In computing, time is not important.

However in security, we pay a lot of attention to time

* E.g brute forcing.
* Claims about knowing things are time-based

Ransomware

* Infected systems around the world using 0days.
* Infecting unpatched old Windows systems.
* MS released a patch soon after the 0days were published.
* <10% of people applied the patch.
* The Ransomware used the 0day to spread itself on a local network, not only through phishing and other means

The Effect of Time on Knowledge

* My prediction
* The Sting
* TOCTOU
* Forward Secrecy
* Brute Forcing

Incidence Response

* In an exam, we can be asked about a random real-world scenario / event.
* Talk about:
  + What have we learnt from this
  + If I was the Head of Security / Head of IT when the Ransomware begun to break out, what would I have done?
* What would we have done
  + RECOMMENDATIONS:
    - Patch all your system / making sure.
    - Telling your staff / education your staff about not to open suspicious links / download suspicious files.
    - Backing up your files.
* Other people’s recommendations
  + Disconnect all your cables / networks and backup your files.
  + Don’t tell staff to open attachments (not a very strong recommendation because people would still end up opening files nevertheless and if just one person opened the file, the entire system could be infected)
  + Assess your own systems to see if you’re vulnerable or not.
    - How do you know you are vulnerable?
  + Have a ransomware fund.
    - Set aside some money every year for paying off ransomware.
* Problems with some solutions:
  + PATCHING: You might not know that even the recent patches may fix the issue. You may end up having to change everything.
  + SMASH EVERYTHING: Attacks are happening all the time. You can’t smash your router everytime an attack happens. You need to have a more logical response.
* With the benefit of hindset, you can do things a lot differently
  + In retrospect, when you know the consequences, you would always know the right solution to a situation.
  + When you’re doing incidence response, you don’t know what the right response would be
* Having a measured response
  + If you break the fire-alarm glass, would you save lives?
  + Or if you break the fire-alarm glass, would you just annoy your boss and cause a nuisance as it costs a lot of money to replace?
  + What is the right move?
  + You have to think about a measured action to take and the consequences of that action.
* So many companies have cut links with old manual systems
  + This can be bad, because if new systems break then there would be nothing to work off. Your entire system would be frozen.
  + Example: Pizza Hut, if your networks go down, how do people order anymore? Assume phone ordering isn’t a thing anymore. So you would be losing millions of dollars while your networks are done because people can’t order anything and there are no apps to help track your orders / deliveries etc.

Time of an attack

* If you were a bad person and you wanted to attack an organisation, the best time to attack would be:
  + Friday afternoon, News Years eve, Public Holidays etc.
  + People’s attention levels would change depending on the timing.
  + They don’t pick a time when everyone is relaxed and waiting
  + If a company is moving their offices from A 🡪 B, that is a good time to attack.
  + **A good attacker will NOT attack when the victim is prepared.**
* How do you know that something is true?
  + A lot of governments etc. don’t like to spread information that they don’t like.
  + E.g. Tiananmen Square
  + How do we sort out what is true and what is not?
  + **The Authentication Problem**
  + When we look back in history books, how do we figure out what is the truth or not?
* **Time of Check Time of Use Errors (TOCTOU)**
* Wikileaks
  + They encrypt something, then post it online.
  + On the date of release, they release the key.

**Zero-knowledge protocol**

* Lets you prove you know something without letting anyone know that you know it.

Prove that he can break into any house

* I pick a house
* Richard recreates a replica house of that one
* We can to choose if we want to:
  + How to break into the replica house
  + Show us where the real house is