Applied Cryptology

Daniel Page

Department of Computer Science,
University Of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB. UK.
⟨csdsp@bristol.ac.uk⟩

September 5, 2025

Keep in mind there are *two* PDFs available (of which this is the latter):

1. a PDF of examinable material used as lecture slides, and
2. a PDF of non-examinable, extra material:
   - the associated notes page may be pre-populated with extra, written explaination of material covered in lecture(s), plus
   - anything with a "grey'ed out" header/footer represents extra material which is useful and/or interesting but out of scope (and hence not covered).

Notes:

Notes:

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,

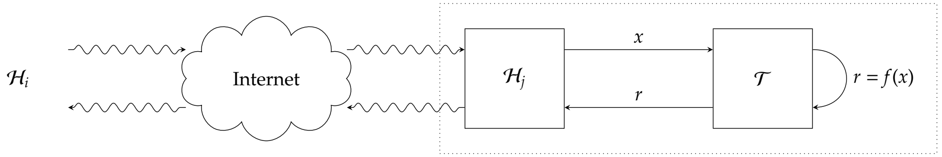
  with the overarching goal of clarity, and enabling early progress.

Notes:

AttackHW (1)

Overview

- Scenario (more abstract):



i.e.,

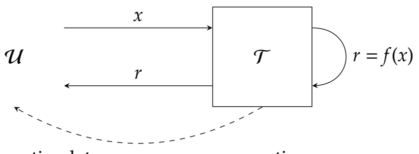
- there's a host $\mathcal{H}_j$ connected to the Internet,
- $\mathcal{H}_j$ uses TLS to communicate with, e.g., $\mathcal{H}_i$,
- $\mathcal{H}_j$ uses a co-processor $\mathcal{T}$ to support TLS-related functionality.

Notes:

AttackHW (2)

Overview

- Scenario (less abstract):



$\Lambda \models$ execution latency, power consumption, ...

i.e.,

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

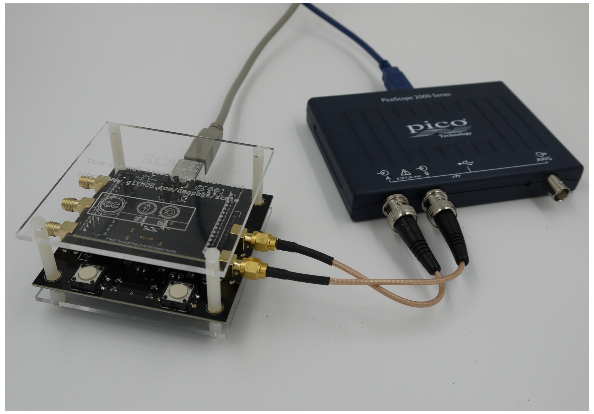
  stemming from or during execution of f.

Notes:

AttackHW (3)

Overview

- Scenario (concrete):



such that

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

Notes:

- Structure:

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

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

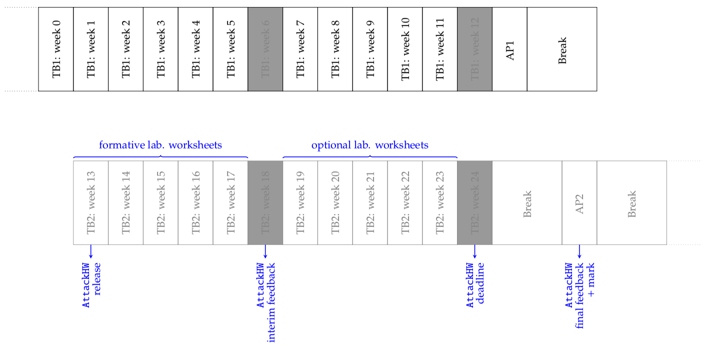
Notes:

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

Notes:

AttackHW (5)
FAQs

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



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

Notes:

AttackHW (6)
FAQs

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

Notes:

`AttackHW` (6)

FAQs

- 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.

Notes:

`Encrypt` (7)

FAQs

- Question: "how will my submission be marked"?

Notes:

Encrypt (7)

FAQs

- 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.).

Notes:

AttackHW (8)

FAQs

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

Notes:

AttackHW (8)

FAQs

- 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.

Notes:

AttackHW (9)

FAQs

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

Notes:

AttackHW (9)

FAQs

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

Notes:

AttackHW (9)

FAQs

- 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,
     - ...

Notes:

AttackHW (10)

FAQs

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

Notes:

AttackHW (10)

FAQs

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

COMS30049	↦	more emphasis on	earlier,	implementation-focused stages
COMSM0054	↦	more emphasis on	later,	analysis-focused stages

as detailed by marksheet.

Notes:

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.

Notes:

Conclusions (2)

Questions?

Notes:

References

Notes: