Nathan Seidle
Joel Bartlett
Rob Reynolds

Combos in 45 minutes or less!*

*Totes Guaranteed
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 wall and wait for the display to zero out (four seconds). Proceed at normal walking pace towards the sensor and wait for the display to update. You will hear a beep when you go over the speed limit. The 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 emits an invisible infrared laser and times how long it takes for the light to return. The change in distance over time equates to 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 copier!
MAKE ME A SANDWICH.

SUDO MAKE ME A SANDWICH.

WHAT? MAKE IT YOURSELF.

OKAY.
Power!

Motor with 8400 tick encoder

Servo with feedback

Handle puller

Erector set (Actobotics)

Credit: Pololu
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
Problem Domain:
$100^3$ combinations
10 seconds per test
115 days (worst case)
Combinations: $100^3$ combinations

Exploits
Combinations:

$100^3$ combinations

$33^3$ combinations = 4.15 days

Exploits
Exploits
Combinations:

$100^3$ combinations

$33^3$ combinations = 4.15 days

Disc C has 12 indents

$33^2 * 12 = 1.5$ days

Exploits
Exploits

Disc C:

Outer diameter: 2.815” (71.5mm)
Width of solution slot: 0.239”
Width of 11 indents: 0.249” +/- 0.002”

8.84” (Circumference) / 8400 ticks

0.001” / tick

~10 ticks smaller
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
‘New’ Disc C:

Outer diameter: 2.456” (62.4mm)
Width of solution slot: 0.250”
Width of 11 indents: 0.201” +/- 0.002”

7.72” (Circumference) / 8400 ticks

0.00092” / tick

~54 ticks LARGER
(5 times easier to hack)
New Disc C:
Outer diameter: 2.456” (62.4mm)
Width of solution slot: 0.250”
Width of 11 indents: 0.201” +/- 0.002”
7.72” (Circumference) / 8400 ticks
0.00092” / tick
~54 ticks LARGER (5 times easier to hack)

6) Set starting combos
7) Calibrate handle servo
8) Test handle button
9) Test indent centers
5) Start cracking

How many measurements would you like to take? (Start with 1) 1


Largest indent number: 6
Largest indent is now set to test
Indent locations recorded to EEPROM
Press key to continue
New Disc C:
Outer diameter: 2.456" (62.4mm)
Width of solution slot: 0.250"
Width of 11 indents: 0.201" +/- 0.002"
7.72" (Circumference) / 8400 ticks
0.00092" / tick
~54 ticks LARGER (5 times easier to hack)

6) Set starting combos
7) Calibrate handle servo
8) Test handle button
9) Test indent centers
5) Start cracking

How many measurements would you like to take? (Start with 1)1


Largest indent number: 6
Largest indent is now set to test
Indent locations recorded to EEPROM
Press key to continue
New Disc C:
Outer diameter: 2.456" (62.4mm)
Width of solution slot: 0.250"
Width of 11 indents: 0.201" +/- 0.002"

7.72" (Circumference) / 8400 ticks
0.00092" / tick
~54 ticks LARGER (5 times easier to hack)

Set starting combos
Calibrate handle servo
Test handle button
Test indent centers
Start cracking

How many measurements would you like to take? (Start with 1) 1


Largest indent number: 6
Largest indent is now set to test
Indent locations recorded to EEPROM
Press key to continue
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 large 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
Exploits

Test Time:

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

1.2 hours
45 minutes!
How do I protect myself!?
One of these is not like the others...
“The S&G 6730 ... 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.”

-Hayman Safes: Lock Ratings
The S&G 6730 dial lock 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>Indent 8: [1911] / [1130]</th>
</tr>
</thead>
<tbody>
<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: [2083] / [1100]</td>
</tr>
<tr>
<td>Indent 6: [2114] / [1096]</td>
</tr>
</tbody>
</table>

Measuring complete
Smallest to largest width [Width]/[Depth]
Future Research
Future Research

Credit: iRobot
Future Research
Is it open yet?

nathan@sparkfun.com
Demo fail!