# Writing secure software

## Question 1:

In a group:

Look at “DevSecOps” on the Web (e.g. this), and its variants.
Contrast it to what we learned in class (causes for vulnerabilities in software; what’s to blame).
Where does this approach help?
Where does this approach not help?

Bonus: Look at other procedures for introducing security into the software development process, and do a similar analysis & discussion.

# convincing the consumer

Aka. “Where did the trust go?” :-)

## Question 2:

You are a software consumer, interested in purchasing software from AmazingSoft, Inc.

**(A)**
You purchase a piece of software from AmazingSoft, Inc.
You receive a binary.
You run it.
What do you trust?

**(B)**
Consider instead that:
You receive a binary, along with a proof of its correctness.
You verify this proof, before running the binary.
What do you trust now?
What trust moved to where, compared to the initial scenario?

## Question 3:

You are managing a team at AmazingSoft, Inc., that is writing a module with security goals, for a larger software product.

**(A)**
The team writes the module in Java.
(no libraries, etc.)
It compiles.
What do you trust?

**(B)**
The team writes the module in Java.
They use open-source libraries for encryption.
It compiles.
What do you trust now?
What trust moved to where, compared to the initial scenario?

**(C)**
The team writes the module in Paragon.
It compiles.
What do you trust now?
What trust moved to where, compared to the initial scenario?