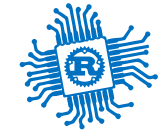

Secure Execution

Lecture 10

Secure Execution

- Security Model
  - Secure
  - Non Secure
  - Non Secure Callable
- ARM TrustZone
- RP2350 Secure
- Software

Memory Types

Type	Symbol	Description
Secure	**S**	Can be accessed only by code running in **secure mode**
NonSecure Callable	**NSC**	code running in **non-secure mode** can make function calls into it with some restrictions
NonSecure	**NS**	any code running in **any mode** can access it

Security Attribution Unit