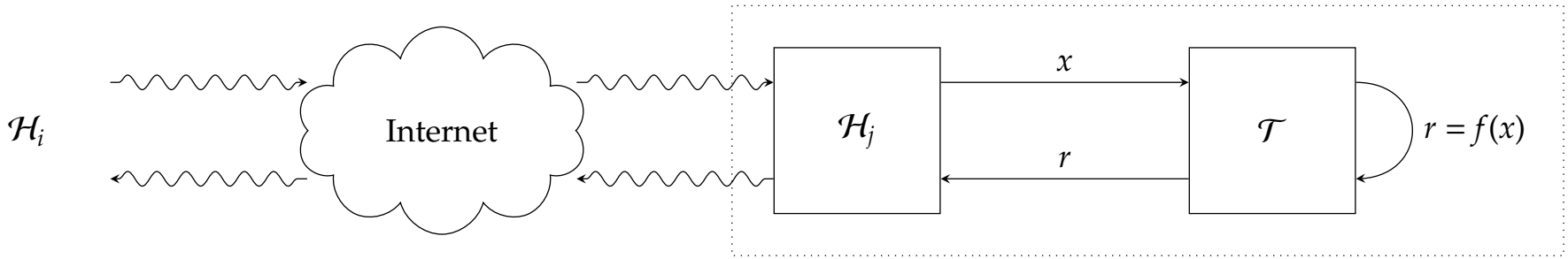
COMS30048 lecture: week #13

- Agenda: a somewhat technical introduction to the coursework assignment, i.e.,
  - overview of the assignment motivation and content,
  - answer any FAQs,
  - answer any non-FAQs,

  with the overarching goal of clarity, and enabling early progress.

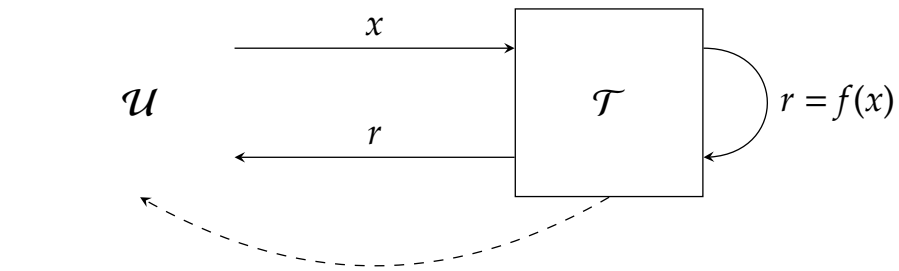
- Scenario (more abstract):



i.e.,

- there's a host $\mathcal{H}_j$ connected to the Internet,
- $\mathcal{H}_j$ uses TLS to communicate with, e.g., $\mathcal{H}_i$,
- $\mathcal{H}_j$ uses a co-processor $\mathcal{T}$ to support TLS-related functionality.

- Scenario (less abstract):

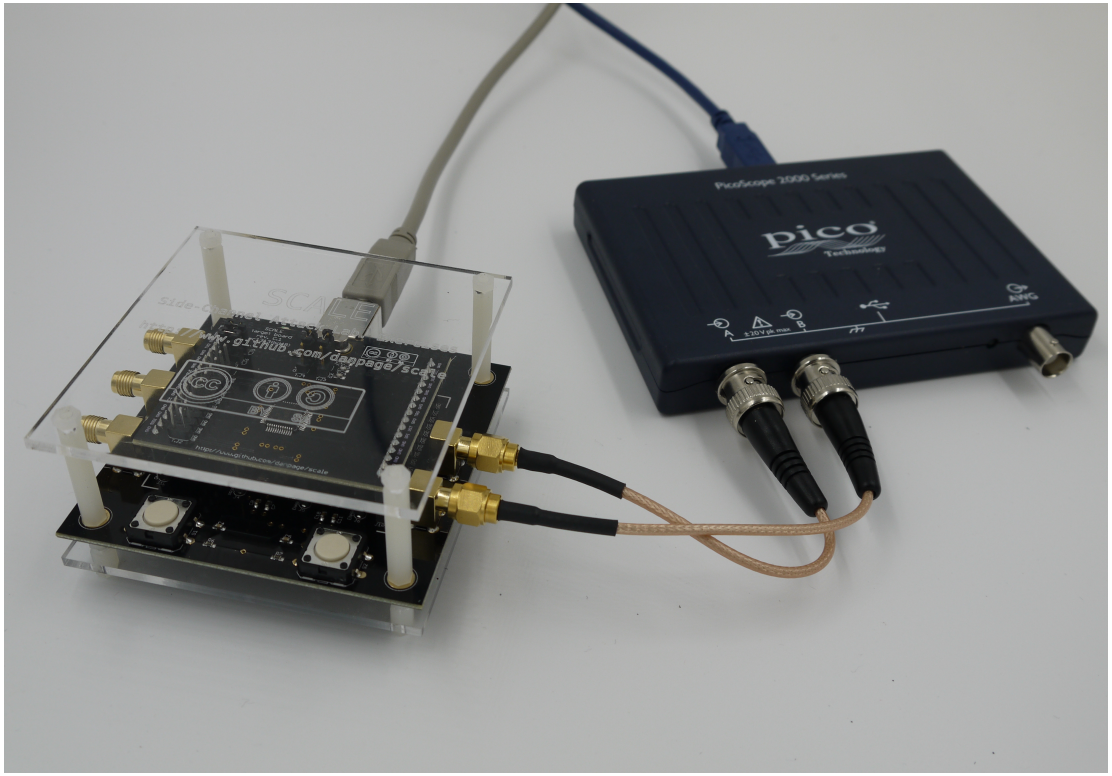


i.e.,

- there's a user $\mathcal{U}$ with physical access to $\mathcal{T}$,
- $\mathcal{U}$ can monitor
  - execution latency,
  - power consumption,
  - ...

  stemming from or during execution of f.

- Scenario (concrete):



such that

$$\mathcal{T} \simeq \text{Cortex-M3 development board} \Rightarrow \text{lab. worksheet \#1.1}$$
$$\mathcal{U} \simeq \text{workstation + oscilloscope} \Rightarrow \text{lab. worksheet \#1.2}$$

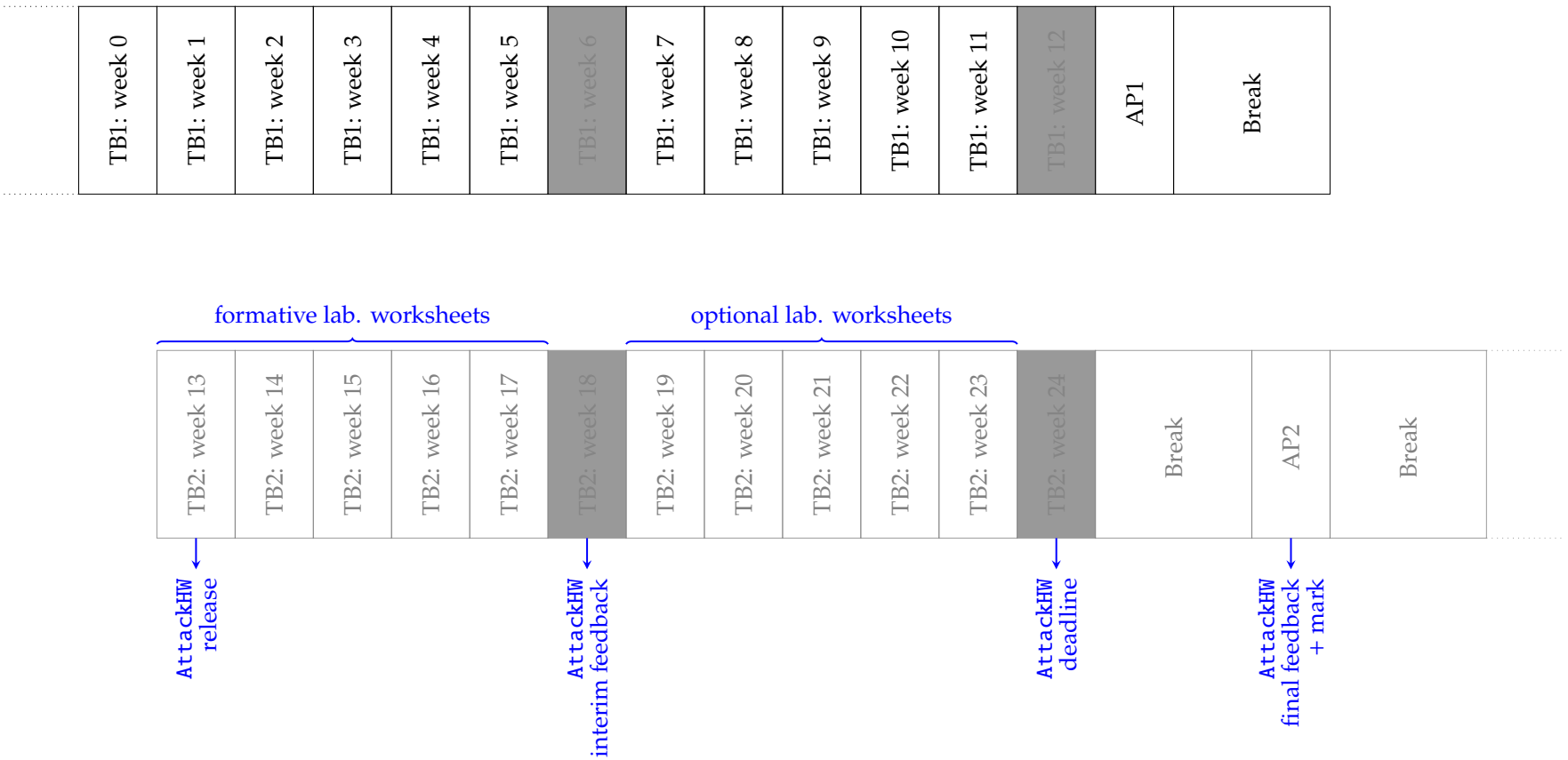
- Structure:

stage 1	$\Rightarrow$	implement a primitive	(i.e., AES)
stage 2	$\Rightarrow$	implement an attack	(against stage 1)
stage 3	$\Rightarrow$	design and implement a countermeasure	(against stage 2)
stage 4	$\Rightarrow$	design support for a protocol	(i.e., TLS)

so, roughly speaking, address challenges around realisation of $\mathcal{T}$.

- Question: "*when* should I start; *when* should I invest effort"?

- Question: "*when* should I start; *when* should I invest effort"?
- Answer: basically,



and so *could* start ≃ week 13, whereas *should* start ≃ week 18.

- Question: "*how* should I start; *how* should I invest effort"?

- Question: "*how* should I start; *how* should I invest effort"?
- Answer: basically,
  - attempt to complete relevant lab. worksheet(s),
  - work step-by-step through stages, e.g.,
    1. invest in understanding problem and, e.g., tools, workflow, etc.,
    2. produce an on-paper solution,
    3. implement the solution,
    4. test the implementation.
  - note that said stages are only *somewhat* dependent, e.g.,

$$\text{stage 1} \not\rightsquigarrow \text{stage 2}$$

in the sense that you *could* make progress via the download'able data set.

- Question: “how will my submission be marked”?

- Question: "how will my submission be marked"?
- Answer: manually (although tool-assisted in some cases), noting that the marksheet details
  - for 1., a per-stage break down of marks, and
  - for 2., a non-exhaustive set of quality metrics (e.g., style, efficiency, robustness, generality, etc.).

- Question: “I’m concerned about academic integrity, and, e.g., plagiarism”?!

- Question: "I'm concerned about academic integrity, and, e.g., plagiarism"?!
- Answer:
  1. an accessible overview can be found at

     https://www.bristol.ac.uk/students/support/academic-advice/academic-integrity
  2. the more detailed policy can be found, e.g., via Sec. 3 of

     https://www.bristol.ac.uk/academic-quality/assessment/codeonline.html
  3. we do apply (semi-)automatic tools to identify potential transgression.

- Question: is the equipment available outside the lab. slots?

- Question: is the equipment available outside the lab. slots?
- (Short) Answer: no.

- Question: is the equipment available outside the lab. slots?

- (Long) Answer: no, but it's important to understand this policy is
  1. by design, motivated by a need to e.g., control your workload,
  2. carefully calibrated based on evidence from previous years,
  3. carefully mitigated by the assignment design:
     - can work on stage 1 independently then "port" to equipment,
     - can work on stage 2 independently using example data set,
     - can work on stage 4 independently since no implementation is involved,
     - ...

- Question: how does the assignment differ between COMS30049 and COMSM0054?

- Question: how does the assignment differ between COMS30049 and COMSM0054?
- Answer: the *tasks* are the same, but their *assessment* differs in that

COMS30049	$\mapsto$	more emphasis on earlier, implementation-focused stages
COMSM0054	$\mapsto$	more emphasis on later, analysis-focused stages

as detailed by marksheet.

Conclusions (1)

- Take away points: the assignment is designed to (ideally) balance

1. short-term challenge:

intellectual	:	demands *thinking* versus simply *doing*
technical	:	stresses formative understanding of some concepts, resources, etc.
definitional	:	some aspects are partially defined, or go beyond taught content
logistical	:	demands effective planning and time management
	⋮	

2. long-term outcome:

rewarding	:	simulate (limited) experience of *real* versus explanatory task
useful	:	hands-on vehicle for exploring (and understanding) taught content
	⋮	

in the sense that the former aren't negative, *provided* the latter are true.

Questions?

References