

Correctness (Safety) vs Security

Safety

Satisfy specifications

“for reasonable inputs,
get reasonable outputs”

Security

Resist attacks

“for **un**reasonable inputs,
get reasonable outputs”

The attacker is an active entity

Correctness (Safety) vs Security

Safety

Satisfy specifications

“for reasonable inputs,
get reasonable outputs”

Security

Resist attacks

“for **un**reasonable inputs,
get reasonable outputs”

The attacker is an active entity

One say that such program/os is more vulnerable

Some are ...	so ...
more deployed than others	more targeted/audited by hackers/researchers
more complex than others	multiple points of failure, larger attack surface
more open to third-party code than others	more “amateur” codes, permissive execution