Measuring the Loss of Privacy from Statistics

Michael Carl Tschantz
Carnegie Mellon University
Pittsburgh, PA, USA

Aditya V. Nori
Microsoft Research India
Bangalore, India
Meat
Meat
Meat
What does the average “179” tell us about Blue’s weight?
What does the list “165, 233, 138” tell us about Blue’s weight?
Adversary

• An adversary attempts to learn private info
  – What is Blue’s weight?

• Has some prior beliefs
  – About 130

• Updates them based on statistic
  – An average of 179?! People weigh more than I thought
Goal

• Given program that computes statistics about a list of survey responses, characterize how much information the statistic provides about what an adversary is attempting to learn
Formal Model

• Program is a random variable \texttt{STAT} from survey responses to a statistic
• \texttt{STAT} takes on the actual value of \texttt{stat} based on the actual survey responses
• What the adversary would like to know is the value of a random variable \texttt{ADV}
• The adversary has prior beliefs \texttt{P} about the value that \texttt{ADV} takes on
Problem Statement

• Given
  – **STAT** program that computes statistics
  – **stat** the value the statistic takes on
  – **ADV** what the adversary wants to know
  – **P** an adversary's prior beliefs

• Compute the distribution for **ADV** under **P** given **STAT=stat** and compare to **ADV** under **P**
  
  \[ P(ADV \mid STAT=stat) \text{ vs. } P(ADV) \]
Measures of Change

• From the two distributions $P(\text{ADV})$ and $P(\text{ADV} \mid \text{STAT}=\text{stat})$ one can calculate:
  – Mutual information (change in entropy)
    $H(\text{ADV}) - H(\text{ADV} \mid \text{STAT}=\text{stat})$
  – Change in Kullback–Leibler divergence
    $\text{Dist}(\text{ADV, adv}) - \text{Dist}(\text{ADV} \mid \text{STAT}=\text{stat, adv})$
  – your favorite measure of distribution difference...
Adversary's Beliefs?

• Normally unknown
• From survey, we have an estimation of the actual probability distribution that produced the samples
• Use that in place of adversary’s beliefs to model an adversary that knows this distribution
Problem Statement

• Given
  – $\text{STAT}$ program that computes statistics
  – $\text{stat}$ the value the statistic takes on
  – $\text{ADV}$ what the adversary wants to know
  – $P$ an estimation of the underlying distribution

• Compute the distribution for $\text{ADV}$ under $P$ given $\text{STAT}=\text{stat}$ and compare to $\text{ADV}$ under $P$
  
  $P(\text{ADV} \mid \text{STAT}=\text{stat})$ vs. $P(\text{ADV})$
Approach

- Monte Carlo Simulation
- Sample according to Prior-Beliefs $P$
- See how often $\textsc{STAT}$ takes on the value $\textsc{stat}$ for each value of $\textsc{ADV}$

$P(\textsc{ADV}=\text{adv} \mid \textsc{STAT}=\text{stat})$

$= P(\textsc{AVD}=\text{adv} \& \textsc{STAT}=\text{stat}) / P(\textsc{STAT}=\text{stat})$

$\approx #(\textsc{AVD}=\text{adv} \& \textsc{STAT}=\text{stat}) / #(\textsc{STAT}=\text{stat})$
Performance

- The more samples, the more accurate
- Time linear in the number of samples and the amount of time STAT takes
- Memory linear in the range of ADV and memory usage of STAT
Convergence for Parity of $X_1$

- $H(\text{Adv}) - H(\text{Adv} | \text{Stat} = \text{stat}) = 1 \approx 0.999999797$
## Comparison of Mutual Information

| Statistic | H(Adv) – H(Adv | Stat=stat) | Time (min) |
|-----------|----------------|------------|
| Parity    | 0.9999999      | 10.65      |
| Mean      | 0.012523       | 11.4       |
| Median    | 0.002059       | 24.97      |
| Mode      | 0.037691       | 40.73      |
Related Work: Analyses for Mutual Information

- Mutual information is not always enough
Related Work:
Analyses for Mutual Information

• Clark, Hunt, Malacaria – Static analysis
• McCamant and Ernst – Dynamic analysis
• Not exact enough (stove = meat grinder)

• Newsome and Song – Dynamic analysis
• Would be accurate enough with a theorem prover that finds all solutions to a logical formula
Related Work

Clarkson, Myers, Schneider

- Theory using adversary’s beliefs
- No implementation
- Could be implemented using our work given adversary’s beliefs
Related Work: Differential Privacy

- Dwork et al.
- Adds noise to protect privacy
- Does not distinguish between deterministic programs (stove = meat grinder)
Future Work

• Doesn’t work for really large sample spaces
• Doesn’t work if STAT is slow
• Modeling prior knowledge P is hard
• What to use for ADV
Questions?

• Implementation:
  http://www.cs.cmu.edu/~mtschant/mcqif/
Mean varying Survey Size

![Graph showing the mean varying survey size with different survey sizes (n=4, n=16, n=64, n=256, n=1024) on a log2 scale. The graph plots the number of bits against the exponent of the number of samples. The curves illustrate how the mean varies with different survey sizes.]
Related Work: Mutual Information

- D. Clark, S. Hunt, P. Malacaria
- Mutual info: $H(\text{ADV}) - H(\text{ADV} \mid \text{STAT=}\text{stat})$
- Static system for measuring mutual info from single point to output
  - Not exact enough (stove = meat grinder)
  - Not always complete picture
Change in Beliefs

• M. R. Clarkson, A. C. Myers, F. B. Schneider
• $\text{Dist}(\text{ADV, adv}) - \text{Dist}(\text{ADV} | \text{STAT} = \text{stat, adv})$
  – Relative entropy
• Also not complete picture
• No implementation
Channel Capacity

- Newsome and Song
- Converts single execution trace of program to a logical formula
- Use theorem prover to find all solutions
  - Can only provide lower bound in practice
- Bounds information flow for that trace for any input distribution
  - We use a fixed input distribution