

More Entropy, Please!

More Entropy, Please!

2015-08-16 Debconf15 @ Heidelberg Germany
Niibe family + Yukiharu Yabuki

More Entropy, Please!

"More Entropy, Please" is a story written by me:
<http://www.gniibe.org/memo/development/gnuk/mg/more-entropy-please.html>

In the story, I insist that more entropy is required.
In this context, entropy means randomness.

In This Talk

- Promotion of "More Entropy, Please!"
 - Let's Play! (during this conference)
- Philosophy
- Product
- (I wanted a talk which family can join)

The Game: Monty Hall Problem (1)

In <http://marilynvossovant.com/game-show-problem/>, it is described:
Suppose you're on a game show, and you're given the choice of three doors.
Behind one door is a car, behind the others, goats.
You pick a door, say #1, and the host, who knows what's behind the doors, opens another door, say #3, which has a goat.
He says to you, "Do you want to pick door #2?"
Is it to your advantage to switch your choice of doors?

The Game (2)

- Host
Today, it's me (Yutaka).
- Three Doors (1 CAR, 2 GOATS) (R, B, and G)
Random Lady: Hitoe
Boy: Hiroshi
Girl: Ayumi
- Player

The Game (3)

1. Host puts a CAR behind one of doors.
 2. Host asks Player the initial choice.
 3. Player answers the initial choice.
 4. Host opens another door with a GOAT (which must not be Player's choice).
 5. Host asks Player the final choice: Stick or Switch?
 6. Player answers the final choice.
 7. Host opens a door of the final choice.
 8. If it's a CAR, Player wins.
- Let's Play!

Possible Strategies of Player

- Chose randomly, then, always stick the initial choice
- Chose randomly, then, always switch the choice
- ...

Fair Host

- Initially, for choice of a door with a CAR, randomness is important.
- When opening a door with a GOAT, his computation to decide should be **constant time** and **always gets randomness** even if it is not used.
- Why?
 - When Player's initial choice is a door with a CAR:
 - Host does random selection between two doors.
 - When Player's initial choice is a door with a GOAT:
 - It is deterministic. It's another door with a GOAT.
 - Clever Player can observe Host's behavior to answer the final choice.

The Lesson

- To be fair Host,
- Randomness is important.
 - Even if it's not used directly or it appears it were not needed, we actually need randomness. (Please see the article at www.gniibe.org for detail.)
 - So, I insist "More Entropy, Please!", even for this simple game.
 - If it's for our computing (specifically for encryption), "more entropy" is more important.

Philosophy

Why "more entropy?" (1)

- People deserve to control their own computing.
- Backdoors and vulnerabilities are common, these days.
- Massive surveillance is difficult to avoid/escape.
- Thus, we use encryption.
 - Let's Encrypt: <https://letsencrypt.org/>
 - Email Self-Defence: <https://emailselfdefense.fsf.org/>
 - GnuPG, Tor, OTR, ...
- For encryption, **key** is important, literally.
- Key includes: static key, session key, nonce, etc.

Why "more entropy?" (2)

- People deserve to control their own computing.
- We use more encryption, thus, more **randomness** make sense.
- In the central of computing freedom, we need random number generation which **no one can control**.

Product

Product

- non-product: DIY
STM32 Nucleo F103RB can be NeuG USB Deice which generates good random number sequence by 80 kb/s.
- GnuPG T-shirt: available at FSFE booth.
- Flying Stone Technology

Product Description	Price
FST-01 (tube) NeuG 1.0.3 + micro SD	195EUR
FST-01 (case) GnuK 1.1.7 + above	195EUR

DIY: STM32 Nucleo F103RB

STM32 Nucleo F103RB can be NeuG USB Deice which generates good random number sequence by 80 kb/s.



FST-01

Flying Stone Technology ZERO-ONE

Product Description	Price
FST-01 (tube) NeuG 1.0.3 + micro SD	195EUR
FST-01 (case) GnuK 1.1.7 + above	195EUR



Happy Hacking! and Let's Play
More Entropy Please!