BISHOP FOX

Untwisting the Mersenne Twister

KILLING PRNGS

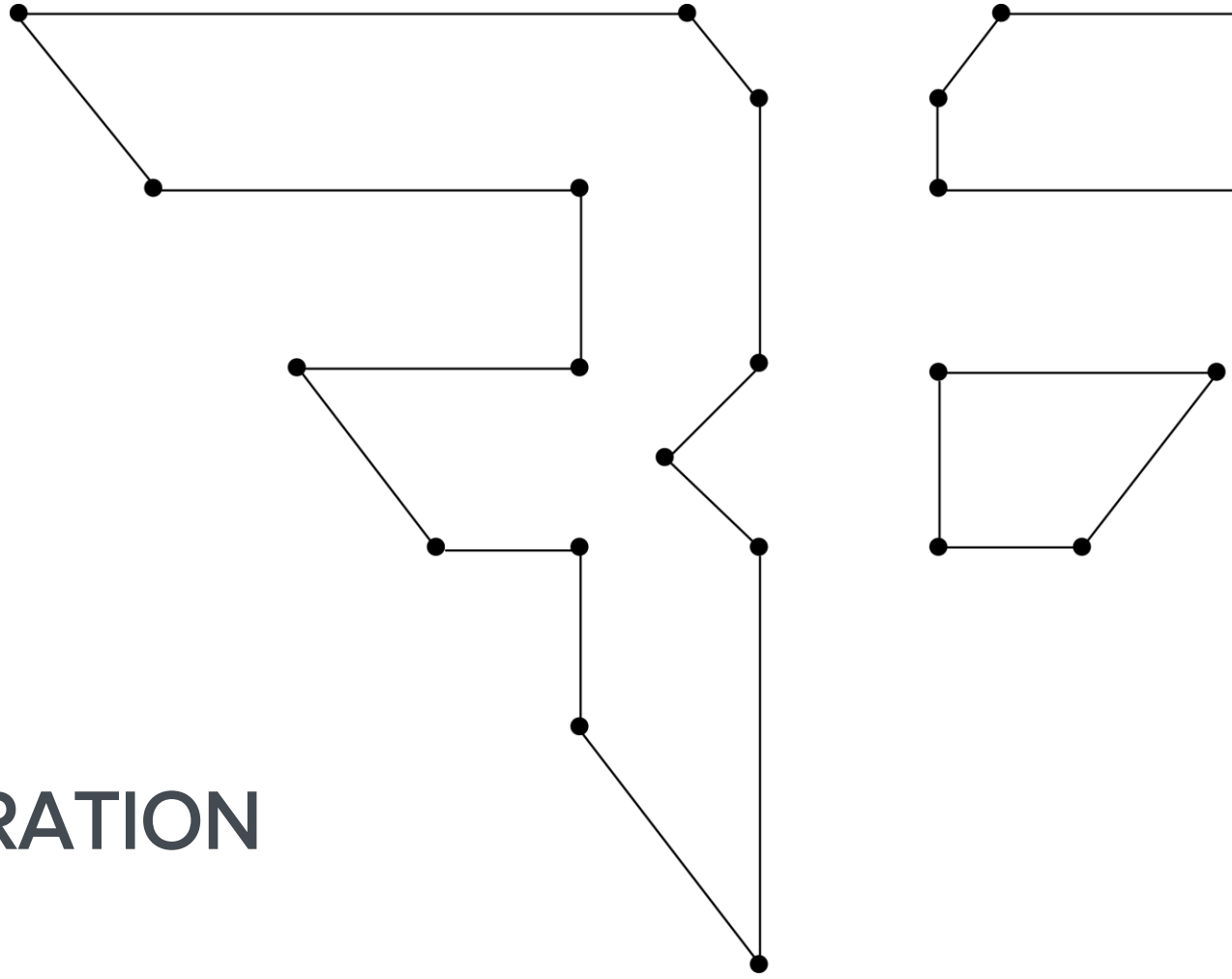
November 5, 2014

WHOAMI

UNTWISTING THE MERSENNE TWISTER

Bishop Fox

- Dan Petro
  Sr. Security Analyst
  - *PHX 2600*
  - *Nova / Honeyd*
  - *Rickmote*
- Moloch
  Security Associate
  - *Root the Box*
  - *[buffer]overflow*
  - *iSpy*



DEMONSTRATION

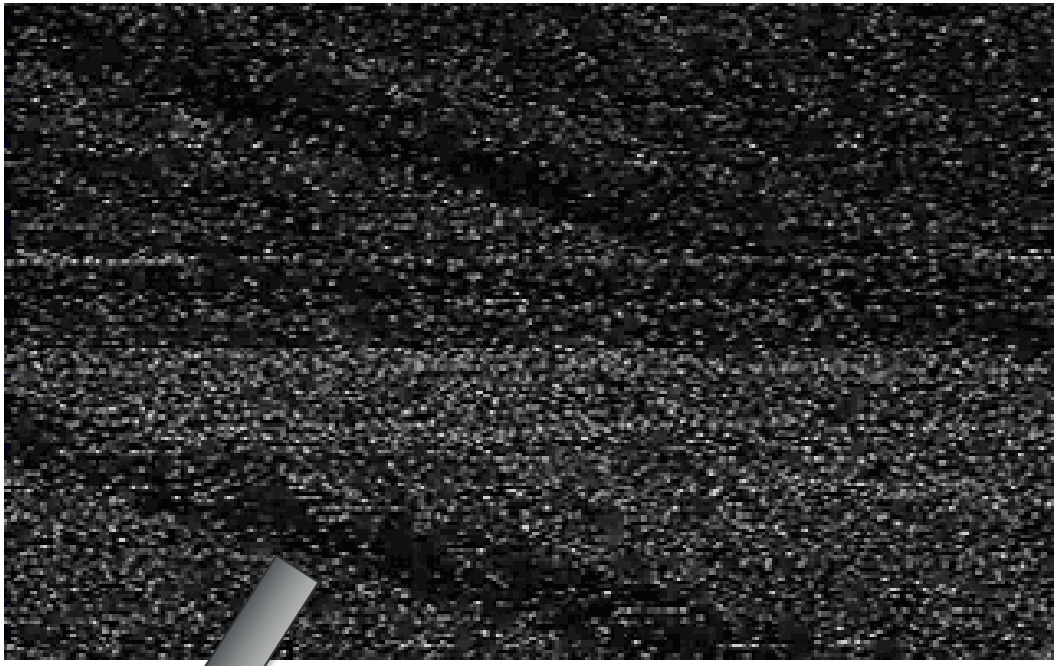
CROSS FINGERS

WHAT IS PSEUDORANDOM

A QUICK HISTORY LESSON

Nature

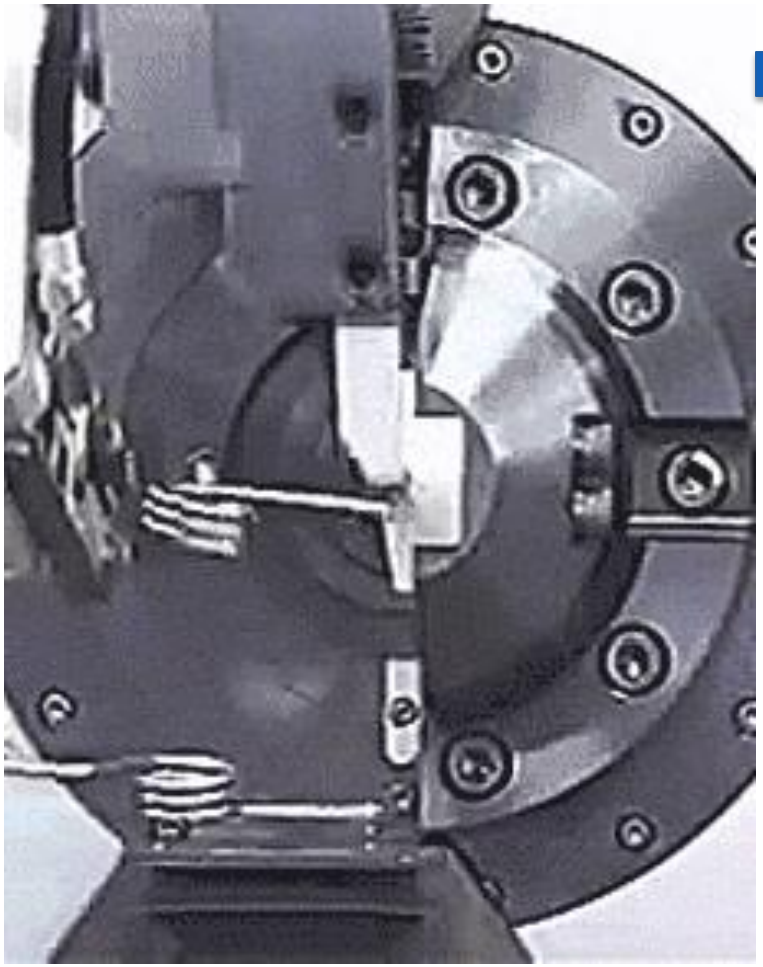
BY THE NUMBERS



57983427917349817398417987193824798 1

Machines

DETERMINISTIC



57983420

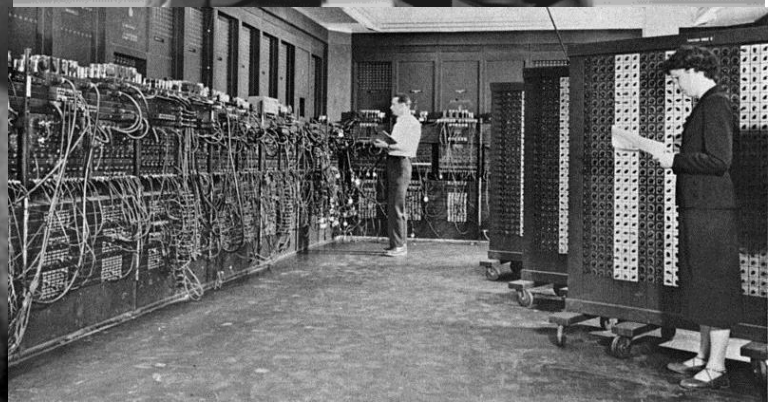
57983420

57983420

...

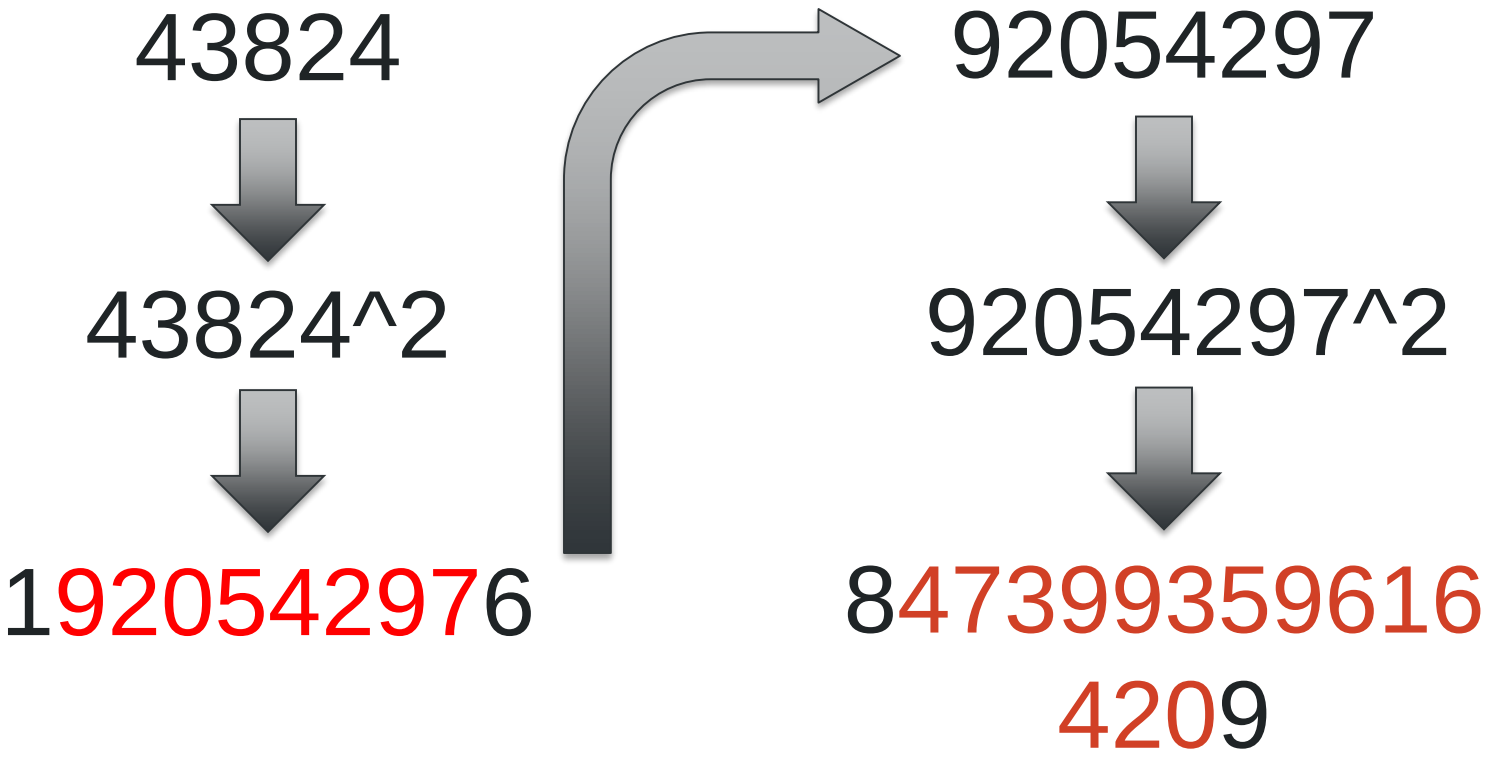
Early Pseudorandom Generators

JOHN VON NEUMAN



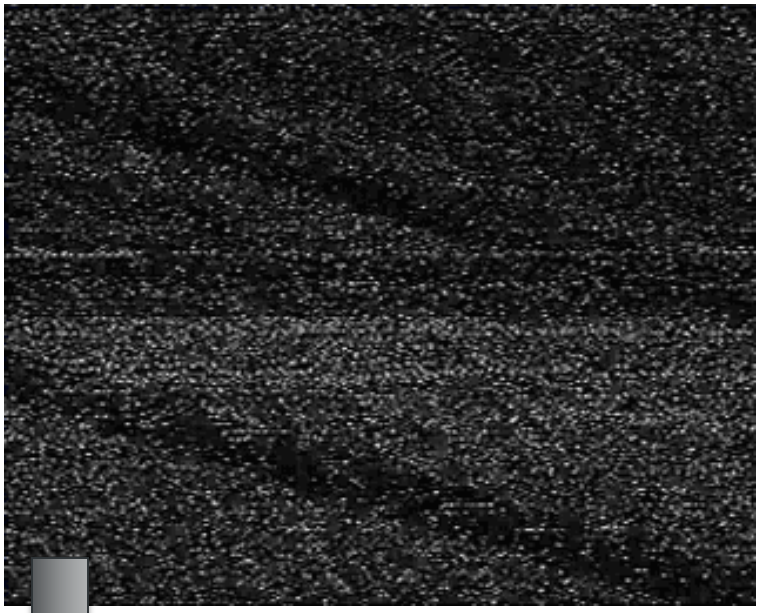
Middle Squares Method

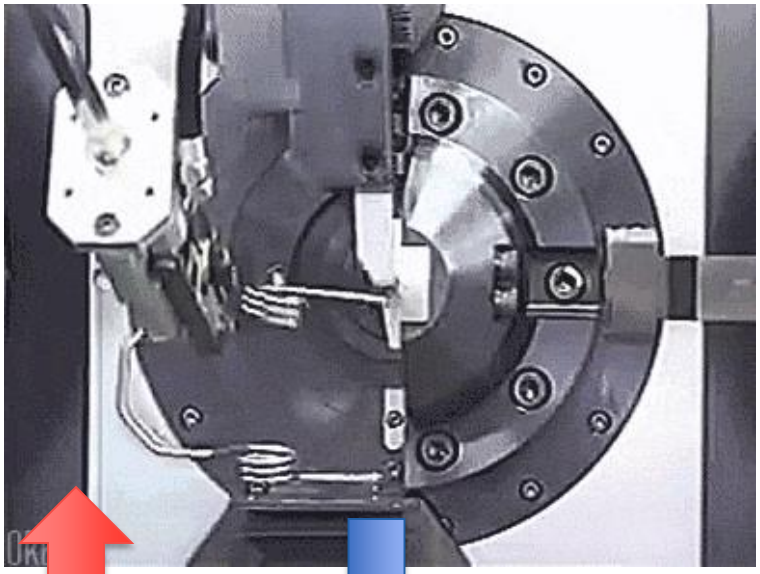
PRNG



Random vs. Pseudorandom

DETERMINISTIC RANDOMNESS

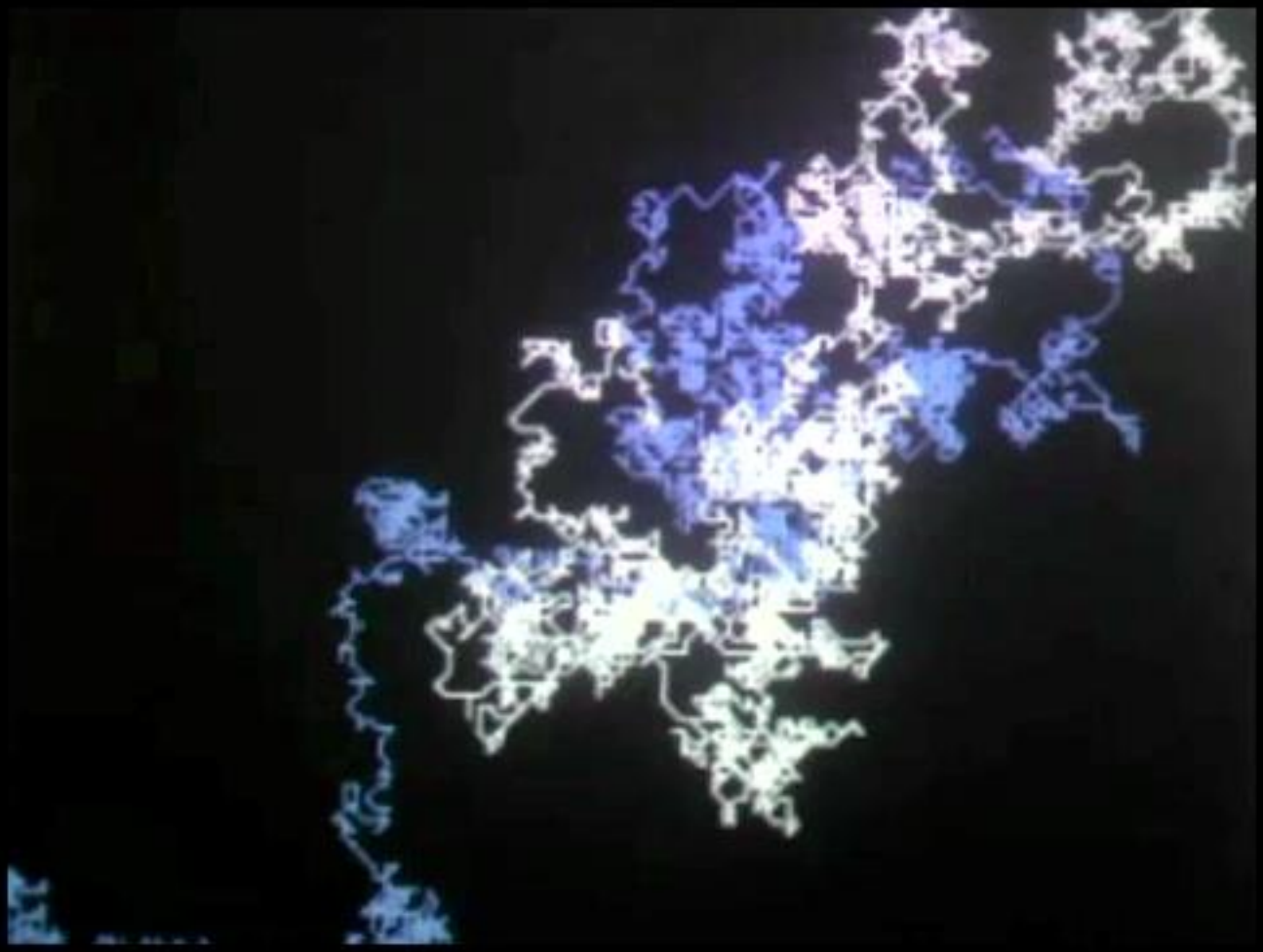




983427917349817…

5480

7983349817…



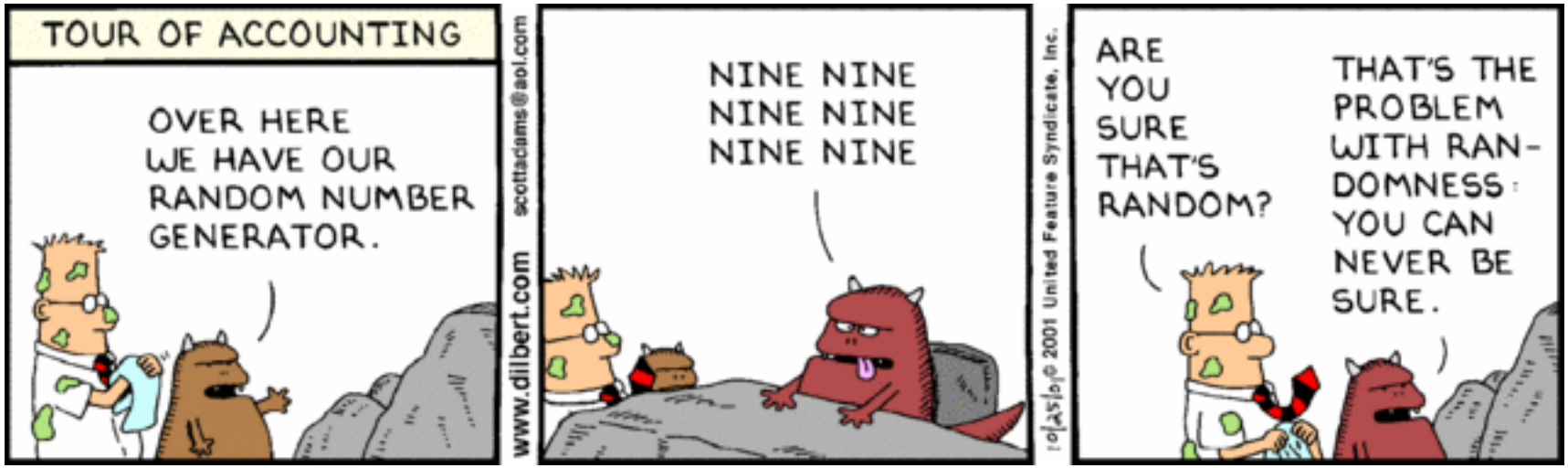
PRNG Period Size

THE MERSENNE TWISTER

(2^19937)-1 =

Can you be sure?

EVALUATING RANDOMNESS



The Die Hard Tests

TESTING RANDOMNESS

Die Hard Randomness Tests

999999999999 …

- Birthday attacks
- “Craps” tests
- Count the 1s
- Monkey tests
- Parking lot tests
- Squeeze tests
- Etc.

SEEDS

HOW DO THEY WORK?

Do You Want Vulns?

CHOOSING A “SECURE” SEED

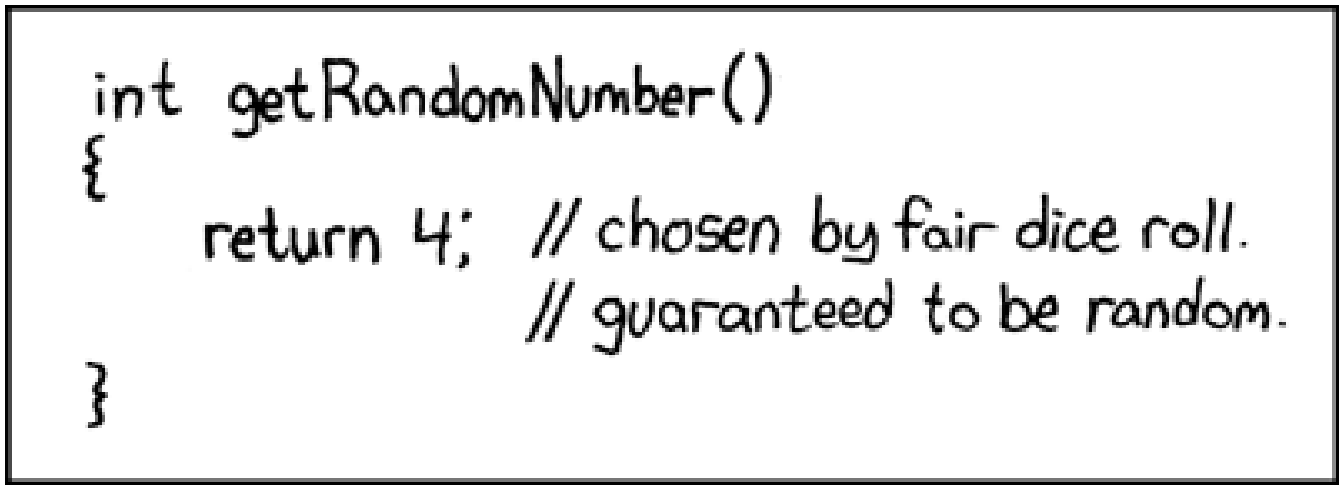
- Time
- PIDs
- Stack memory
- Hardcoded “random” seed
- Combinations of any of the above

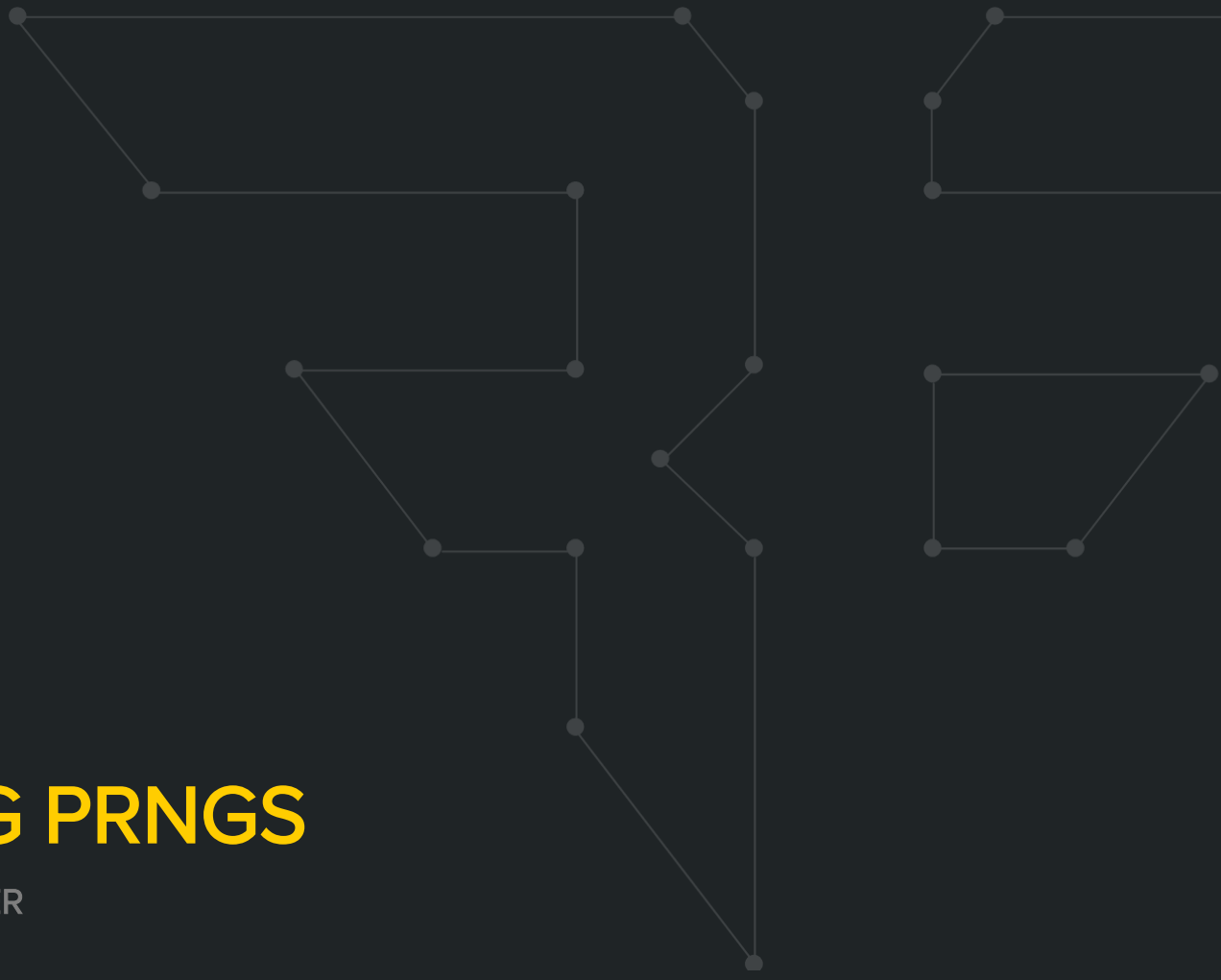
Vulns.

THAT’S HOW YOU GET THEM

Sony's ECC Random

EVALUATING RANDOMNESS





ATTACKING PRNGS

UNTWISTING THE TWISTER

Bruteforce

EVEN CHOOSING A SEED WELL CAN'T SAVE YOU

- 32 bit seeds on most algorithms
  - 4,294,967,296 values
  - Enumerable
- Offline attack
  - Limited only by CPU power
- Timestamp based seeds
  - 31,557,600 values

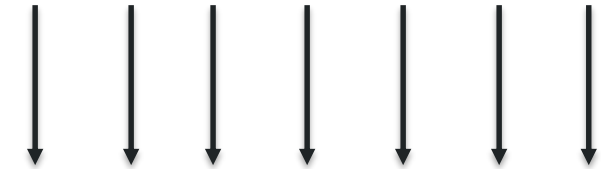
Algorithm

USED IN UNTIWSTER

- Given set of observed numbers
  - 42, 61, 27, 75, 89, 34, 12
- Calculate random numbers
  - One by one
  - Compare to head of observed list
  - If it matches, look for the next observed #
  - Continue until match is found
- Allows for missing values
  - Don’t have to be sequential

Algorithm

USED IN UNTIWSTER



42, 61, 27, 75, 89, 34, 12

45, 33, 42, 97, 61, 27, 75, 49, 51, 89 34, 12,

,

Problem of Depth

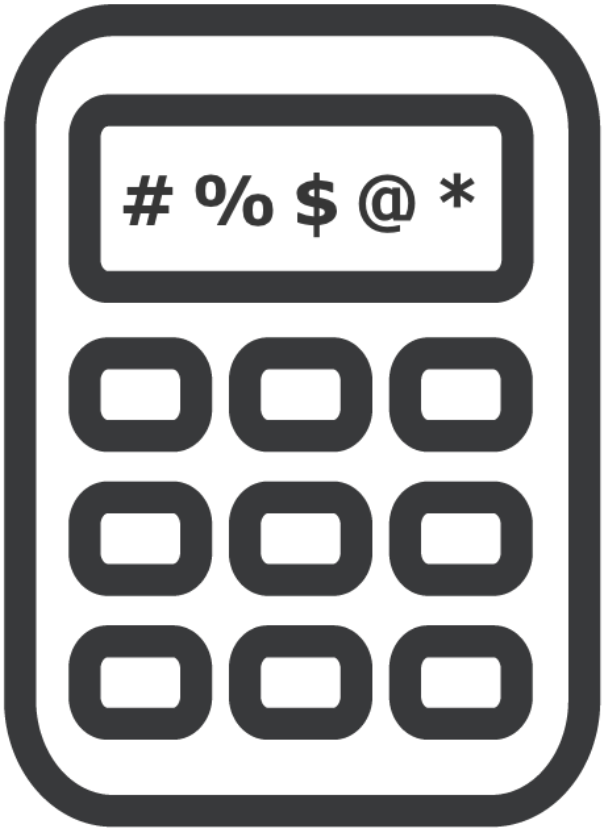
WHERE TO HALT

- How do you know you're deep enough?
  - Maybe the correct numbers are just about to appear
  - Haven't yet
- Halting problem
  - Depth is given as input
  - Give up after depth is explored
- Efficiency vs Completeness Tradeoff

State Inference

MATH IS HARD

- Crack RNG state
  - Predict future and past values
  - Without knowing the seed!
- Much easier with sequential numbers
  - Current implementation requires it*
- Small state size helps, too



glibc rand()

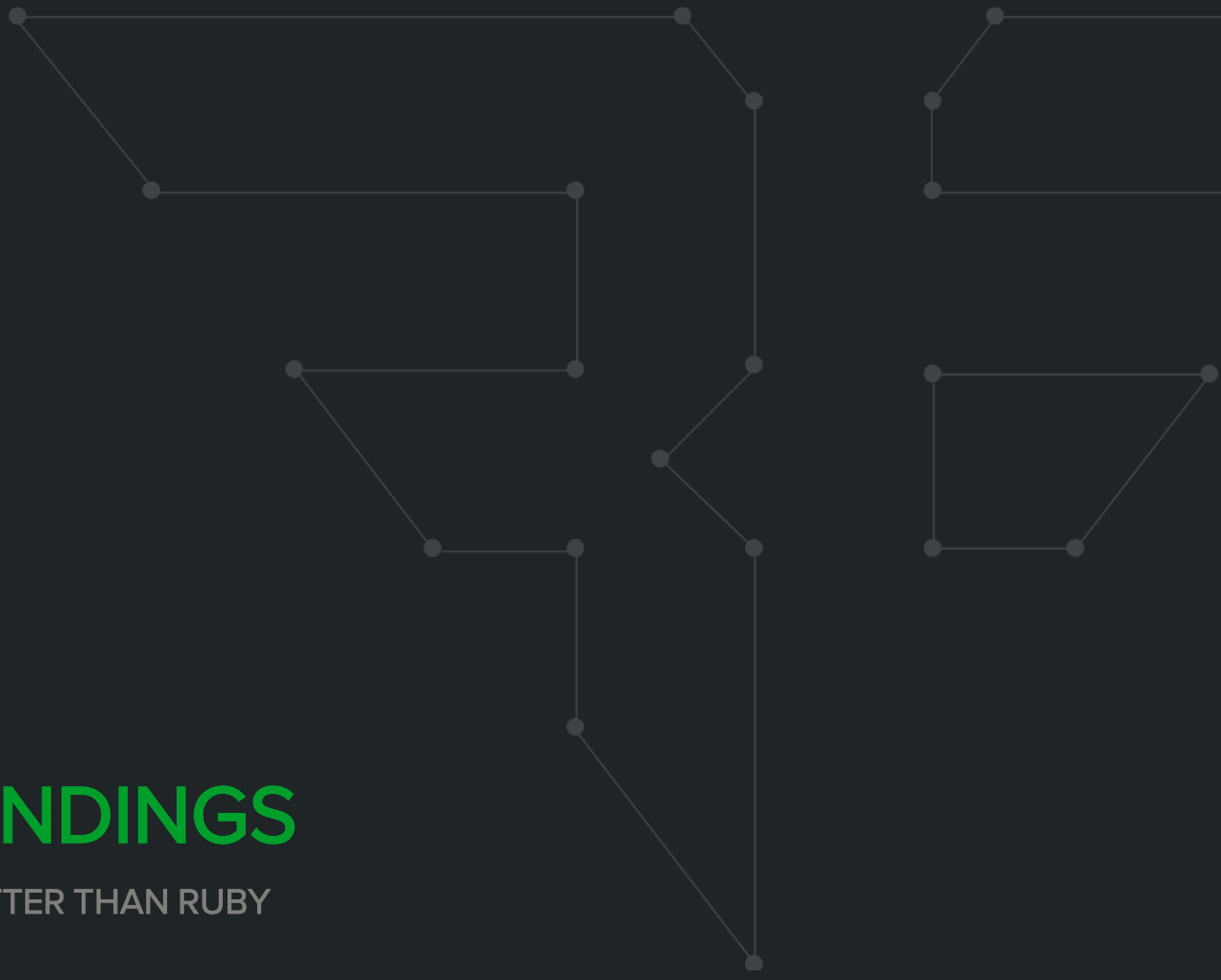
MATH IS HARD

- **Very simple algorithm**
  - r[i] = r[i-3] + r[i-31]
  - With the LSB chopped off
- **Produces 31 bit numbers**
  - Internal state has 32 bit numbers
- **Observe 32 sequential numbers**
  - This IS the internal state
  - Missing the LSBs

glibc rand()

MATH IS HARD

- **LSB reconstruction**
- **Guess-and-check**
  - Use state to predict random numbers
  - Measure how well it predicts
  - Try with 0 and 1 LSB
  - Go with the better guess!
- **Boolean Algebra**
  - Really long Boolean equation
  - Only guaranteed for ~132 consecutive outputs



PYTHON BINDINGS

BECAUSE PYTHON IS BETTER THAN RUBY

The Python GIL

THREADING ISSUES IN PYTHON

- Bytes codes do not execute concurrently
- The GIL is not going anywhere
- Threads are still useful for certain tasks, but not performance

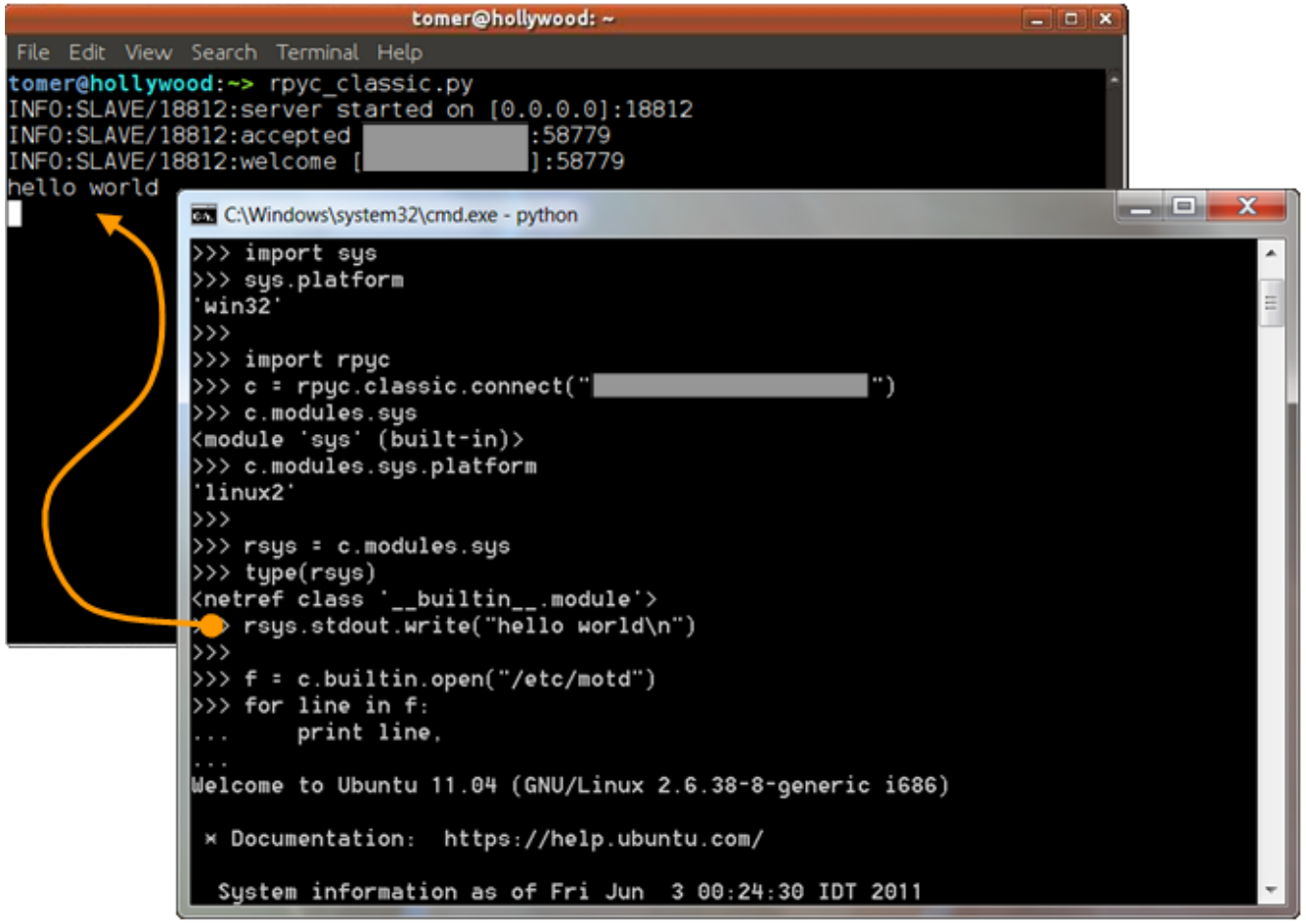
Code Sample

THE C++ // PYTHON BRIDGE

```
    /* Suspend Python's thread, so we can use native C++ threads */

    PyThreadState* pyThreadState = PyEval_SaveThread();

    StartBruteForce(threads, answers, (double) minimumConfidence,
lowerBoundSeed, upperBoundSeed, depth, rng);



    /* Clean up and restore Python thread state */

    PyEval_RestoreThread(pyThreadState);

    pyThreadState = NULL;
```

Distributed Computing

REMOTE PYTHON CALL



Contact Us

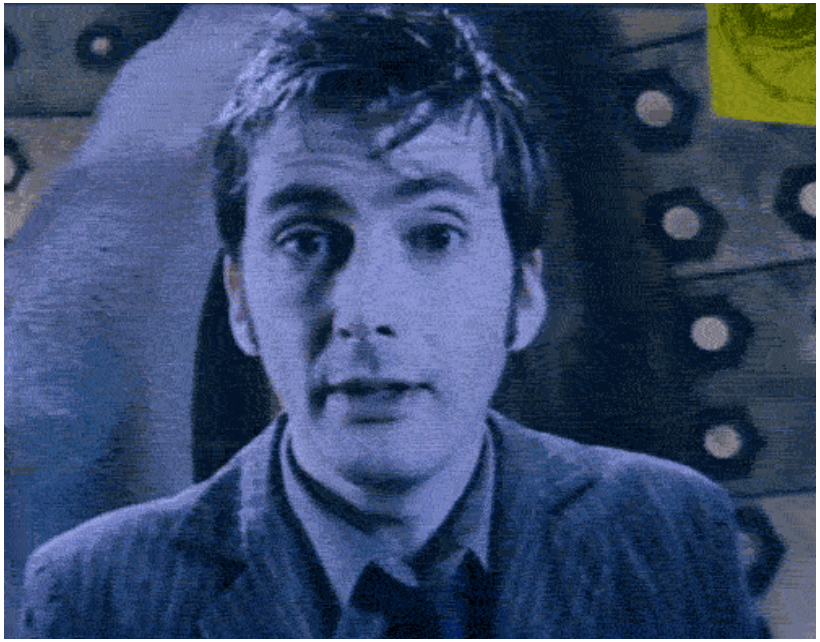
bishopfox.com

@bishopfox

BishopFox
AltF4
Moloch--

BISHOP FOX®

Thank You



BSIDES

BISHOP FOX®

We’re Hiring

bishopfox.com

careers@bishopfox.com

Especially if you know how to make final slides...immediate hire.

BISHOP FOX®