Setuid bit: Duct Tape of Unix Security

Mismatched kernel and system policies

Trusted setuid-to-root binaries patch the problem

Opportunities for privilege escalation!

Least Privilege Principle

“Grant minimal privilege required for a given function

Setuid-root violates least privilege principle

Example: Linux mount

Kernel : only root can mount anywhere

System : user can mount at safe locations

/* Parse /etc/fstab */
if (ruid == 0 || user_mount_ok(args))
sys_mount(args);

User

Kernel sys_mount() {
  if (!capable(CAP_SYS_ADMIN))
    return -EPERM;

Real-World Study

Lintian reports: popularity contest of 119 binaries

26 Binaries on 89% systems

83 Binaries on <0.89% systems

Protego Approach

Study policy:
26 most popular (28 total)

1. Why is root needed?
2. Simpler alternative in kernel?

Protego mount

User

root
Privileged
Daemon

/* parse fstab */
sys_mount(args);

Kernel

if (!security_mount_ok(args))
  return -EPERM;

System Abstractions for Setuid Binaries

<table>
<thead>
<tr>
<th>Interface</th>
<th>Used</th>
<th>What do we do?</th>
</tr>
</thead>
<tbody>
<tr>
<td>mount, umount</td>
<td>3</td>
<td>Whitelisting safe locations and options</td>
</tr>
<tr>
<td>socket (ping)</td>
<td>5</td>
<td>Firewall rules on raw sockets</td>
</tr>
<tr>
<td>Cred. databases (passwd)</td>
<td>5</td>
<td>Fragment to per-user or per-group files, w/ DAC granularity.</td>
</tr>
<tr>
<td>ioctl (pppd)</td>
<td>2</td>
<td>LSM hooks to verify new routes</td>
</tr>
<tr>
<td>bind (mail)</td>
<td>3</td>
<td>Map low port to (binary, userid)</td>
</tr>
<tr>
<td>setuid, setgid (sudo)</td>
<td>7</td>
<td>Delegation Framework: LSM hooks to check delegation rules &amp; recency</td>
</tr>
</tbody>
</table>

Video driver control state (X) | 1 | Kernel Mode Switching: Context switches video devices in kernel |

Evaluation

Perf. Overhead: 0 ~ 2.5% in general, < 7.4% worst case

Functionality: equivalent to Linux

Trusted Computing Base:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Services</td>
<td>1,600</td>
</tr>
<tr>
<td>Kernel</td>
<td>715</td>
</tr>
<tr>
<td>Total Addition to TCB</td>
<td>2,315</td>
</tr>
<tr>
<td>De-privileged LoC by Protego</td>
<td>15,047</td>
</tr>
<tr>
<td>Net LoC de-privileged</td>
<td>12,732</td>
</tr>
</tbody>
</table>

Information and code release:
http://protego.cs.stonybrook.edu