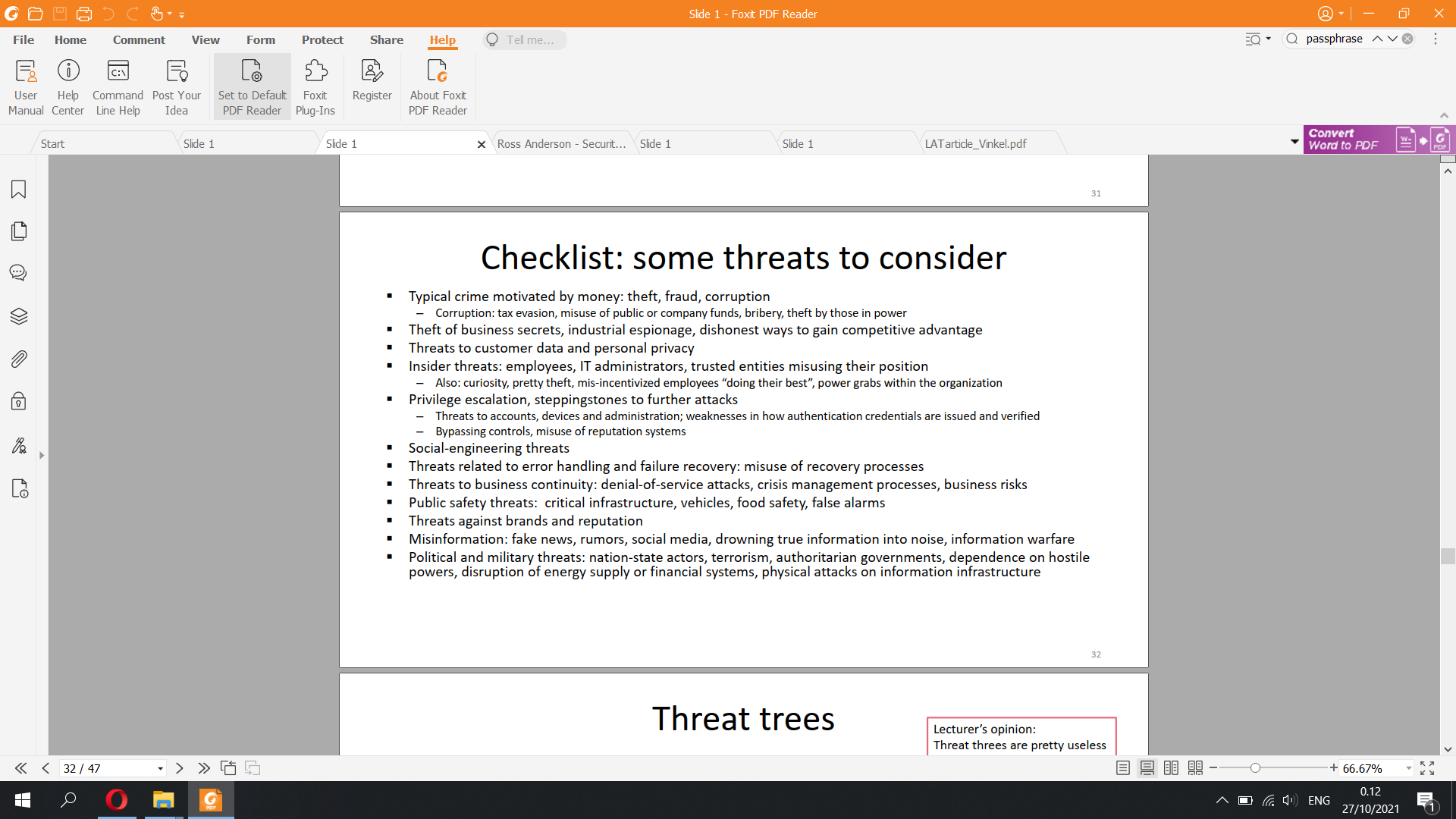


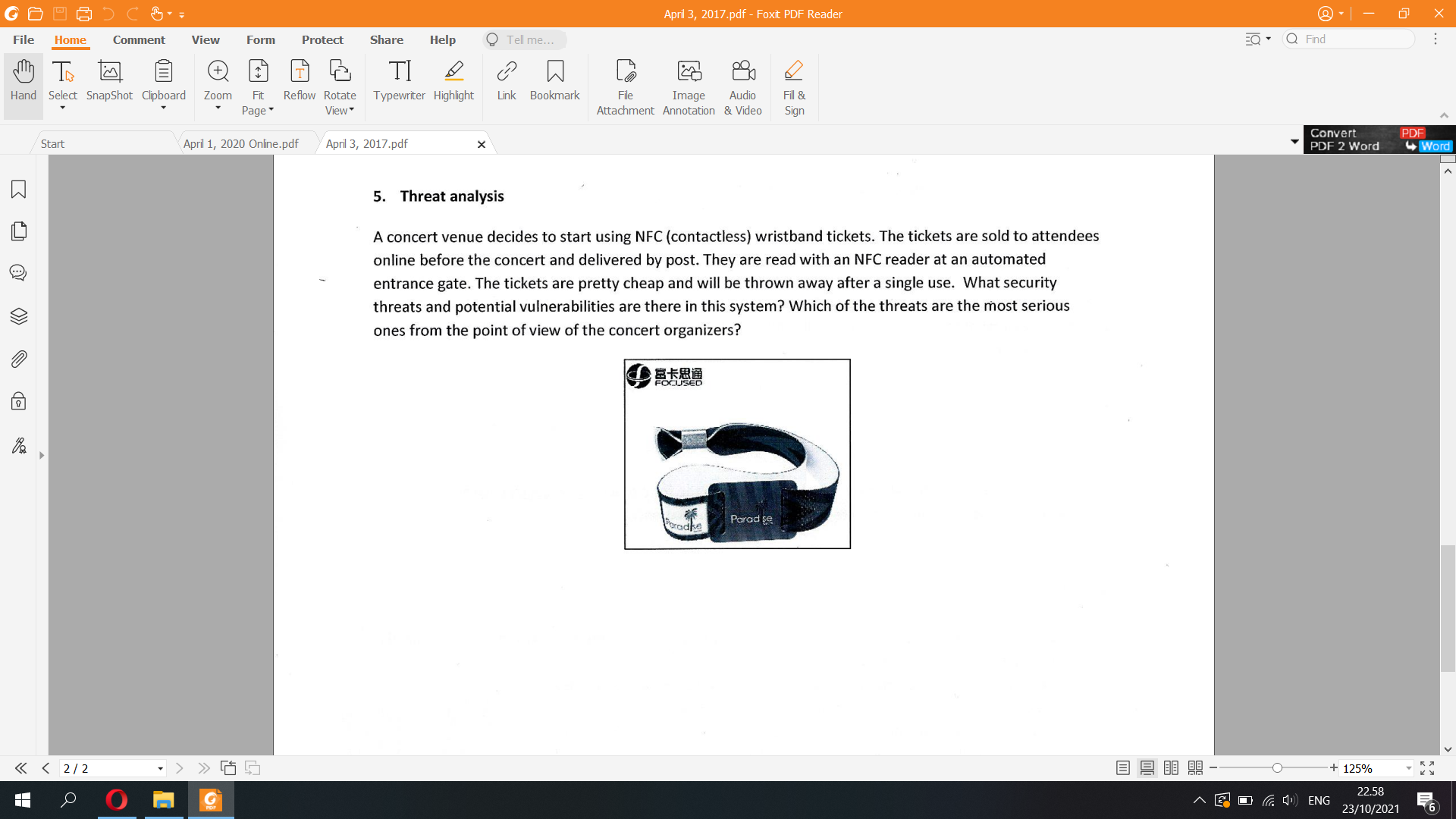
Advertise open events with a link to the meeting

Insider threats: an exclusive meeting link can be joined by an unwanted member in an organization  
Misinformation: making use of open nature of the links to spread the fake information and post the link on public forums, hoping someone to click on.  
Personal privacy: transcribing and record what others say as a proof when the conversation is not meant to be recorded.



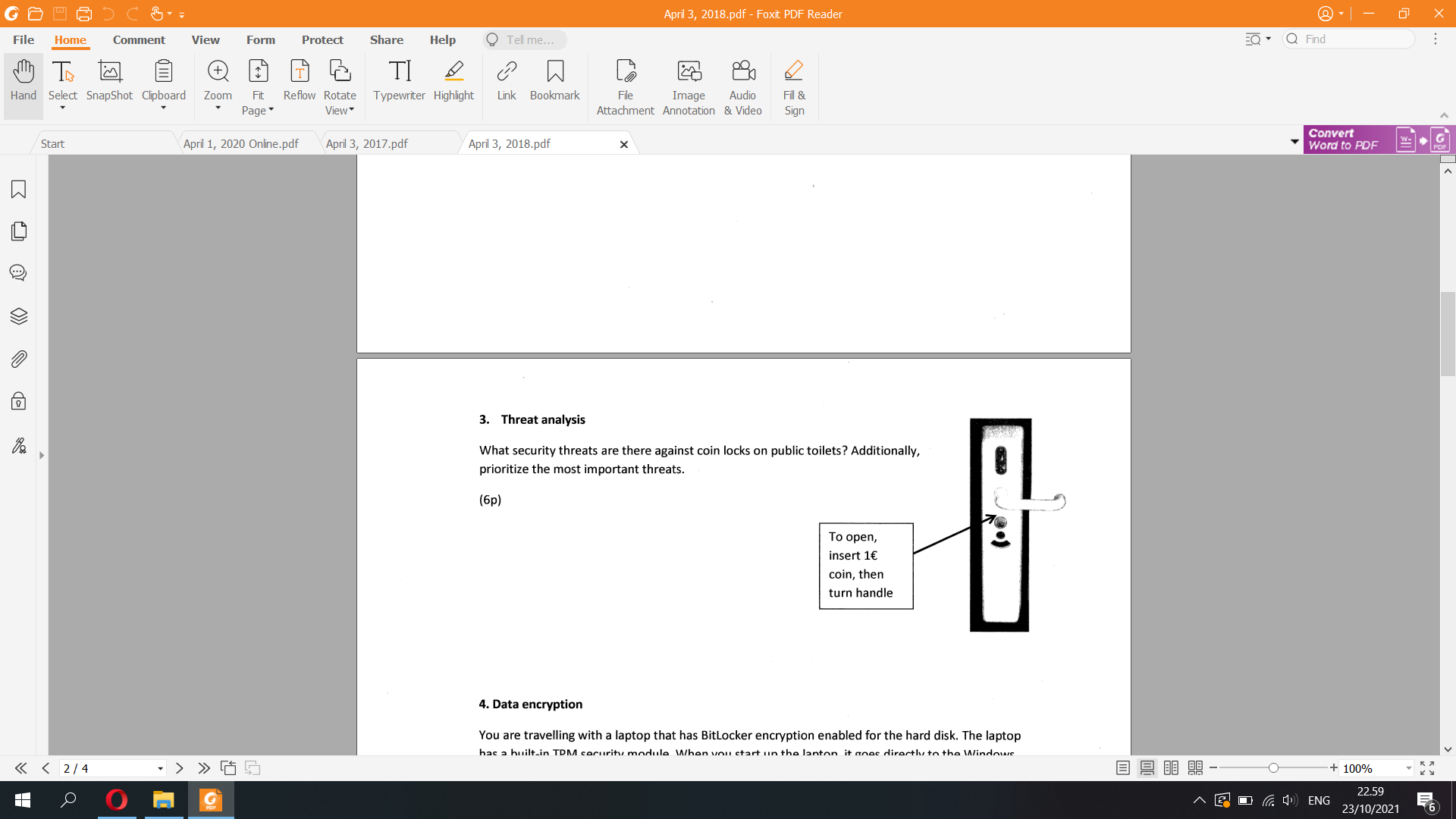
Threat analysis

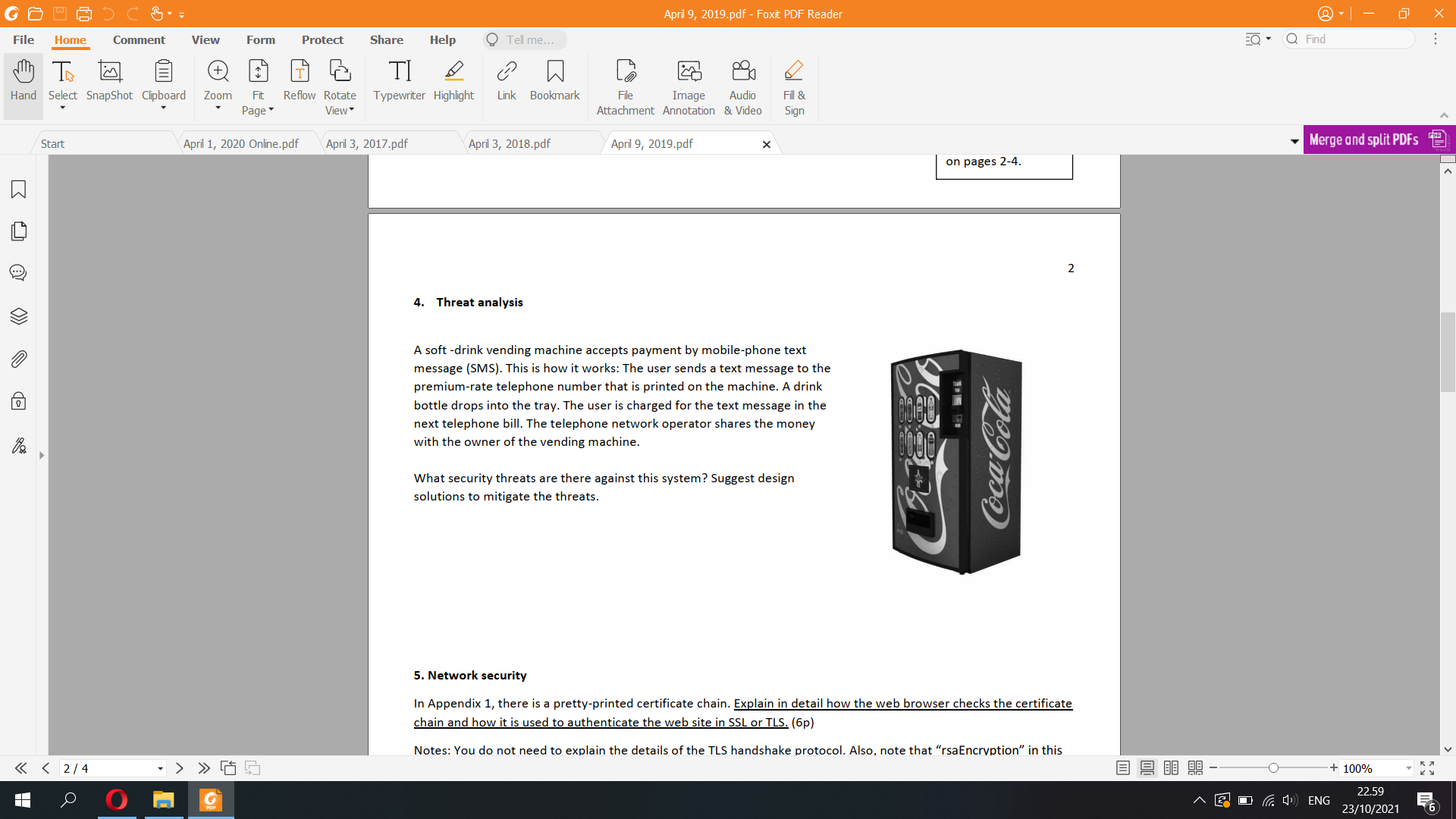
Online meeting services such as Zoom, Microsoft Teams and Google Hangouts are now commonly used for business meetings, teamwork, online lectures, student tutoring, and personal conversations. Users can schedule meetings, invite attendees from inside and outside their organization, and even advertise open events with a link to the meeting. The service features include video and audio conferencing, screen sharing for presentations, remote assistance, team chat, file sharing, video recording, and transcription. Analyze the security threats in online meeting tools when used at a university or school for educational purposes.



5. Threat analysis A concert venue decides to start using NFC (contactless) wristband tickets. The tickets are sold to attendees online before the concert and delivered by post. They are read with an NFC reader at an automated entrance gate. The tickets are pretty cheap and will be thrown away after a single use. What security threats and potential vulnerabilities are there in this system? Which of the threats are the most serious ones from the point of view of the concert organizers?

Ticket can be copied  
Ticket can be reused  
More than one person can use the ticket since the checker is automated, not checked by humans





May use the phone number that isnt link to any phone bills or it’s linked to an empty bank account that doesnt have any money

