# Quantitative Information Flow Measurement

PI: Stephen McCamant, University of Minnesota
http://www.cs.umn.edu/~mccamant/flowcheck/

RAs: Seonmo Kim, Navid Emamdoost

## Combining capacity analysis and model counting

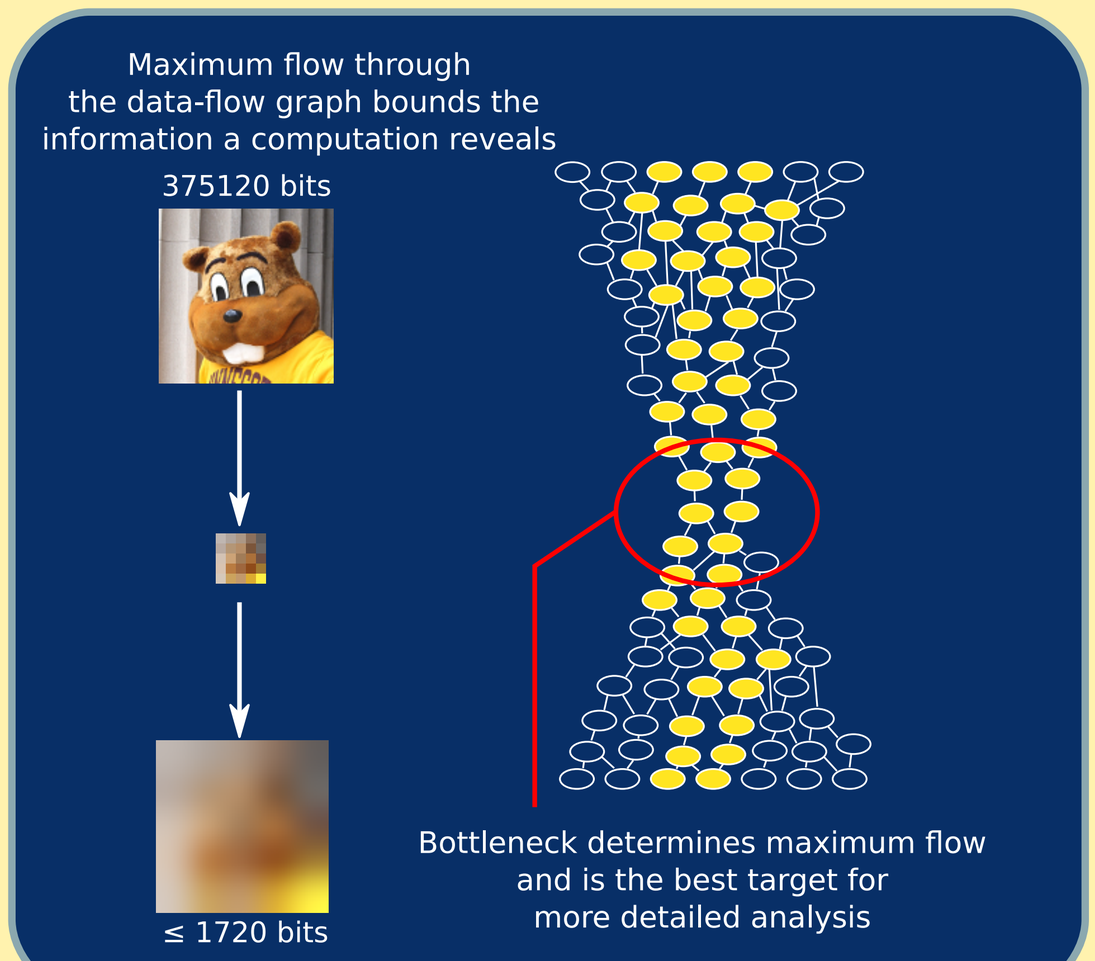
The objective of this project is to develop tools that can precisely measure the information revealed by computations on sensitive inputs.

- The presence of secret information in program output may not be directly visible

- Isolation (e.g., enclaves) or cryptographic protection still must reveal a computation's result

For a discrete, noiseless process like a program execution, the *channel capacity* is equal to the base-2 logarithm of the number of distinguishable outputs.

This is a useful definition to build on for security analysis because it does not require an assumption about a probability distribution.




## Approach

### Capacity analysis

- Build dynamic bit-capacity data flow graph with static annotations for implicit flows

- Compute maximum flow and minimum cut between secret inputs and outputs

### Model Counting

- Model count is the number of satisfying assignments to a formula

- Exact computation is #P-hard, so approximate by using random hashing to reduce the number of solutions

## Capacity analysis tool: Flowcheck

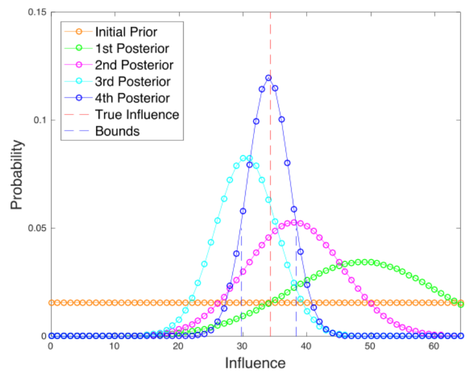
Dynamic data-flow analysis extends Valgrind Memcheck's bit-level undefined value tracking

Enclosure region annotations provide a static bound on the locations modified in implicit flows

New version compatible with recent Linux distributions

http://www.cs.umn.edu/~mccamant/flowcheck/

## Model counting tool: SeachMC




Uses a statistical model to adaptively choose queries

Implemented for CNF and bit-vector/floating point SMT

Exploring integration with CryptoMiniSAT

https://github.com/seonmokim/SearchMC/

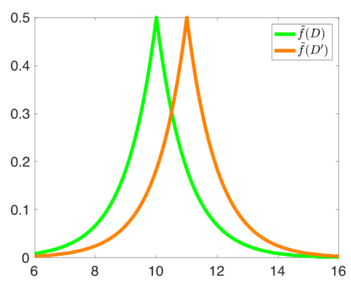
## Integration with FuzzBALL

- Minimum cut and memory/register taint identify a region for more detailed analysis
- Binary control-flow analysis (DynInst) determines a single-exit region
- Binary symbolic execution with FuzzBALL converts each execution path into an SMT formula for model counting

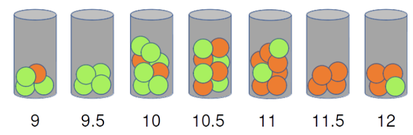
https://github.com/bitblaze-fuzzball/fuzzball

## Model counting and differential privacy

Continuous ideal:




Discrete reality:




Floating point model counting confirms severity of Mironov (CCS 2012) attack

Interested in meeting the PI? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

University of Minnesota
Driven to Discover℠