Lecture 13

Wednesday, 29 March 2023 13:29

Side and covert channels

information does not necessarily leak through communication channel

side channels allow information leakage through unintended channel

physical

outside main information channel

a covert channel is a side channel which is controlled for one's own purposes

From Side to Covert channels

- In a Side Channel, you do not have control over the acquired information
- You act as a passive party, simply acquiring information and using it to extract valuable knowledge
- When someone can have control over a side channel, and use it, this become a Covert Channel
- Covert channels can be used both for benign and malicious purposes
  - ○Exfiltrating information
  - ○Communicating despite the adversary
  - ○Communicating with other devices

examples

defensive

possibly intended channel

offensive

i.e. difficult to control/unintended channels

electromagnetic emanations

wireless RF channels

network traffic packet size, packet frequency

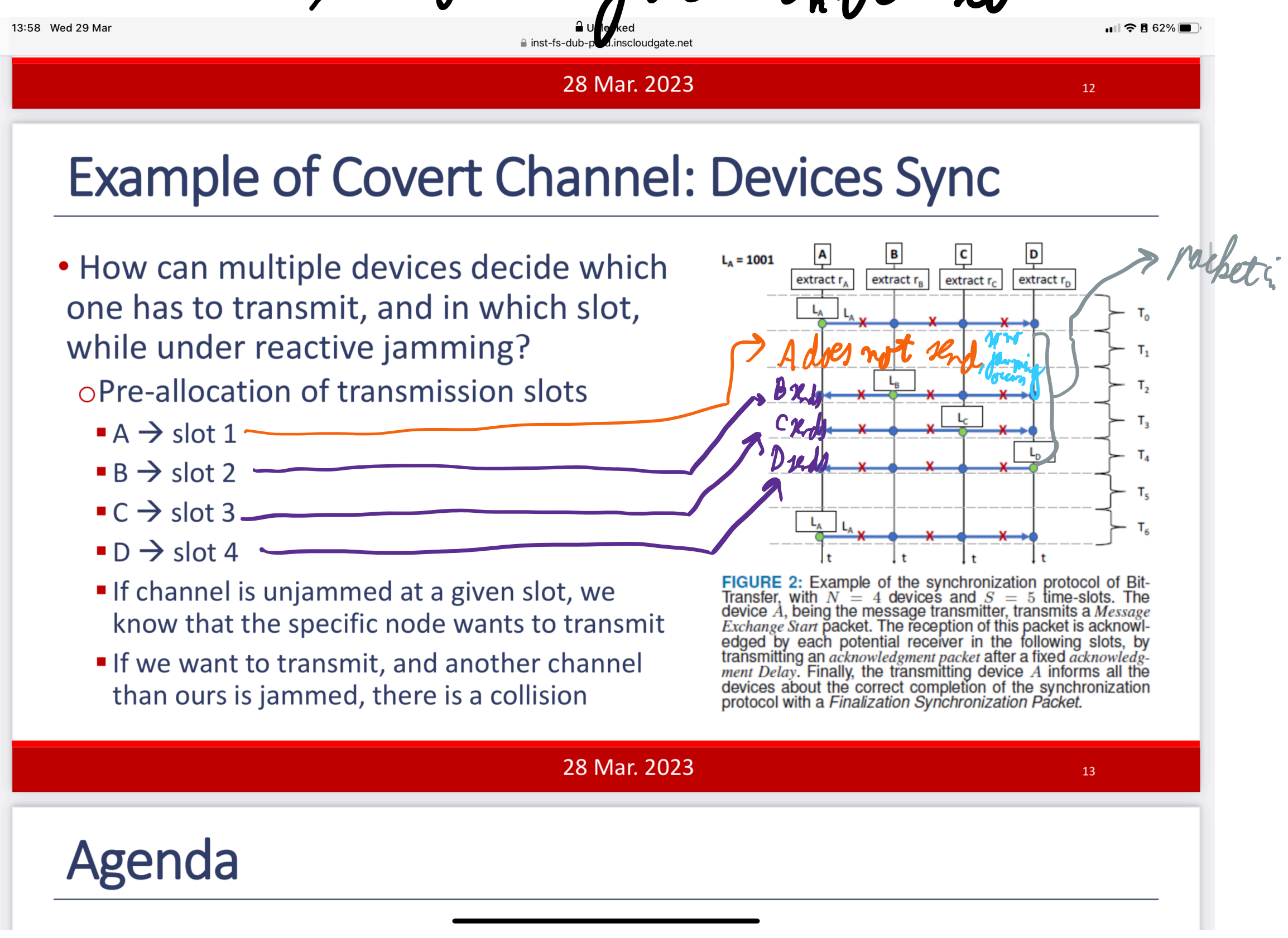
vibrations

acoustic emanations

Anti-jamming solution (silence/send) = covert channel

from jamming lecture

to agree on time-slots, the following idea can be used



13:58 Wed 29 Mar

Unlocked

inst-fs-dub-prod.inscloudgate.net

62%

28 Mar. 2023 12

Example of Covert Channel: Devices Sync

- How can multiple devices decide which one has to transmit, and in which slot, while under reactive jamming?
  - ○Pre-allocation of transmission slots
    - A → slot 1
    - B → slot 2
    - C → slot 3
    - D → slot 4
    - If channel is unjammed at a given slot, we know that the specific node wants to transmit
    - If we want to transmit, and another channel than ours is jammed, there is a collision

FIGURE 2: Example of the synchronization protocol of Bit-Transfer, with $N = 4$ devices and $S = 5$ time-slots. The device A, being the message transmitter, transmits a *Message Exchange Start* packet. The reception of this packet is acknowledged by each potential receiver in the following slots, by transmitting an *acknowledgment packet* after a fixed *acknowledgment Delay*. Finally, the transmitting device A informs all the devices about the correct completion of the synchronization protocol with a *Finalization Synchronization Packet*.

packets T_0 come from A

28 Mar. 2023 13

Agenda

wireless keyboards are event-driven devices, which may leak inter-keystroke timing information

it can even be done with acoustic information from e.g. a skype call

possible final exam (oral) question: how to prevent (USB) fingerprinting in given context