Network Security (NetSec)

IN2101 – WS 17/18

Prof. Dr.-Ing. Georg Carle

Dr. Heiko Niedermayer
Quirin Scheitle
Acknowledgements: Dr. Cornelius Diekmann

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Chapter 9: Random Numbers

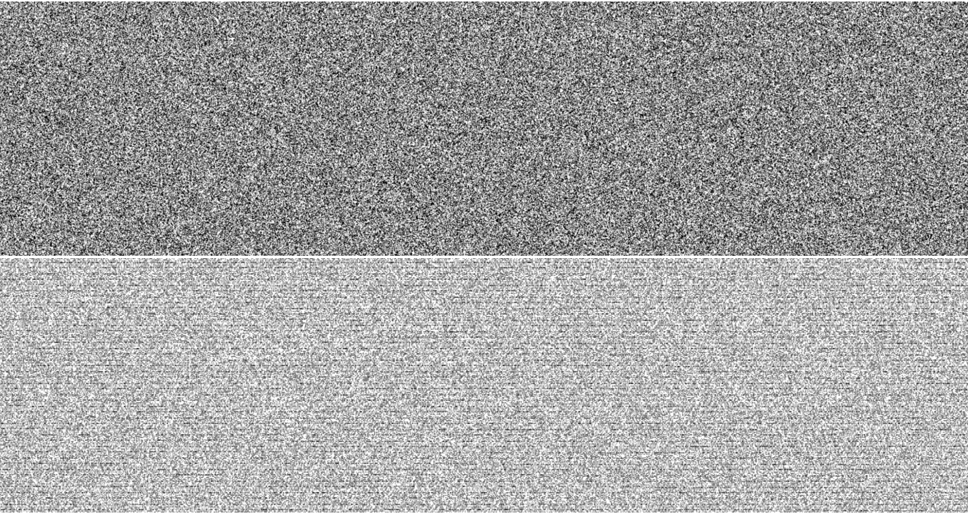
What does ‘Random’ mean?

Entropy

Cryptographically Secure Pseudo Random Number Generator – CSPRNG

Quiz

What does ‘Random’ mean?



Random noise in your browser: Safari (top); V8 (bottom).

CC-BY 2.0, Mike Malone, Betable CTO, https://medium.com/@betable/tifu-by-using-math-random-f1c308c4fd9d

Entropy

- “randomness” can be described by unpredictability
- A measure for “unpredictability” is “entropy”
- Let X be a random variable which outputs a sequence of n bits
- The Shannon information entropy is defined by:

$$H(X) = -\sum_{x} P(X = x)\ln_2(P(X = x))$$

- Entropy is maximized for a uniform distribution
  - I.e. every Bit is equally likely
  - Def.: truly random
- In this case: $H(X) = n$

Entropy: Example

- A key of 128 Bit should have an entropy of 128
- What about the password `TTTTTTTTTTTTTTTT`?

Entropy: Example

- A key of 128 Bit should have an entropy of 128
- What about the password `TTTTTTTTTTTTTTTT`?
- 16 8-bit characters, 128 Bit. Entropy?
- If all bits chosen uniformly at random, entropy is 128

Entropy: Example

- A key of 128 Bit should have an entropy of 128
- What about the password `TTTTTTTTTTTTTTTT`?
- 16 8-bit characters, 128 Bit. Entropy?
- If all bits chosen uniformly at random, entropy is 128
- Assume the attacker knows it’s ASCII
- Ascii: every 8th Bit is zero: entropy at most 112

Entropy: Example

- A key of 128 Bit should have an entropy of 128
- What about the password `TTTTTTTTTTTTTTTT`?
- 16 8-bit characters, 128 Bit. Entropy?
- If all bits chosen uniformly at random, entropy is 128
- Assume the attacker knows it's ASCII
- Ascii: every 8th Bit is zero: entropy at most 112
- Assume attacker knows that it consists of 16 equal characters
- All 16 Characters are equal: entropy at most 7

Entropy: Example

- A key of 128 Bit should have an entropy of 128
- What about the password `TTTTTTTTTTTTTTTT`?
- 16 8-bit characters, 128 Bit. Entropy?
- If all bits chosen uniformly at random, entropy is 128
- Assume the attacker knows it's ASCII
- Ascii: every 8th Bit is zero: entropy at most 112
- Assume attacker knows that it consists of 16 equal characters
- All 16 Characters are equal: entropy at most 7
- Assume the attackers knows the password is printable
- Entropy is about 6.66

Collecting Entropy

- Hardware-based; physical phenomena
  - time between emission of particles during radioactive decay
  - thermal noise from a semiconductor diode or resistor
  - frequency instability of a free running oscillator
  - the amount a metal insulator semiconductor capacitor is charged during a fixed period of time
  - noise of microphone or camera
- Software-based
  - the system clock
  - elapsed time between keystrokes or mouse movement
  - buffers
  - user input
  - OS stats, e.g. network load
- Attacker must not be able to guess/influence the collected values

Collecting Entropy

- Getting entropy is expensive
- Pseudo-Random Number Generator (PRNG):
    - Deterministic algorithm
    - Input: truly random binary sequence of length, seed
    - Output: sequence of random-looking numbers
- seed: small amount of initial entropy
- ‘cheap’ randomness

PRNG – Example

- linear congruential generator

$$y_i = a \cdot y_{i-1} + b \quad MOD \; q$$

- predictable $\rightarrow$ not cryptographic!

Cryptographically Secure Pseudo Random Number Generator – CSPRNG

- The length of the seed should be large enough to make brute-force search over all seeds infeasible
- The output should be indistinguishable from truly random sequences
  - no polynomial-time algorithm can correctly distinguish between an output sequence of the generator and a truly random sequence
- The output should be unpredictable for an attacker with limited resources, without knowledge of the seed

Chapter 9: Random Numbers

Quiz

- A CSPRNG produces a bitstring of 2048 bit
- What is the max. possible entropy of this string?

Quiz

- A CSPRNG produces a bitstring of 2048 bit
- What is the max. possible entropy of this string?
- min(Length of the seed, 2048)
- usually: Length of the seed