RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

THE NIST RANDOMNESS BEACON

SESSION ID: ASEC-T07B

Rene Peralta

Computer Security Division
National Institute of Standards and Technology.

Outline of talk

- What the Beacon is and isn't.
- Motivation and usage.
- The bigger picture.
- A verifiable source of random bits.
- Summary.

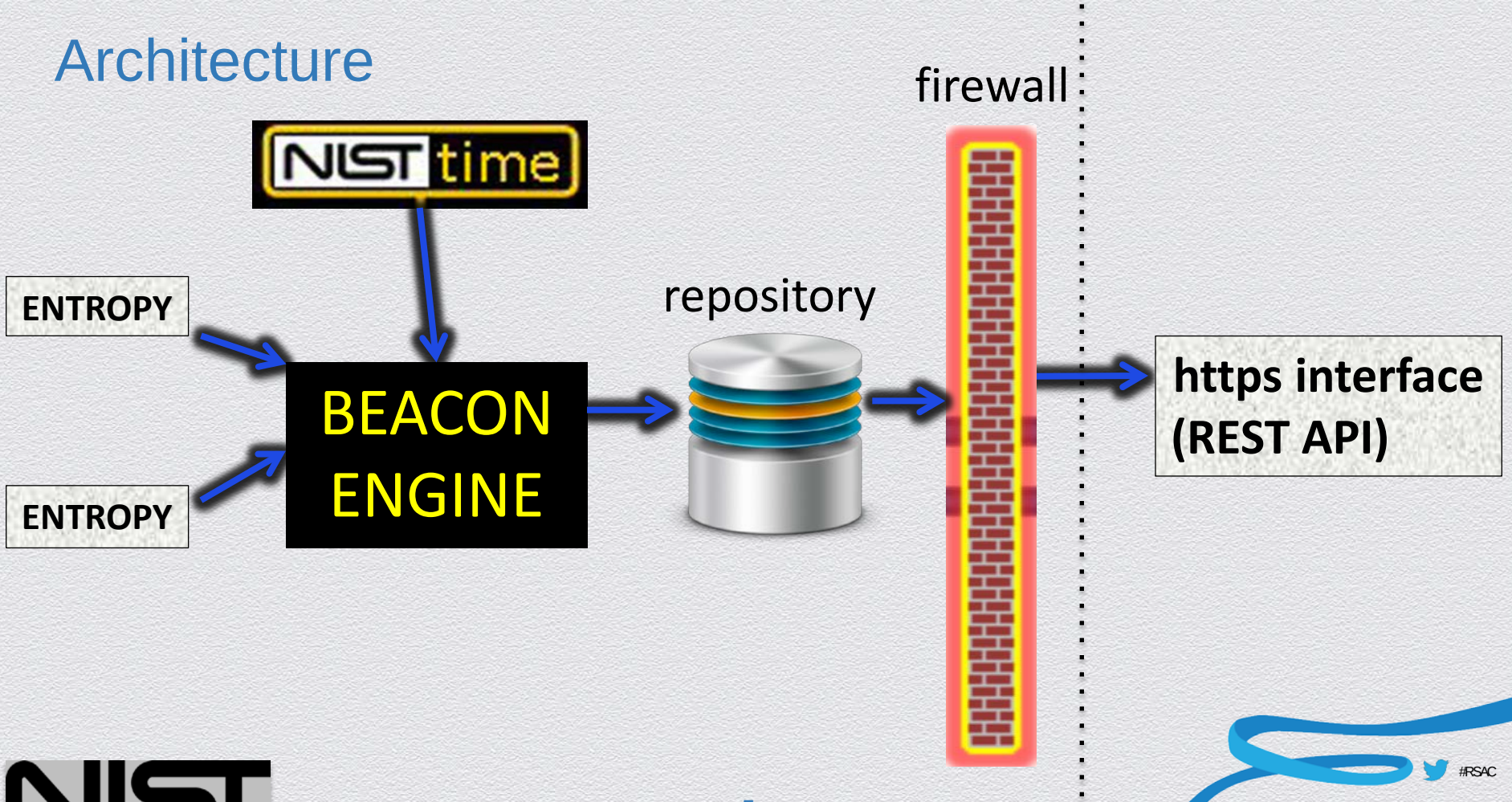
What this is not

- **This is not for generation of secret keys.**

What this is

- Public randomness
  - publish model
  - digitally signed and time-stamped
  - https://beacon.nist.gov/home

Architecture



Motivation

- Public, time-bound randomness is a valuable resource
- A standard for such a resource is needed so that others can set them up.

Properties

- Unpredictability
- Autonomy
- Consistency
- “Forever” unforgeable public record

Sample applications

- Provably random sampling
- Selective disclosures. This aligns with the goals of the National Strategy for Trusted Identities in Cyberspace (NSTIC)

Selective Disclosure Scenario

- Suppose authenticated and encrypted data about you exists somewhere

DATA

You have 

- At a later time, a function of this data is required for a given transaction (e.g. F(DATA) = “over 21 or doctor authorization”)
- A “discreet” proof that F holds can be constructed using the key and a string from the Beacon

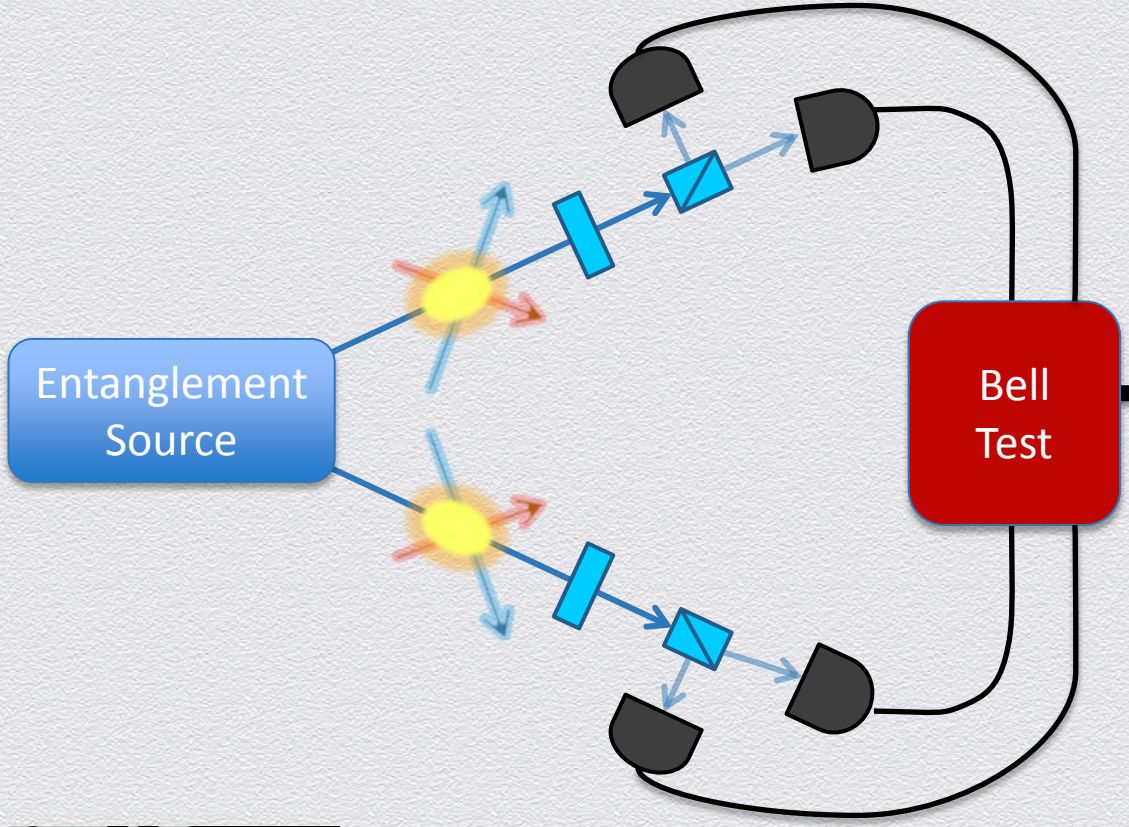
Can you trust it?

- You don’t have to!
  - can combine with other sources
  - can flip a few bits and hash it
  - a “cooked” number could only target one application
  - chained mode implies even an insider cannot undetectably change a previous output value

Entropy

- Currently using two independent commercial RNGs
- We plan to implement a “verifiable source”. This is a collaborative project between NIST’s Information Technology and Physical Measurement laboratories.

Verifiable quantum randomness source



Output uncorrelated with anything outside the apparatus.

The bigger picture

- We view this as a type of “trust anchor” for the Internet
  - something that is hard to subvert for gain
  - a primitive that can be leveraged for many purposes
- We hope it will encourage other such “anchors”
  - e.g. bulletin boards, “after time x” timestamps…
  - my favorite one: a service that certifies that (0,0) is not among a set of bit commitments.

Summary

- We are enabling “verifiably random” sampling
- The Beacon can simplify existing digital interactions and enable new ones
- We hope people will find innovative ways of using it
- We are working to develop the best randomness source in the world
- Project page at http://www.nist.gov/itl/csd/ct/nist_beacon.cfm

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

THE NIST RANDOMNESS BEACON