Data Confidentiality and Integrity

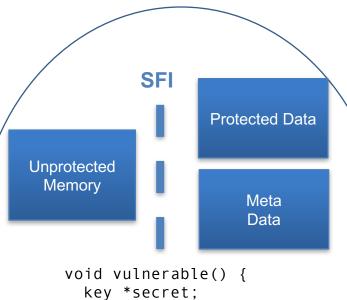


Challenge:

- Applications written in C/C++ are prone to memory corruption
- Existing solutions are incomplete or have high overhead

Solution:

- Key finding: only some data is security critical
- Provide strong integrity and confidentiality for sensitive data, coarse protection for all



```
void vulnerable() {
  key *secret;
  int cmd[5];
  secret = load_key();
  input(cmd); //
vulnerability
}
```

Scientific Impact:

- Selective security
 policies allow tunable
 trade-off between
 performance and
 security
- Improve security of legacy and new C/C++ code

Broader Impact:

- DCI protect the integrity and confidentiality of people's system
- DCI is easy to use in practice: compiled software is protected
- DCI is being taught as part of a new software security course

PI: Mathias Payer (Purdue University), http://hexhive.github.io CNS-1464155 CRII: SaTC: Lockdown: Guarded Control-Flow and Data Privacy for Sensitive Data