Safe Analysis of Long-Term DNS Data

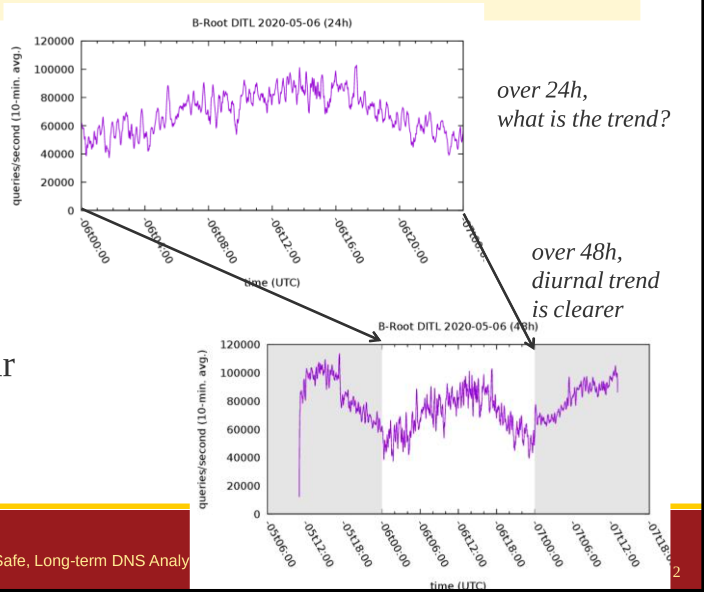
John Heidemann and Wes Hardarker

USC/ Information Sciences Institute

2020-07-22

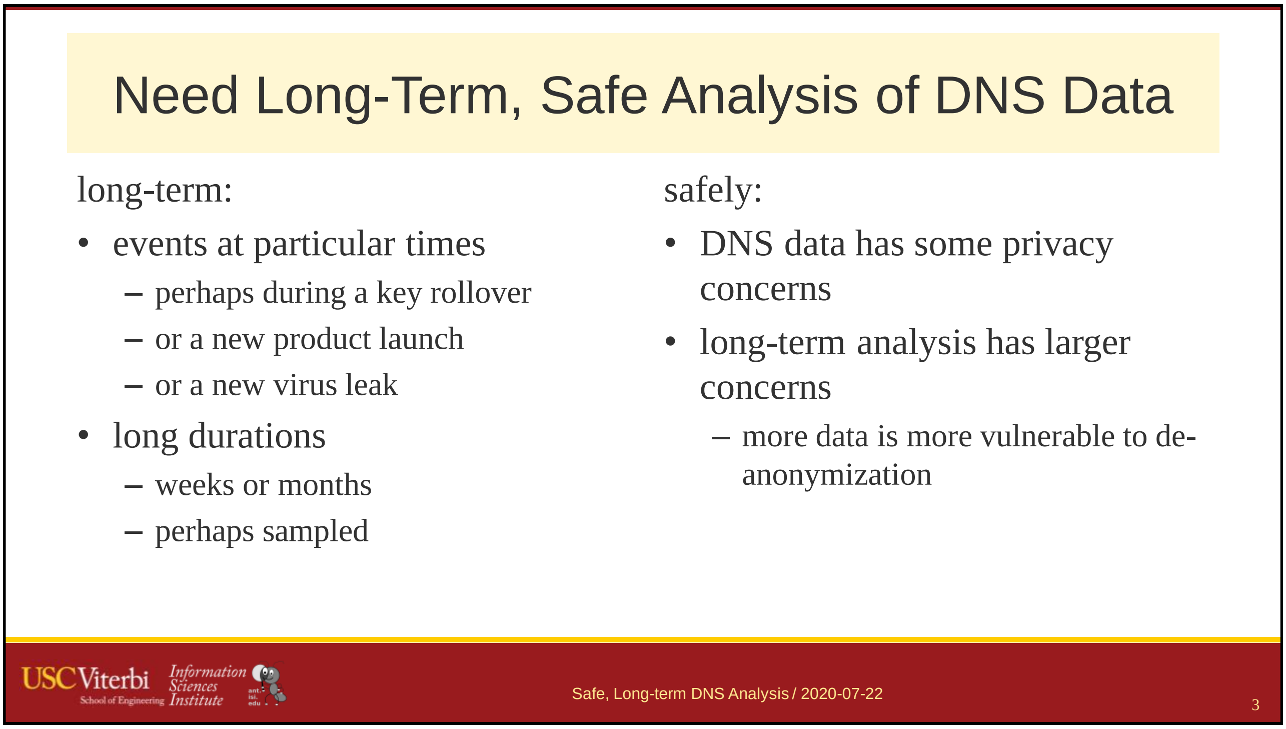
What’s Happening in DNS?

- let’s look at the data!
- we can use DITL (at right)
- sometimes 1 day is insufficient
  - trends
  - rare events
- sometimes you need a particular day



over 24h, what is the trend?

over 48h, diurnal trend is clearer



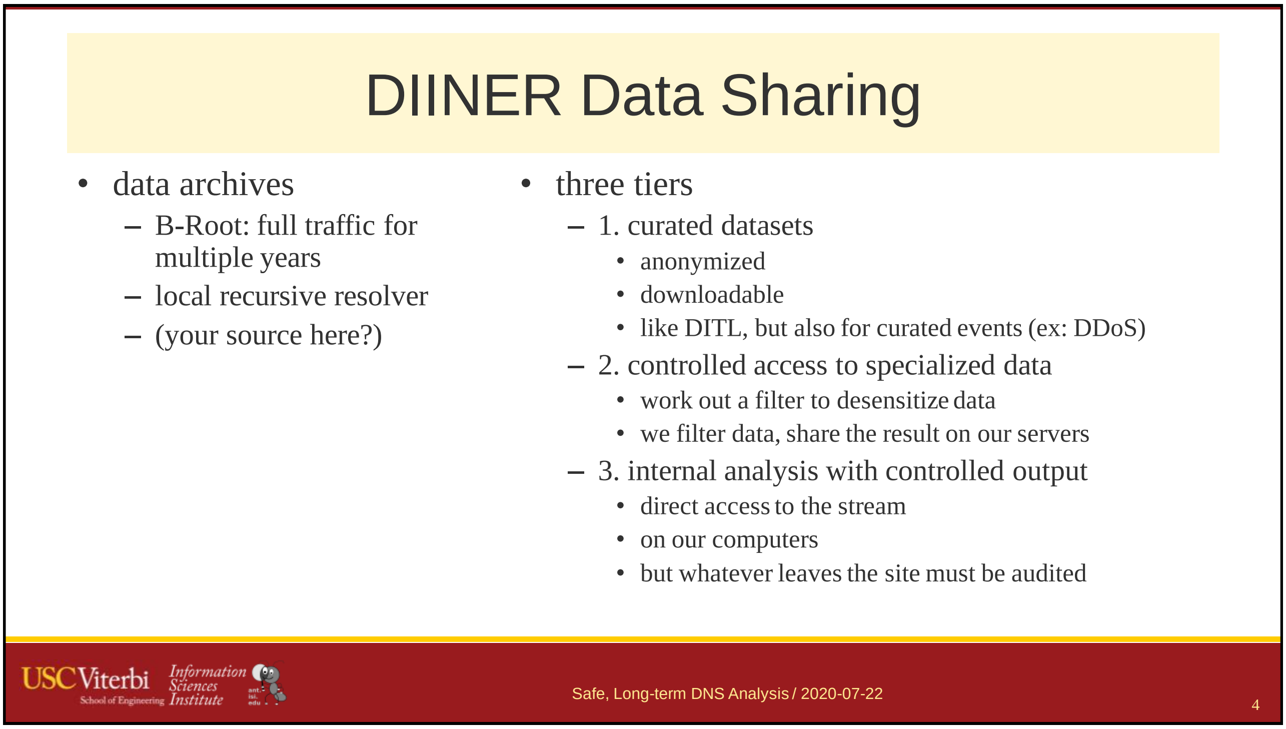
Need Long-Term, Safe Analysis of DNS Data

long-term:

- events at particular times
  - perhaps during a key rollover
  - or a new product launch
  - or a new virus leak
- long durations
  - weeks or months
  - perhaps sampled

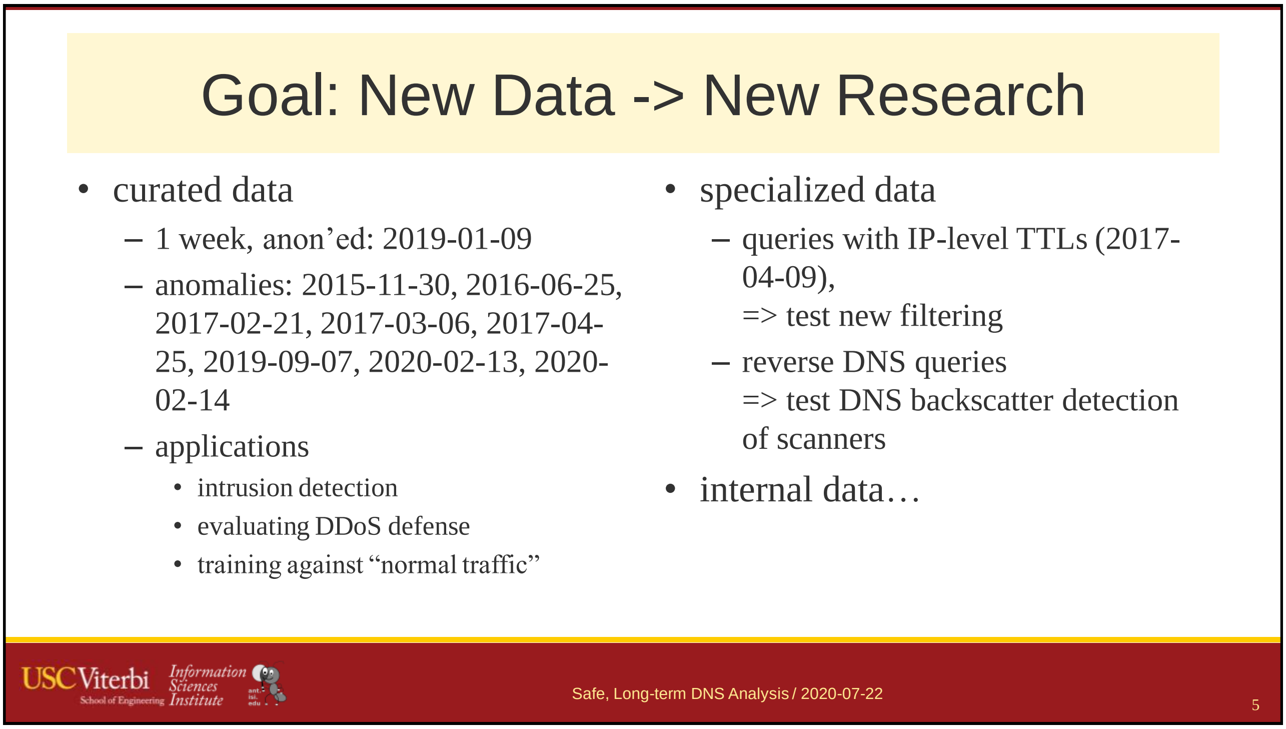
safely:

- DNS data has some privacy concerns
- long-term analysis has larger concerns
  - more data is more vulnerable to de-anonymization



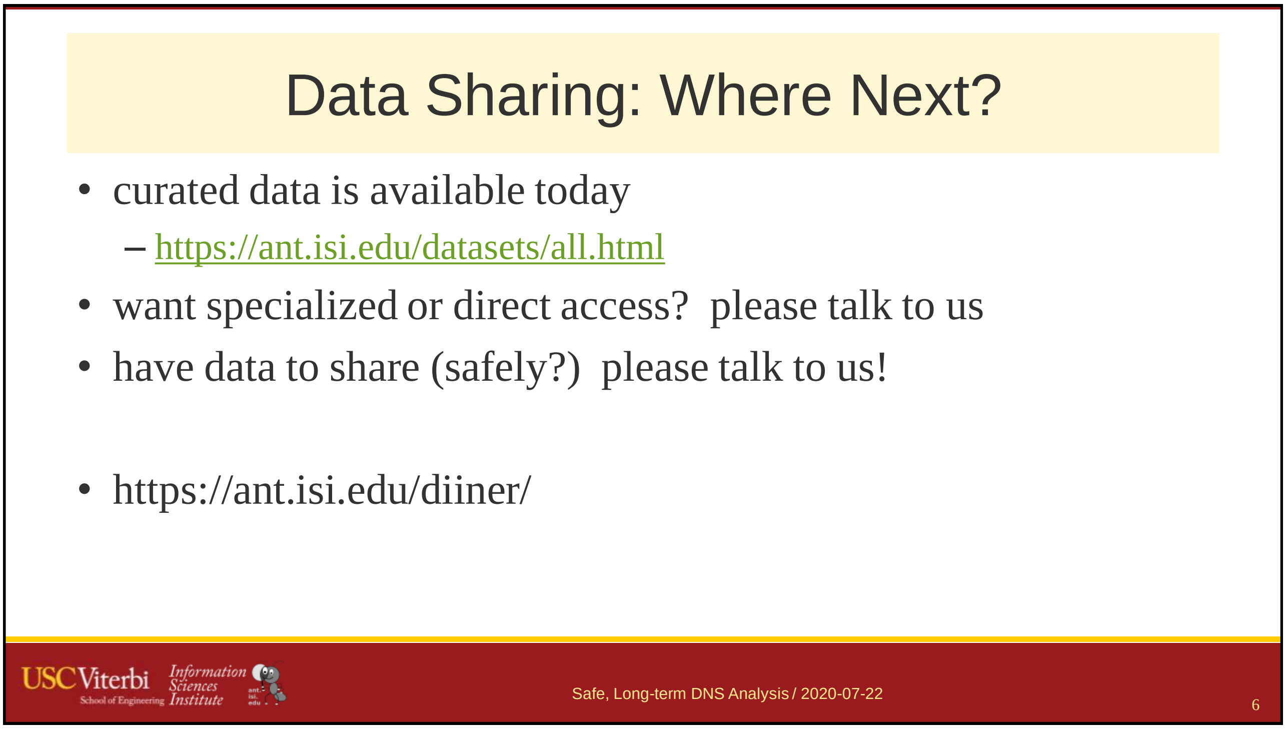
DIINER Data Sharing

- data archives
  - B-Root: full traffic for multiple years
  - local recursive resolver
  - (your source here?)
- three tiers
  - 1. curated datasets
    - anonymized
    - downloadable
    - like DITL, but also for curated events (ex: DDoS)
  - 2. controlled access to specialized data
    - work out a filter to desensitize data
    - we filter data, share the result on our servers
  - 3. internal analysis with controlled output
    - direct access to the stream
    - on our computers
    - but whatever leaves the site must be audited



Goal: New Data -> New Research

- curated data
  - 1 week, anon’ed: 2019-01-09
  - anomalies: 2015-11-30, 2016-06-25, 2017-02-21, 2017-03-06, 2017-04-25, 2019-09-07, 2020-02-13, 2020-02-14
  - applications
    - intrusion detection
    - evaluating DDoS defense
    - training against “normal traffic”
- specialized data
  - queries with IP-level TTLs (2017-04-09),
    => test new filtering
  - reverse DNS queries
    => test DNS backscatter detection of scanners
- internal data…



Data Sharing: Where Next?

- curated data is available today
  - https://ant.isi.edu/datasets/all.html
- want specialized or direct access? please talk to us
- have data to share (safely?) please talk to us!

- https://ant.isi.edu/diiner/