Quantitative Information Flow Measurement

Project full title: TWC: Small: Confidentiality Measurement of Complex Computations
using Quantitative Information Flow

University of Minnesota
Driven to Discover℠

Challenge:

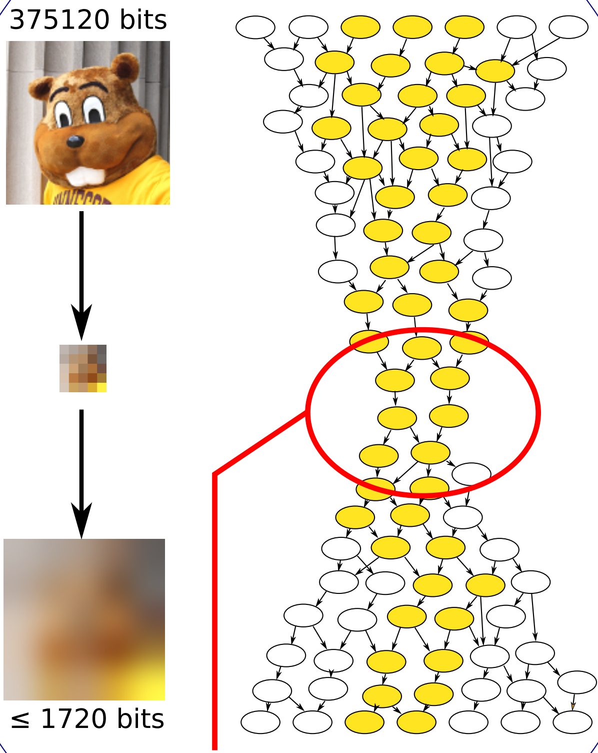
- Overall goal: measure how much sensitive information is present in the output of a computation
- *Precision*: avoid over- or under-estimation, for accurate security/privacy decisions
- *Scalability*: efficiently get results from large and complex software, for widest applicability

Solution:

- Statistical adaptive algorithms: query-efficient control for model counting
- Hybrid with capacity-based bounds: use faster analysis to focus use of more expensive model counting

Award no. 1526319
PI: Stephen McCamant

Maximum flow through data-flow graph bounds the information a computation reveals



375120 bits

≤ 1720 bits

Bottleneck determines maximum flow and is the best target for more detailed analysis

Scientific Impact:

- Faster #SAT model counting and first bit-vector + floating-point model counting
- Most scalable quantitative information-flow measurement for binary executables

Broader Impact:

- Provide an independent assessment of purported privacy protections
- Feeding back tool fixes and improvements to open-source tool developers