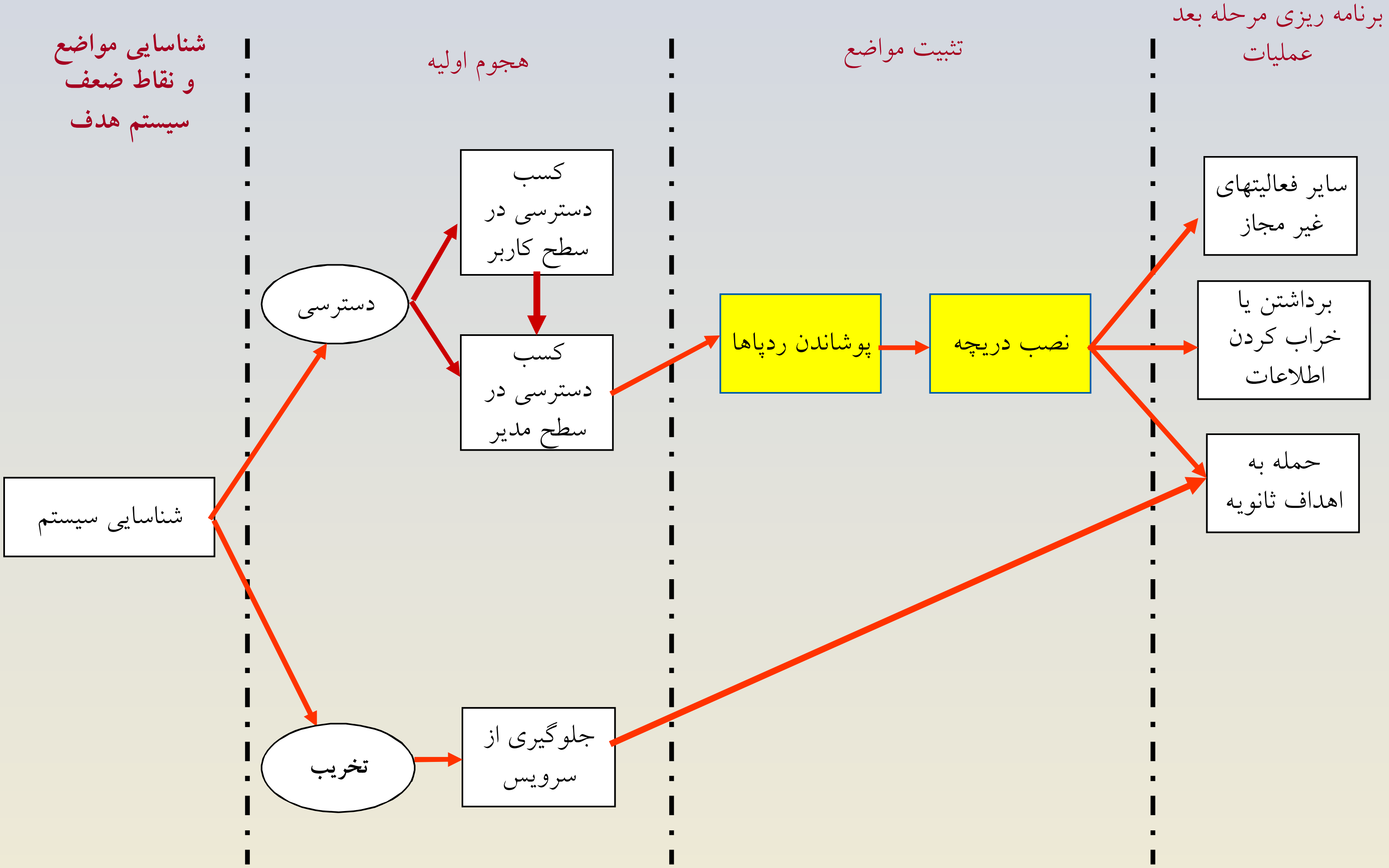
مروری بر نفوذگری و امنیت در سیستم‌های کامپیوتری

تثبیت مواضع

روند نمای کلی انجام یک حملهٔ کامپیوتری



Contents

- Definitions
- Spywares
- Trojan horses
- Rootkits
- Covert channels

Definitions

A general term for a program that secretly monitors your actions. While they are not sometimes malicious, but like a remote control program used by a hacker receive your private information. Software companies have been known to use Spyware to gather data about customers.

SPYWARE

Definition from: *BlackICE Internet Security Systems - http://blackice.iss.net/glossary.php*

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

TROJAN HORSE

Definition from: *Texas State Library and Archives Commission - http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html*

Summary of Effects

- Collection of data from your computer without your agreement
- Execution of code without your agreement
- Assignment of a unique code to identify you
- Collection of data pertaining to your habitual use
- Installation on your computer without your agreement
- Inability to remove the software
- Performing other undesirable tasks without agreement

Similarities / Differences

<table>
<tr><th>Spyware</th><th>Trojan Horses</th></tr>
<tr><td>Commercially Motivated</td><td>Malicious</td></tr>
<tr><td>Internet connection required</td><td>Any network connection required</td></tr>
<tr><td>Initiates remote connection</td><td>Receives incoming connection</td></tr>
<tr><td>Purpose: To monitor activity</td><td>Purpose: To control activity</td></tr>
<tr><td>Collects data</td><td>Unauthorized access and control</td></tr>
<tr><td>Legal</td><td>Illegal</td></tr>
<tr><td>Not Detectable with Virus Checker</td><td>Detectable with Virus Checker</td></tr>
<tr><td>Age: Relatively New (< 10 Years)</td><td>Age: Relatively Old (> 20 Years)</td></tr>
<tr><td colspan="2">Memory Resident Processes</td></tr>
<tr><td colspan="2">Secretly installed without user’s consent or understanding</td></tr>
<tr><td colspan="2">Creates a security vulnerability</td></tr>
</table>

Source – Table derived and produced by; Andrew Brown, Tim Cocks and Kumutha Swampillai, February 2004.

Contents

- Definitions
- Spywares
- Trojan horses
- Rootkits
- Covert channels

Image Source - http://www.clubpmi.it/upload/servizi_marketing/images/spyware.jpg

Software Examples

- GAIN / Gator
- Gator E-Wallet
- Cydoor
- BonziBuddy
- Google Toolbar
- Yahoo Toolbar
- DownloadWare
- BrowserAid
- Dogpile Toolbar

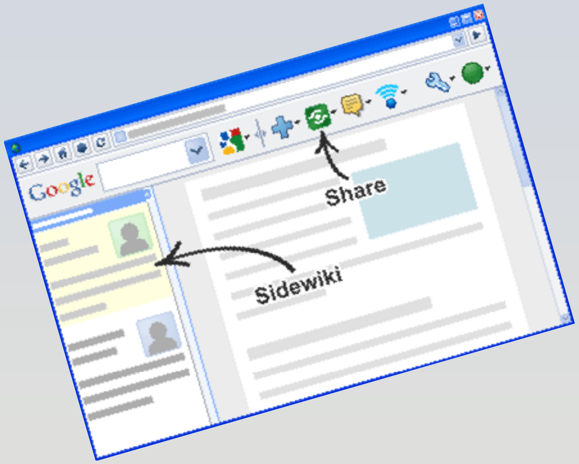


Image Sources…

GAIN Logo – The Gator Corporation – http://www.gator.com
BonziBuddy Logo – Bonzi.com - http://images.bonzi.com/images/gorillatalk.gif
DownloadWare Logo – DownloadWare - http://www.downloadware.net

Spyware Defence

User Initiatives…

- Use Legitimate S/W Sources
- Improved Technical Ability
- Choice of Browser
- Choice of OS

Technical Initiatives...

- Spyware Removal Programs
- Firewall Technology
- Disable ActiveX Controls
- E-Mail Filters
- Download Patches

Deep view: Cookie Marketing

- Basic cookie mechanism: Place a piece of information, retrieve it for customization on subsequent visits
- Functions available: read, write, delete
- Creative application1: Initialize a cookie called counter to 1. Every time user visits, retrieve counter, increment by 1 and re-write.
- Creative application2: When a user visits, write system date/time in a cookie. Next visit get cookie for last visit. Overwrite with current date/time.

Cookie Scope: Cannot Do

- Have automatic access to personal information like name, address, email
- Read or write data to hard disk
- Read or write information in cookies placed by other sites
- Run programs on your computer

Cookie Scope: Can Do

- Store and manipulate any information you explicitly provide to a site
- Track your interaction with parent site such as pages visited, time of visits, number of visits
- Use any information available to web server including: IP address, Operating System, Browser Type, etc

Cookie Types and Taxonomy

- By Lifespan

  - Session Cookies (RAM)
  - Persistent Cookies (Disk)

- By Read-Write Mechanism

  - Server-Side Cookies (HTTP Header)
  - Client-Side Cookies (JavaScript)

- By Structure

  - Simple Cookies
  - Complex Cookies

Cookie based Marketing

- **How does it work?**
- Companies like DoubleClick.net, adserver.com and adflow.com have developed an innovative system (using standard technologies) for this purpose.
- They tie up with popular websites like Yahoo, Amazon to create an extensive data and information sharing network
  - Code developed by the company is placed on these web sites.
  - When you hit another such site, it sends data placed in your cookies to DoubleClick and retrieves marketing information about you enabling them to customize ads etc
  - Result: One person may see ads for sports goods and another for baby clothes

Tracking Cookie Defence

- Replace tracking cookies with write protected zero length files of the same name.
- Disable cookies
  - Makes many websites unusable
- Delete cookies after session
- Spyware remover (Ad-aware)

Contents

- Definitions
- Spywares
- Trojan horses
- Rootkits
- Covert channels

Types of Trojan Horse

- **Remote Access Trojan**: allow attacker to gain control over the victim's pc.
- **Data sending Trojan**: provide the attacker confidential data such as password, credit card information.
- **Destructive Trojan**: designed to destroy or delete files.
- **Proxy Trojan**: to use the victim's computer as the proxy server for the attackers.
- **FTP Trojan**: designed to open ftp port (port 21) on your computer, enable the attacker to connect your PC through File Transfer Protocol.
- **Security software disabler Trojan**: designed to stop or kill security software program such as antivirus program and internet security program.
- **Denial of Service (DoS) attack**: the attacker try to bring down the network service by flooding the useless traffic over the network.

Trojan Horse: installation

- Secretly installed when an infected executable is run
  - Much like a virus
  - Executables typically come from P2P networks or un-trusted websites
- ActiveX controls on websites
  - ActiveX allows automatic installation of software from websites
  - User probably does not know what they are running

Trojan Horse: Effects

- Allows remote access
  - To spy
  - To disrupt
  - To relay a malicious connection, so as to hide the attacker’s location (spam, hacking)
  - To access resources (i.e. bandwidth, files)
  - To launch a DDoS attack

Trojan Horse Examples

- Hardware
  - Key loggers
  - More advanced?
- Magic Lantern
  - FBI developed
  - Legal grey area (until recently!)

Solutions

Short Term

- Firewall
- Virus Checker
- Spyware Remover
- Frequent OS updates
- Frequent back-up
- Learning problems

Long Term

- Add Spyware to Anti-Virus
- Automatic maintenance
- Education on problems
- Biometric access

Contents

- Definitions
- Spywares
- Trojan horses
- Rootkits
- Covert channels

What is a Rootkit?

- A rootkit is a tool that is designed to hide itself and other processes, data, and/or activity on a system.
- "A tool used to protect backdoors and other tools from detection by administrators"
- A rootkit is not
  - An exploit
  - A virus or worm

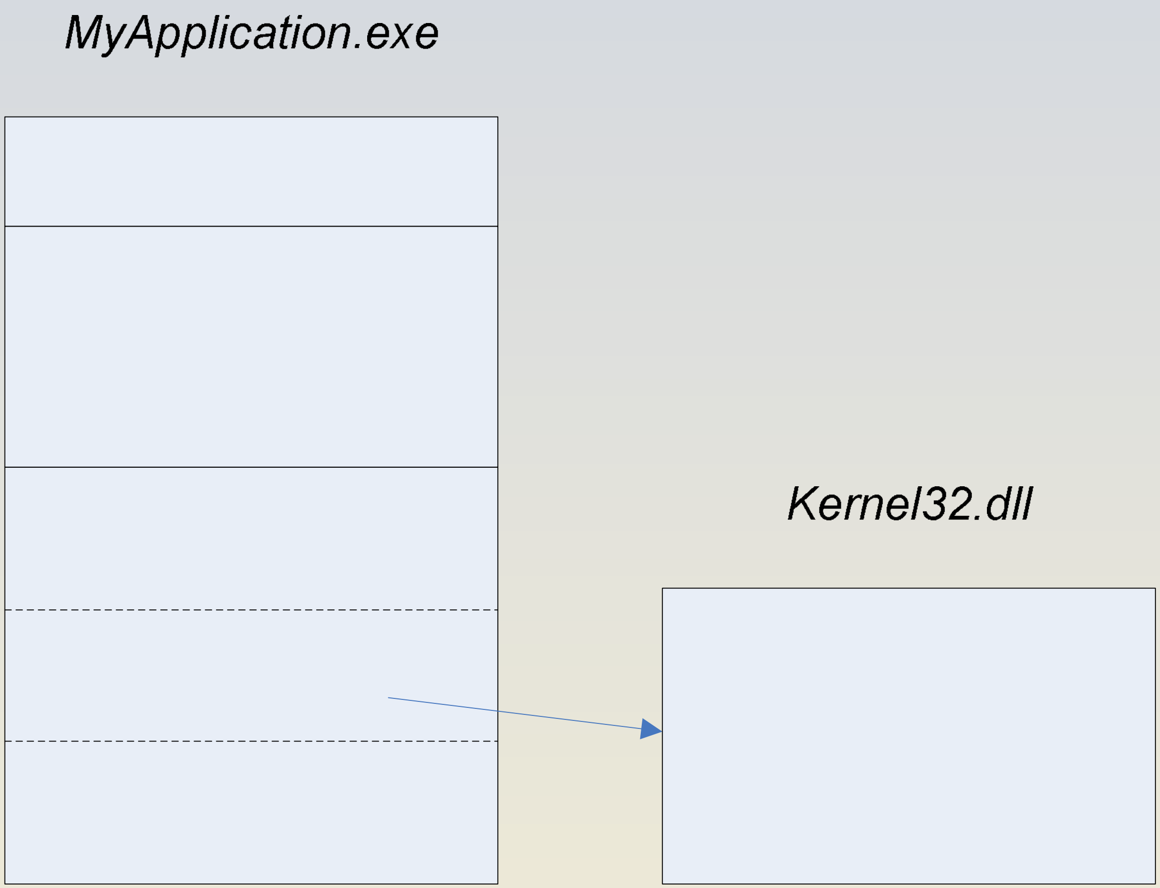
Rootkits - Why Should You Care?

- If you can’t detect a backdoor on any given machine, how do you know your machine is clean?
- New viruses will use new rootkit technology

Rootkits - How They Work?

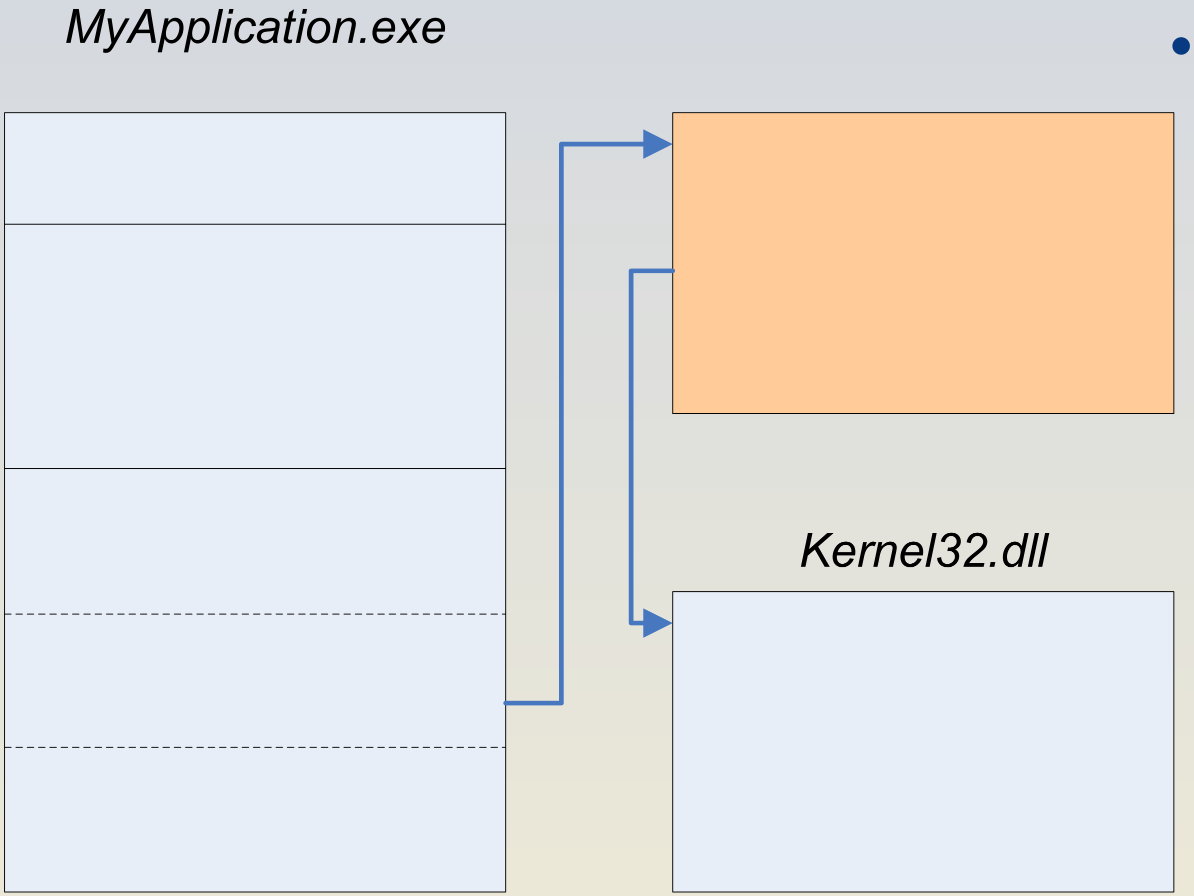
- To hide in a system you have to control a system
- Act as a gatekeeper between what a user sees and what the system sees
- Requires administrator privileges to install

How Rootkits Work - Hooking



- A standard application

How Rootkits Work - Hooking



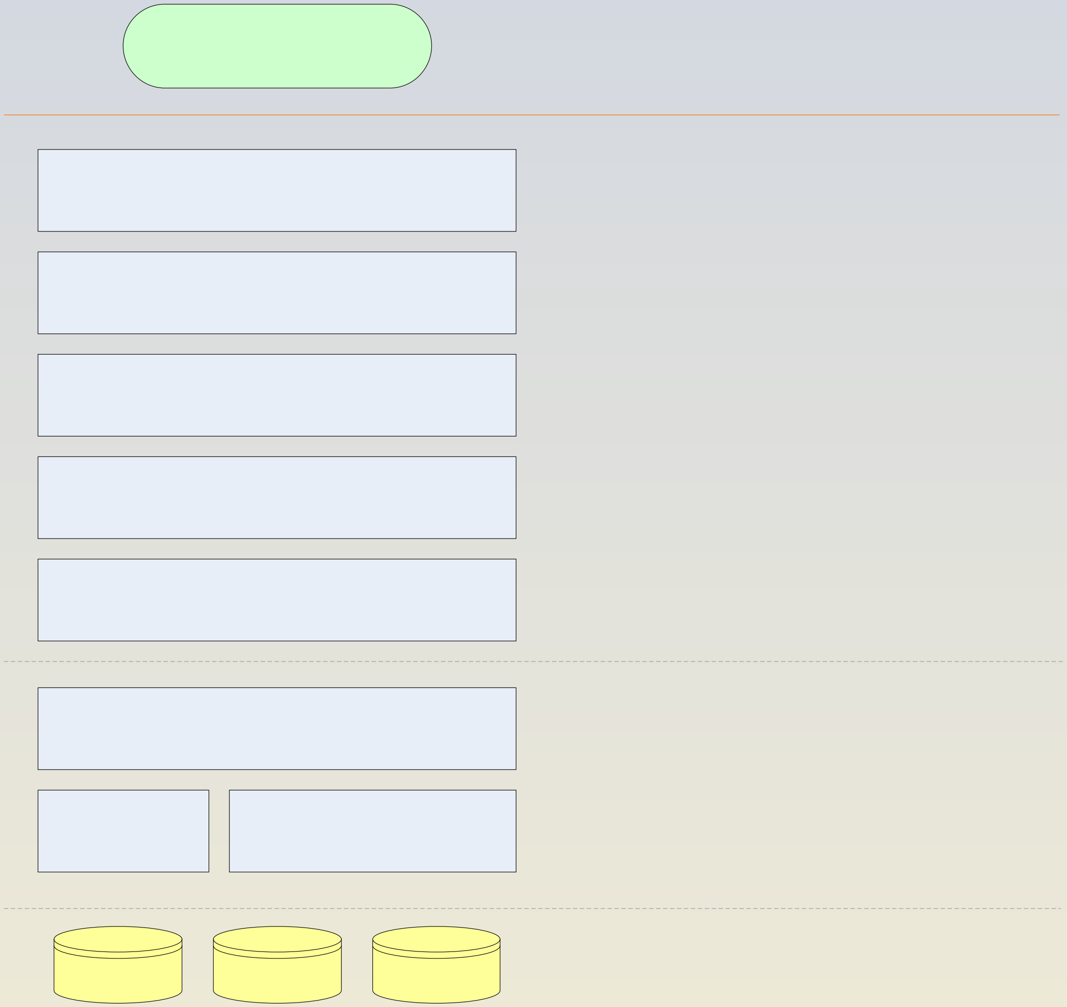
- **A hooked application**

Rootkits – How They Work?

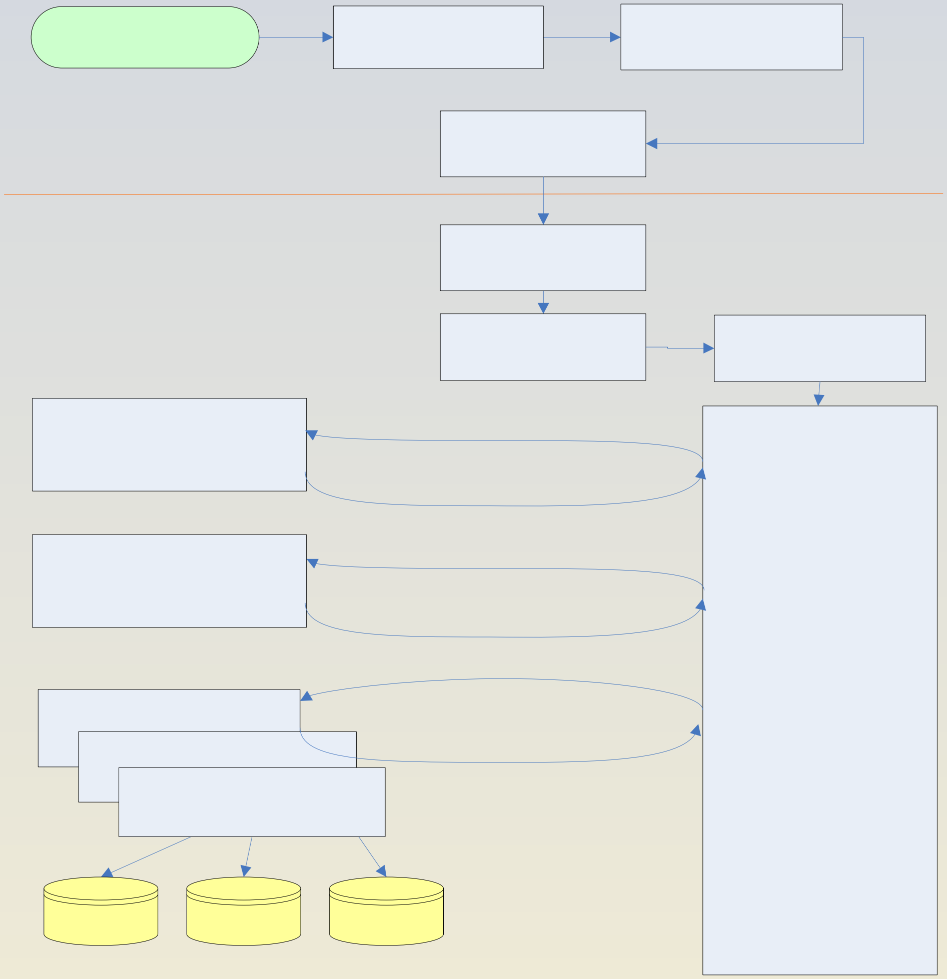
- To hide what is taking place, an attacker wants to:
  - Hide processes
  - Hide services
  - Hide listening TCP/UDP ports
  - Hide kernel modules
  - Hide drivers

Levels of Access in Windows

- User Land
  - User
  - Administrator
  - System
- Kernel Land
  - Drivers

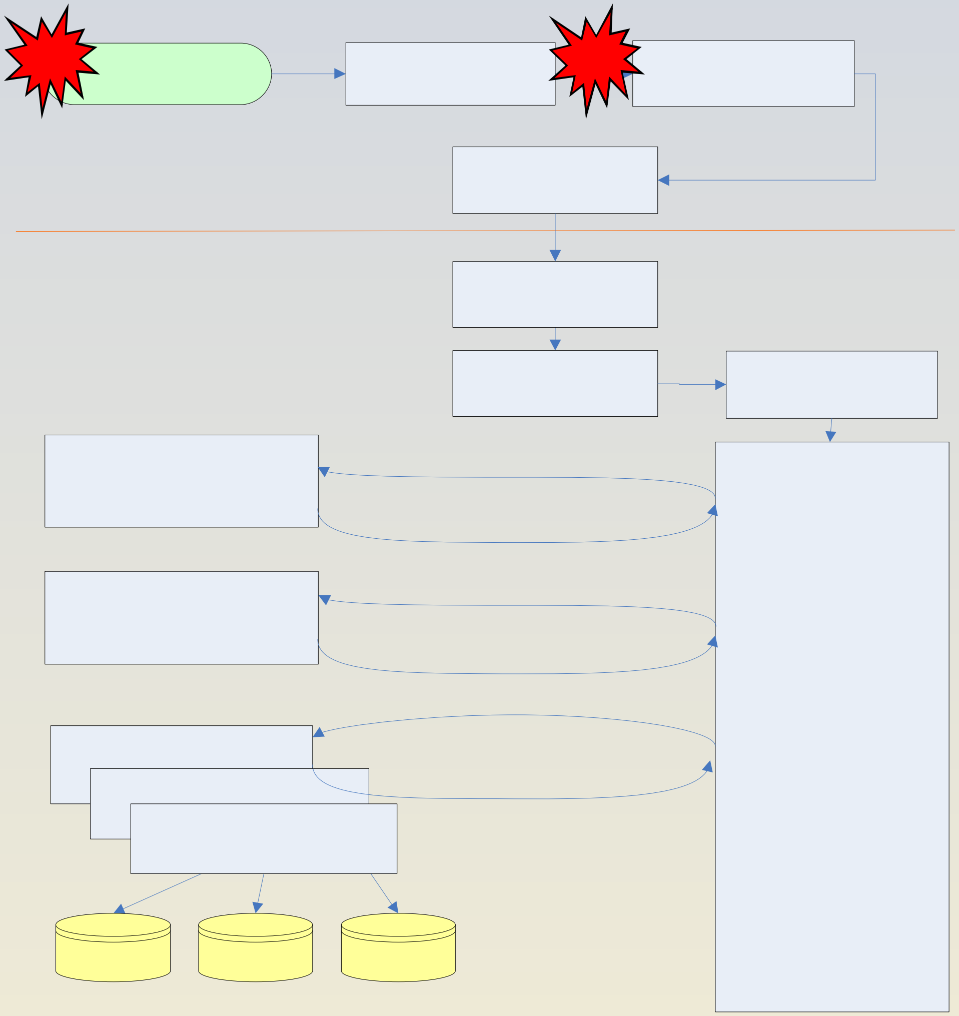


What Happens When You Read a File?



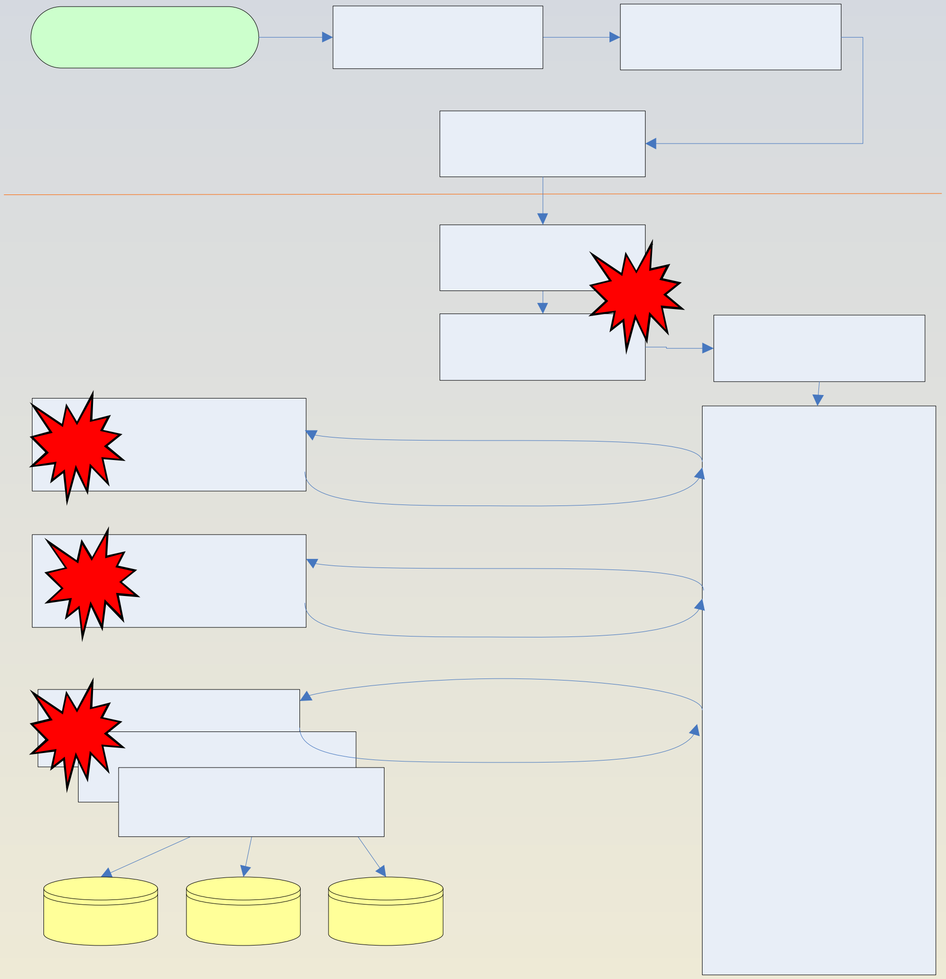
- Readfile() called on File1.txt
- Transition to Ring 0
- NtReadFile() processed
- I/O Subsystem called
- IRP generated
- Data at File1.txt requested from ntfs.sys
- Data on disk 2 requested from disk.sys

Userland (Ring 3) Rootkits



- Binary replacement eg modified Exe or Dll
- Binary modification in memory eg He4Hook
- User land hooking eg Hacker Defender
  - IAT hooking

Kernel (Ring 0) Rootkits



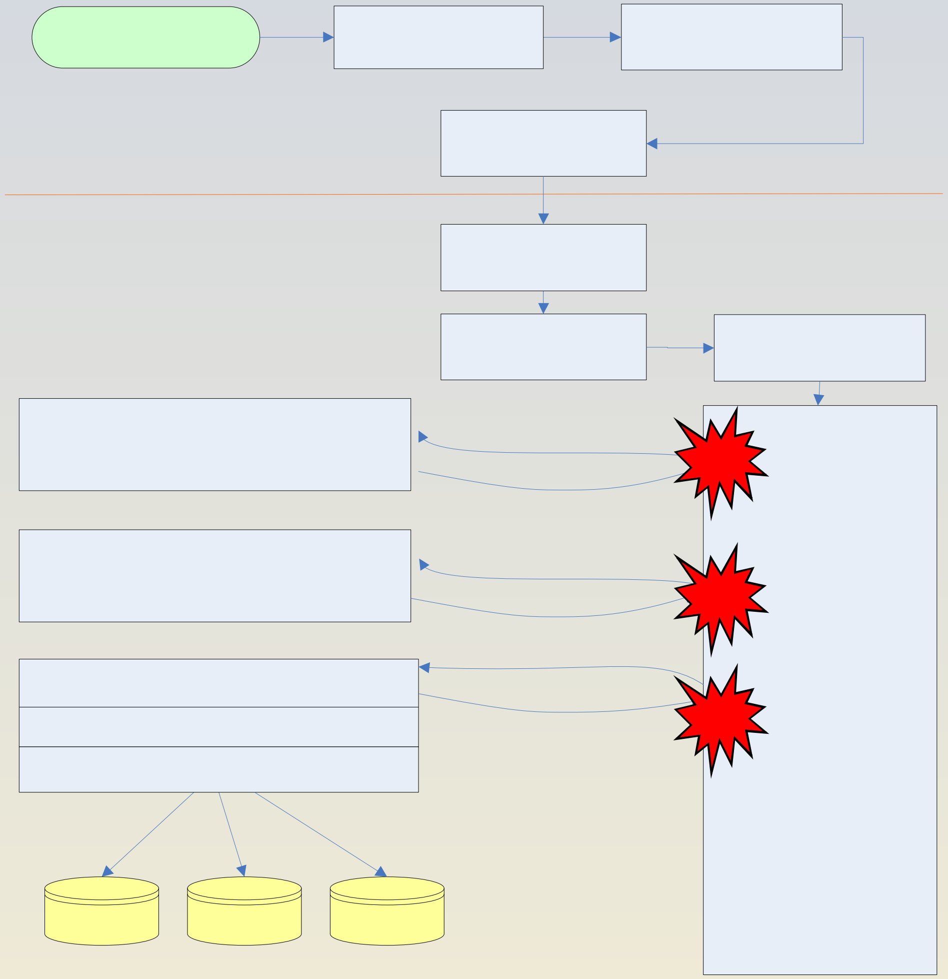
- Kernel Hooking

  E.g. NtRootkit

- Driver replacement

  E.g. replace ntfs.sys with ntfss.sys

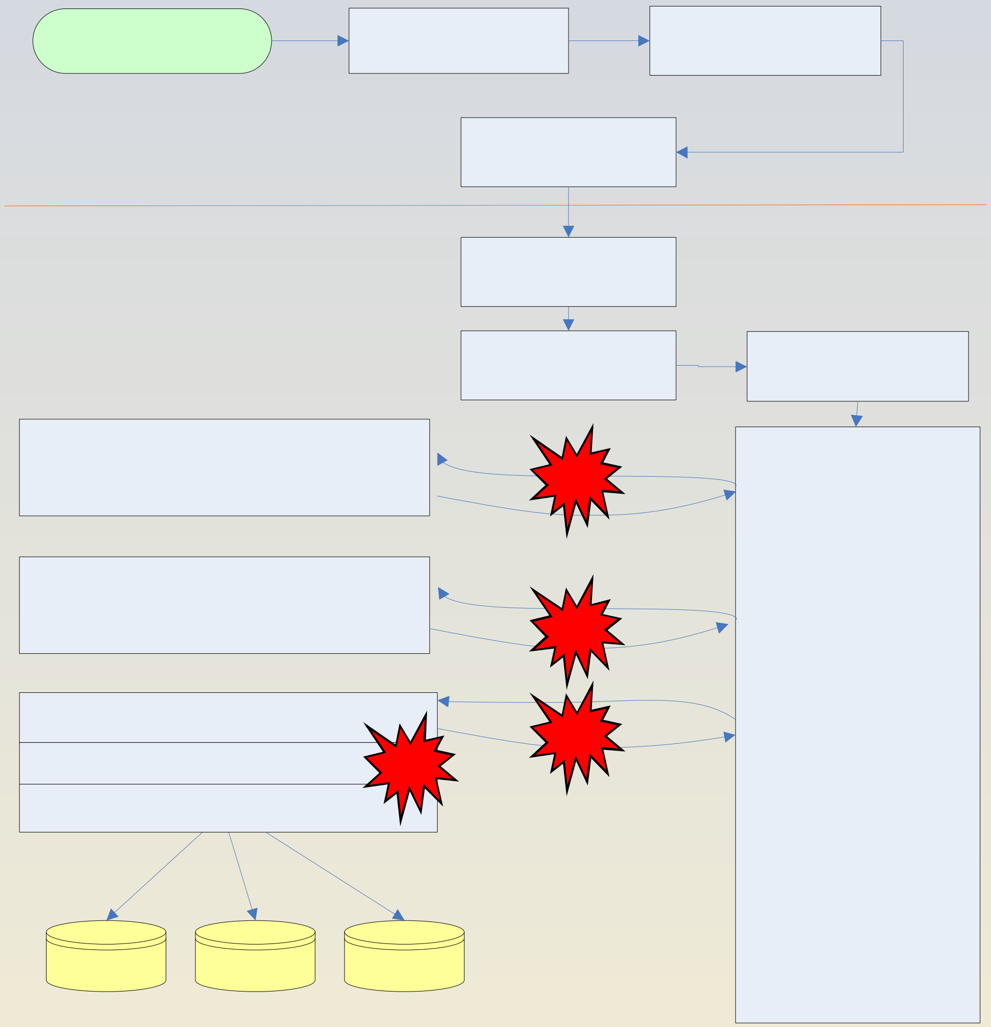
Kernel (Ring 0) Rootkits



- **IO Request Packet (IRP) Hooking**
  - IRP Dispatch Table

E.g. He4Hook (some versions)

Kernel (Ring 0) Rootkits



- **Filter Drivers**
- **Types**
  - File system filter
  - Volume filter
  - Disk Filter
  - Bus Filter

Current Rootkit Capabilities

- Hide processes
- Hide files
- Hide registry entries
- Hide services
- Completely bypass personal firewalls
- Undetectable by anti virus
- Covert channels - undetectable on the network
- Install silently

Detection Methodologies

- Traditional Detection
  - Check integrity of important OS elements against a hash database (sigcheck)
  - Look for unidentified processes (task manager)
  - Check for open ports (netstat)

Detection Methodologies

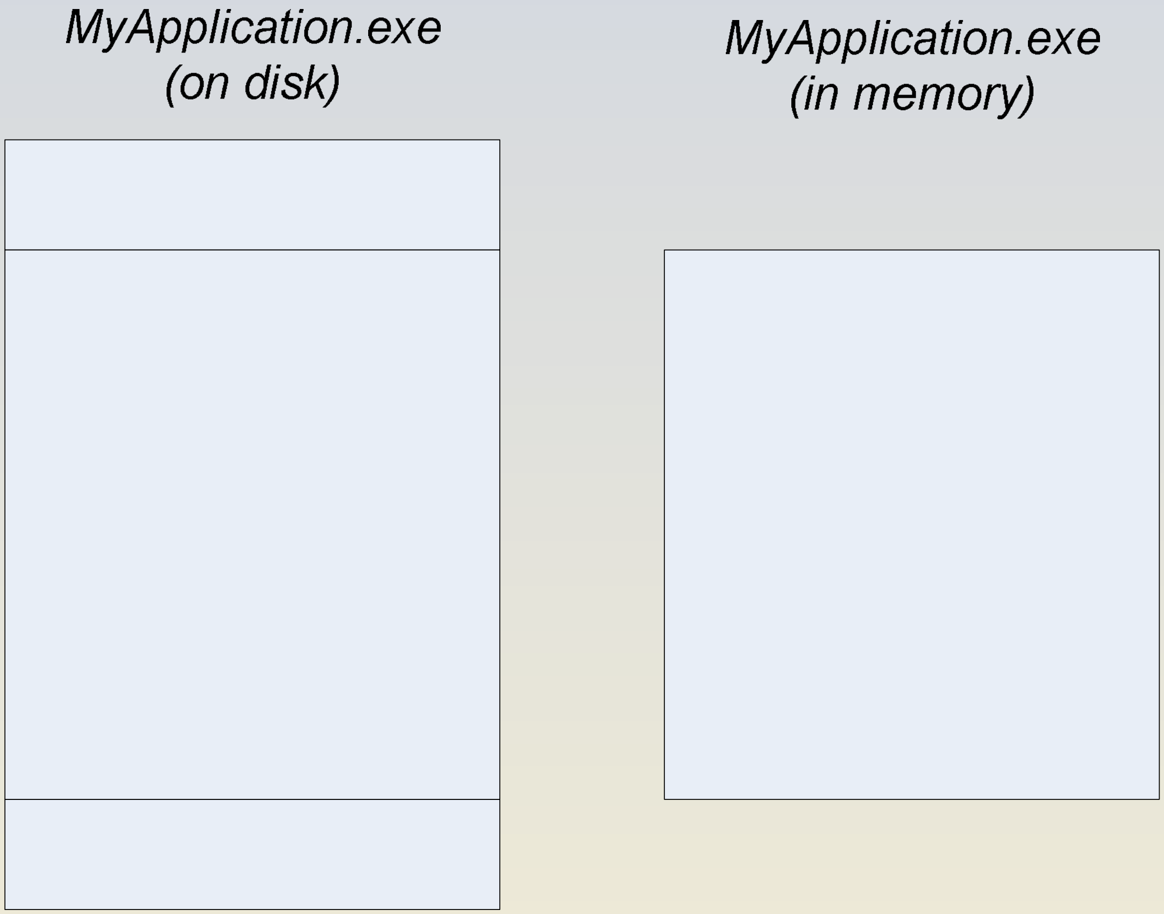
- Signature based
  - Look for known rootkits, viruses, backdoors
  - Antivirus
  - Look for “bad things” living in memory

- Problems
  - Requires updated databases
  - Doesn’t detect anything it hasn’t seen before

Detection Methodologies

- Code verification
  - Code sections are read only in all modern OSes
  - Programs should not modify their own code
  - Check to see if the files on disk match what is running in memory

Detection Methodologies: Code Verification



MyApplication.exe
(on disk)

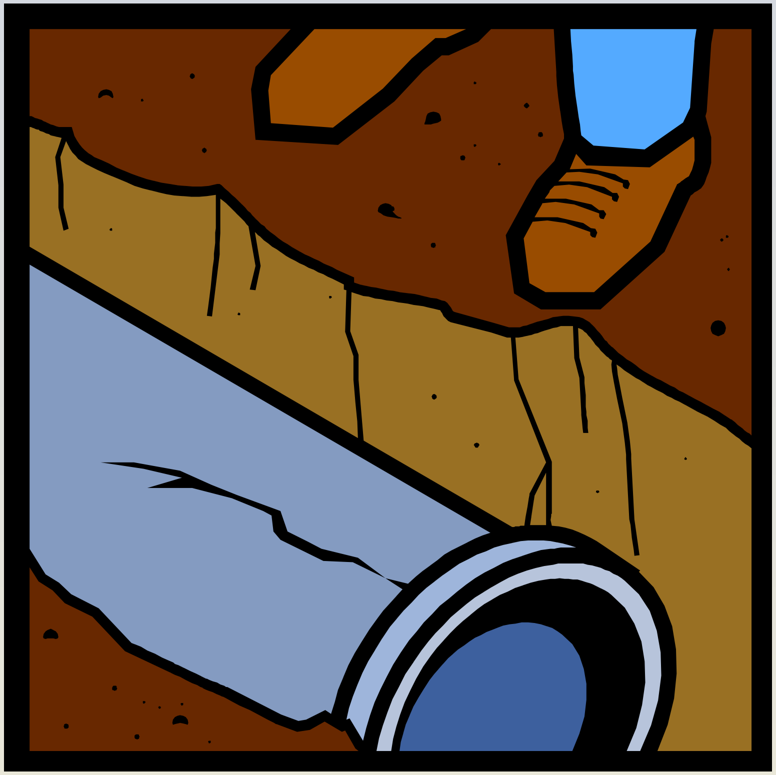
MyApplication.exe
(in memory)

Hardware Rootkits

- A OS reinstall won’t save you
- Hard to remove.
  - Device is usually destroyed
- Difficult to implement
- With more and more memory on devices they are becoming prevalent with time
- VideoCardKit (http://www.rootkit.com)
  - Stores code in FLASH or EEPROM
- EEye Bootroot
  - Installs in real mode via network PXE boot

Contents

- Definitions
- Spywares
- Trojan horses
- Rootkits
- Covert channels



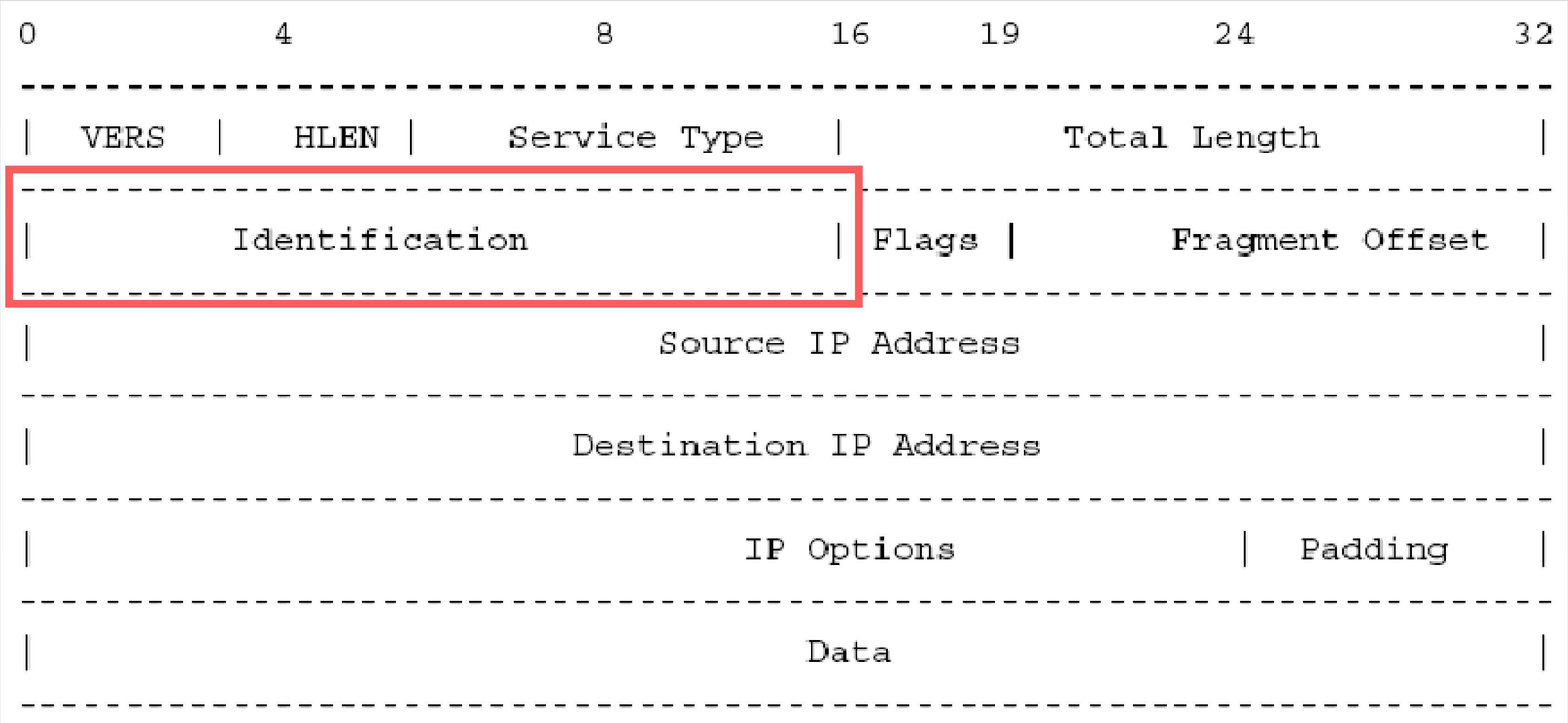
Definition

- Covert channels are a means of communication between two processes
- Processes may be:
  - Authorized to communicate, but not in the way they actually are
  - Prohibited from communicating

Why Are They Important?

- Difficult to detect
- Can operate for a long time and leak a substantial amount of classified data to uncleared processes
- Can compromise a secure system

IP Channels

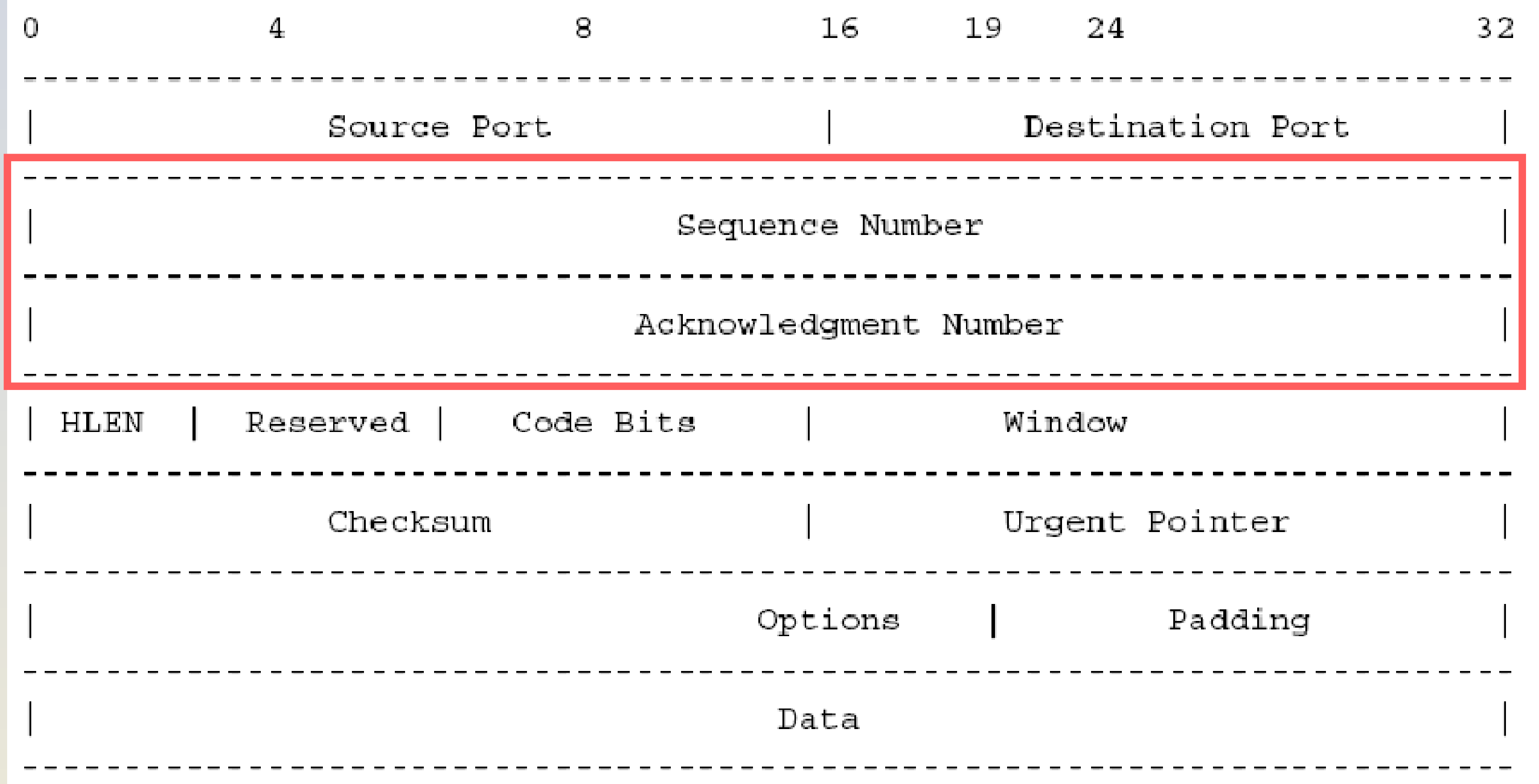


```
0             4                 8            16      19           24               32
---------------------------------------------------------------------------------------
|   VERS    |    HLEN  |     Service Type      |           Total Length               |
---------------------------------------------------------------------------------------
|           Identification                     | Flags  |       Fragment Offset       |
---------------------------------------------------------------------------------------
|                                   Source IP Address                                 |
---------------------------------------------------------------------------------------
|                              Destination IP Address                                 |
---------------------------------------------------------------------------------------
|                                      IP Options                  |    Padding       |
---------------------------------------------------------------------------------------
|                                          Data                                       |
---------------------------------------------------------------------------------------
```

Figure 1. The IP protocol header

Murdoch, Lewis 2005, “Embedding Covert Channels into TCP/IP”

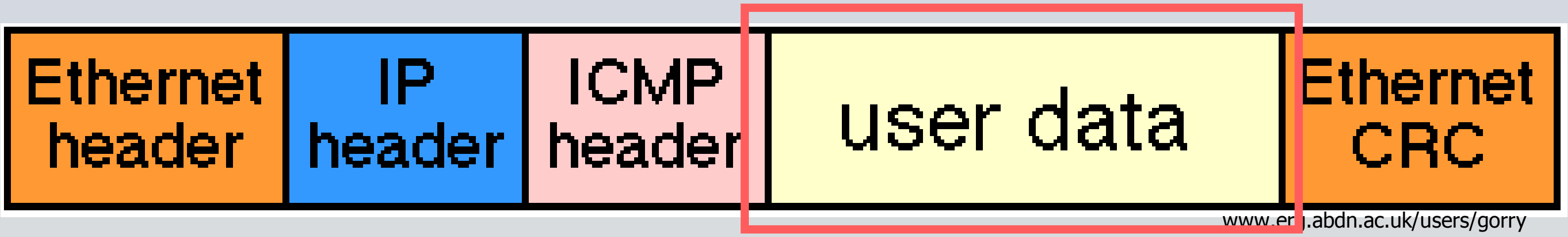
TCP Channels



```
0        4           8        16    19   24            32
------------------------------------------------------------
|           Source Port          |     Destination Port    |
------------------------------------------------------------
|                      Sequence Number                     |
------------------------------------------------------------
|                  Acknowledgment Number                   |
------------------------------------------------------------
| HLEN | Reserved | Code Bits     |         Window          |
------------------------------------------------------------
|           Checksum            |      Urgent Pointer      |
------------------------------------------------------------
|                          Options   |      Padding        |
------------------------------------------------------------
|                              Data                        |
------------------------------------------------------------
```

Figure 2. The TCP protocol header

ICMP Channels



www.erg.abdn.ac.uk/users/gorry

- ICMP echo request/reply can tunnel arbitrary user data
  - Payload capacity depends on path MTU (this feature often used to measure PMTU)

Sohn, Noh, Moon 2003, "Support Vector Machine Based ICMP Covert Channel Attack Detection"

Conclusions

- Difficult to detect
- Can exist even in formally verified systems
- Should be analyzed during system design