CMUF Entropy Working Group

Lisa Rabe
Global Certifications Team
Cisco Systems, Inc.

Agenda

History of the Entropy Working Group

EWG Membership

Value of the EWG

EWG Accomplishments

Topics and Presentations

Future Topics

History

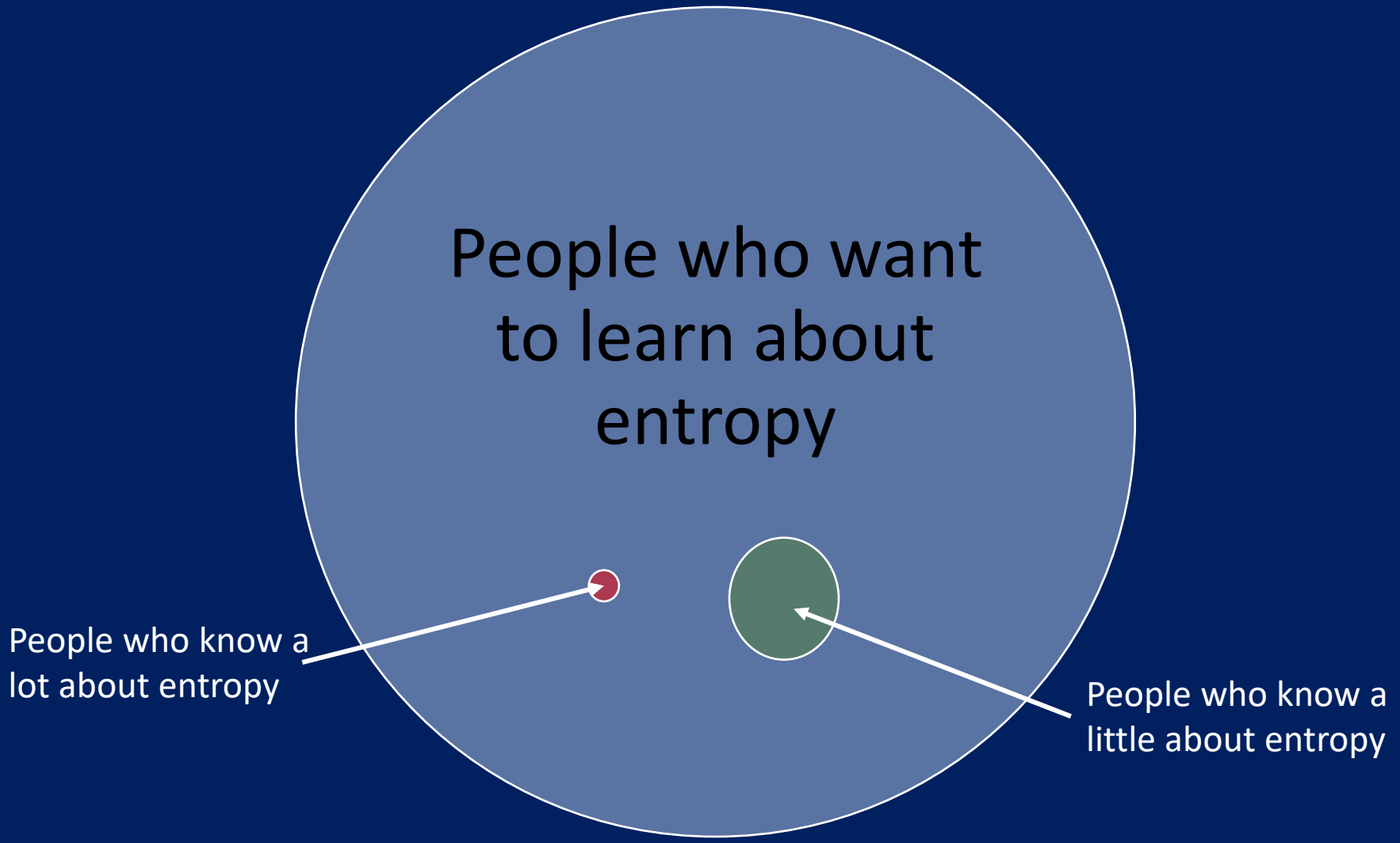
Nov 7, 2018 – first meeting of the Entropy Working Group (EWG)

10 attendees

Topics:

- Difficulties of gathering restart data
- Intel entropy
- Reuse of entropy certs
- Raw entropy testing (will NIST really insist on it?)

Who Joins the EWG?



EWG Membership

Current EWG:

- 155 members
- 50-70 people on each call

Strength of the group lies in its diverse membership:

- Vendors
- Labs
- HW RNG designers
- Non-physical entropy source designers
- NIST:
  - CMVP
  - CAVP
  - 90 series authors
  - ESV experts
- BSI

NIST Participation

NIST's participation in the group was critical. That gave the group the ability to:

- Ask questions and get answers
- Push back on things that didn't make sense
- Provide NIST with different points of view
- Discuss issues before they became policy

What Happens in the EWG Meetings?

EWG members:

- Ask questions
- Share experiences/difficulties/challenges
- Point out problems
- Start discussions
- Give presentations
- Learn

Value of the EWG to NIST

The EWG:

- Provides valuable feedback to NIST in the form of comments on draft documents and IGs
- Gives NIST insight to practical aspects of entropy source design and usage
- Increases knowledge of participants, which (ideally) increases the quality of the entropy reports

Value of the EWG to the Members

The EWG:

- Gives us access to industry experts
- Allows us to ask questions in an informal setting
- Gives us advance notice of things the CMVP is thinking
- Allows us to push back early on things that are problematic
- Most importantly, it gives us a chance to learn about entropy in a comfortable, casual setting

Benefits Reaped by EWG Members

- Opportunity to learn about potential entropy sources:
  - ❖Intel RDRAND/RDSEED
  - ❖CPU Jitter – Basis of at least 1/3 of the ESVs
  - ❖LRNG – Linux RNG – kernel patch to make the Linux PRNG compliant with 90B
- Early access to Intel entropy reports and test data
- Early access to draft documents
- Ability to contribute comments to draft documents that will have the weight of the whole group behind them
- Access to notes and/or recordings from previous 4.5 years

EWG Accomplishments

- IG 7.19 (now D.K) –
  - ❖started in August 2019
  - ❖published 13 months later
- Comments on IG 7.18, SP 800-90B, SP 800-90C, Shall Statement Matrix
- EAR Template
- PUD Template

Making a Difference

- DRBG chaining

  "For the chains of DRBGs, several people pointed out that getting rid of these will cause a huge problem. We got it wrong. We're going to figure out how to allow these in different contexts. Clearly, we have to allow chains of DRBGs. A bunch of stuff breaks if we don't have it, so we'll add that back."

- Reuse of entropy reports
- Chains of conditioning components
- NIST SP 800-90B test suite

Frequent or Ongoing Discussion Topics

- CPU Jitter
- Linux entropy
- Health tests
- NIST SP 800-90B Test Suite
- Discrepancies between 90A, 90B and 90C
- EAR and PUD
- Adding OEs to an ESV cert
- Public vs private ESV certs

Presentations

- Intel DRNG
- CPU Jitter
- LRNG (Linux RNG)
- Ring Oscillators
- Linux PRNG and how it relates to 90B and 90C
- Health tests (particularly vendor-defined health tests)
- RISC V Entropy Source
- SP 800-90C (discussions on multiple drafts)
- Entropy Estimation
- Entropy Extractors
- HB 150-15 Annex H
- Common Entropy Report Pitfalls

Joshua Hill, DJ Johnston, Stephan Mueller, John Kelsey, and others

Interesting Discussions

- Full entropy definition
- Linux PRNG – validity apart from compliance
- DRBGs as conditioning components
- Common failure modes of different types of entropy sources
- Entropy expertise in the labs
- Multiple entropy sources for redundancy
- Ring oscillator entropy sources

Future Topics

- DRBG chaining
- 90 A/B/C refinements
- Entropy and PQ crypto
- Stochastic modeling

Please join!

NIST has specifically asked us to try to increase our membership because they value our contribution. If you want to have a voice in the entropy community, please join us!

Email:
Lisa Rabe (lirabe@cisco.com) and
Trish Wolff (trwolff@cisco.com)