

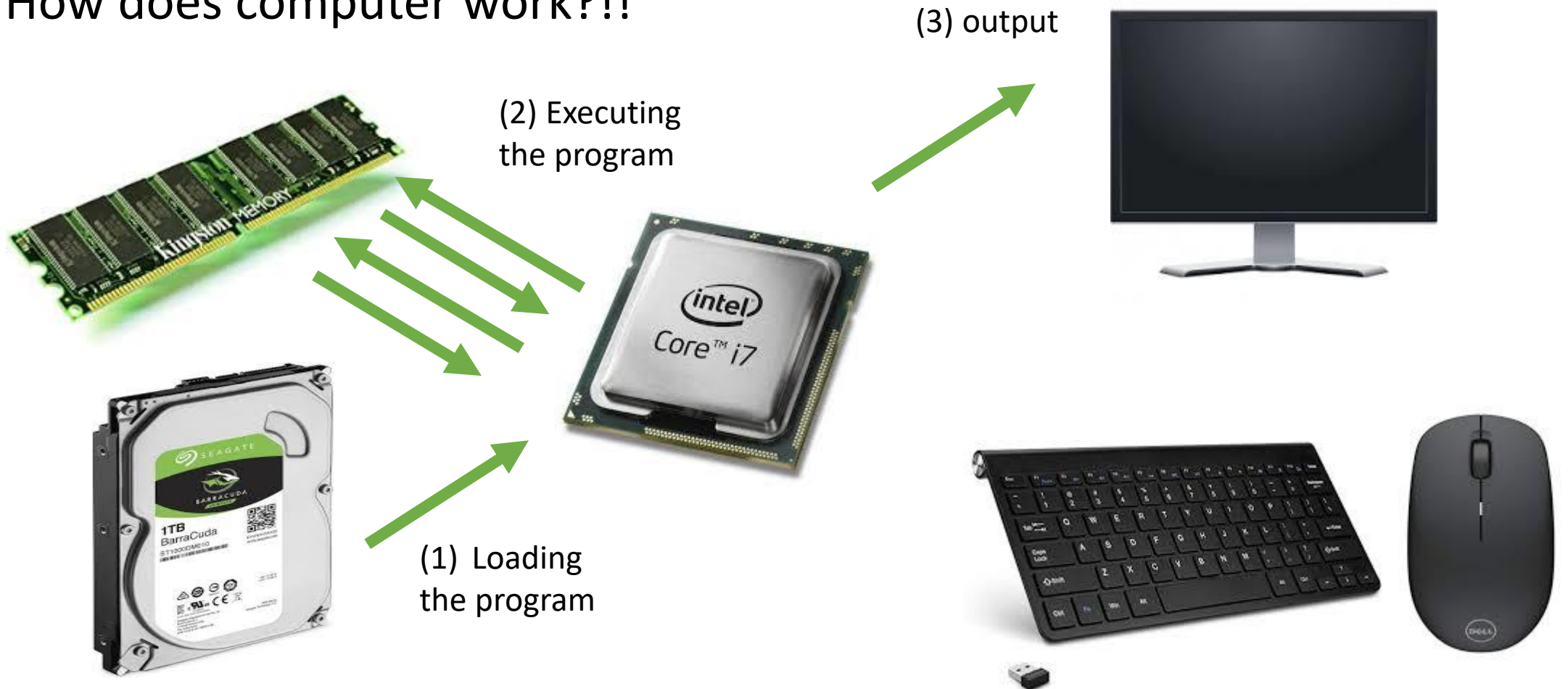


Case Studies

Tutorial sheet 5

What are Meltdown and Spectre attacks?

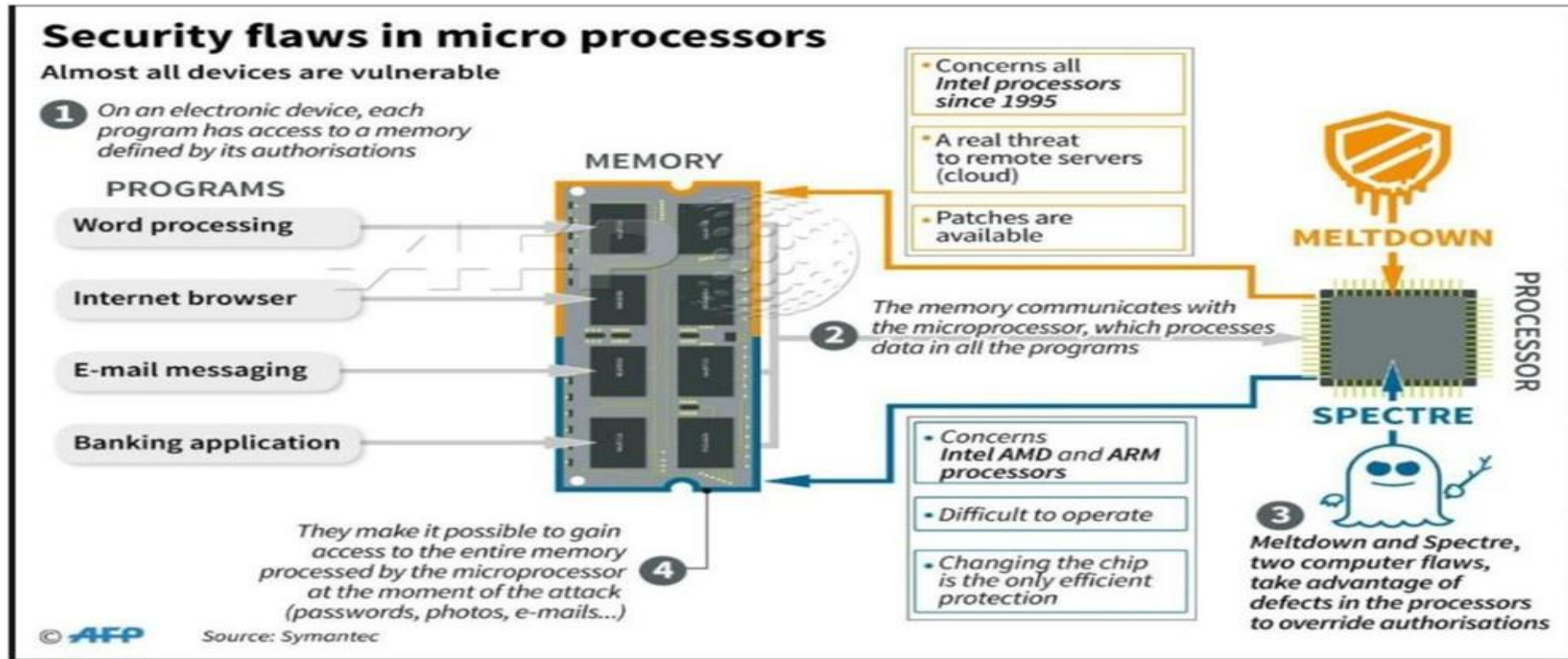
- How does computer work?!!



What are Meltdown and Spectre attacks?

Meltdown is a bug that “melts” security boundaries.

Spectre is a vulnerability which the attacker exploits to implement data exfiltration attack (i.e., collecting important information from memory)

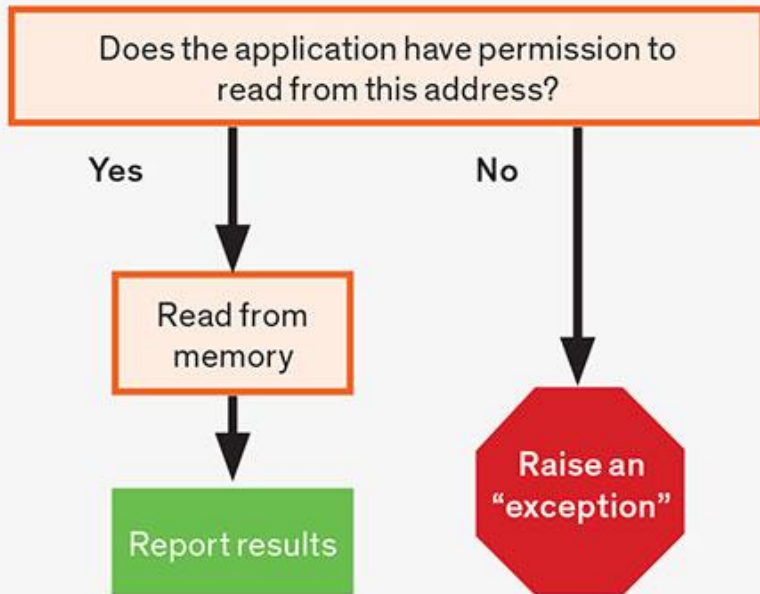


What are Meltdown and Spectre attacks?

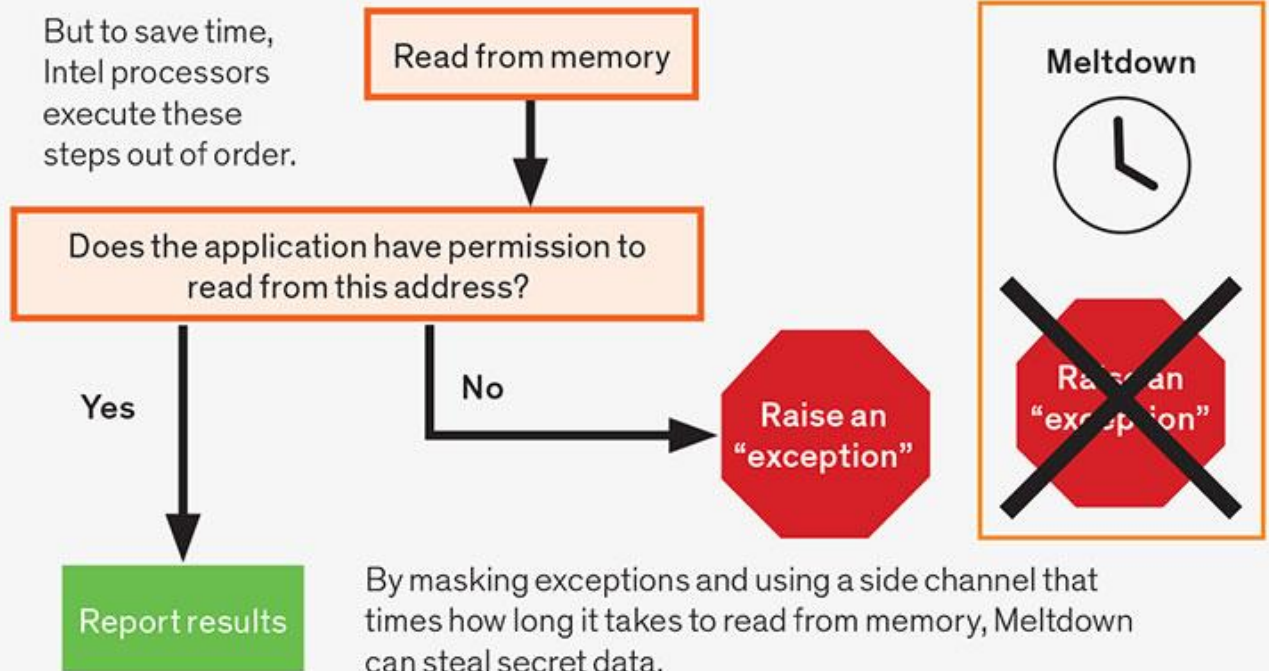
More details:

MELTDOWN

Logically, reading from memory should work like this:



But to save time, Intel processors execute these steps out of order.



What is NOTPetya attack?



What is NOTPetya attack?



You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/N19fvE>
<http://petya5koahtsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

If you already purchased your key, please enter it below.

Key: _

What is NOTPetya attack?

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address :

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbbWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net . Your personal installation key:

mFSbvr- thFa7x-UkLKM7-hFsjHD-NMndbJ-9pitDG-COxnDN-1AZxjD-rLh3Th

If you already purchased your key , please enter it below.

Key:

NotPetya causes \$10B+ in losses

Paralyzed operations of some of the largest businesses worldwide



The most expensive cyber incident in history

Questions:

- How these kinds of attack techniques could be exploited in an attack on critical infrastructure?
- What mitigations are possible for these kinds of attacks?