## **Lab 4 Part C**

Q. There are several cryptographic uses for a clock. Key management functions are often linked to deadlines. The current time can provide both a unique value and a complete ordering of events. Install either network time protocol (NTP) or precision time protocol (PTP) in your computer and check if it is working. List and give examples of attacks that can be mounted against a system with a clock. You may wish to read the following book chapter and a paper. Write at most four paragraphs and upload the report in Webcourses.

A. There are a few ways to mount attacks on a system with a clock. One example of this would be **Setting the clock back.** In this example, we say that an ex-employee that work on the system and had access to it. If the system wrongly believes that it is in the past, the ex-employee will still be an employee to the systems knowledge and there for still allow him/her access to the sensitive data in the system which could be saved and distributed. Another example is if a business has automatic transactions to the employees’ bank account and it is set for a certain time. The user could wait until it has executed its attack and then rewind the clock and executed multiple times until there is nothing left in the business’ bank.

Another attack that could be mounted is **Stopping the clock.** In the same example above according to payments, an attacker could stop the clock and none of the employees would get paid at all. Also, putting the wrong date or time on important documents e.g. legal documents could cause serious problems if tampered with. Also, maybe in a stock exchange if the real-time changes are not portrayed, it could have a serious impact on the brokers and their firms.

Another attack that could be **Setting the clock forward.** This could be used to cause problems with credit card transactions e.g. making the computer think it lives in the future so credit cards would be read as out of date so the transaction or payment would be declined or refused. Also trying to book flights would be impossible because according to the system the date one wishes to depart will be in the past according to the system.