Nathan Seidle
SparkFun Electronics

Combos in 45 minutes or less!*

*You know what these mean…
Way more versatility than just radio, the bladeRF x 40.

EXPLORE THE REAL RADIO STAR
This is the SparkFun Speed Trap. Stand next to the copier and wait for the display to zero out (four seconds). Then proceed at normal walking pace towards the sensor. The max starting range is around where the copier is located.

How does it work? The Speed Trap uses a laser distance sensor to determine distance. The PulsedLight LIDAR sensor emits an invisible infrared laser and times how long it takes for the light to return. The change in distance over time is velocity. If we know you moved 200cm in 1 second that equates to 4.5 miles per hour!

Be careful! Please don’t run into the wall or the sign.
Animation:
How combination safe works
Power!

Motor with 8400 tick encoder

Servo with feedback

Arduino

Handle puller

Magnets

Erector set (Actobotics)

Motor with 8400 tick encoder
The super freaking amazing nautilus gear that made this all work

Standard servo with analog feedback hack

'Come back here' spring

Very fancy string
Go! Btn
Servo and feedback
Motor Driver
Current Sensor
Beep!
RedBoard = Arduino
Display
Go! Btn
‘Home’ Photogate
Motor control and feedback
12V External Hard Drive Power Supply
Power Supply
Problem Domain:
$100^3$ combinations
10 seconds per test
115 days (worst case)
Combinations:
$$100^3$$ combinations
Combinations:

$100^3$ combinations

$33^3$ combinations = 4.15 days

Exploits
Combinations:

$100^3$ combinations
$33^3$ combinations $= 4.15$ days

Disc C has 12 indents
$33^2 \times 12 = 1.5$ days

Exploits
Exploits
Disc C:
   Outer diameter: 2.815” (55.5mm)
   Width of solution slot: 0.239”
   Width of 11 indents: 0.249” +/- 0.002”

17.69” (Circumference) / 8400 ticks
0.0021” / tick
~5 ticks smaller

Exploits
Combinations:

$100^3$ combinations
$33^3$ combinations $= 4.15$ days

Disc C has 12 indents

$33^2 \times 12 = 1.5$ days

Disc C has a skinny indent

$33^2 \times 1 = 3$ hours

Exploits
Test Time:
Resetting Dials = 10s / test

Exploits
Test Time:
  Resetting Dials = 10s / test
  ‘Set testing’ = 4s / test
1.2 hours

Exploits
Test Time:

- Resetting Dials = 10s / test
- ‘Set testing’ = 4s / test

1.2 hours

45 minutes!
Animation: How Set Testing Works
How do I protect myself!?
One of these is not like the others...
The S&G 6741 … can be dialed up to 1.25 digits above or below the actual set number and still open, essentially giving you a 2.5 digit window to hit. The S&G 6730, however, has only a +/- .5 dialing tolerance, essentially giving a 1 digit window to hit. While many locksmiths might prefer the S&G 6730, it can be notoriously difficult to open and very unforgiving to human error. In addition, slight alterations to the lock (for example, if the dial or the dial ring was bumped during shipping) can shift the combination, rendering the lock unusable.
The S&G 6741 has a dialing tolerance up to 1.25 digits above or below the actual set number and still open, essentially giving you a 2.5 digit window to hit. The S&G 6730, however, has only a +/- .5 dialing tolerance, essentially giving a 1 digit window to hit. While many locksmiths might prefer the S&G 6730, it can be notoriously difficult to open and very unforgiving to human error. In addition, slight alterations to the lock (for example, if the dial or the dial ring was bumped during shipping) can shift the combination, rendering the lock unusable.
Future Research

<table>
<thead>
<tr>
<th>Measuring complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smallest to largest width [Width]/[Depth]</td>
</tr>
<tr>
<td>Indent 8: [1911] / [1130]</td>
</tr>
<tr>
<td>Indent 1: [1925] / [1122]</td>
</tr>
<tr>
<td>Indent 3: [1953] / [1091]</td>
</tr>
<tr>
<td>Indent 0: [1955] / [1099]</td>
</tr>
<tr>
<td>Indent 11: [1966] / [1105]</td>
</tr>
<tr>
<td>Indent 2: [1992] / [1100]</td>
</tr>
<tr>
<td>Indent 9: [1994] / [1126]</td>
</tr>
<tr>
<td>Indent 7: [2011] / [1098]</td>
</tr>
<tr>
<td>Indent 10: [2036] / [1096]</td>
</tr>
<tr>
<td>Indent 4: [2077] / [1109]</td>
</tr>
<tr>
<td>Indent 5: [2085] / [1100]</td>
</tr>
<tr>
<td>Indent 6: [2114] / [1096]</td>
</tr>
</tbody>
</table>
Future Research
Future Research
Is it open yet?
nathan@sparkfun.com