Fair Results From an Unfair Coin

12 Oct 2017 - NYC Python Lightning Talks - Manhattan, NY

Presented By

Vi Grey
Independent Security Researcher
Software Engineer
https://vigrey.com

Who Am I?

- Information Security Researcher
- Software Developer
- Physical Security Enthusiast
- Primary Focus of Research: Applied Cryptography
- Web Developer and Designer

What is a Fair Coin Flip?

- Chance of HEADS is 50%
- Chance of TAILS is 50%
- Future outcomes should not be predictable by past outcomes

What if the Coin is Biased?

- Chance of HEADS and TAILS are not 50% each
- You may not know how biased a coin is before flipping it
- It might be hard to figure out if a coin is biased
  - Example: 49% chance HEADS/51% chance TAILS

How Can Remove Bias from the Coin?

- Flip the same coin twice
  - If the results are the same, ignore the results and try again
  - If the results are different, use the first flip result
- Biased or fair coin, HEADS TAILS is just as likely as TAILS HEADS

Biased Coin Flip Example (60%/40%)

HEADS - 60%
TAILS - 40%

HH - 36% *(60% * 60%)*
HT - 24% *(60% * 40%)*
TH - 24% *(40% * 60%)*
TT - 16% *(40% * 40%)*

Biased Coin Flip Example (10%/90%)

HEADS - 10%
TAILS - 90%

HH - 1% *(10% * 10%)*
HT - 9% *(10% * 90%)*
TH - 9% *(90% * 10%)*
TT - 81% *(90% * 90%)*

Fair Coin Flip Example (50%/50%)

HEADS - 50%
TAILS - 50%

HH - 25% *(50% * 50%)*
HT - 25% *(50% * 50%)*
TH - 25% *(50% * 50%)*
TT - 25% *(50% * 50%)*

Python Coin Flip Debiaser (fairflip.py)

```
1     import random
2     import sys
3
4     heads_percent = int(sys.argv[1]) # Integer value of argument
5
6     while heads_percent > 0 and heads_percent < 100: # Loop if valid heads_percent
7         # If random number is under heads_percent, then flip is HEADS
8         flip1 = heads_percent > random.randint(0, 100) # True if HEADS result
9         flip2 = heads_percent > random.randint(0, 100) # True if HEADS result
10        if flip1 != flip2: # Restart loop if flip1 and flip2 are the same
11            if flip1: # If first flip is HEADS, print HEADS
12                print("HEADS")
13            else: # If first flip is TAILS, print TAILS
14                print("TAILS")
15            break # break out of infinite loop
```

```
$ python3 fairflip.py 70
TAILS
```

Get fairflip.py

GitHub.com/ViGrey/fairflip

vigrey.com
GitHub.com/ViGrey
Twitter.com/ViGreyInfoSec