exploit mitigations

idea: turn vulnerablity to something less bad

e.g. crash instead of machine code execution

many of these targetted at buffer overflows

mitigation agenda

we will look briefly at one mitigation — stack canaries

then look at exploits that don't care about it

then look at more flexible mitigations

then look at more flexible exploits

mitigation priorities

effective? does it actually stop the attacker?

fast? how much does it hurt performance?

generic? does it require a recompile? rewriting software?

backup slides