

# BitSquatting

...or infinite monkeys theorem...

"Three monkeys hitting keys at random on typewriters for an infinite amount of time will almost surely produce Hamlet."

-- David Ives in "Words, Words, Words"

# Not new...

Based on work by Artem Dinaburg

- *Paper: Bitsquatting: DNS Hijacking without Exploitation Blackhat 2011*
- Slides: BITSQUATTING
- Video: *Defcon 19: Artem Dinaburg - Bit-squatting: DNS Hijacking Without Exploitation*

# Explanation...

www.twitter.com:

| ASCII  | t        | w        | i        | t        | t        | e        | r        |
|--------|----------|----------|----------|----------|----------|----------|----------|
| Binary | 01110100 | 01110111 | 01110100 | 01110100 | 01110100 | 01100101 | 01110010 |

www.4witter.com:

| ASCII  | 4         | w        | i        | t        | t        | e        | r        |
|--------|-----------|----------|----------|----------|----------|----------|----------|
| Binary | 001110100 | 01110111 | 01110100 | 01110100 | 01110100 | 01100101 | 01110010 |

| Type                  | Failures In Test/Mbit | Hours until error (128MB) | Hours until error (16GB) |
|-----------------------|-----------------------|---------------------------|--------------------------|
| Mfg1,4GB DIMM         | 4,100                 | 240                       | 1.92                     |
| Mfg6,4GB DIMM         | 11,000                | 89                        | 0.71                     |
| Micron Est., 256MByte | 120 (- 240)           | 8,100                     | 64                       |

# Srsly?!....

**Table 1: Memory errors per year:**

| Platf.  | Tech. | Per machine   |              |              |                  |               |
|---------|-------|---------------|--------------|--------------|------------------|---------------|
|         |       | CE Incid. (%) | CE Rate Mean | CE Rate C.V. | CE Median Affct. | UE Incid. (%) |
| A       | DDR1  | 45.4          | 19,509       | 3.5          | 611              | 0.17          |
| B       | DDR1  | 46.2          | 23,243       | 3.4          | 366              | –             |
| C       | DDR1  | 22.3          | 27,500       | 17.7         | 100              | 2.15          |
| D       | DDR2  | 12.3          | 20,501       | 19.0         | 63               | 1.21          |
| E       | FBD   | –             | –            | –            | –                | 0.27          |
| F       | DDR2  | 26.9          | 48,621       | 16.1         | 25               | 4.15          |
| Overall | –     | 32.2          | 22,696       | 14.0         | 277              | 1.29          |

| Platf.  | Tech. | Per DIMM      |              |              |                  |               |
|---------|-------|---------------|--------------|--------------|------------------|---------------|
|         |       | CE Incid. (%) | CE Rate Mean | CE Rate C.V. | CE Median Affct. | UE Incid. (%) |
| A       | DDR1  | 21.2          | 4530         | 6.7          | 167              | 0.05          |
| B       | DDR1  | 19.6          | 4086         | 7.4          | 76               | –             |
| C       | DDR1  | 3.7           | 3351         | 46.5         | 59               | 0.28          |
| D       | DDR2  | 2.8           | 3918         | 42.4         | 45               | 0.25          |
| E       | FBD   | –             | –            | –            | –                | 0.08          |
| F       | DDR2  | 2.9           | 3408         | 51.9         | 15               | 0.39          |
| Overall | –     | 8.2           | 3751         | 36.3         | 64               | 0.22          |

# So what?....

```
138.246.253.5 - - [13/Sep/2018:04:27:52 +0000] SNI: twitter.com "HEAD /
HTTP/1.1" 200 0 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.85 Safari/537.36"
"_"
71.62.75.209 - - [13/Sep/2018:14:10:03 +0000] SNI: www.twitter.com "GET /
HTTP/1.1" 200 647 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
"_"
163.172.4.153 - - [14/Sep/2018:06:31:53 +0000] SNI: - "GET / HTTP/1.1" 200
647 "http://twitter.com/" "Mozilla/5.0 (Windows NT 6.3; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
"_"
```

```
root@ron[0]:~/tmp/tmp# grep twitter * | wc -l
102
```

# Cool story, bro....

|                        |                            |                                |                            |
|------------------------|----------------------------|--------------------------------|----------------------------|
| aarp -> carp           | box -> boy                 | farm -> firm                   | maif -> main               |
| <b>ally -&gt; illy</b> | cab -> car                 | farm -> fare                   | <b>media -&gt; medic</b>   |
| <b>athleta -&gt;</b>   | <b>cafe -&gt; safe</b>     | film -> file                   | <b>natura -&gt; nature</b> |
| <b>athlete</b>         | career -> carder           | fire -> five                   | post -> port               |
| beer -> bear           | charity -> clarity         | fish -> dish                   | raid -> rail               |
| beer -> bees           | crown -> brown             | food -> good                   | rest -> best               |
| best -> rest           | cruises -> cruiser         | food -> fool                   | safe -> save               |
| bet -> bat             | dance -> lance             | <b>glade -&gt; glide</b>       | save -> cave               |
| bet -> bed             | <b>data -&gt; date</b>     | glass -> class                 | save -> wave               |
| <b>bike -&gt; bake</b> | <b>dating -&gt; eating</b> | <b>gold -&gt; golf</b>         | save -> safe               |
| bing -> ring           | dell -> tell               | gripe -> grape                 | seek -> week               |
| boo -> foo             | <b>dish -&gt; fish</b>     | help -> hemp                   | swatch -> switch           |
| book -> cook           | <b>docs -&gt; dogs</b>     | hockey -> jockey               | town -> down               |
| <b>booking -&gt;</b>   | dodge -> lodge             | host -> lost                   | watch -> witch             |
| <b>cooking</b>         | duck -> luck               | <b>infiniti -&gt; infinity</b> | wedding -> welding         |
| box -> boy             | duck -> deck               | <b>living -&gt; diving</b>     | <b>wine -&gt; wife</b>     |

Hi! My name is (what?)

My name is (who?)

My name is Slim Shady...

'cos I'm Slim Shady

Yeah, I'm the real Shady

All you other Slim Shadys  
are just imitating...

So won't the real Slim  
Shady please stand up...