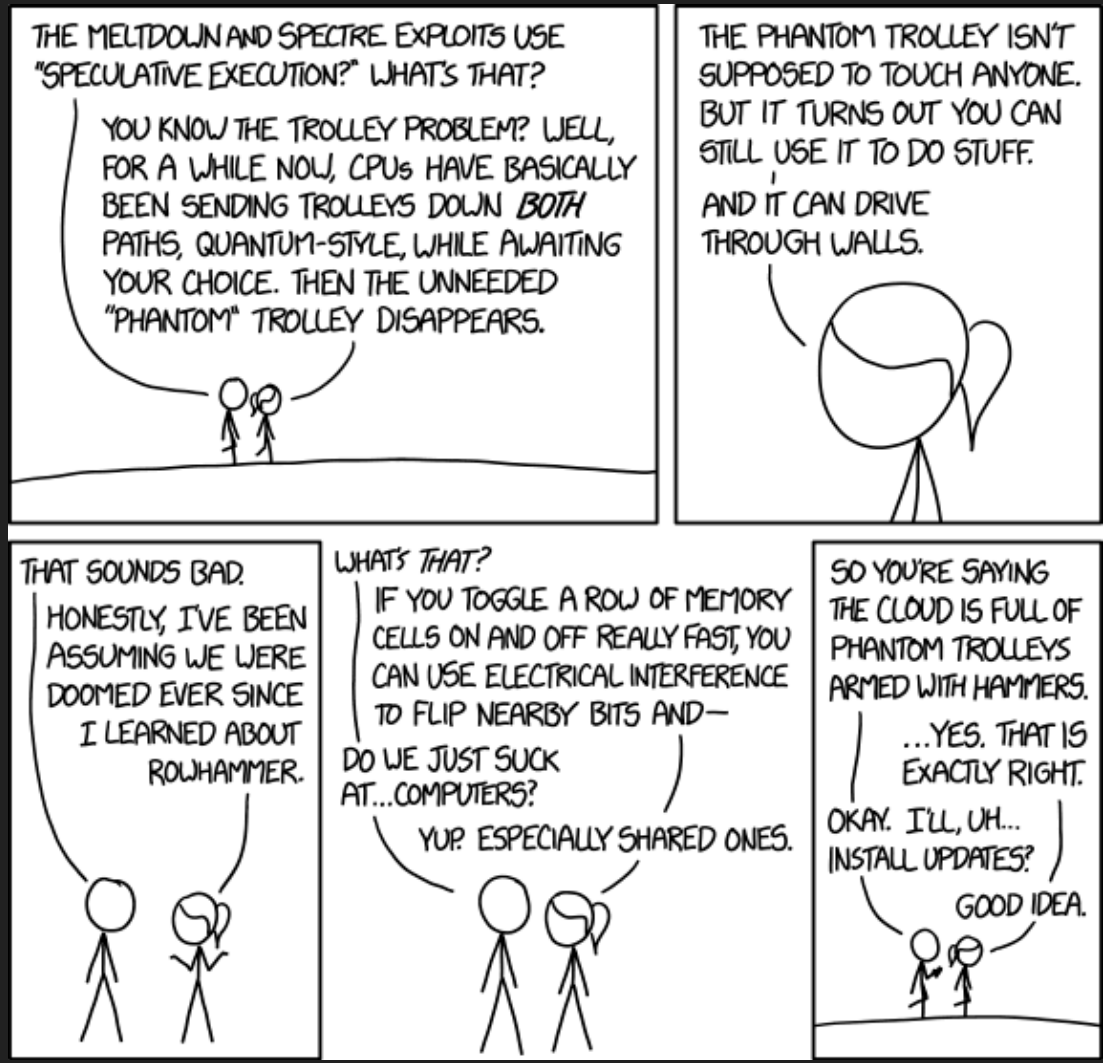
# Beyond the Password

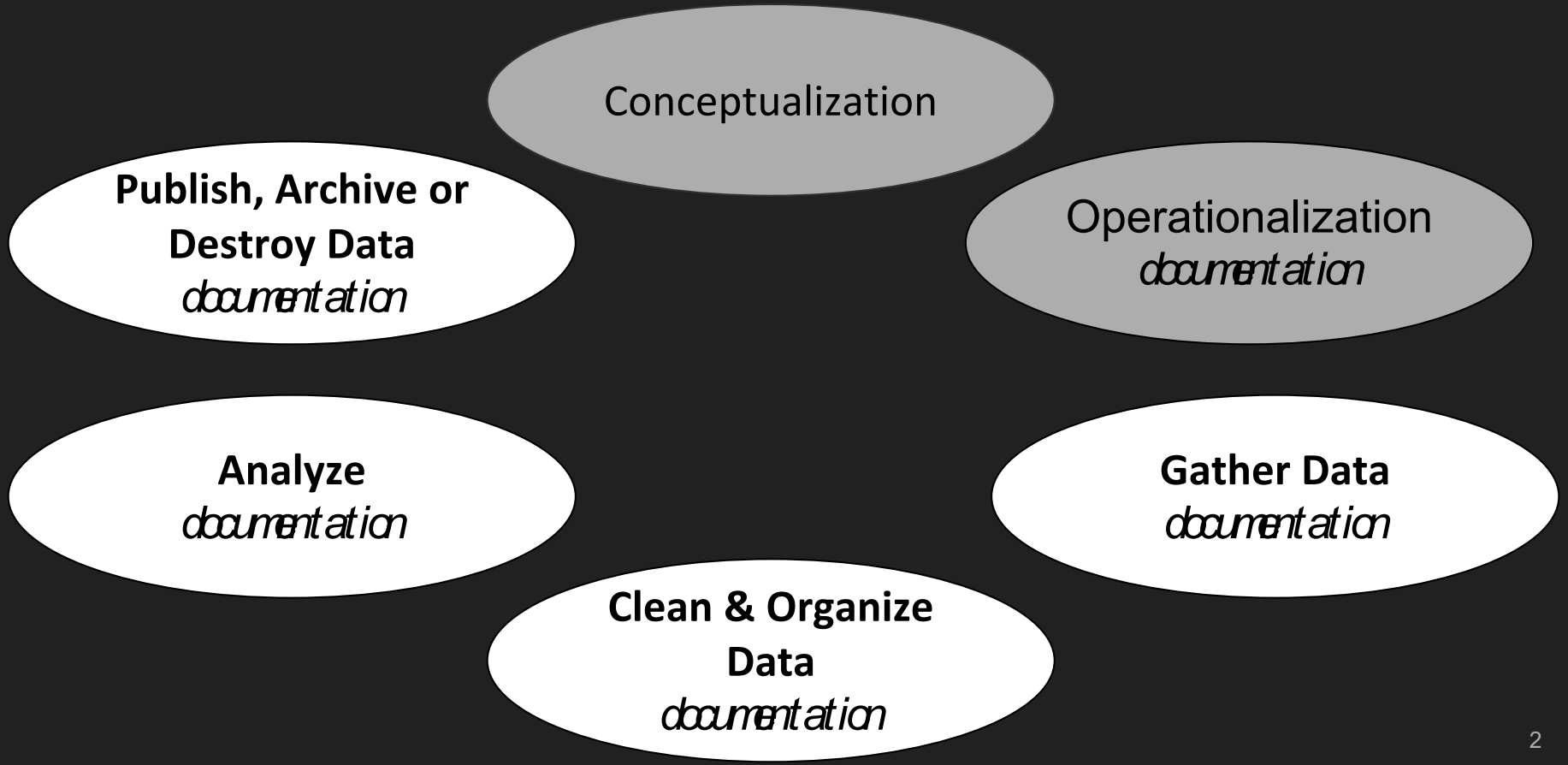
## *Getting Real About Data Security*

*By Kim Smith & Paula Lackie for the Carleton College community. Last revised 3/8/2018*

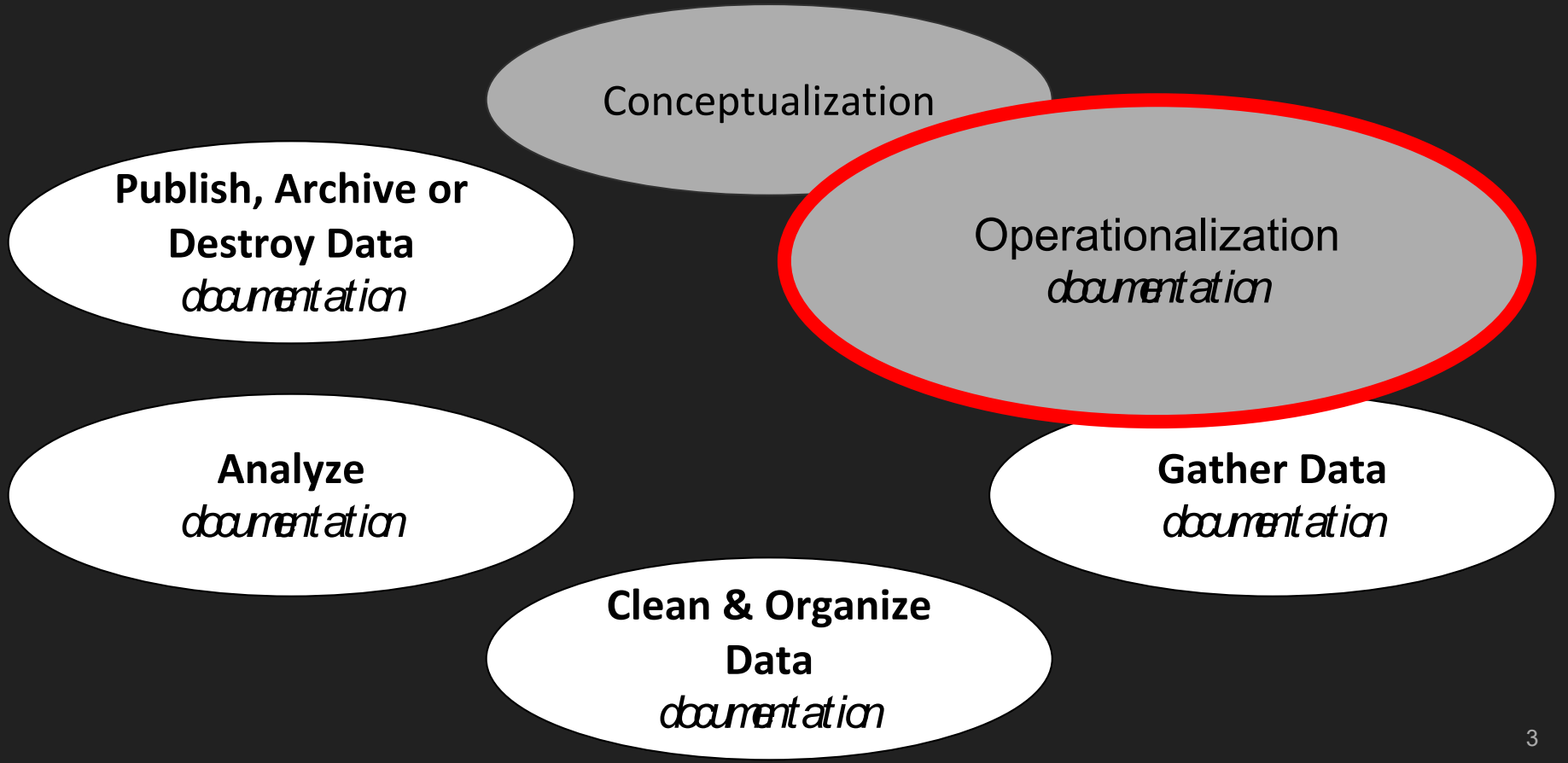



https://xkcd.com/1938/

# A Research Data Lifecycle



# A Research Data Lifecycle



# Threats & Vulnerabilities

- major threats
  - Accidental “publication”
  - phishing
- sources of vulnerability
  - Evildoers
  - You
  - Your team
  - Border Control

# Solution: A Data Plan!

## A Data Plan should address:

- Where you're keeping data
- How many copies and where they are
- How you share data (with your team)
- How you're going to update data
- What happens to data after you're through

# Basic Protection

1. Which information (data) am I collecting?
2. Which devices will have access to the information/data?
    a. Where am I & team members storing all of the related information/data?
    b. Who has access to those devices?  How am I making them secure?
3. Will I be sharing my data?  If so, how?
4. Will I be archiving my data (and metadata)?  If so, where, how, and for how long?
5. When and how will you destroy your data?

# Higher protection: for sensitive data

What additional strategies would you use to increase security?

Enc

- Encryption
- Clear protocols for separating working data from original / not de-identified data
- VPN (Traveling?)

# Highest protection: *super-sensitive*

- Enclaves
- Talk to us...

# Sensitive secondary data

- Problems:
  - Allegedly de-identified data may not really be de-identified

- Solutions:
  - Look at all the variables!
  - Aggregate the data
  - Treat it all as identifiable data

# A Research Data Lifecycle