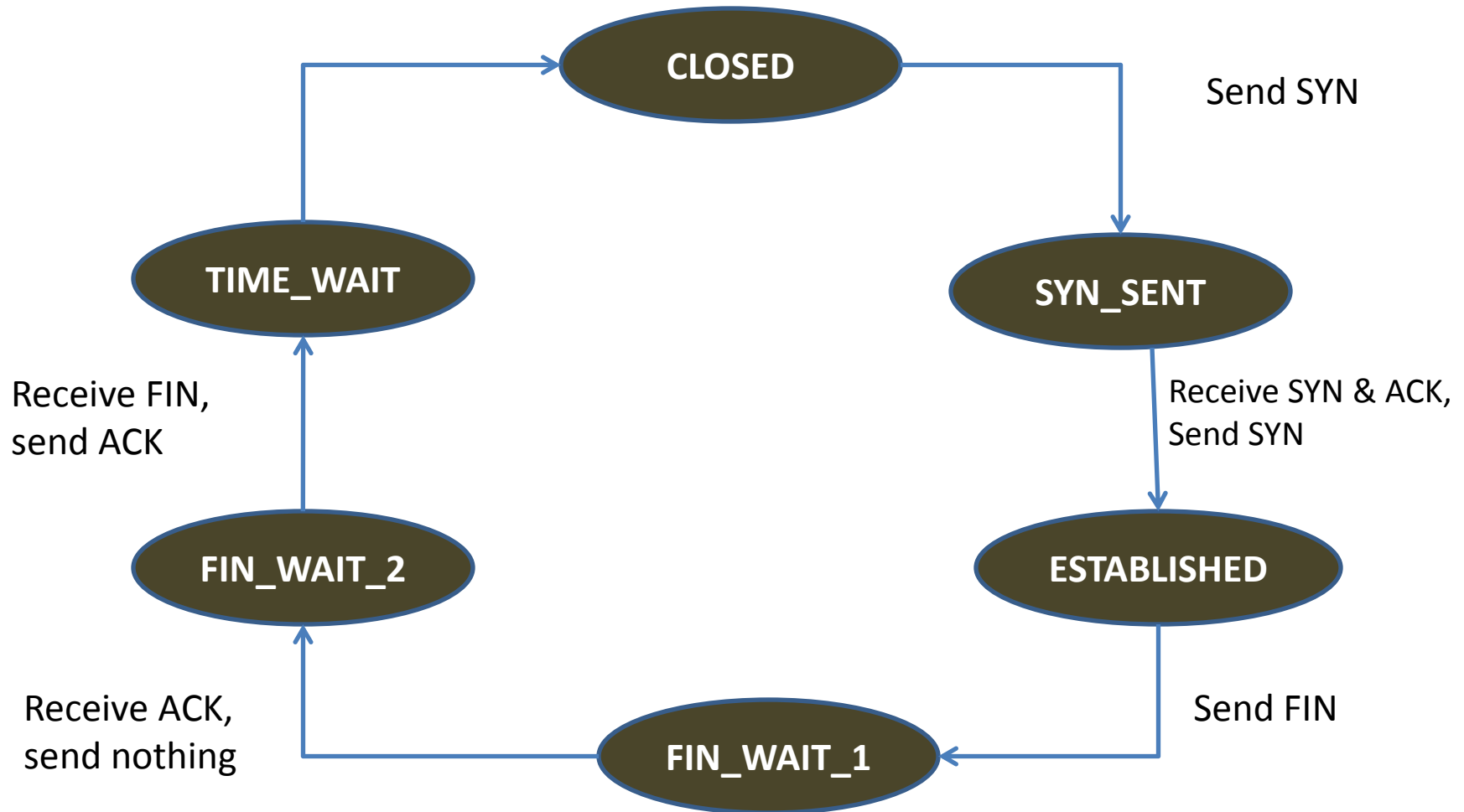
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 13 Jun 2002 05:00:06 GMT
Content-Length: 2135
Content-Type: text/html
Set-Cookie: ASPSESSIONIDGQQGGUEY=FOHLGDBAHDOCBCIDNHEHAFNN; path=/
Cache-control: private
```

```
<!doctype html public "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>File Transfer Utility</title>
<link href="include/global.css" rel=stylesheet>
</head>
<style>
input {      font: 8pt Verdana; }
body {      font: 8pt Verdana; }
</style>
<body>
<center>
```

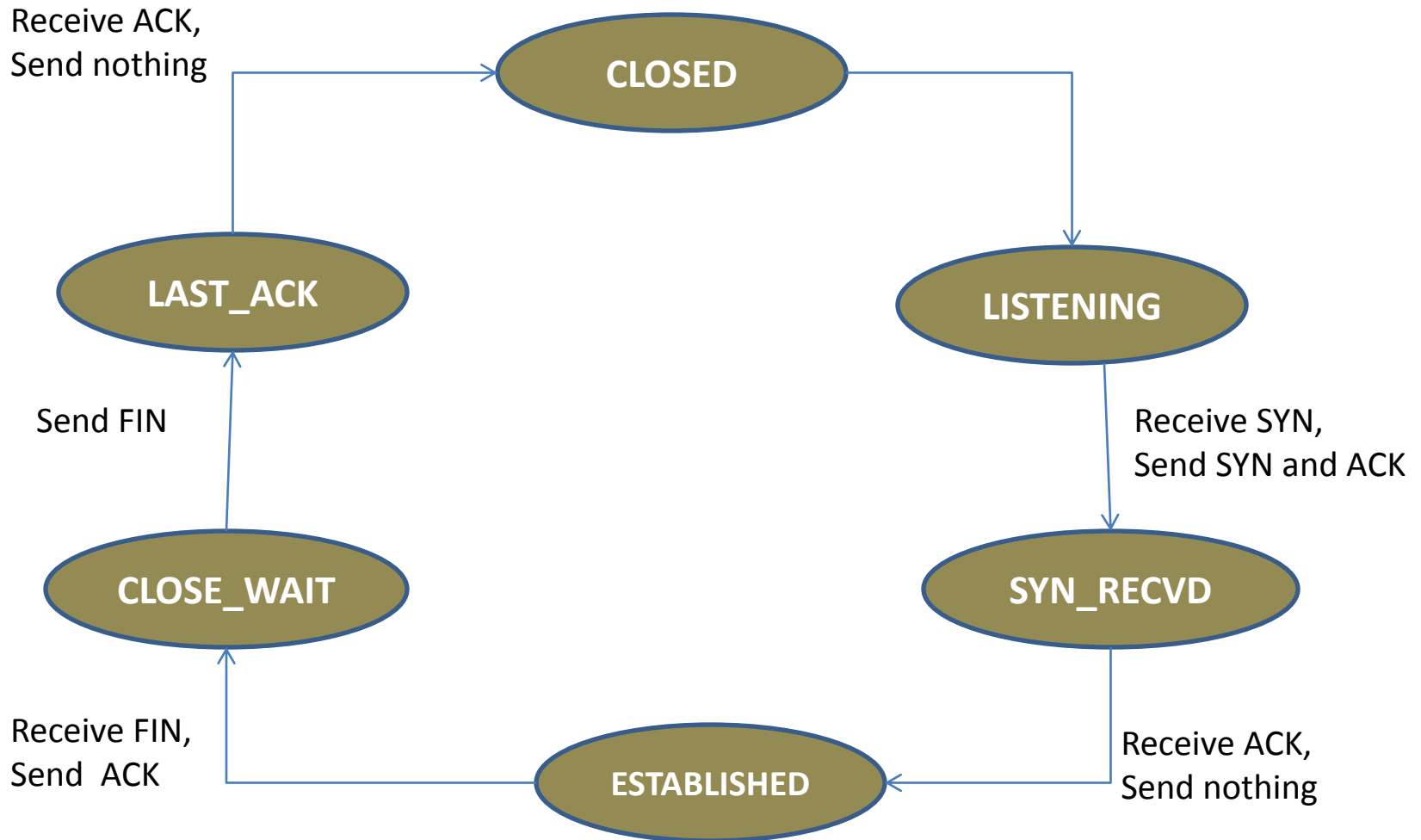
Three way TCP Handshake



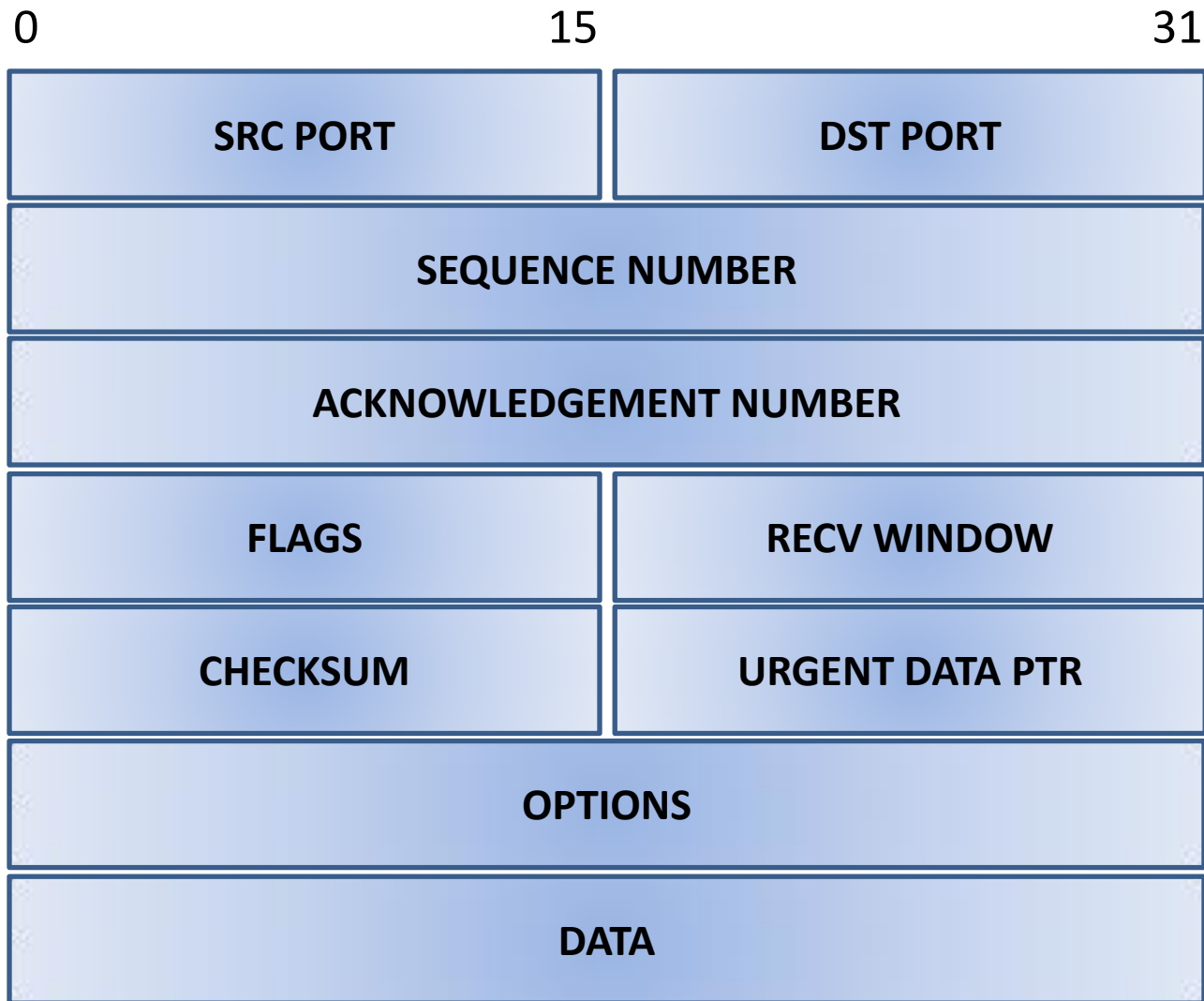
States for a TCP Client



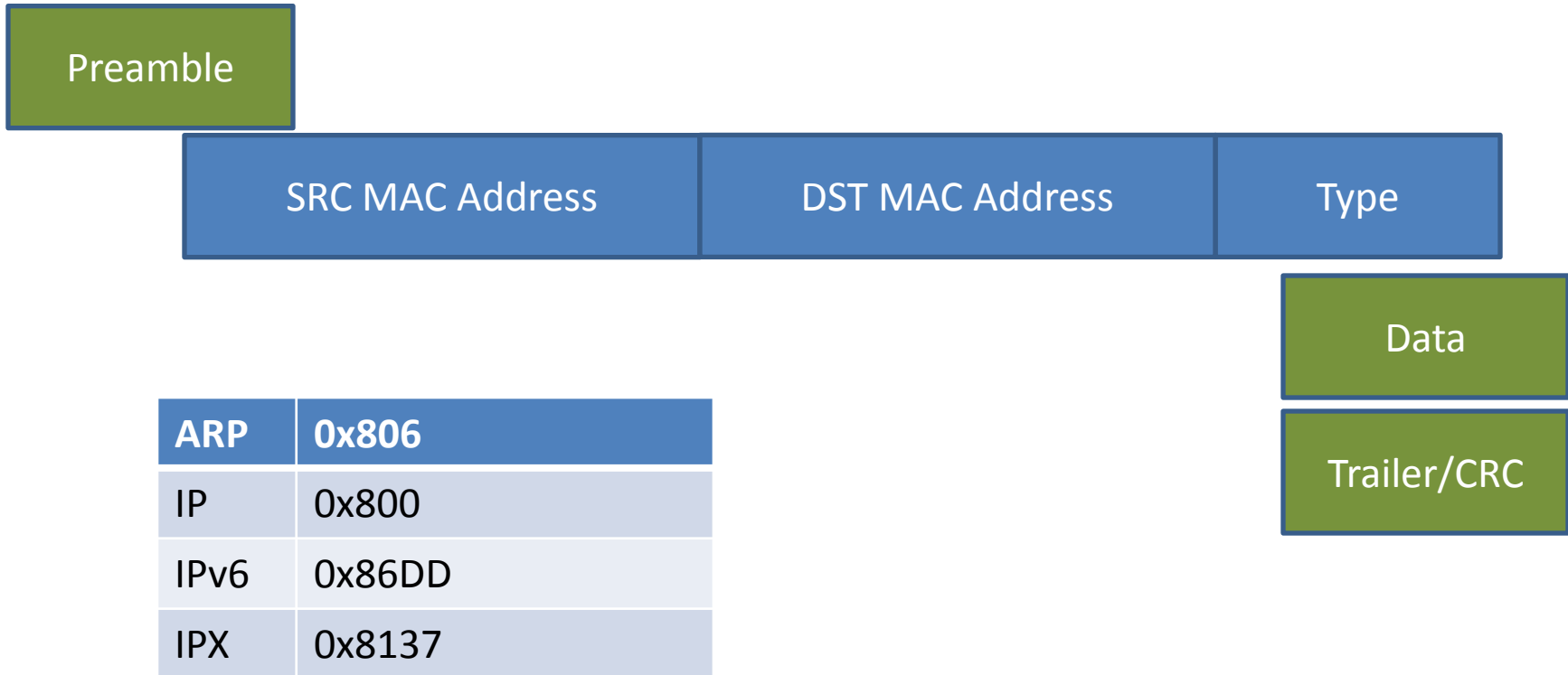
States for a TCP Server



TCP Segment



Ethernet Frame



Analysis of mal-activities

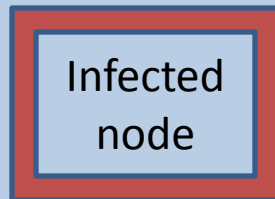
- Automated Analysis for detecting attacks
 - Using HIDS / HIPS / Network Security Solution
 - OSSEC, OSIRIS, EnSAFE, Sana, Server IPS
- Manual analysis
 - Why it is important
 - A simple case
- Cost of ownership should be compared.
- Ability to handle encryption
- Useful in reversing the malware
- No single point of failure as in case of NIDS/NIPS

LAN

Antivirus updated



IDS



1. makes a *silent* scan of network
2. Detects a Vista system
3. Trying to connect at 137

Do it regular

- **Checked ARP entries with command**
 - ‘arp -a’
- **Found a suspicious entry x.x.x.12**
- **Started WIRESHARK**
 - It was sending ARPs to all the hosts in a small intervals of time
- **Allowed to scan my system 😊**
- **Sent SYNs to 137**
- **Use TCP View to check concerned process (to ports) on both the victim system**
- **You can carry out the manual malware cleaning then.**

Continued

- Network packet monitoring
 - WIRESHARK (wireshark.org)
 - Network Miner (networkminer.wiki.sourceforge.net)
 - MS Network Monitor (Microsoft)
- Application level
 - Want to monitor application behavior
 - Anomaly detection at system call level
 - System call interception
 - Is it feasible with growing security requirements?

Traffic analysis of mal-activities

- IP Scanner

Traffic analysis of mal-activities

- A scan of a particular system

Traffic analysis of mal-activities

- Ms04-011 vulnerability getting exploited through a system
 - Stack overflow in LSASS service
- <http://www.microsoft.com/technet/security/Bulletin/MS04-011.msp>

System Window Help

Cancel Find

Exploits All loaded exploit modules (261)

- windows
 - smb
 - ms04_011_lsass** Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
 - ms04_011_pct Microsoft Private Communications Transport Overflow
- Auxiliary All loaded auxiliary modules (46)

Jobs

Job ID	Module
Jobs	

Sessions

Target	Type
1 192.168.53.65:4444	shell

Module Information Module Output

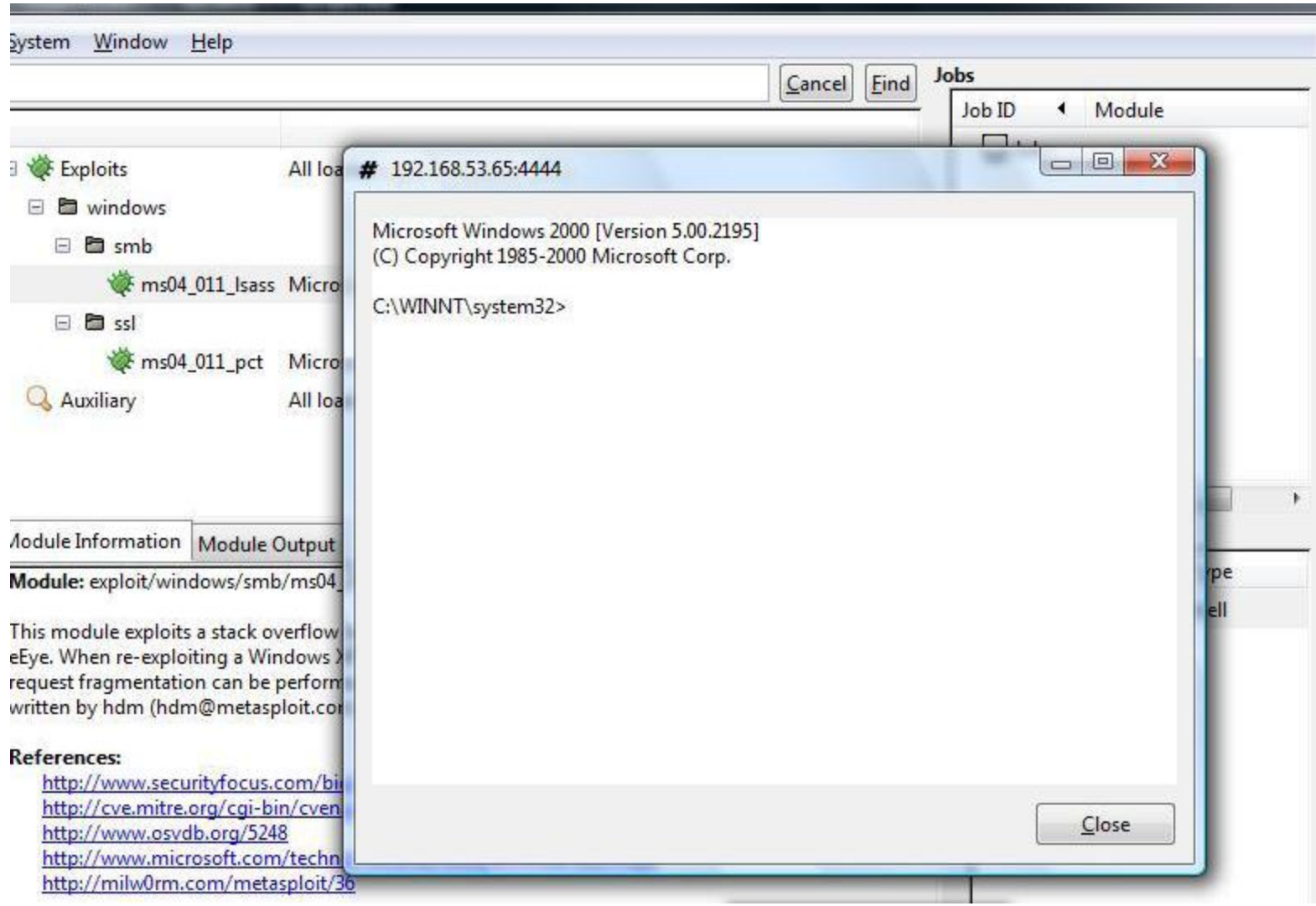
Module: exploit/windows/smb/ms04_011_lsass

This module exploits a stack overflow in the LSASS service, this vulnerability was originally found by eEye. When re-exploiting a Windows XP system, you will need need to run this module twice. DCERPC request fragmentation can be performed by setting 'FragSize' parameter. This exploit module was written by hdm (hdm@metasploit.com)

References:

- <http://www.securityfocus.com/bid/10108>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0533>
- <http://www.osvdb.org/5248>
- <http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>
- <http://milw0rm.com/metasploit/36>

Loaded 261 exploits, 117 payloads, 17 encoders, 6 nops, and 46 auxiliary



System Window Help

Cancel Find

Jobs

Job ID Module

- Exploits All loaded
 - windows
 - smb
 - ms04_011_isass Microsoft
 - ssl
 - ms04_011_pct Microsoft
- Auxiliary All loaded

Module Information Module Output

Module: exploit/windows/smb/ms04_011_isass

This module exploits a stack overflow in the eEye. When re-exploiting a Windows machine, request fragmentation can be performed. Written by hdm (hdm@metasploit.com)

References:

- <http://www.securityfocus.com/bid/17557>
- <http://cve.mitre.org/cgi-bin/cvenum.cgi?id=CVE-2003-0655>
- <http://www.osvdb.org/5248>
- <http://www.microsoft.com/technet/security/bullet/03-022.mspx>
- <http://milw0rm.com/metasploit/36>

Close

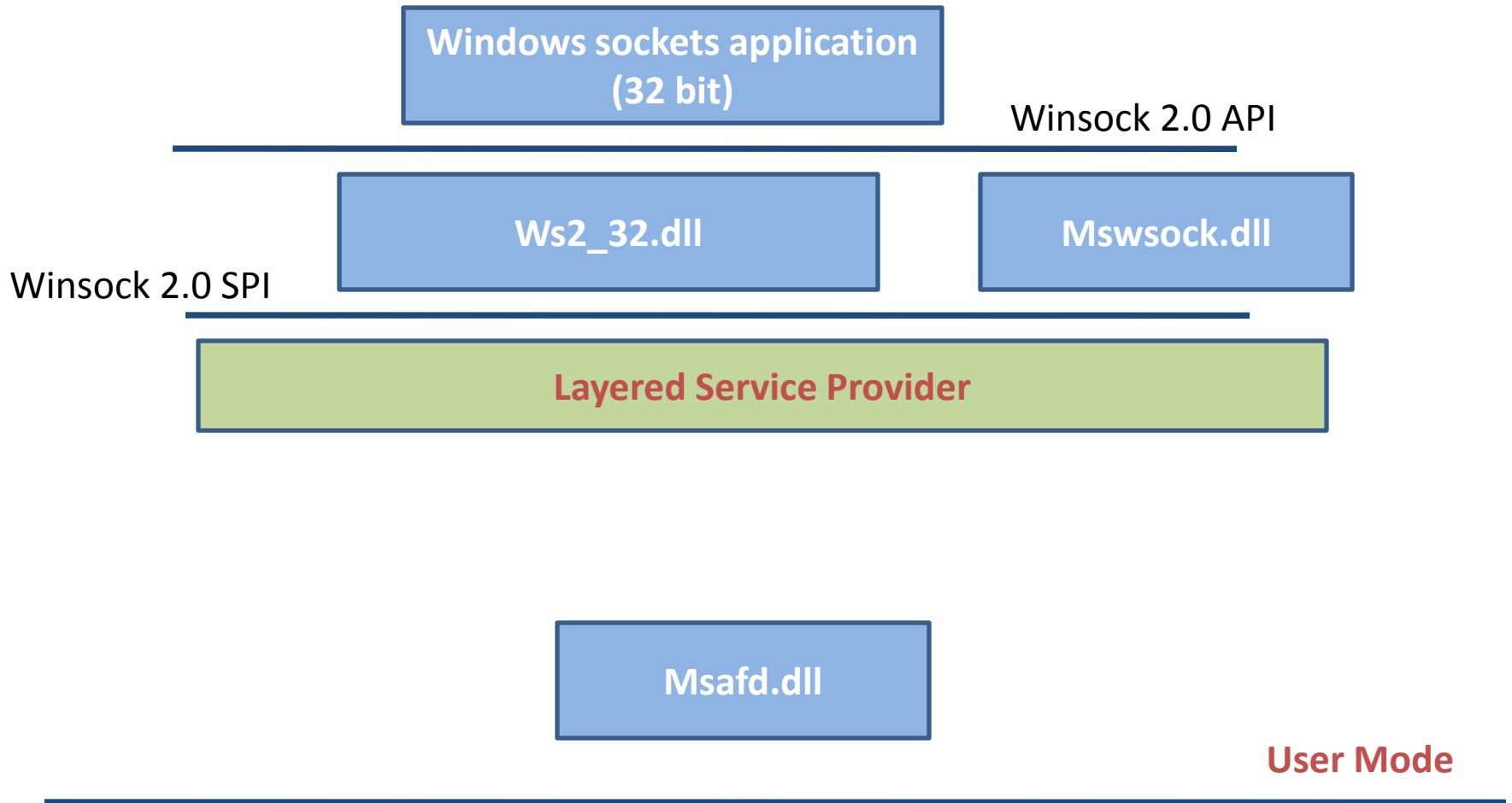
Other Tools For Analysis

- PacketMon
- IP Sniffer
- Network Probe
- Sniff_hit
- UfaSoft Sniff for capturing packets at Wi-Fi links
- CaptureBAT (Honeynet Project)

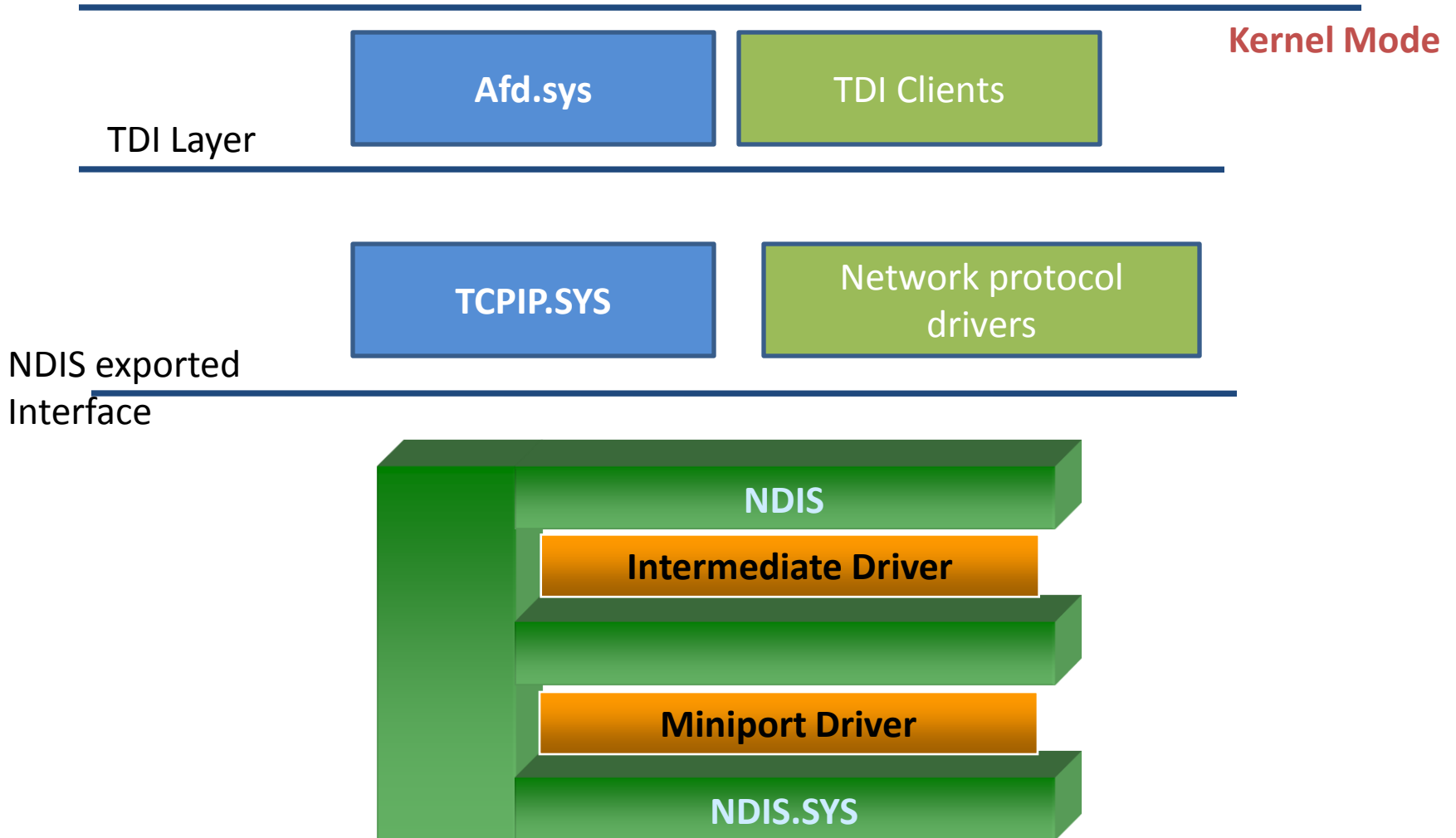
Tip: help in reversing malware binary

- Run malware binary using virtualized OS
 - MS Virtual PC
 - Sun xVM VirtualBox
- Use any tool to monitor its network activity
 - Use snort to monitor the activity
 - http request packet analysis

Windows networking architecture © Microsoft



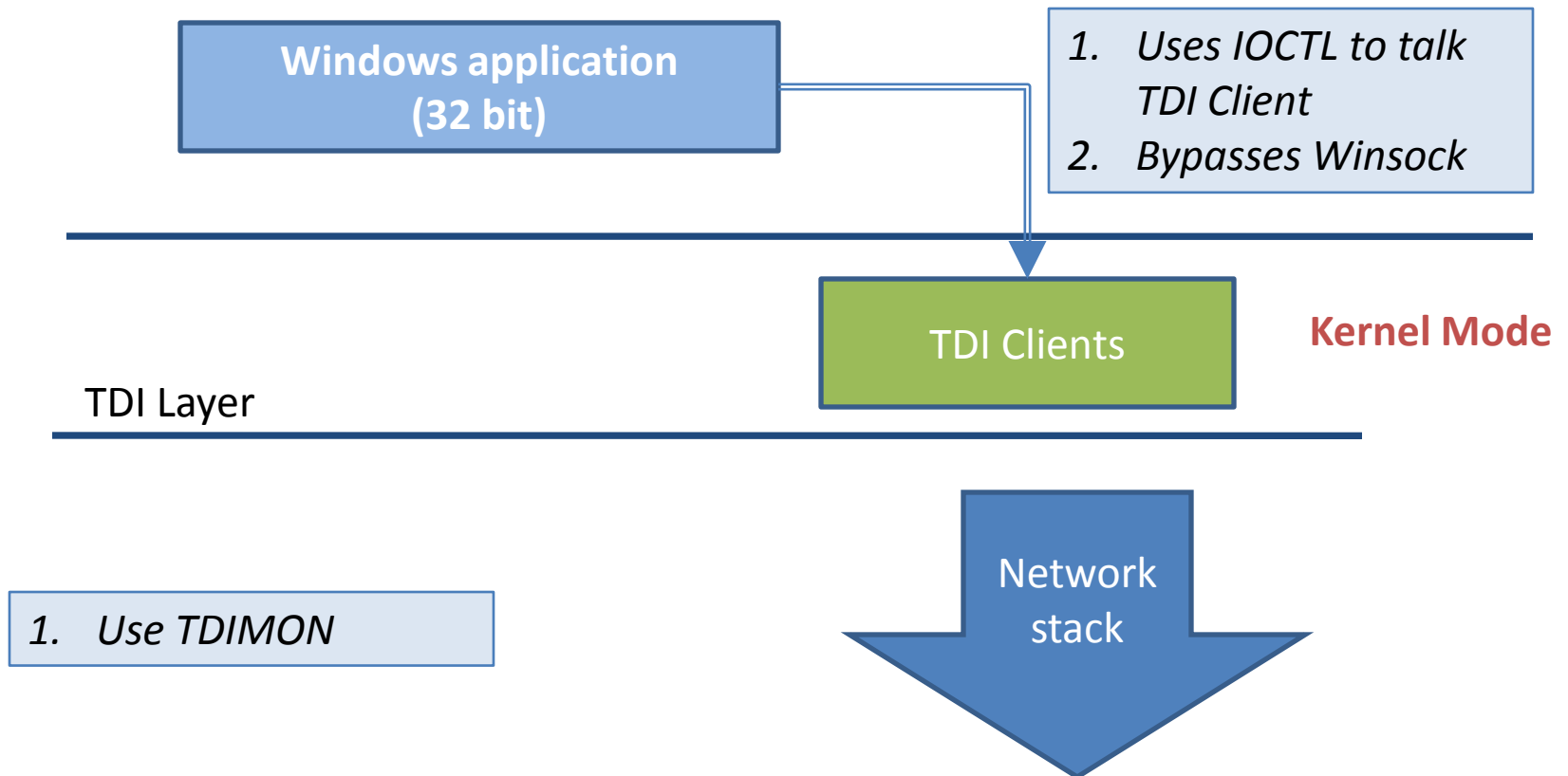
Contd.



Application level analysis

- System call interception
 - Not supported
 - Rootkits
- Documented interfaces
 - LSP
 - WSP APIs in the SDKs, direct mapping for network related calls.
 - WFP
 - Provides APIs in user mode to filter the packets
 - Doesn't support MAC based filtering
 - Callout Drivers
 - Write kernel mode drivers to develop firewalls, IDS, application based filtering

Application level analysis



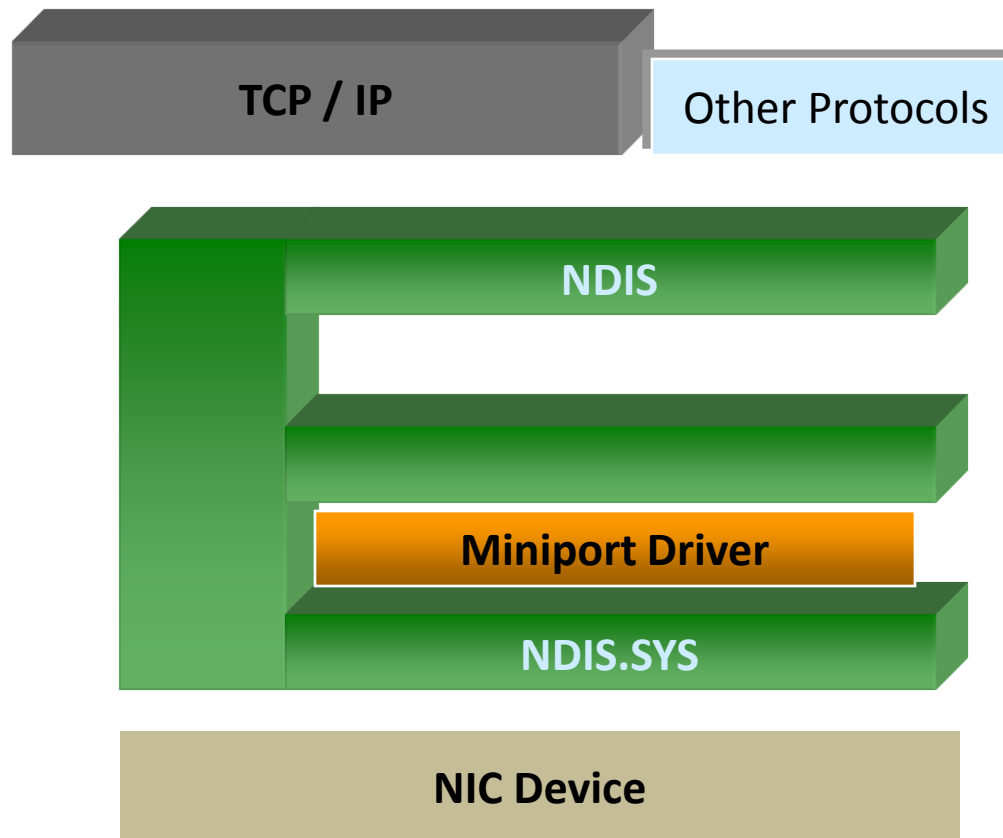
Modeling approaches

- Behavior based approaches
- Knowing the bad behavior and protecting against them
- Knowing the good behavior of the application
 - FSM
 - Artificial Neural Networks
 - N-gram
 - Probability Suffix Trees
- Anomaly Detection
- Issues with system call hooking
 - Discouraged by OS vendors
 - Used by rootkits
 - not supported on 64 bit windows (carry patch guard)

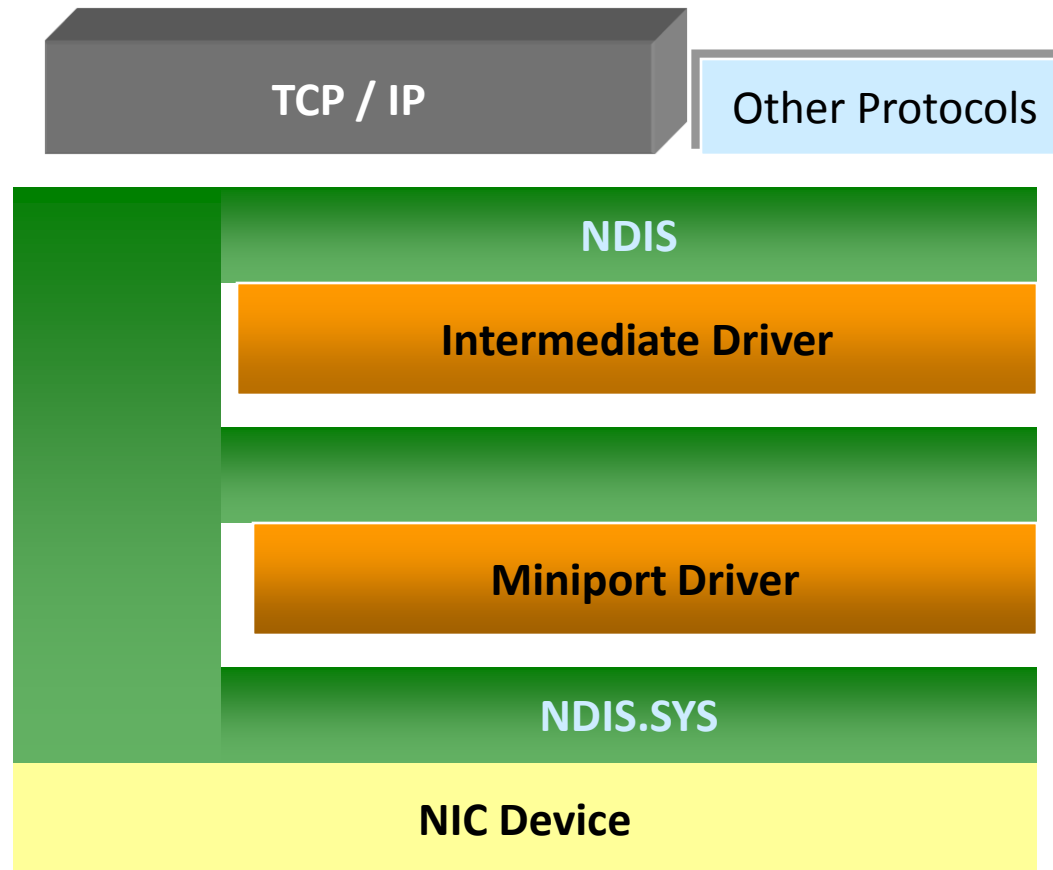
Implementing packet capture

- NDIS
 - IM Filter Driver
 - Miniport Driver
 - Protocol Driver

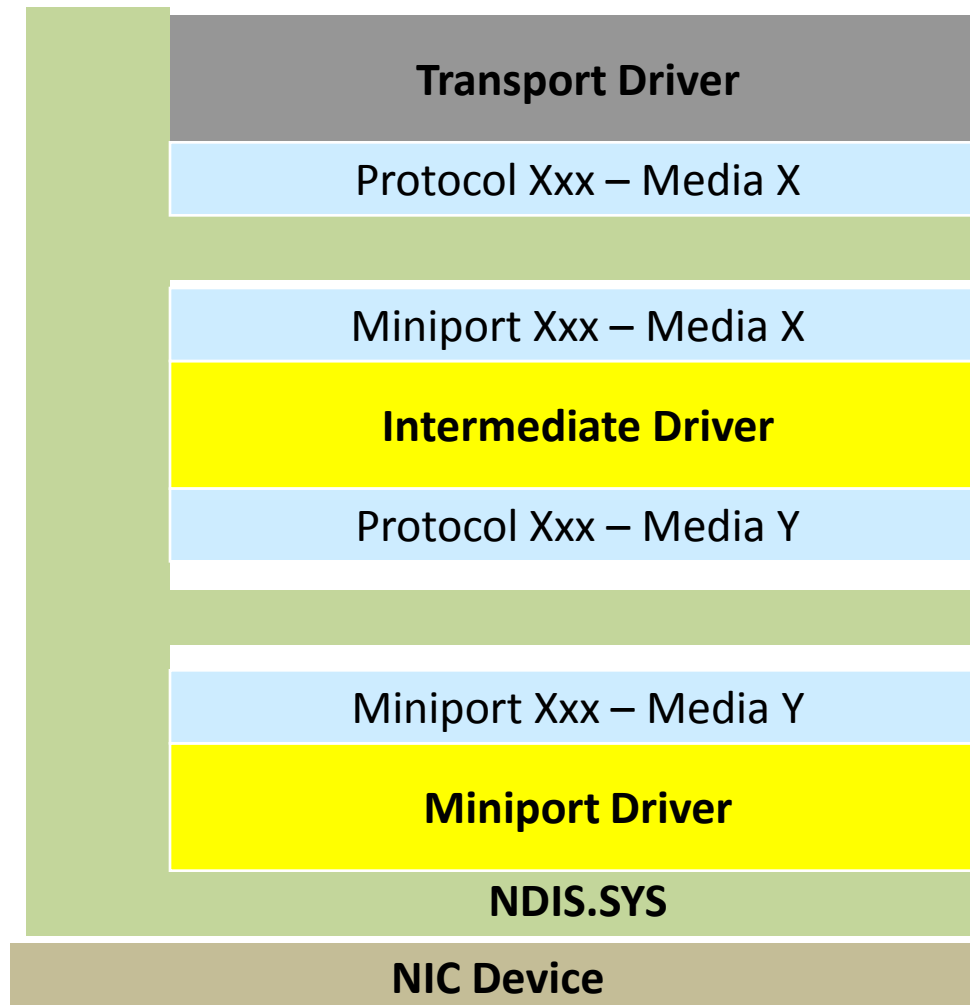
Relationships Between NDIS, Miniport Drivers, and Protocol Drivers



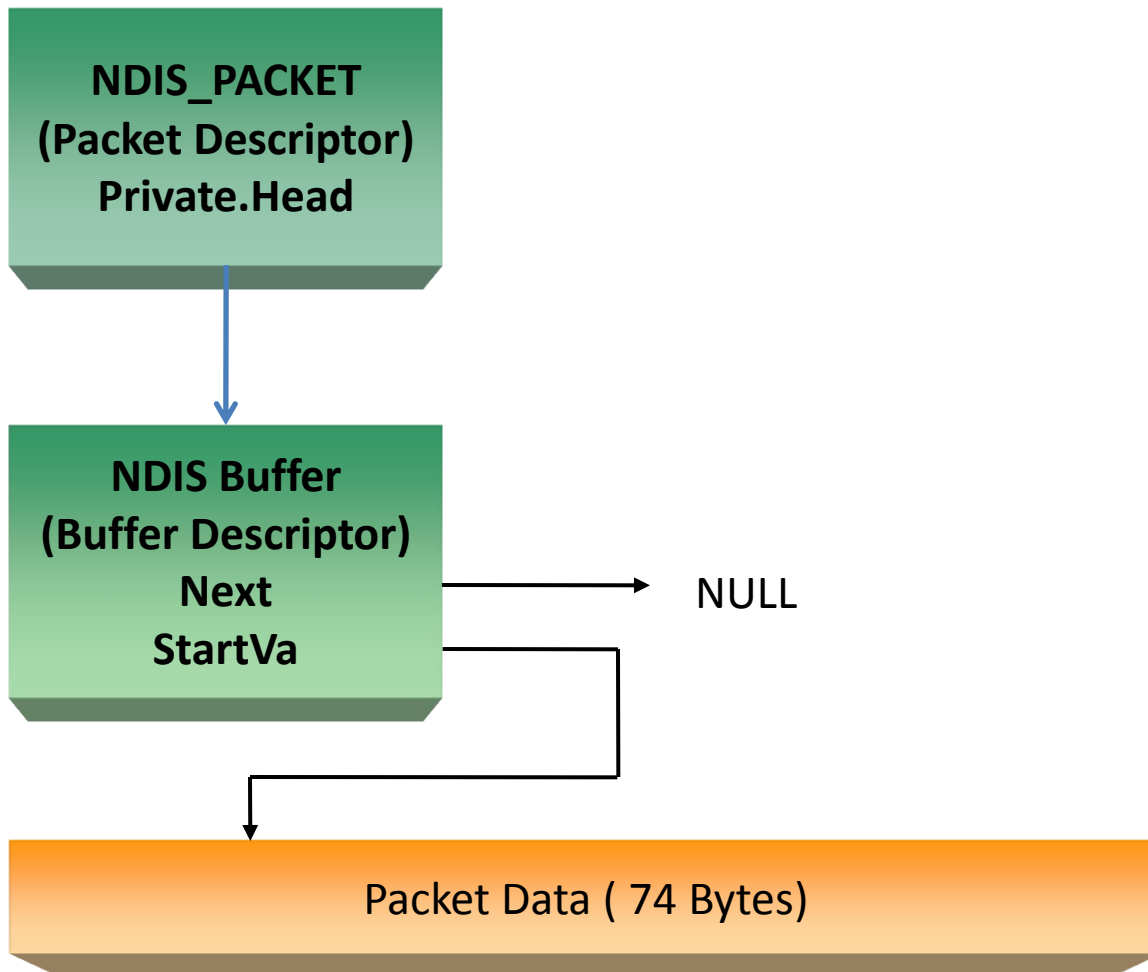
Intermediate Driver in the NDIS Driver Stack.



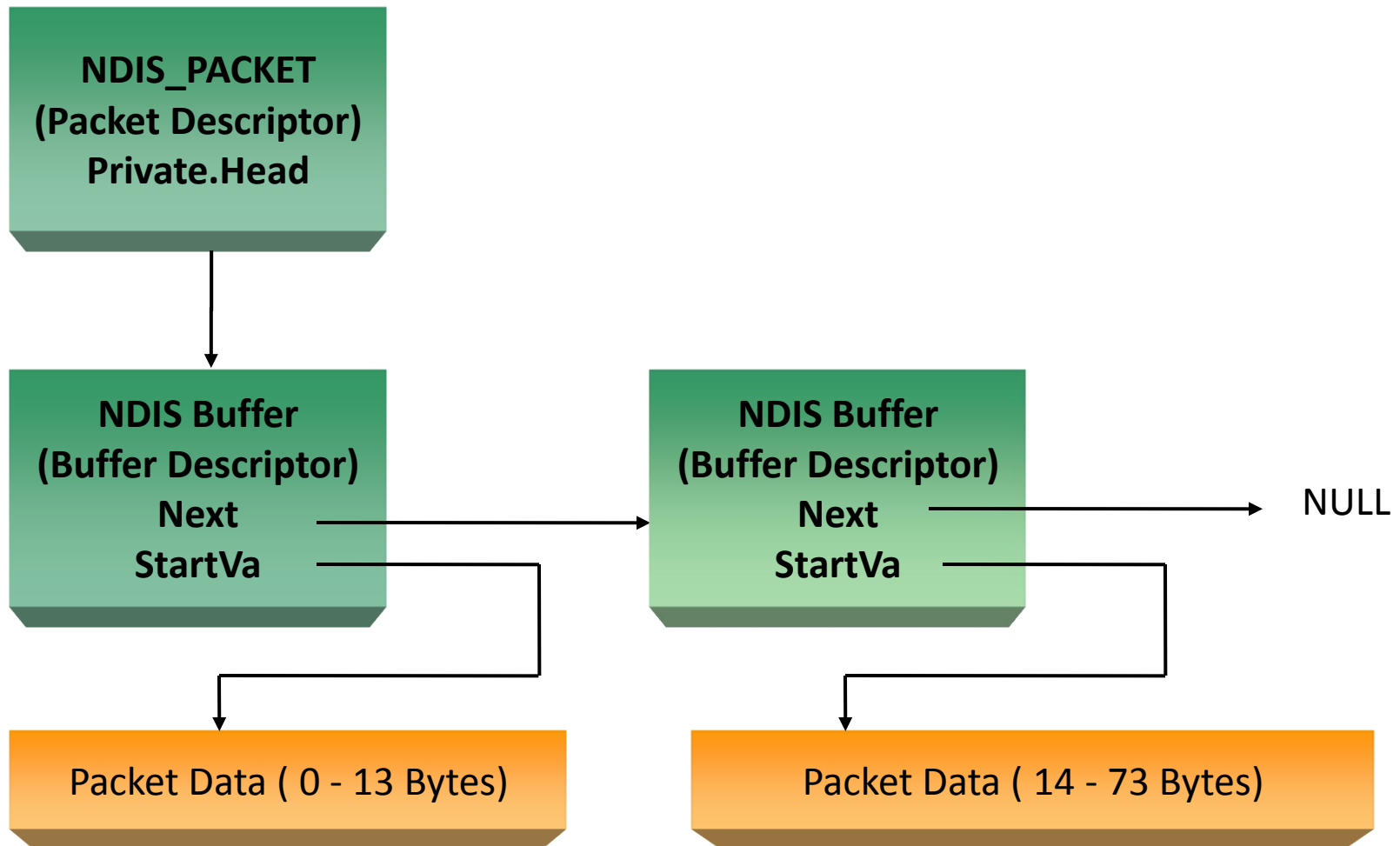
Intermediate Driver Layered Between Miniport Driver and Transport Driver



Simple NDIS_PACKET Illustration



A More Complex NDIS_PACKET Representation



Research opportunities

- Secure development practices.
- Apple Mac, Windows Azure.
- Malware with Virtualization.
- Type 3 Malware.

References | | Further Reading

- Wireshark documentation
- www.ietf.org
- Computer Networking: A Top Down Approach (Kurose/Ross)
- MS-Windows Platform SDK
- Microsoft Windows Driver Kit
- www.openrce.org
- Fighting malicious code (James, Malin)

References || Further Reading

- http://www.winpcap.org/docs/docs_41b5/html/group_NPF.html
- Windows, WFP, Callouts are trademarks and products of Microsoft, US. Reference is given to these. Information presented in the presentation is taken from freely available resources. Microsoft holds the copyright.
- Procexp, procmon, tcpview are freely downloadable tools from technet.
- NDIS was jointly developed by 3com and Microsoft.
- More on NDIS: DDK Documentation, www.ndis.com and www.pcausa.com

Thank you && Discussions | | queries