

At the Elbonian airport

+) powered down laptop. Laptop has TPM, when powered up, it goes to windows login screen

+) officer has the laptop for one hour

Since the computer is locked with PIN, the officer can utilize

**Cold boot attack**:

First, the officer will attach an external hard disk of USB memory stick containing the attack software that can record the encryption key in the RAM. To make the memory fading much slower and retain the exact memory copy, the officer can use a specialized cooler that applies directly onto the RAM. Then, the officer can cut the power of the laptop by removing its battery. The memory will fade very slowly that the original memory barely changes thanks to the cold applied above.The USB memory stick also has a program that can fix bit errors in the retrieved memory. The officer then quickly insert the battery back and turn on the laptop. This time, it will boot from that external hard disk that can run the attack software such as BitUnlocker. After analyzing the stolen data from RAM, the software searches for the secret key and when it is found, the software uses it to decrypt the hard drive and the officer can read and steal all data.   
After stealing the data, he detaches the USB stick and returns everything to normal, so his interference with the laptop cannot be detected.

Cold boot attack: consequences

▪ Attacker with physical access to a running computer

– can break software-based full-disk encryption

– can bypass most OS access controls

▪ Sleeping laptop = running laptop

– Lost and stolen laptops are vulnerable if in sleep mode

▪ BitLocker in TPM-only mode is vulnerable even if

powered down or hibernating

– Attacker can boot it up and then do the cold-boot attack

**Direct Memory Access (DMA) attack:**

A DMA Attack, short for "direct memory access" attack, is when an attacker accesses a computer via ports on the computer which grant direct memory access to high-data-transfer-speed devices.

Normally, memory access is strictly managed by the operating system. Certain devices, such as external hard drives and camcorders, use technology which allows very fast data transfer speeds. The most common examples are Firewire, Thunderbolt, ExpressCard, and PCI. In order to achieve these very high data rates, the device communicates directly with the computer memory, bypassing the operating system's memory management and bypassing all access controls.

Simply plugging in an infected device can allow an attacker to read and manipulate the current contents of the computer memory. They can steal private encryption keys, run commands with escalated privileges, install malware, or add a backdoor to be used later.

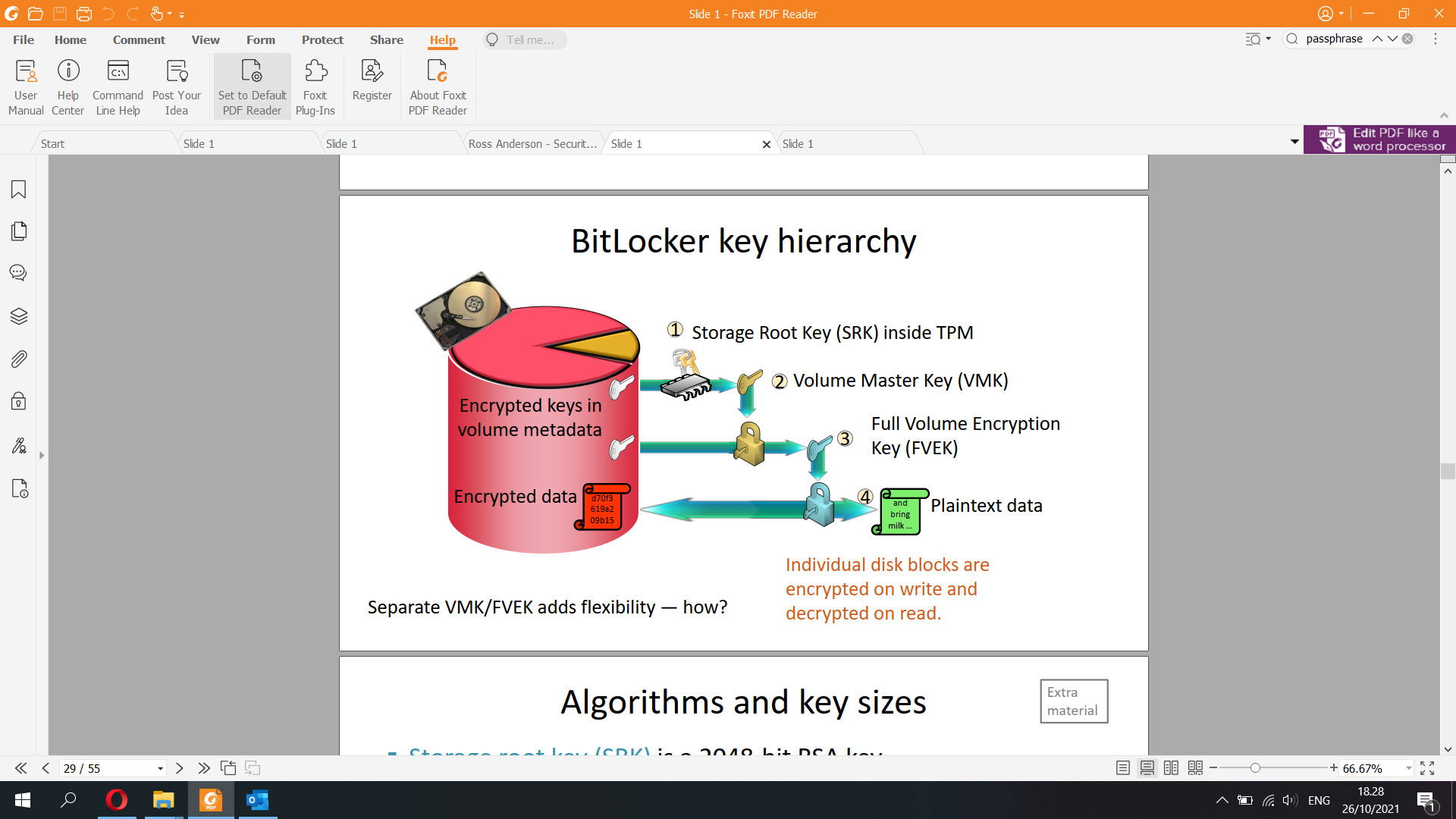
▪ DMA memory dump attack: Attacker connects malicious device to a

DMA port, reads the memory, and recovers the key (FVEK)

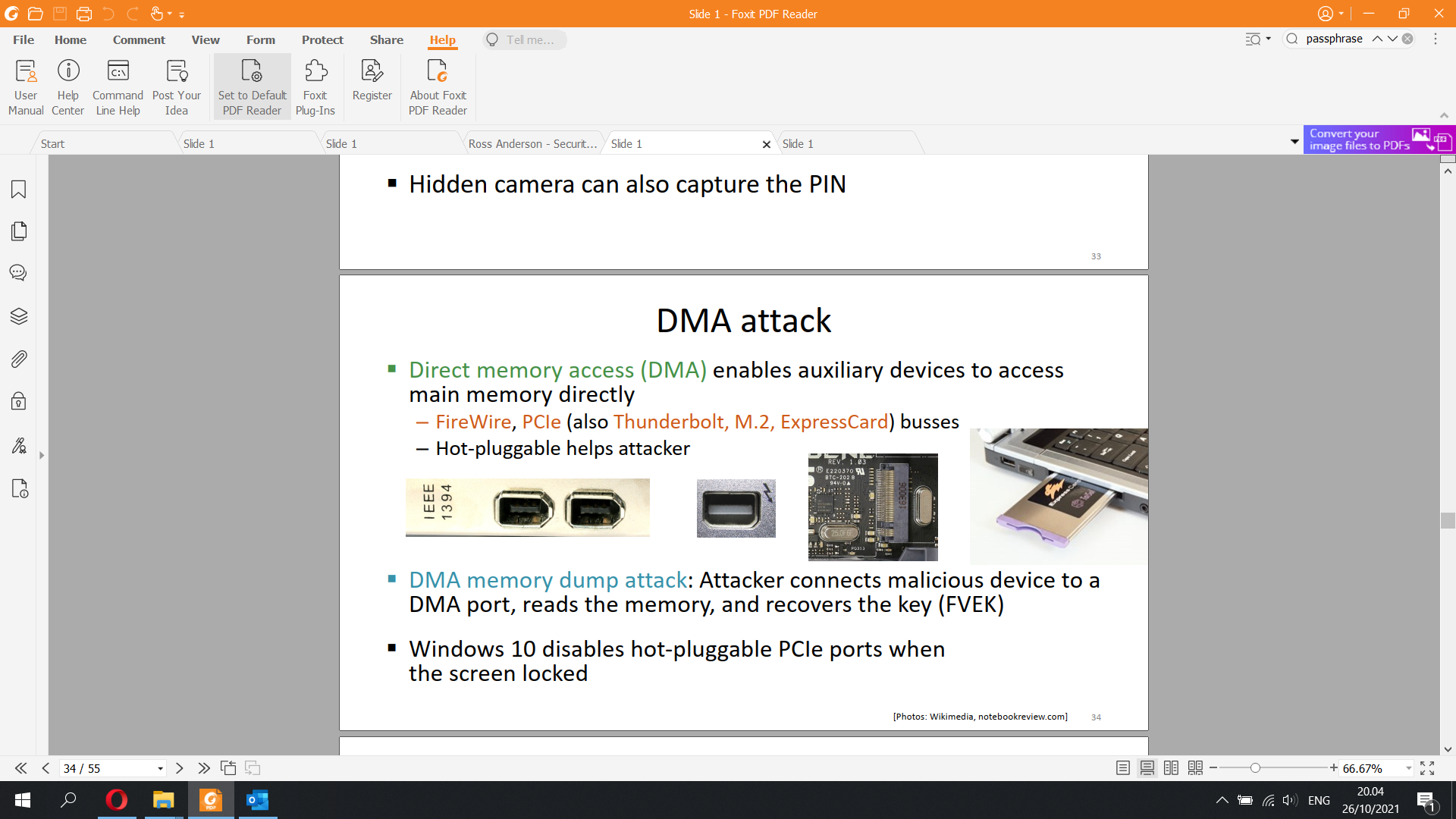
DMA Hacking Tools

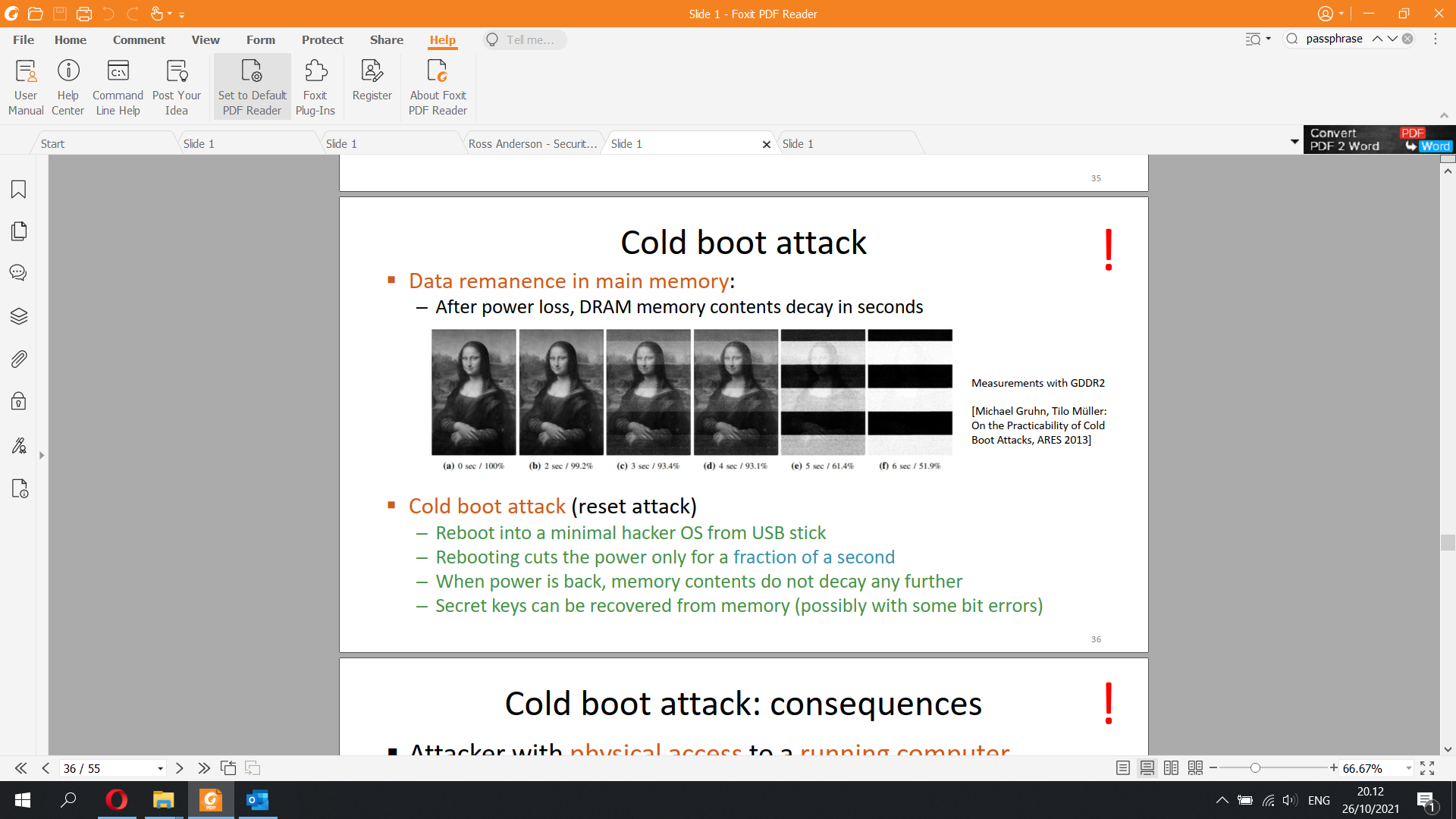
Reading and writing to server memory is highly technical and not a skill which everyone possesses. However, there are tools which attackers can use which will launch a DMA Attack and handle the technical details of memory access for them.

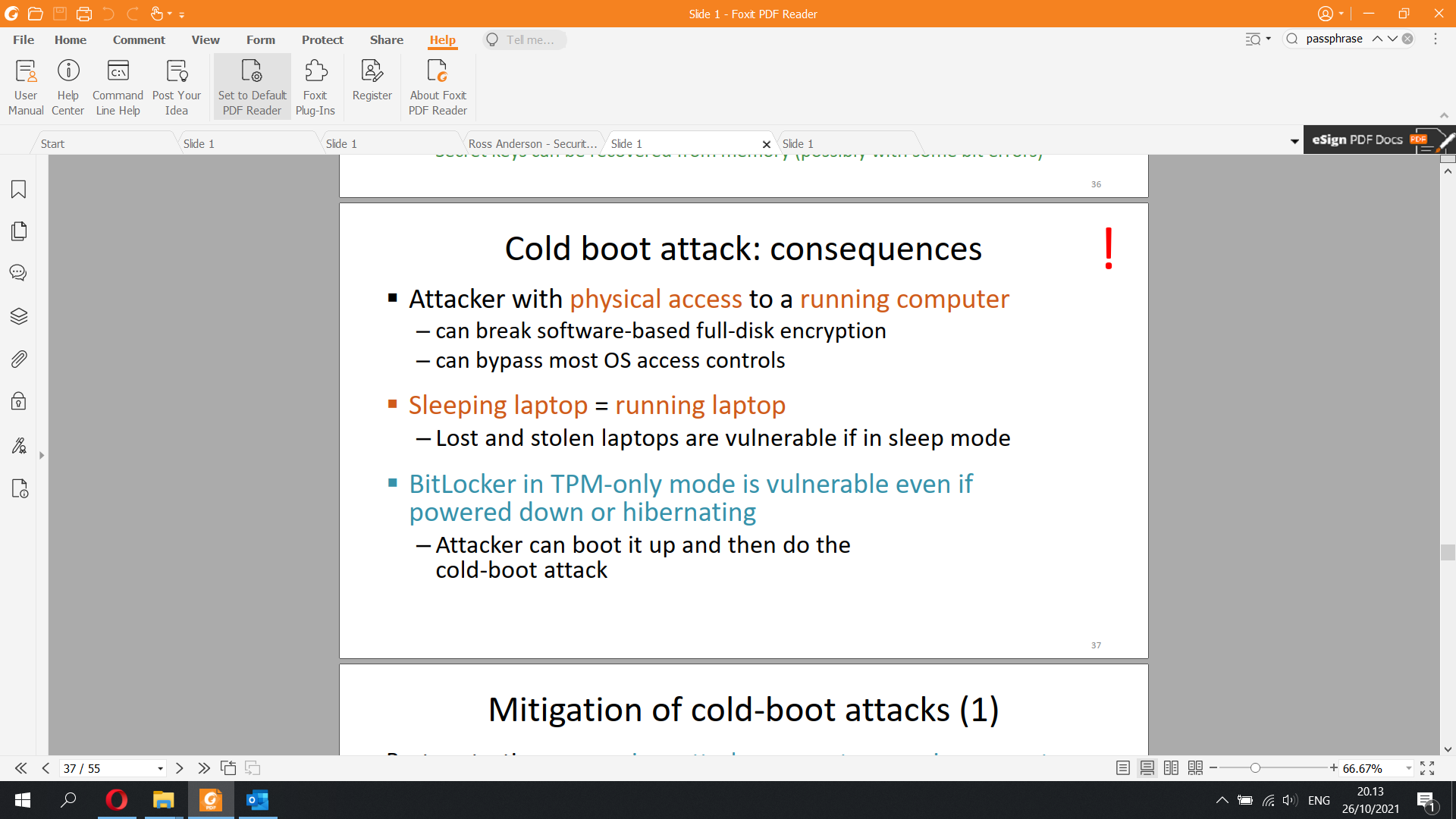
All DMA attacks are dependent on using the computer port which allows high speed access. Physically removing these ports from the computer will prevent external devices from being connected. In addition, the drivers for these device types should be disabled or removed. This provides protection should another port type (such as PCMCIA) be used as an adapter for a high-speed port.

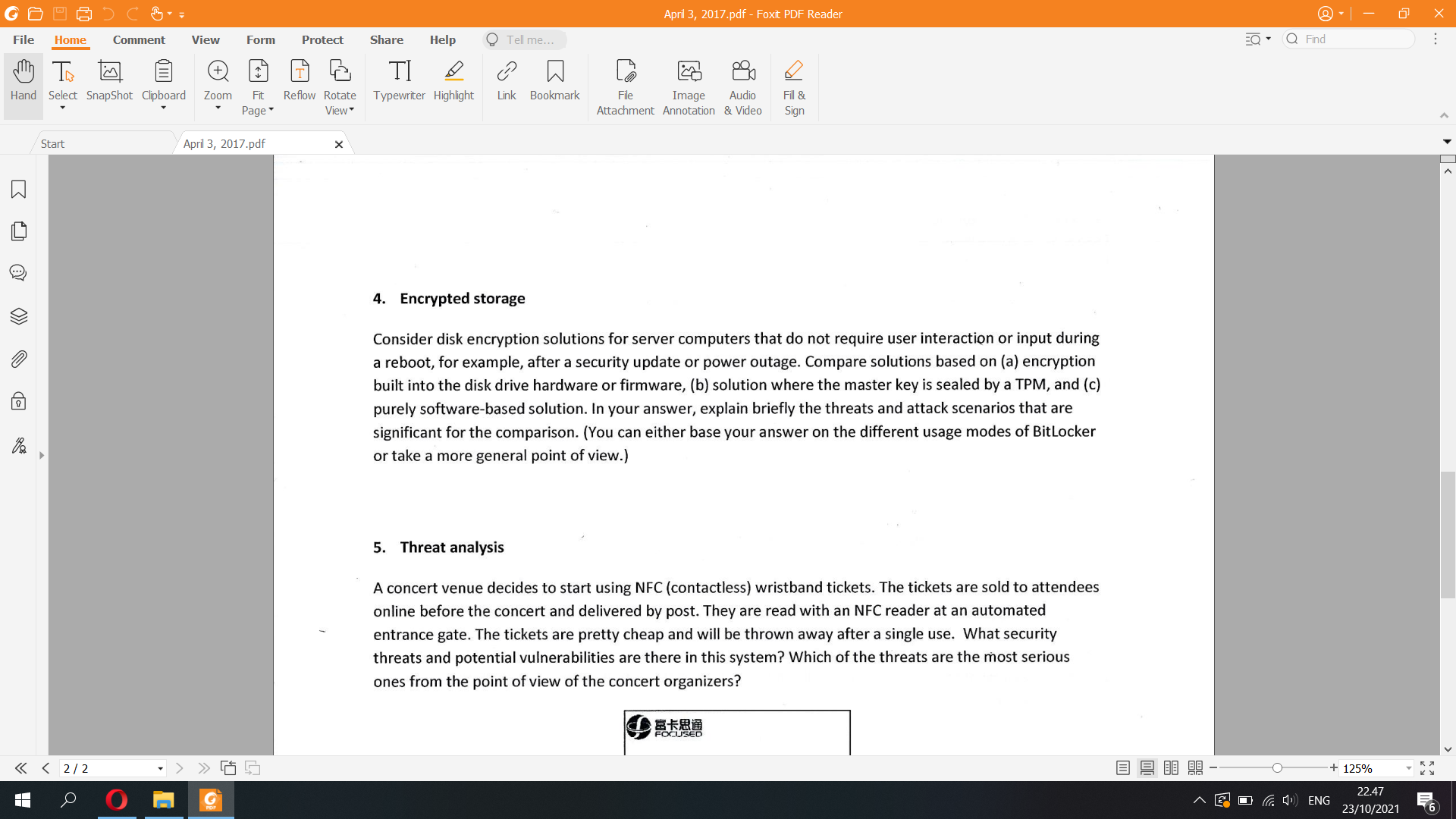


DMA attack









Disk encryption solutions for server comps that don't require user interaction or input during reboot after sec update or power outage

a) encryption built into disk drive hardware or firmware

Hardware-based full disk encryption (FDE) is available from many hard disk drive (HDD/SSD) vendors, including: ClevX, Hitachi, Integral Memory, iStorage Limited, Micron, Seagate Technology, Samsung, Toshiba, Viasat UK, Western Digital. The symmetric encryption key is maintained independently from the computer's CPU, thus allowing the complete data store to be encrypted and removing computer memory as a potential attack vector.

**Attacker could capture keys on the PCIe/SATA/ SCSI bus during transfer. When a computer with a self-encrypting drive is put into sleep mode, the drive is powered down, but the encryption password is retained in memory so that the drive can be quickly resumed without requesting the password. An attacker can take advantage of this to gain easier physical access to the drive, for instance, by inserting extension cables => DMA attack**

Serial ATA (SATA, abbreviated from Serial AT Attachment) is a computer bus interface that connects host bus adapters to mass storage devices such as hard disk drives, optical drives, and solid-state drives

Three widely used bus standards:

– PCI (Peripheral Component Interconnect)

– SCSI (Small Computer System Interface)

– USB (Universal Serial Bus)

b) master key is sealed by a TPM

**For unsupervised boot (TPM only mode), as the computer reboots within the outage or security update, the attacker can interrupt the boot process and recover VMK from the disk, if the attacker has physical access to the computer as the keys are stored in the memory using cold attack. Attacker may even be able to go to the recovery console**

**▪ BitLocker in TPM-only mode is vulnerable even if powered down or hibernating**

**– Attacker can boot it up and then do the cold-boot attack**

c) pure software-based solution

This solution uses the user’s password as the encryption key that scrambles data, which means it is susceptible to brute force attacks. Even if the computer tries to limit the number of decryption attempts, hackers can access the computer’s memory and reset the attempt counter. This attack is offline and the attacker must have access to the computer.

Hardware-Based Encryption

Uses a dedicated processor physically located on the encrypted drive

Processor contains a random number generator to generate an encryption key, which the user’s password will unlock

Increased performance by off-loading encryption from the host system

Safeguard keys and critical security parameters within crypto-hardware

Authentication takes place on the hardware

Cost-effective in medium and larger application environments, easily scalable

Encryption is tied to a specific device, so encryption is “always on”

Does not require any type of driver installation or software installation on the host PC

Protects against the most common attacks, such as cold boot attacks, malicious code and brute force attacks

Software-Based Encryption

Shares computers resources to encrypt data with other programs on the computer – Only as safe as your computer

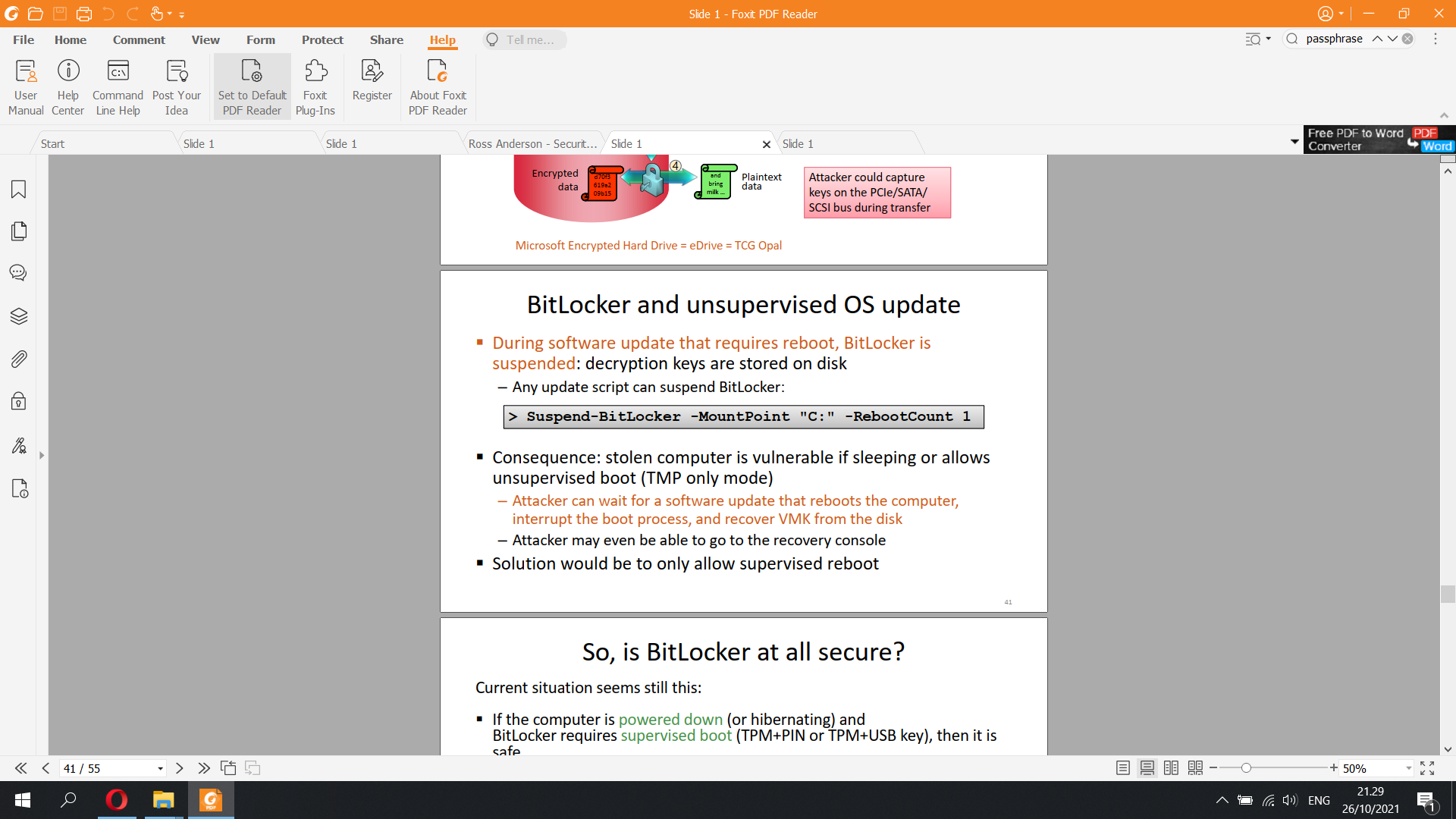
Uses the user’s password as the encryption key that scrambles data

Can require software updates

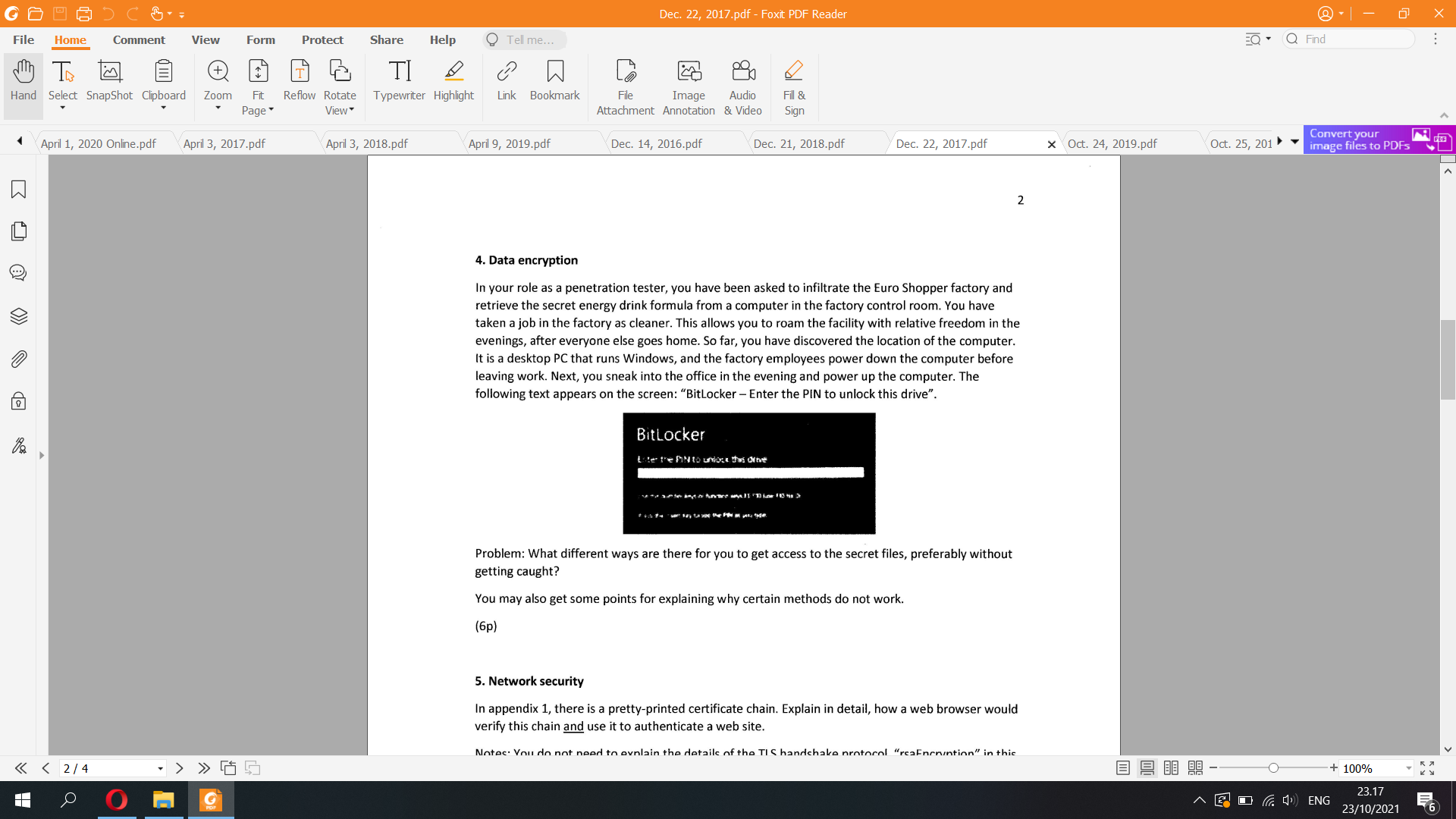
Susceptible to brute force attacks, computer tries to limit the number of decryption attempts but hackers can access the computer’s memory and reset the attempt counter

Cost-effective in small application environments

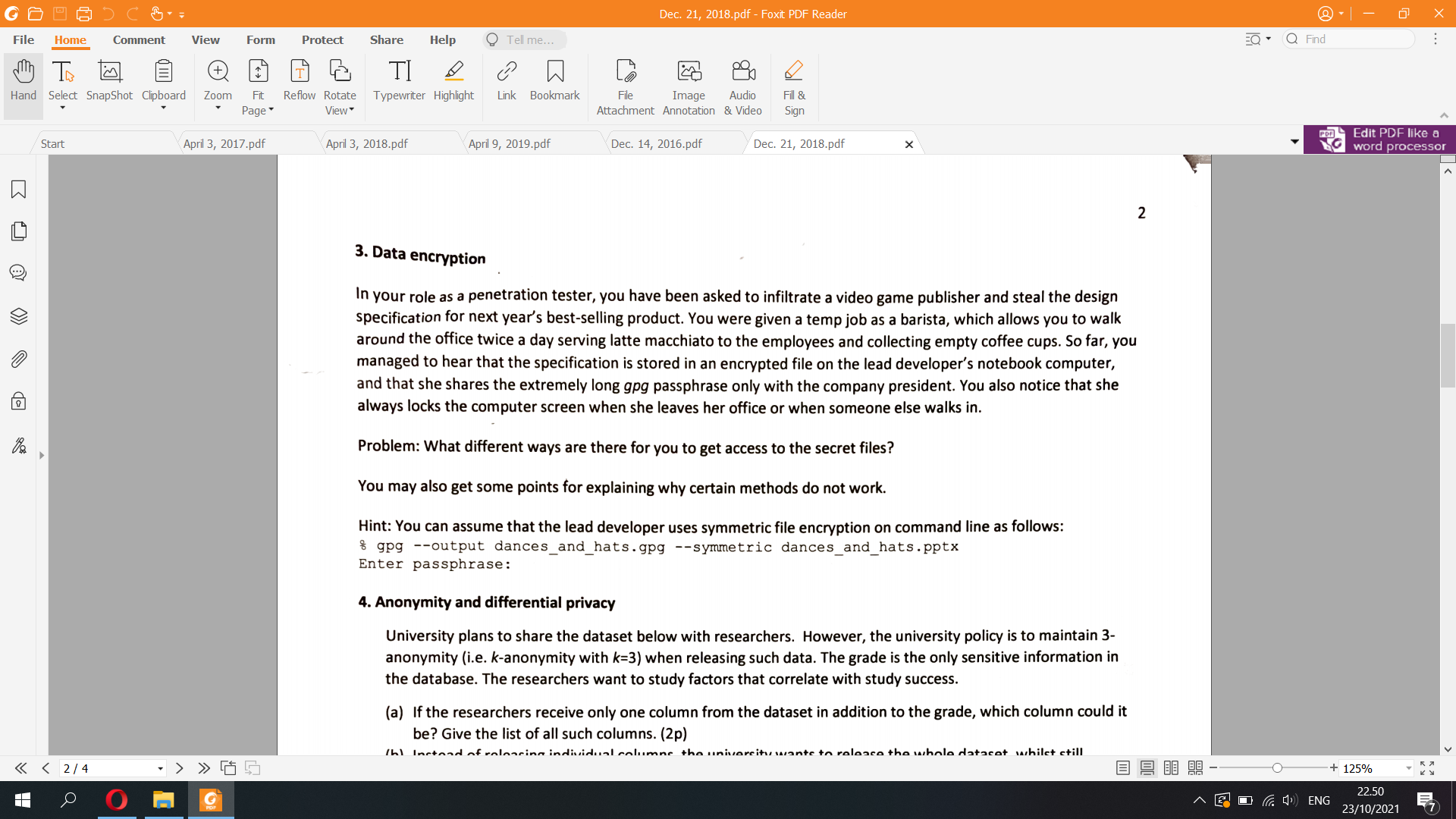
Can be implemented on all types of media







+) Know comp location, comp runs Windows. It is powered down before the employee left.   
+) Next evening, u sneaked into office in evening, power up and it uses Bitlocker, enter the PIN to unlock this drive  
Like elbonian  
Method that does not work: If the desktop PC runs on windows 10 and it has only a high-data-transfer-speed of hot-pluggable PCle, then direct memory access attack isn't possible



+) Specifications of the product is stored in an encrypted file dances\_and\_hats.gpg in lead dev’s laptop  
+) Lead developer and company president have the extremely long gpg passphrase  
+) The file use symmetric encryption

+) She locks computer screen when she leaves office or someone walks in

There are several limitations of file encryptions like this

▪ User action needed, and users are lazy

– Automation (scripting) is difficult. How to store passphrase?

▪ Passphrase can be brute-forced

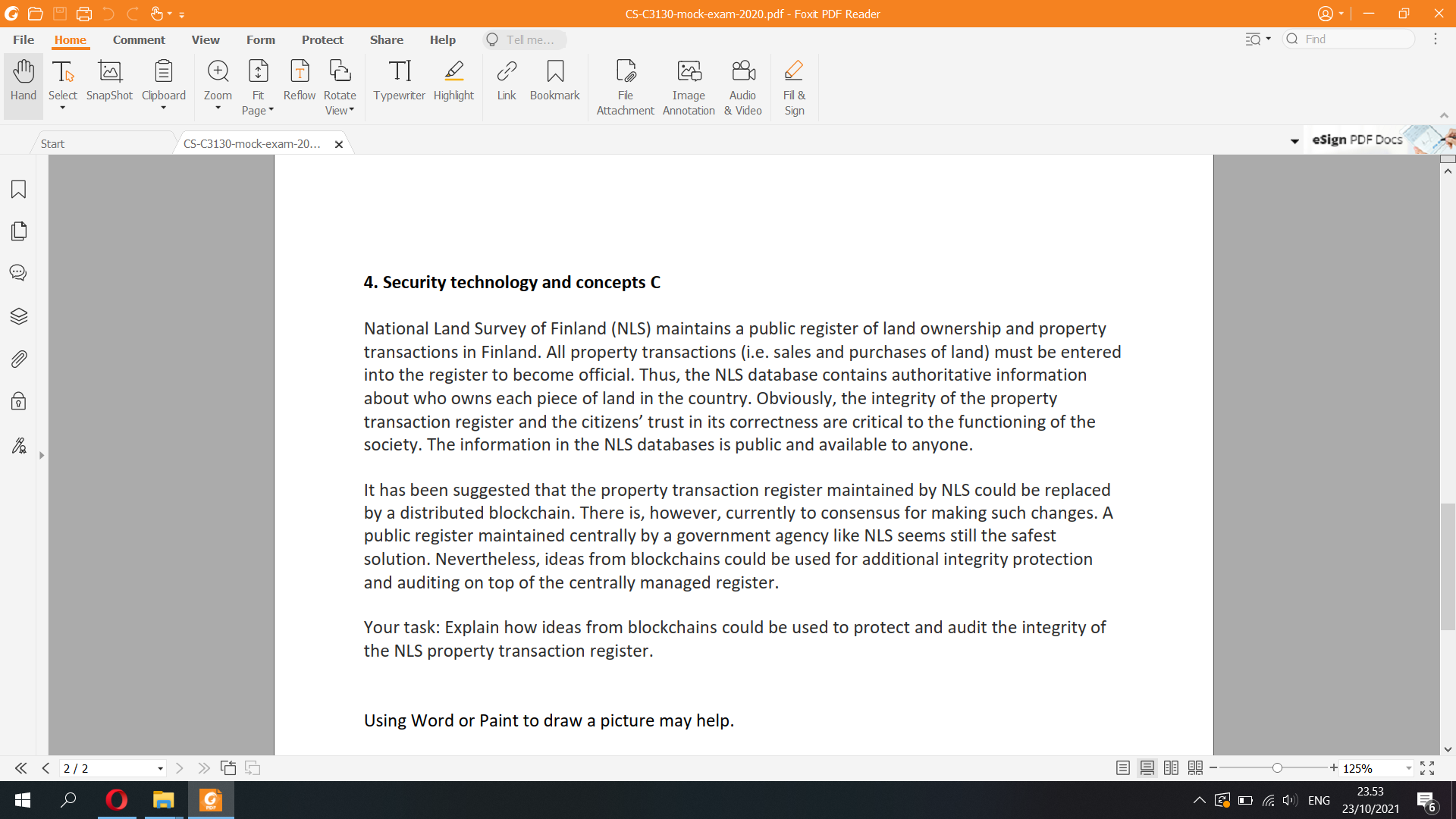
▪ After encryption, what happens to the old plaintext file?

▪ Software creates temporary files and backup copies

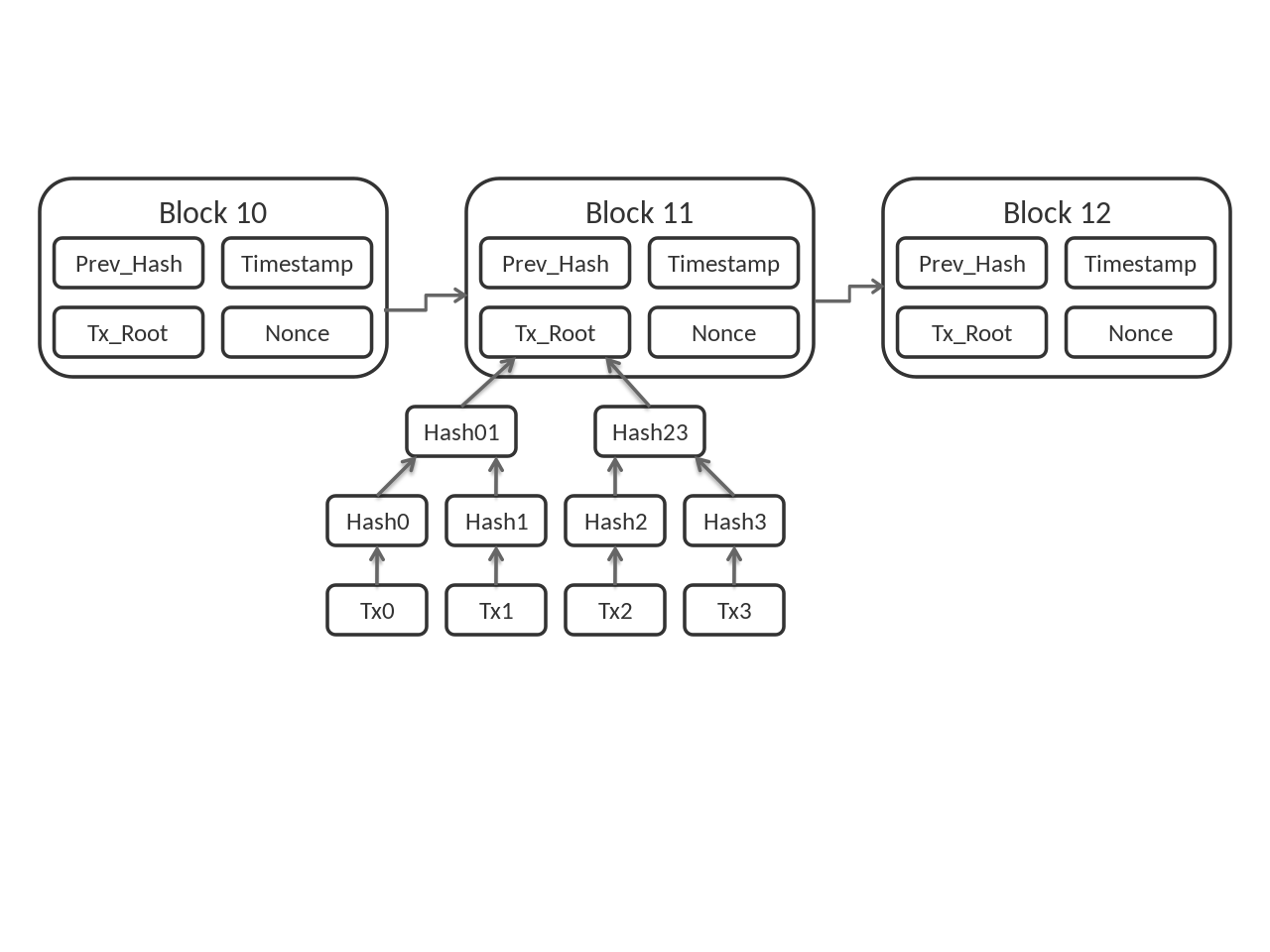
– Unencrypted file versions and data fragments may be left on disk

=> First method: steal the passphrase from company president  
Pretend to serve the company president coffee while bringing a microcamera. After successfully serving him coffee, put the microcamera somewhere that can track the typing or the screen of the company president. If he accesses the secret file, the barista can know the passphrase. This method relies on sniffing. Since the encryption method is symmetric, the passphrase obtained from the company president can both encrypt and decrypt the secret files. Since both the lead dev and president has the passphrase, it can be assumed that the president also has the secret files. Try to access the file from the president seems more feasible than the lead dev  
=> Second method: Despite the computer is on lockscreen, the barista can attack the internal disk of the computer, since the software creates temporary files and backup copies, unencrypted file versions of the secret files may be left on disk.

Method that does not work:   
+) try to guess the password of the lock screen: too many attempts will render the computer denial of service, which will raise doubt of the lead computer and she will take more precautions.  
+) brute forcing the passphrase: the passphrase is extremely long and it is infeasible to guess the passphrase while having limited time access to the computer.



A blockchain is a growing list of records, called blocks, that are linked together using cryptography.[1][2][3][4] Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.



By design, blockchains are inherently resistent to the modification of data. Blockchain ledgers are immutable meaning that if data addition or transaction has been made, it cannot be edited or deleted. It is there and it will be there. In addition, blockchains are not only a data structure but a timekeeping mechanism for the data structure so proof of the history of data is easily reportable and updated to the second. Organizations facing an audit, regulatory compliance requirements, or legal challenges can use blockchain technology to improve data integrity and save millions.

One aspect of blockchain technology which is particularly important for improved data integrity is Merkle Tree: it ensures the integrity of data in the Blockchain.

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the cryptographic hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

