Plan for today

Welcome to the course ! (NJ)

The NotPetya case (NJ)

Chapter 1 (NCJ)

Chapter 2 (NJ)

20-minute oral exam based on a written assignment

Oral exam

- the student selects a random question
- among 20 questions
- 3-5 minutes presentation, using written assignment
- Q/A about the question

Teachers present 20 questions

- two questions each course day
- *“In the NotPetya attack, how was encryption used?”*
- *“Following the NotPetya attack, what were the management lessons?”*

Written assignment

- 2-4 pages
- presents main points for each of the 20 questions
- main points = topics, headlines for an oral presentation
- assignment is an incentive to prepare yourself for the oral exam

Written assignment

Q1

Q2

Q3

..

Q20

Q3: Present and discuss the hybrid encryption model for ransomware from Bajpai et al.

Motivation for name: hybrid refers to symmetric + asymmetric encryption

Motivation for studying ransomware: in recent years there are more and more ransomware attacks on private and comporate users.

Key management refers to the challenge that the attack program must first generate a key, then hide it, and finally the attacker must send the key to the victim (if the ransom is paid).

Properties of asymmetric encryption guarantee that if a key for symmetric encryption is encryption using a public key, it can only be read using the corresponding private key.

The oral exam:

- *main basis for grading*
- *student presents for 3-5 minutes*
- *presentation mainly covers the points in the written assignment*

Encryption

NotPetya used AES

AES

- standardized approx. in 2000
- symmetric encryption
- 128 bit keys or larger
  - the “k” in Figure 2 (a)
- 128 bit blocks
  - the “b” in Figure 2 (a)

Exercise

(1) List at least three arguments in favor of using AES for a ransomware attack

(2) What parts of Figure 2 (a) were available on the computer after the attack?

- P_1.. P_n?
- C_1.. C_n?
- b?
- K?

Exercise answers

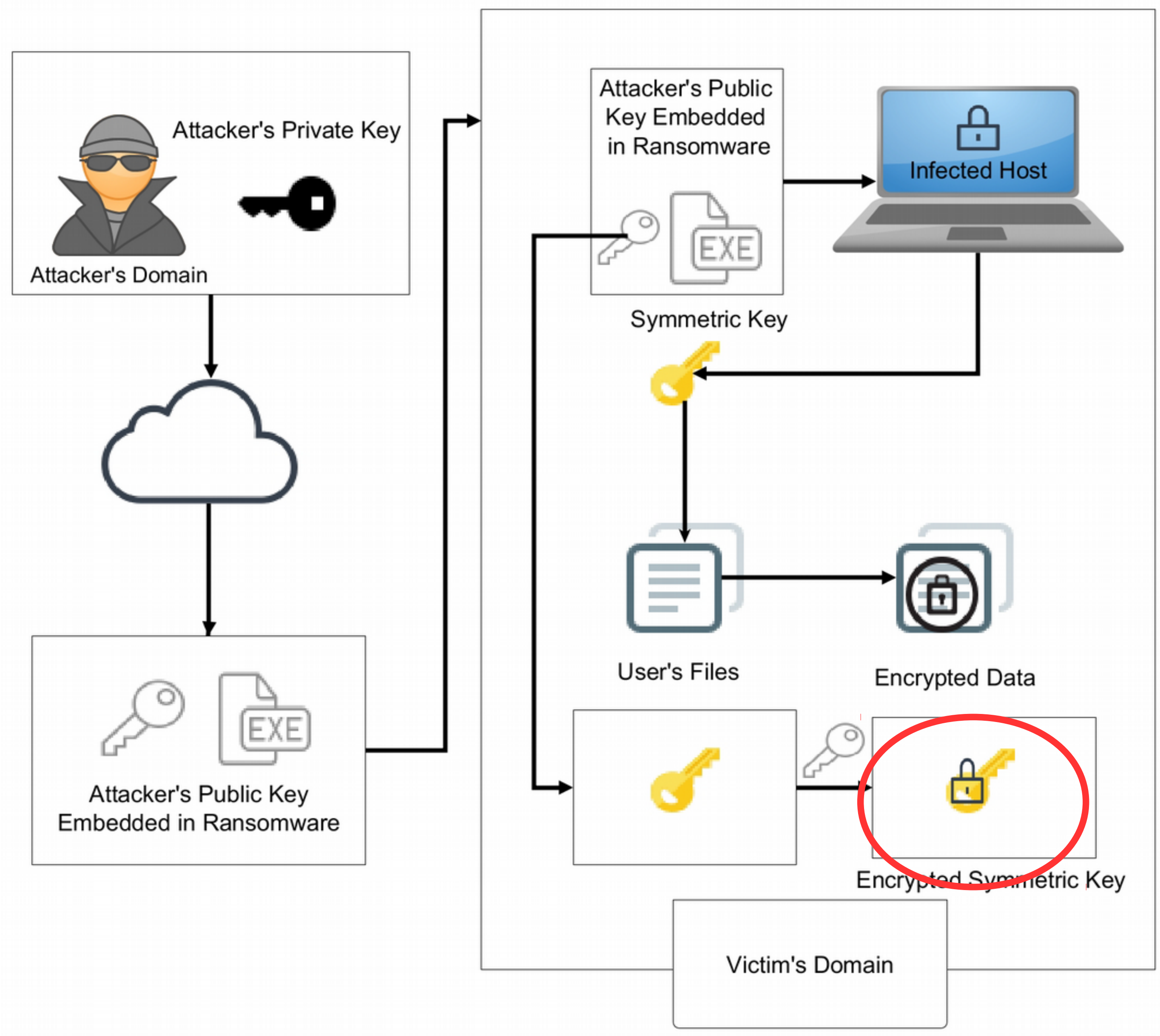
(1) List at least three arguments in favor of using AES for a ransomware attack

i. Symmetric encr. is much faster than asymmetric encr.
ii. AES is faster than DES
iii. Decryption is believed to be infeasible

(2) What parts of Figure 2 (a) were available on the computer after the attack?

- *P_1.. P_n? Not available*
- *C_1.. C_n? Available*
- *b? Can be inferred (128 with AES), but useless*
- *K? Not available, except in encrypted file*

Hybrid encryption model
Figure 1, Bajpai et al.



Feasibility vs. infeasibility of “breaking” an encryption algorithm

We want an encryption algorithm to be strong

Strong (unbreakable)

- = ability to find plaintext based on ciphertext
- without knowledge of the key

However, for no algorithm is there a proof that it is strong

- brute force-attack = try all keys
- in addition, an algorithm may have weaknesses that allows for attacks that are faster than brute force

Brute force-attacks today (Table 2.2)

- modern PC: 0.5 * 10^9 keys per second
- supercomputer: 10^{13} keys per second

Exercise

Suppose Maersk wants to do a brute-force attack on a PC infected by NotPetya? (All use files have been encrypted)

How would you design such an attack
How long time would it require?
(a) Assuming encryption with AES
(b) Assuming encryption with DES

Hint: Use Table 2.2

Exercise answer

Suppose Maersk wants to do a brute-force attack on a PC infected by NotPetya? (All use files have been encrypted)

How would you design such an attack

```
  for i = 0 to .. do {
     select Ki
     decrypt P1
     if P1 is plaintext, Ki is the right key
  }
```

How long time would it require?

(a) Assuming encryption with AES

- *5.3 * 10^{17} years (supercomputer), or 5.3 * 10^{21} (two PCs)*

(b) Assuming encryption with DES

- *1 hour (supercomputer), or 1.125 years (two PCs)*

February 18th: course day #2

Theme A: Computer security technology and principles (ii).

Case: The Petya attack.

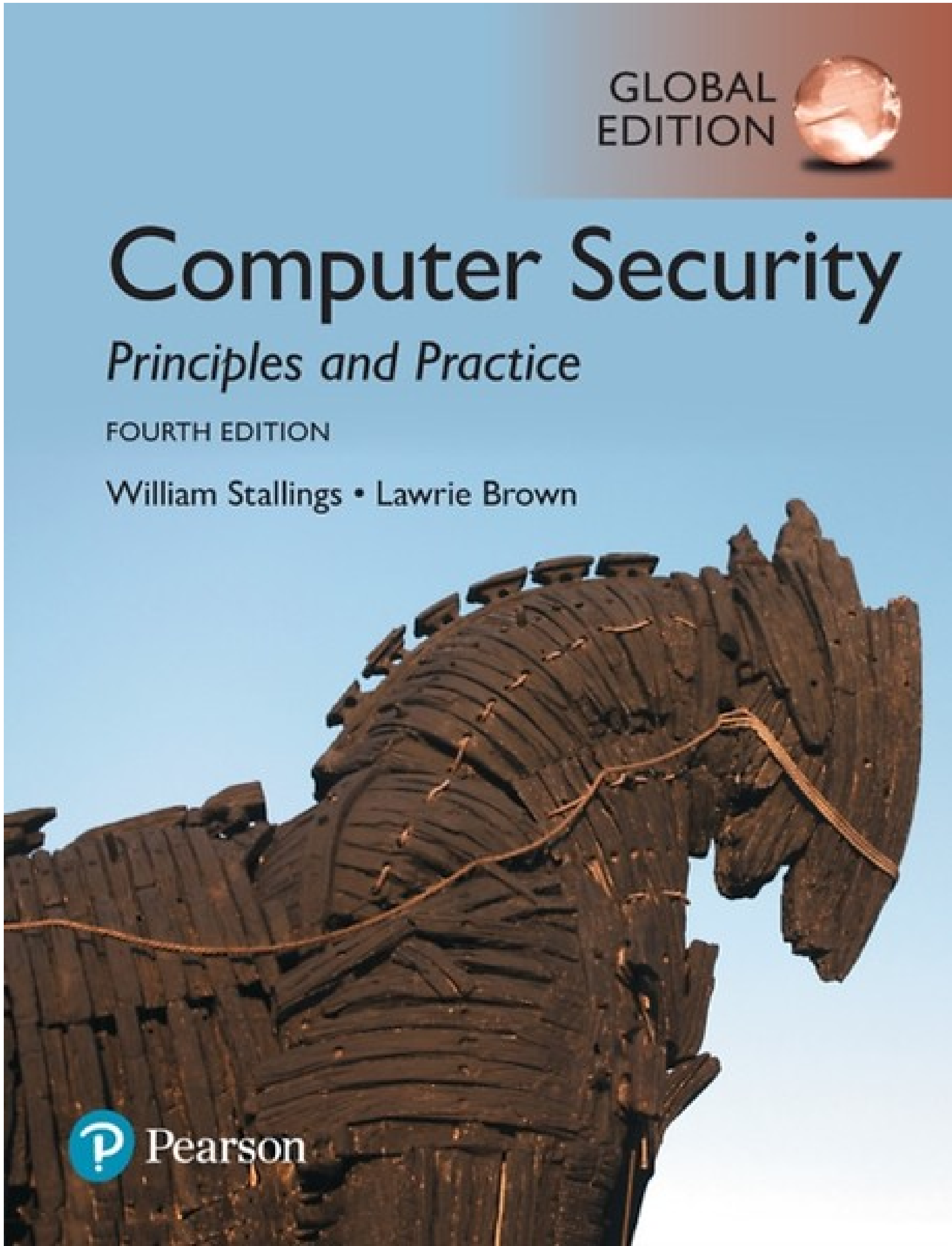
Ransomware. Malicious software.

Stallings & Brown:

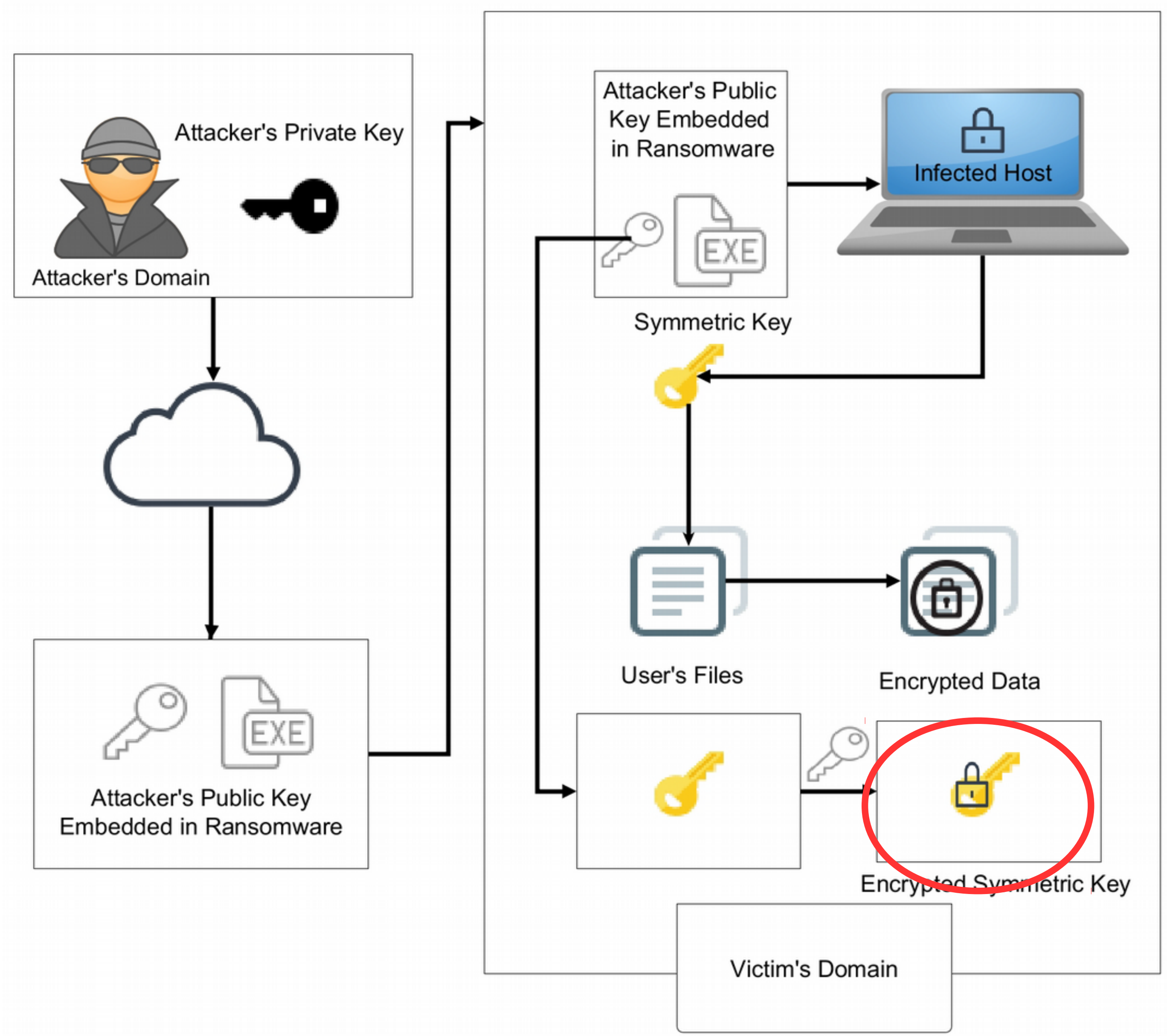
- Chapter 2 (only Section 2.3)
- Chapter 6

Additional literature:

- Pranshu Bajpai et al. A key-management based taxonomy for ransomware. (2018). You may skip Sections IV and V.



Hybrid encryption model
Figure 1, Bajpai et al.



Bajpai et al. *A key-management-based taxanomy for ransomware.*

1) “Hybrid model” is about key-management

- attack phase: generate encryption key, then delete it
- after ransom is paid: send encryption key
- “hybrid model” uses symmetric
  + asymmetric encryption
  - stores symmetric encryption key on victim PC
  - but stored key is encrypted with public key

2) A taxanomy with six levels

- Category 1 (including scareware)
- ..
- Category 6 (flawless encryption model)

Student presentations

1) “Hybrid encryption model” of ransomware
-> Johannes

2) Taxonomy of ransomware
-> Niels