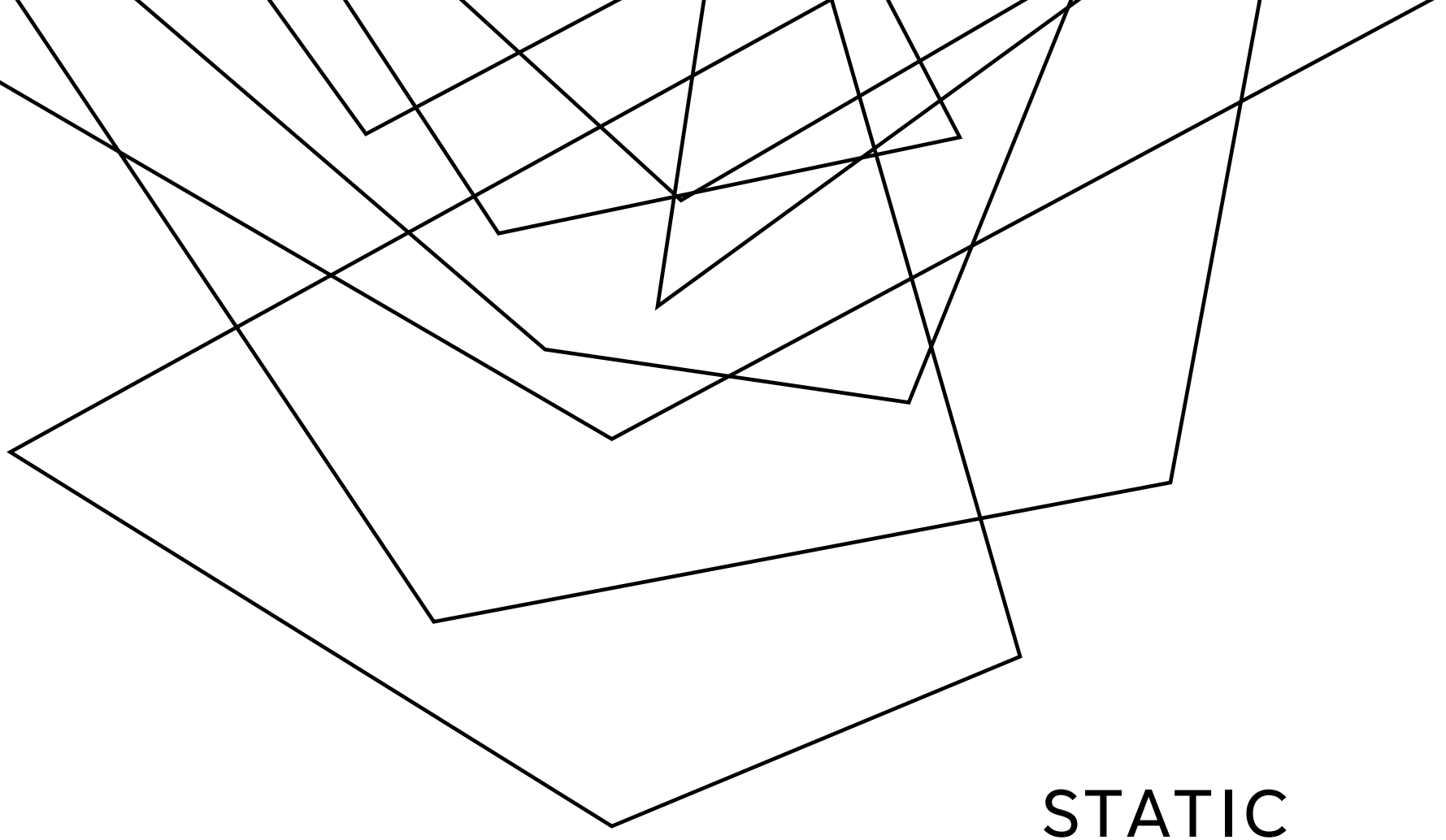
EXERCISE #26

PROGRAM INSTRUMENTATION REVIEW

Write your name and answer the following on a piece of paper

What is the difference between static and dynamic program instrumentation?

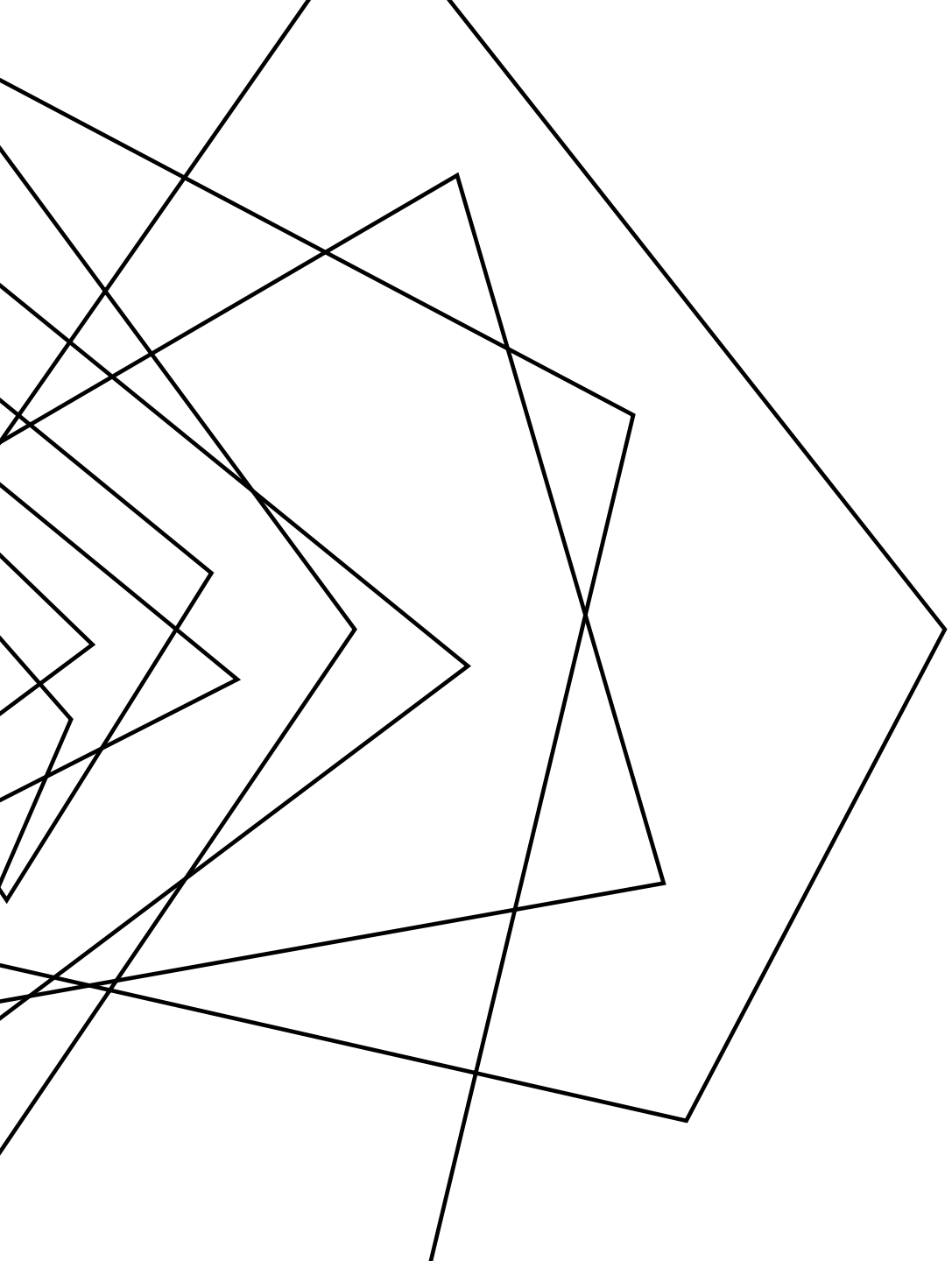
ADMINISTRIVIA AND ANNOUNCEMENTS



STATIC INSTRUMENTATION

EECS 677: Software Security Evaluation

Drew Davidson



WHERE WE’RE AT

EXPLORING PROGRAM INSTRUMENTATION

An approach to dynamic analysis

PREVIOUSLY: PROGRAM INSTRUMENTATION

REVIEW: LAST LECTURE

INSERTING MEASUREMENT PROBES INTO A PROGRAM

NOTABLE ANALYSIS TOOLS

Lint – The original analysis tool
Splint – Security analysis tool

THIS LESSON: STATIC INSTRUMENTATION

REVIEW: LAST LECTURE

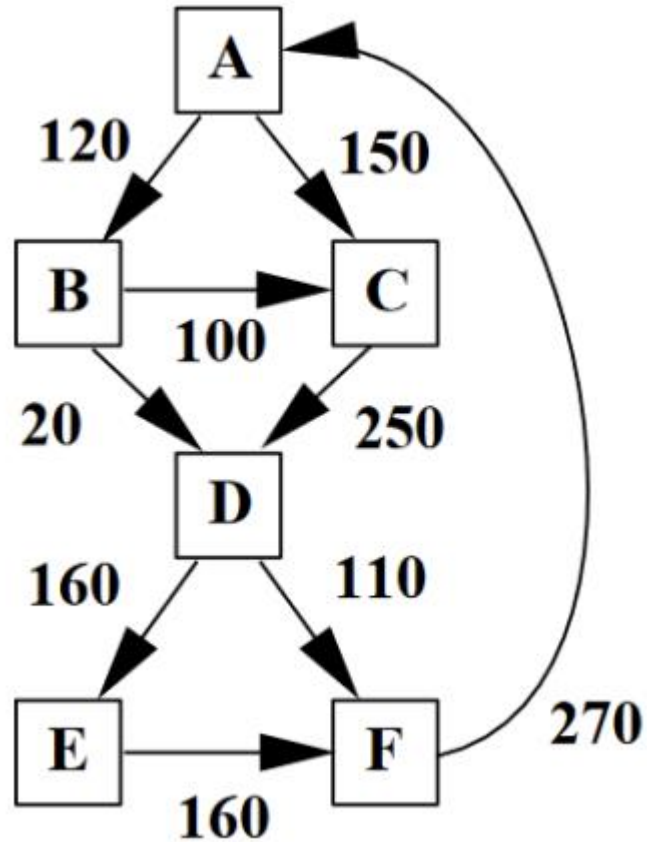
Inserting measurement probes into a program Before it is run

More closely associated with proactive software evaluation – (why?)

PATH FREQUENCY

REVIEW: THE PROBLEM

Path	Prof1	Prof2
ACDF	90	110
ACDEF	60	40
ABCDF	0	0
ABCDEF	100	100
ABDF	20	0
ABDEF	0	20



STATIC INSTRUMENTATION TOOLS

PROGRAM INSTRUMENTATION: APPROACH

Often built right into compiler

LLVM Coverage tools

GCC Coverage tools

Sometimes built upon optimizer

Google's closure compiler

https://github.com/google/closure-compiler

EXAMPLE: LLVM COVERAGE INSTRUMENTATION

PROGRAM INSTRUMENTATION: APPROACH

Big Idea: Inject Basic Block Counters

LLVM Coverage tools

EXAMPLE: LLVM COVERAGE INSTRUMENTATION

PROGRAM INSTRUMENTATION: APPROACH

LET'S TAKE IT TO THE TERMINAL!

CUSTOM INSTRUMENTATION

PROGRAM INSTRUMENTATION: APPROACH

THE PREVIOUS EXAMPLE TOOK ADVANTAGE OF PRE-EXISTING INSTRUMENTATION

What if we wanted to make our own custom instrumentation?

CUSTOM INSTRUMENTATION

PROGRAM INSTRUMENTATION: APPROACH

GETTING STARTED

1) Reference the LLVM API
2) Build our own (trivial) analysis pass
3) Hook into the LLVM opt infrastructure
4) Run our analysis pass

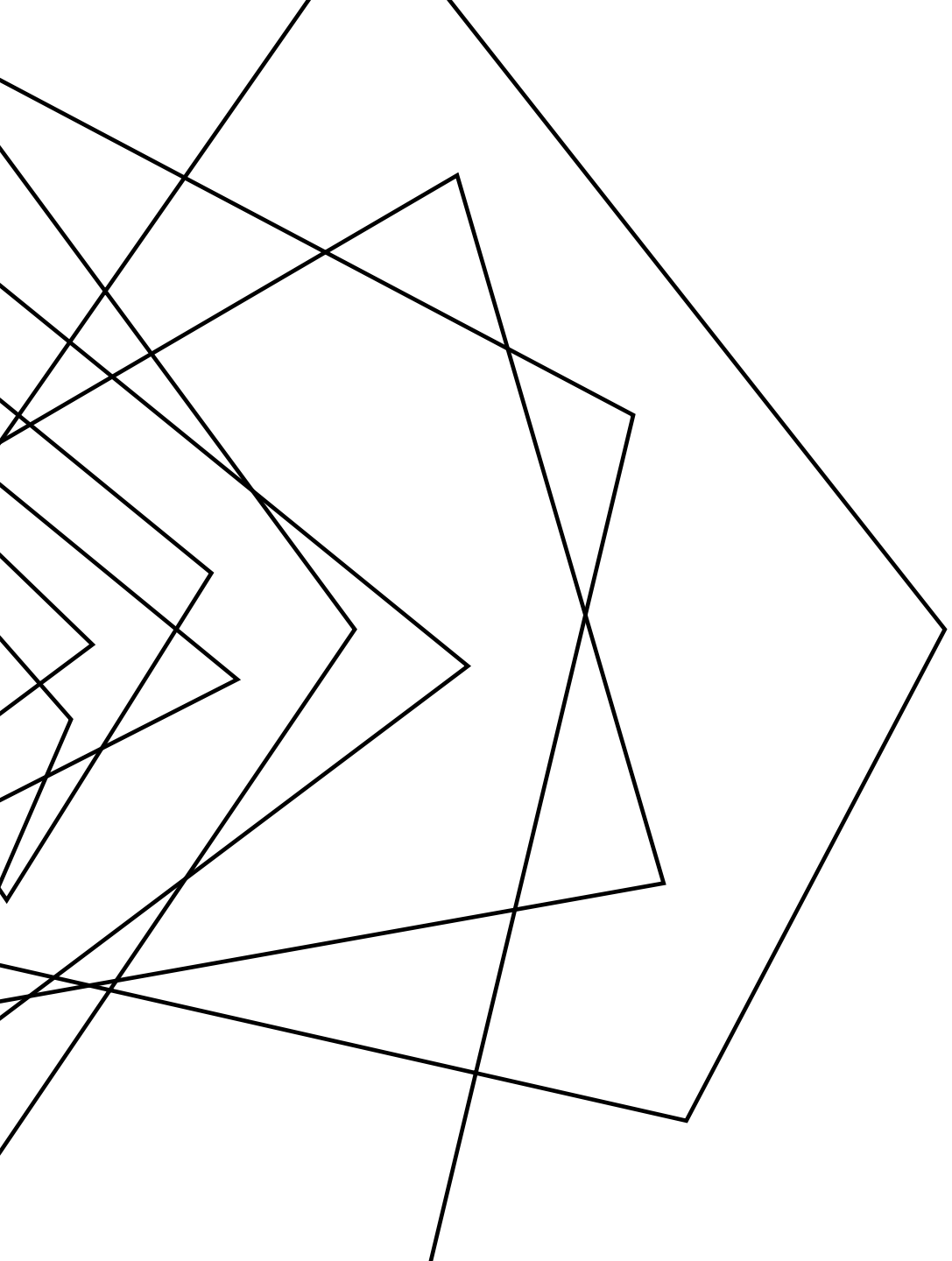
GOING FURTHER

Insert more full-featured functionality
(https://llvm.org/doxygen/classllvm_1_1IRBuilder.html)

TUTORIAL: CUSTOM LLVM INSTRUMENTATION

PROGRAM INSTRUMENTATION: APPROACH

LET'S TAKE IT TO THE TERMINAL!



WRAP-UP

WE'VE DESCRIBED 2 FORMS OF ALTERING THE PROGRAM

More heuristic by nature