"More Entropy, Please!"

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

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

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

Promotion of "More Entropy, Please!"
Let's Play! (during this conference)

Philosophy
Product

In This Talk

- Promotion of "More Entropy, Please!"
- Let's Play! (during this conference)
- Philosophy
- Product

I insist a talk which family can join.

The Game: Monty Hall Problem (1)

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

The Game (2)

- Initially, for choice of a door with a CAR, randomness is important.
- When opening a door with a GOAT, no computation to decide should be constant time and always gets randomness even if it's not used.

- Why?
- When Player's initial choice is a door with a CAR:
  - Host doesn't random selection between two doors.
- When Player's initial choice is a door with a GOAT:
  - It's deterministic. It's another door with a GOAT.
- Clever Player can observe Host's behavior to answer the final choice.

Why "more entropy?" (2)

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

- Even if it's not be used directly or it appears it were not needed, we still need randomness. (Please see the article at www.gniibe.org for detail.)

- When opening a door with a GOAT, no computation to decide should be constant time and always gets randomness even if it's not used.

- Why?
- When Player's initial choice is a door with a CAR:
  - Host doesn't random selection between two doors.
- When Player's initial choice is a door with a GOAT:
  - It's deterministic. It's another door with a GOAT.
- Clever Player can observe Host's behavior to answer the final choice.

Philosophy

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-Defense:
https://emailselfdefense.fsf.org/
GnuPG, Tor, OTR, ...

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-Defense: https://emailselfdefense.fsf.org/
- GNU Privacy, Tor, OTR, ...
- For encryption, key is important. Literally.
- Why includes: static key, session key, nonce, etc.

Product

- non-product: DIY
  - FST-01 can be NeuG USB Device which generates good random number sequence by 80 kB/s.
  - GnuPG T-shirt: available at FSFE booth.

- Flying Stone Technology ZERO-ONE

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>FST-01 (tube) NeuG 1.0.3 + micro SD</td>
<td>35EUR</td>
</tr>
<tr>
<td>FST-01 (case) Gnuk 1.1.7 + above</td>
<td>65EUR</td>
</tr>
</tbody>
</table>

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

The Lesson

To be Fair Host,
Randomness is important.

- Even if it's not be used directly or it appears it were not needed, we still need randomness. (Please see the article at www.gniibe.org for detail.)
- No, I insist a talk which family can join.
- If it's for our computing (specifically for encryption), "more entropy" is more important.

Why "more entropy?"

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

- In the context of computing freedom, we need random number generation which no one can control.

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

In This Talk

- Promotion of "More Entropy, Please!"
- Let's Play! (during this conference)

The Game (1)

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 a 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.

In This Talk

- Promotion of "More Entropy, Please!"
- Let's Play! (during this conference)

The Game (2)

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

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 a 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.

Possible Strategies of Player

- Choose randomly, then, always click the initial choice
- Choose randomly, then, always switch the choice
- ...

Why "more entropy?"

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

- In the context of computing freedom, we need random number generation which no one can control.

Why "more entropy?"

- 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-Defense:
https://emailselfdefense.fsf.org/
GnuPG, Tor, OTR, ...

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-Defense: https://emailselfdefense.fsf.org/
GnuPG, Tor, OTR, ...

Why "more entropy?" (2)

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

In the context of computing freedom, we need random number generation which no one can control.

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

In This Talk

- Promotion of "More Entropy, Please!"
- Let's Play! (during this conference)

The Game (1)

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 a 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.

In This Talk

- Promotion of "More Entropy, Please!"
- Let's Play! (during this conference)

The Game (2)

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

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 a 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.

Possible Strategies of Player

- Choose randomly, then, always click the initial choice
- Choose randomly, then, always switch the choice
- ...

Why "more entropy?"

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

In the context of computing freedom, we need random number generation which no one can control.

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-Defense: https://emailselfdefense.fsf.org/
GnuPG, Tor, OTR, ...

Why "more entropy?" (2)

- People deserve to control their own computing.
- We use more encryption; thus, more randomness make sense.

In the context of computing freedom, we need random number generation which no one can control.

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