Other challenges

- **Taint through operations**
  - `tainted a; untainted b; c=a+b` — is `c` tainted? (yes, probably)
- **Function pointers**
  - What function can this call go to?
  - Can flow analysis to compute possible targets
- **Struct fields**
  - Track the taintedness of the whole struct, or each field?
  - Taintedness for each struct instance, or shared among all of them (or something in between)?
    - Note: objects ≈ structs + function pointers
- **Arrays**
  - Keep track of taintedness of each array element, or one element representing the whole array?

Refining taint analysis

- Can label *additional* sources and sinks
  - Array bounds accesses: must have untainted index
- Can expand taint analysis to **handle *sanitizers***
  - Functions to convert tainted data to untainted data
- Other application: Leaking confidential data
  - Don't want **secret sources** to go to **public sinks**
    - **Implicit flows more relevant** in this setting
  - *Dual* of tainting

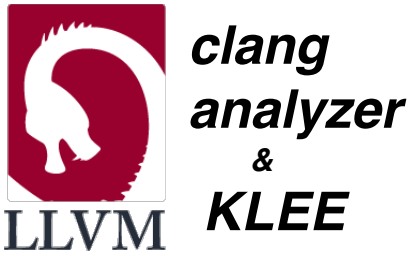
Other kinds of analysis

- **Pointer Analysis** (“points-to” analysis)
  - Determine whether pointers point to the same locations
  - Shares many elements of flow analysis. Really advanced in the last 10 years.
- **Data Flow Analysis**
  - Invented in the early 1970’s. Flow sensitive, tracks “data flow facts” about variables in the program
- **Abstract interpretation**
  - Invented in the late 1970’s as a theoretical foundation for data flow analysis, and static analysis generally.
  - Associated with certain analysis algorithms

Static analysis in practice

Commercial products

Open source tools

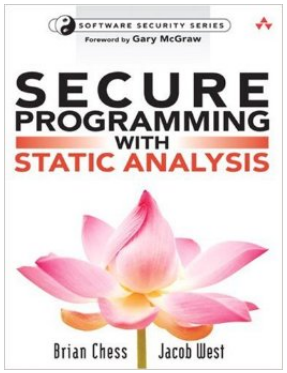


clang analyzer & KLEE

Caveat: appearance in the above list is not an implicit endorsement, and these are only a sample of available offerings

Learning more

- **Secure Programming with Static Analysis**, by Brian Chess, goes into more depth about how static analysis tools work, and can aid secure software development



- **Principles of Program Analysis**, by Nielson, Nielson, and Hankin, is a formal, mathematical presentation of different analysis methods
  - A bit dense for the casual reader, but good for introducing the academic field