

# IT security

Monday 18<sup>th</sup> February  
Course day #2

Theme A (ii)

Case: The Petya attack

Chapter 2.3 + 6

Niels Christian Juul (ncjuul@ruc.dk)  
Niels Jørgensen (nielsj@ruc.dk)

# Four themes (A-D)

- “anatomy” of an attack
- bunch of techniques and principles

A. Computer security technology and principles (Part One in Stallings & Brown)	11 <sup>th</sup> Feb 18 <sup>th</sup> Feb 25 <sup>th</sup> Feb
B. Software and system security (Part Two)	11 <sup>th</sup> March (#5)
C. Management issues (Part Three)	4 <sup>th</sup> March (#4) 18 <sup>th</sup> March 25 <sup>th</sup> March
D. Network security (Part Five)	1 <sup>st</sup> April 8 <sup>th</sup> April

Case: Petya  
Chapter 6: Malware

# Exam questions (see list on moodle)

Q1: In the NotPetya attack, how was encryption used?

Q2: Following the NotPetya attack, what were the management lessons?

Q3: “Hybrid encryption model” of ransomware (Johannes)

Q4: Taxonomy of ransomware (Niels)

Q5: Advantages and disadvantages of biometric authentication

Q6: Privacy issues of digital passports. “Basic access control” and “Extended access control” in EUs standard.

# Plan for today



The Petya attack (NJ)

Taxonomy of ransomware (Niels)

Malware (Chapter 6) (NJ)

Asymmetric encryption (Chapter 2.3) (NJ)

“Hybrid encryption model” of ransomware (Johannes)

Introduction to course day #3

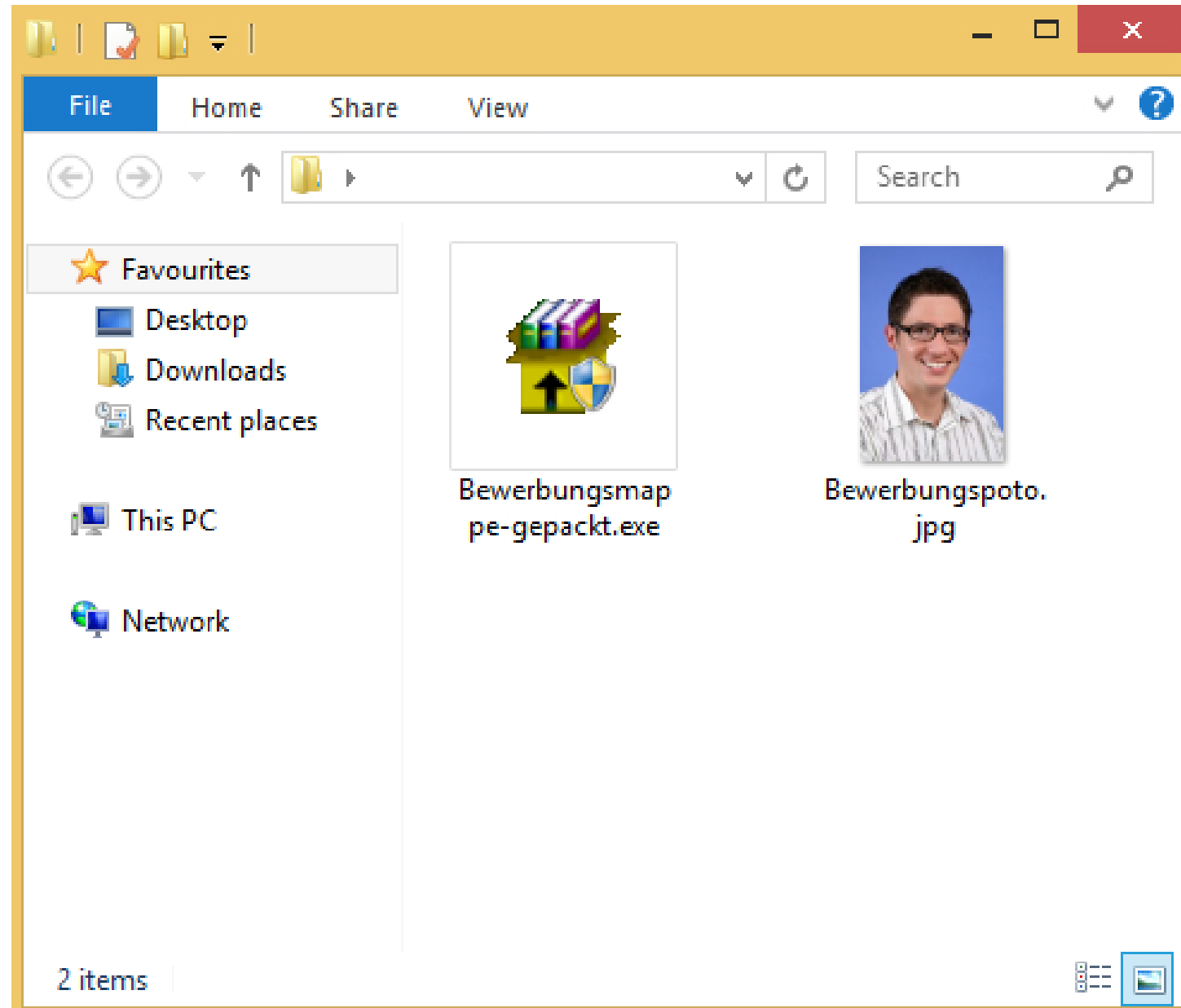
# Petya

Began in Germany,  
in March, 2016.

A email with a dropbox-  
link

- pretending to be a job  
application

At dropbox,  
the user was asked to  
download + execute  
“Bewerbungsmappe.  
gepackt.exe”



# Petya

If the user granted the malware administrator privileges, the malware would reboot the system.

After some steps,  
a ransomware screen  
was shown



The NotPetya screen (2017)  
resembled the Petya-screen

You became victim of the PETYA RANSOMWARE!

The haddisks 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/GFCsUs>  
<http://petya5koahtsf7sv.onion/GFCsUs>

3. Enter your personal decryption code there:

3bPCQ7-cU6Ca j-v5GAP8-GvsHr5-9yb6fF-9cfffN-Nz4czH-qxvsSy-42PyLG-YxTFxz-Yput66-gBXo79-XyZU9m-r9B8tu-K33KZU

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

Key: \_

Ooops, 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 [w0wsmith123456@posteo.net](mailto:w0wsmith123456@posteo.net). Your personal installation key:

74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

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

Key: \_

# Petya - actual ransomware

Petya encrypted files on the host

- message on screen claimed all files were encrypted
- according to Malwarebytes.com, only the Master File Table was encrypted

URL: [blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/](http://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/)

Petya was actual ransomware

- decryption was possible
- some users paid ransom and received decryption key
- later a free tool for decryption was made available
  - exploited a weakness in Petya

How much ransom was paid?

- I can't determine
- probably millions of USD

# Master File Table

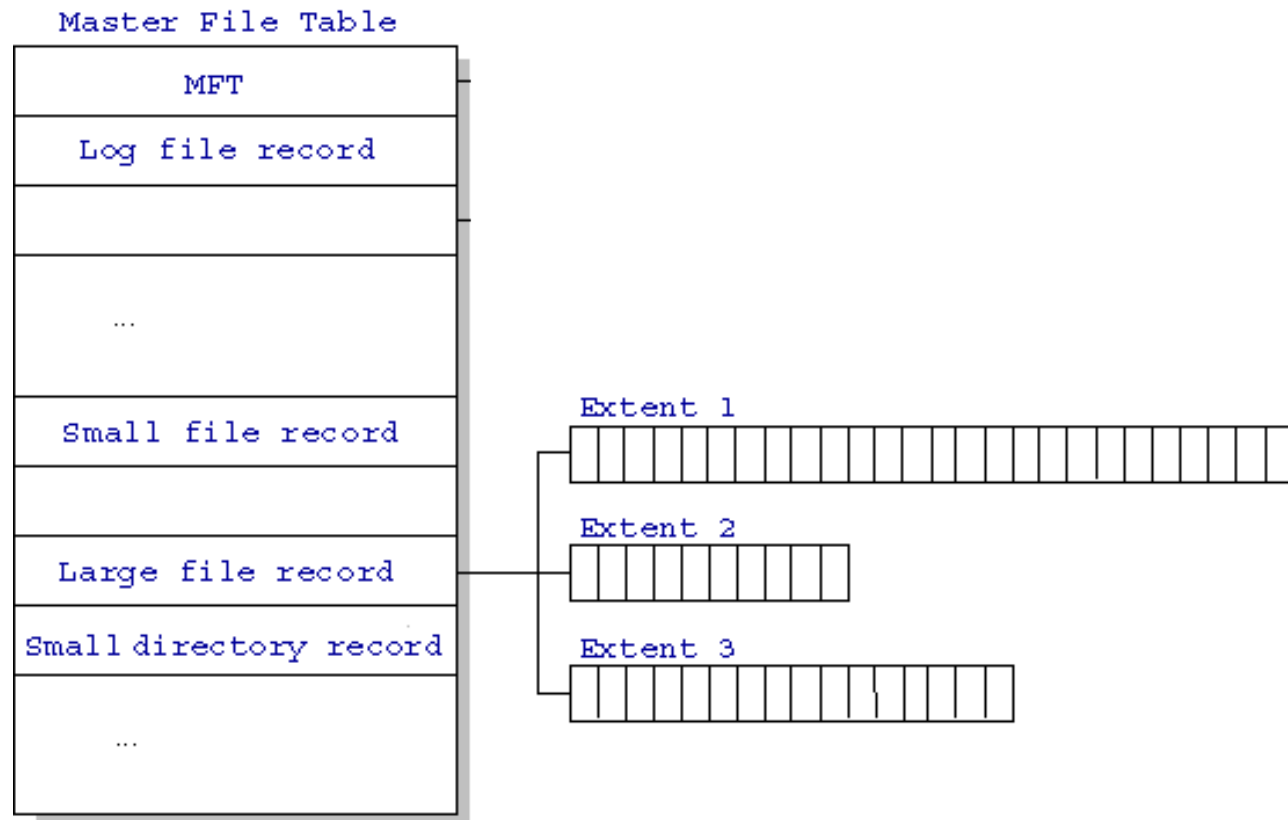
The Master File Table is a special feature of NTFS.

NTFS is the filesystem of Windows NT, 2000 and XP

- most recent release (XP) in 2008

The file table

- very, very big
- contains metadata about all files
- their names, sizes, binary addresses,...
- also contains all small files

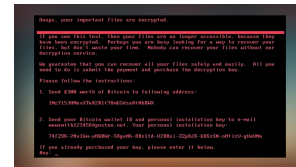




# Petya family of attacks

All members of Petya family

- encrypted Master File Table
- forced a reboot, then executed malicious code, inserted into Master Boot Record, to do the encryption
- displayed ransom message
- similarities suggest code reuse



NotPetya (sometimes also called Petya)

- June 2017
- *pretended to be ransomware*
- but merely destructive
- no published method for recovery
- spread using “Eternal Blue”
  - a vulnerability in MS SMB (Server Message Block protocol)
  - Eternal Blue also used in WannaCry
- also used other propagation methods
- suspicion (not proof) of Russian hackers

Petya

- March 2016
- actual ransomware
- no published suspects
- spread via email pretending to be job application



# Plan for today



The Petya attack (NJ)

Taxonomy of ransomware (Niels)

Malware (Chapter 6) (NJ)

Asymmetric encryption (Chapter 2.3) (NJ)

“Hybrid encryption model” of ransomware (Johannes)

Introduction to course day #3

# A Key-Management-Based Taxonomy for Ransomware

## Category 1

- No actual encryption (fake scareware)
- Demanded ransom before encryption

## Category 2

- Decryption essentials extracted from binary
- Derived encryption key predicted
- Same key used for each infection instance
- Encryption circumvented  
(decryption possible without key)
- File restoration possible  
using Shadow Volume Copies

## Category 3

- Key recovered from file system or memory
- Due diligence prevented ransomware  
from acquiring key
- Click-and-run decryptor exists
- Kill switch exists outside of attacker's control

## Category 4

- Decryption key recovered from a C&C server  
or network communications
- Custom encryption algorithm used

## Category 5

- Decryption key recovered under  
specialized lab setting
- Small subset of files left unencrypted

## Category 6

- Encryption model is seemingly flawless

### WannaCry

- now 3, due to “kill switch” “iudger.....com”
- killed/stops when domain name registered
- so taxonomy considers overall effectiveness,  
not only crypto-potency?

### Petya (first 5-6, then 4)

### Crucial characteristics of Category 6 include:

- unique encryption key for each victim
- so a victim doesn't pass it on to other victims

# Plan for today

The Petya attack (NJ)

Taxonomy of ransomware (Niels)



Malware (Chapter 6) (NJ)

Asymmetric encryption (Chapter 2.3) (NJ)

“Hybrid encryption model” of ransomware (Johannes)

Introduction to course day #3

# Malware

Key concepts include

- viruses, worms, Trojan horses, botnets, denial of service, backdoors, rootkits, ..

Learning goal

- understand the “broad picture” and the terminology
- understand main characteristics of each major type of malware

# Malware is software

X-ware

- software, hardware, middleware, freeware, shareware, ..

*Mal*-ware is the software part of an attack

The non-software part

- launching, eg., dropping an infected USB stick in a parking lot
- social engineering
  - calling, pretending to be it-staffer in need of user's password

# Malware definition (6.1)

Stallings & Brown (NIST)

*“a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim”.*

So this definition

- defines malware as a kind of software (not hardware)
- refers to the CIA goals
- also covers other goals/services (*“otherwise annoying or disrupting..”*)

Exercise:

*Is Petya malware? (according to this definition)*

*NotPetya?*

*If so, which CIA goals were compromised? which other goals?*

# Exercise - answer

Petya: no

NotPetya: yes

Stallings & Brown (NIST), extended **so as to account for ransomware:**

*“a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim, **or with the intent of obtaining a ransom payment in return for reestablishing the system.**”*



# Malware concepts

## Payload

- corruption, zombies, bots, spyware, backdoors, rootkits

*A malware's payload*

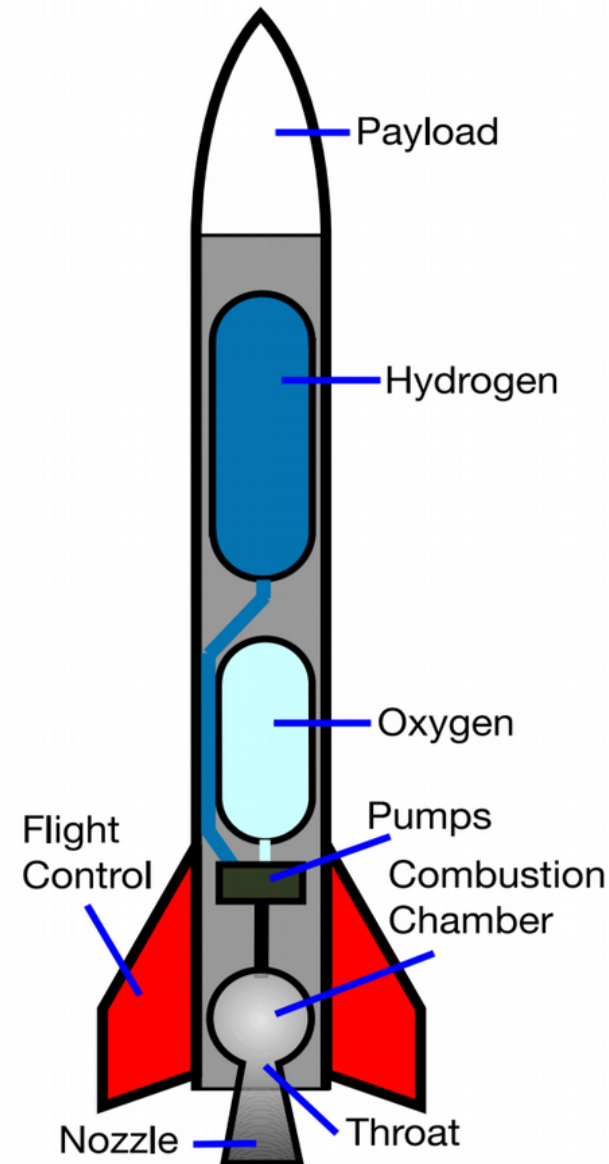
- *is impact on the computer*

## Propagation

- viruses, worms, Trojans, spam e-mail

*A malware's propagation method*

- *how it spreads to other computers*



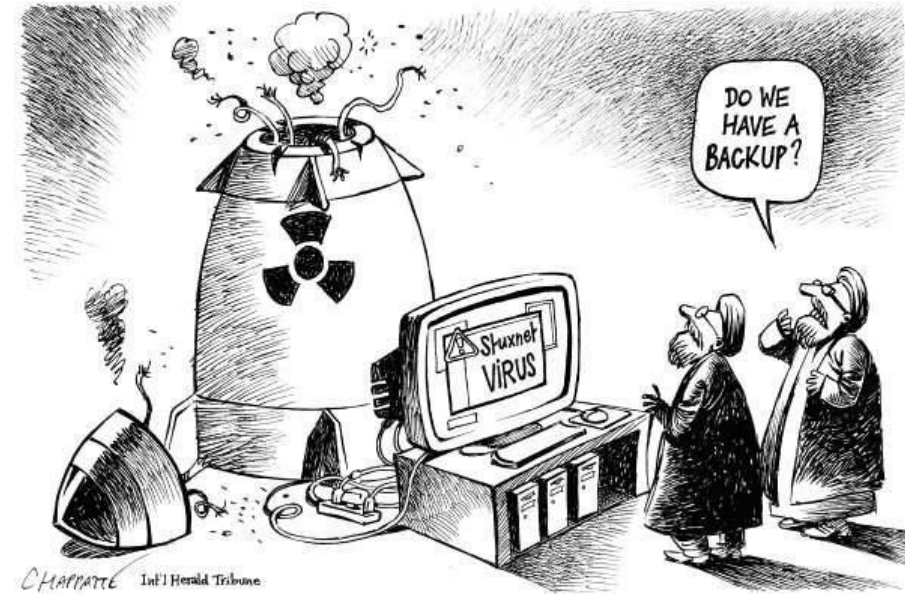
# APT

## Advanced Persistent Threat (6.2)

### Stuxnet (2009-2010)

- an attack on Iran's uranium-enrichment production facilities
  - for nuclear power plants and/or nuclear bombs
- infected industrial plants in other countries as well
- infected "SCADA" systems (Siemens)
- SCADA control specific hardware used in production systems
- infection method included USB sticks
- possibly developed and organized by US and Israeli agencies/groups

Stallings/Brown: Stuxnet is a worm (p221)



### *Advanced*

- *technology, organization*

### *Persistent*

- *long-time effort*

### *Political/military intent*

# Melissa macro virus (1999) (6.3)

```
macro Document_Open
  disable Macro menu and some macro security features
  if called from a user document
    copy macro code into Normal template file
  else
    copy macro code into user document being opened
  end if
  if registry key "Melissa" not present
    if Outlook is email client
      for first 50 addresses in address book
        send email to that address
        with currently infected document attached
      end for
    end if
    create registry key "Melissa"
  end if
  if minute in hour equals day of month
    insert text into document being opened
  end if
end macro
```

*"twenty-two, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."*

Pseudo-code (Figure 6.1)

MS Word macro. Executed when a document is opened.

# Propagation: viruses

Software that *attaches itself to a program, or to a data file containing a program*

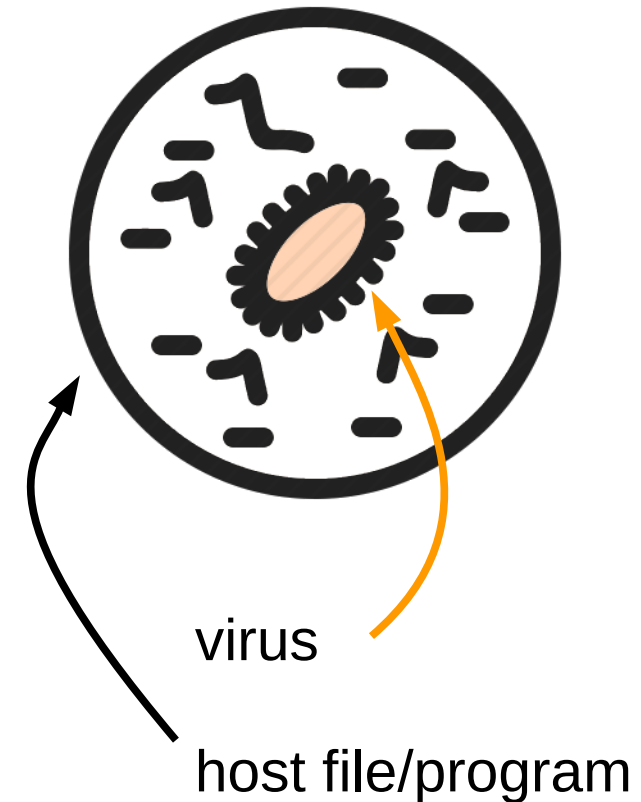
- macros in Excell spreadsheets or Word text documents
- see Stallings & Brown's definition, p210, first line of Section 6.3.

Propagation to new computer

- often via email
- *user does not suspect the "host" file*

Propagation inside computer

- copies itself
- eg., to other spreadsheet files
- inherets privileges from host
  - eg., file access rights



- don't open/click on spreadsheets received by email
- allow only macros to execute if signed by trusted users
- scan macros with anti-virus scanner
- judgement, training

# The Morris worm (1988) (6.4)

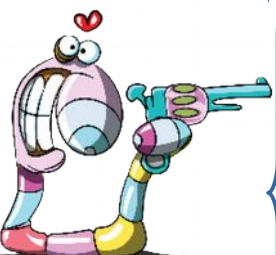
Infected computer #n



Infected computer #n+1



Propagation method #1:



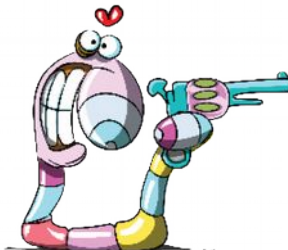
Select user name;  
guess password;  
Send “bootstrap program”;  
Execute bootstrap  
program on #n+1;  
logout.

login

Bootstrap  
program

Bootstrap program  
downloads worm from #n  
Then executes worm  
(bootstrap program ends)

logout



# Worms

A worm is a stand-alone program

- as opposed to a virus which attaches itself to another program

NotPetya is a worm

State-of-the-art “Worm technology” (Stallings & Brown, p222)

- multiplatform
- multiexploit
- polymorphic
- metamorphic

Exercise:

- explain each of the four features of state-of-the-art worm techn.
- which feature applies to Petya and NotPetya

# Worms - exercise answers

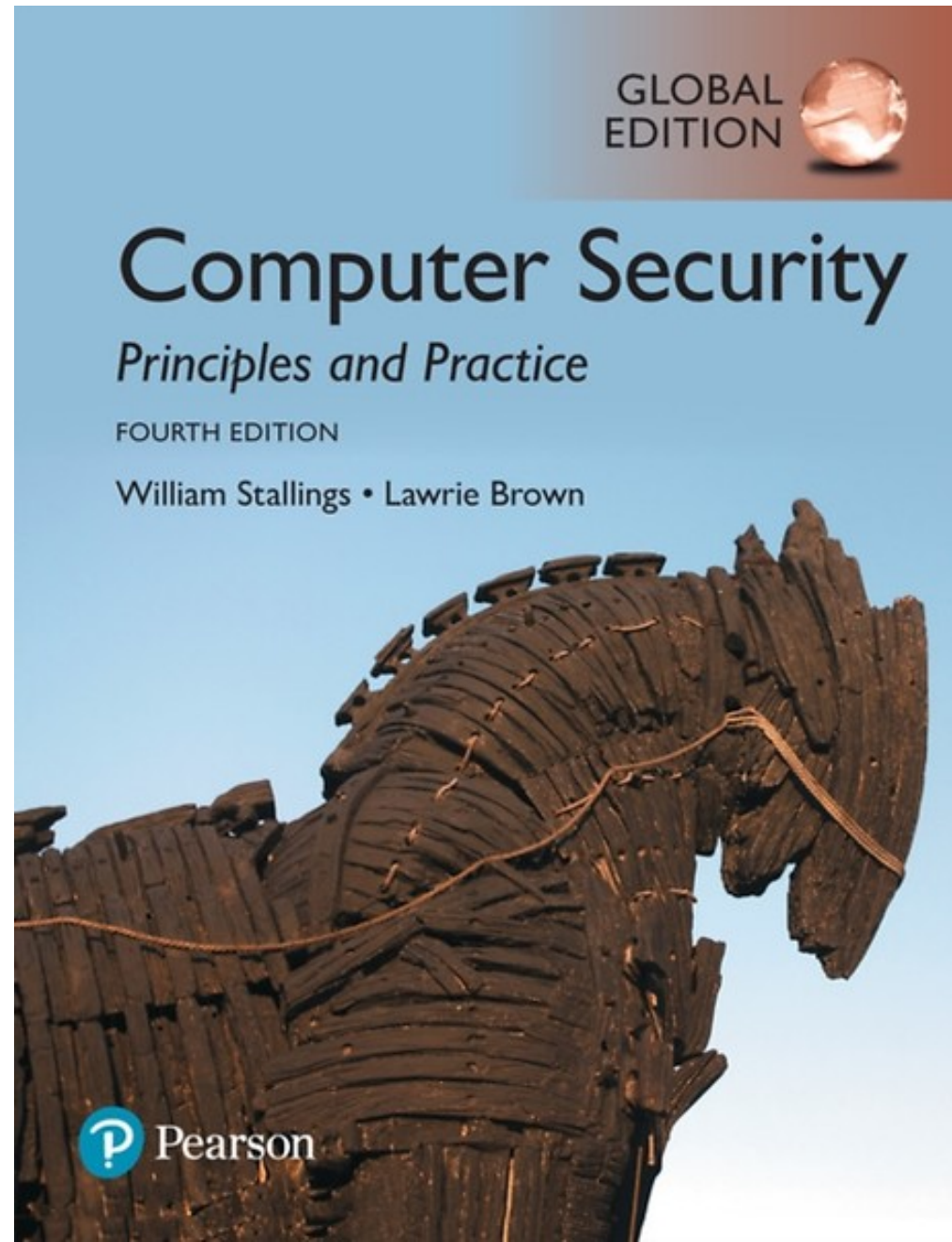
“Worm technology” state of the art (Stallings & Brown, p222)

- multiplatform
  - targets Mac, Unix in addition to Windows (none of Petya/NotPetya)
- multiexploit
  - exploits multiple vulnerabilities (NotPetya)
- polymorphic
  - modifies itself, using different code to obtain the same effect (none)
- metamorphic
  - changes behavior over time (none)



# Trojan Horse (6.5)

- eg., a fake anti-virus scanner
- appears useful (actually useful, or pretending)
- mobile Trojans
  - may be distributed via plain app download for iPhones or Android phones





# Payload: bots (6.7)

Bot (robot)

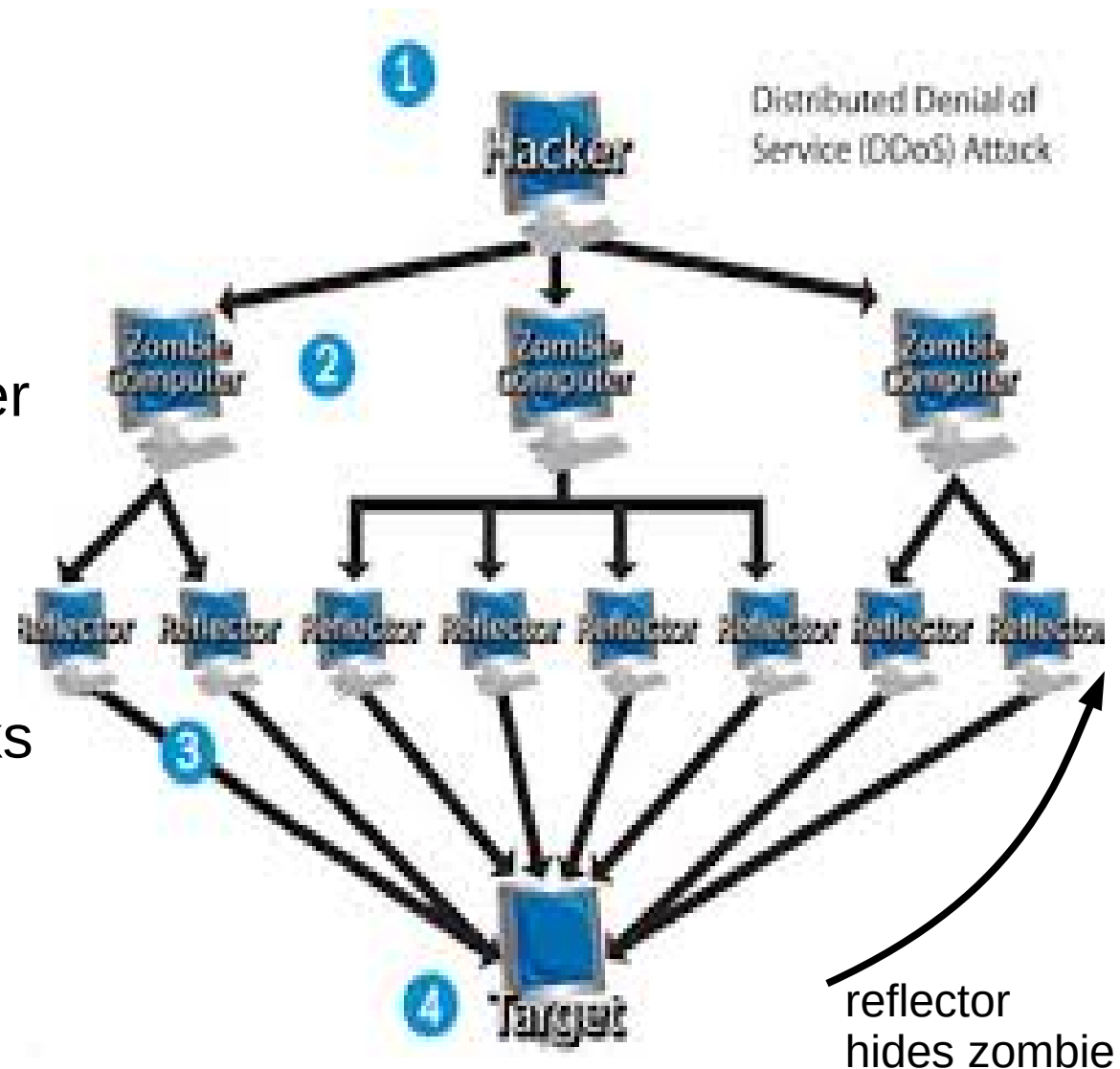
- “zombie”
- computer taken over by hacker
- though may still be usable by owner

A bot can be used for

- DOS (denial of service) attacks
- spam email
- remotely controlled

So a bot is also a method of propagation

- not merely a payload

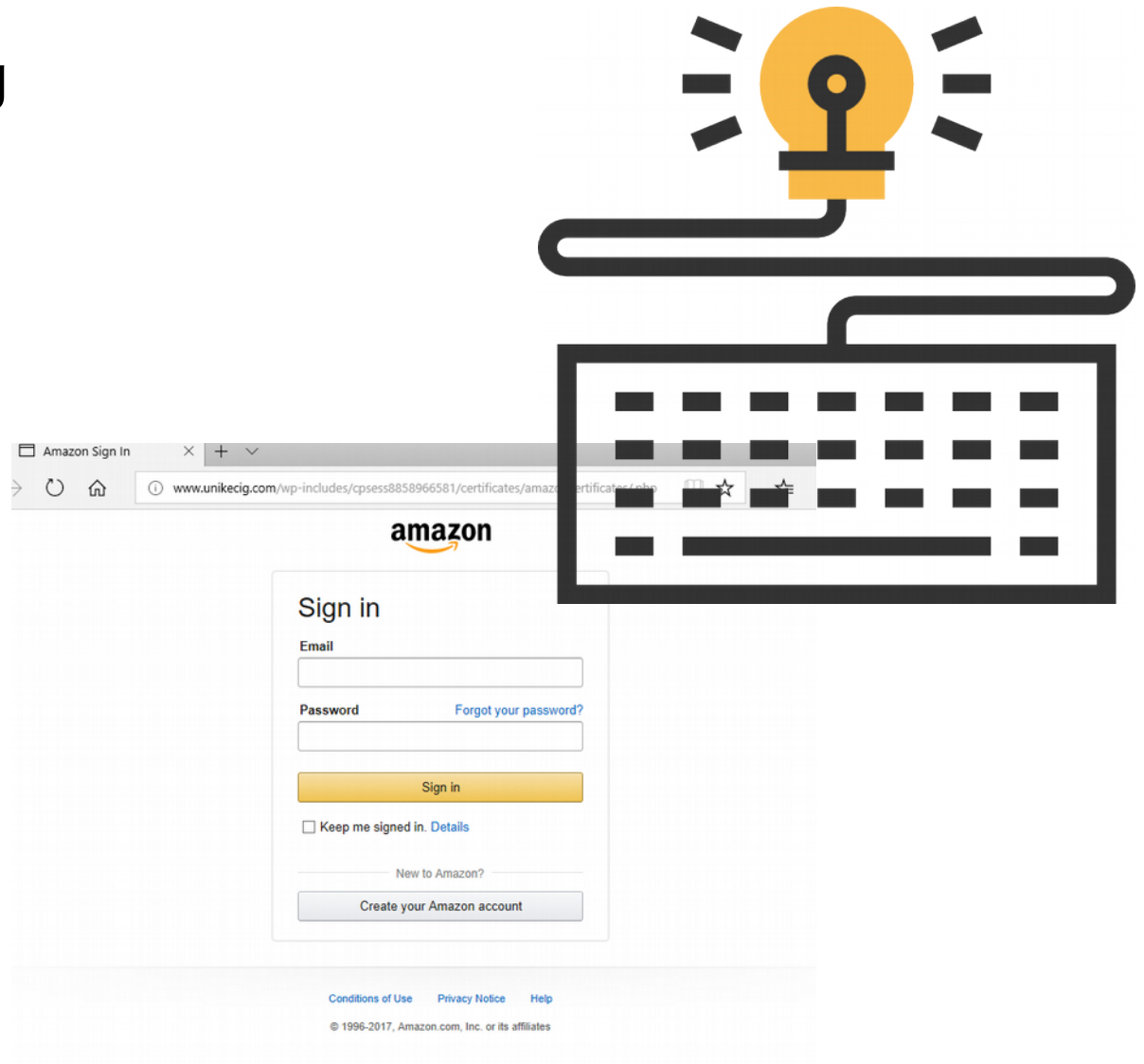


# Payload: theft (6.8)

Theft of data such as passwords or business secrets

Passwords obtained using

- keyloggers
- phishing



# Payload: backdoors and rootkits (6.8)

## Backdoor

- inserted by developer
- bypasses normal access controls

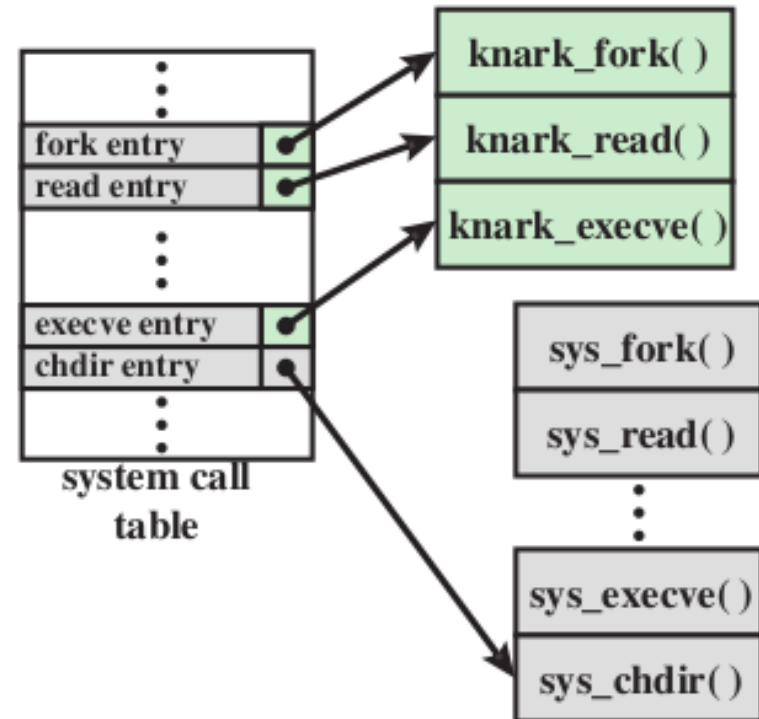


## Backdoor: E-shop for books

- sends prices, contents,.. when user asks for book
- if hacker/user asks for fake book
  - eg., “Hack me” by V. Ictim
- then software sends credit card numbers

## Rootkit

- malware with root/administrator privileges
- not revealed by listing processes or files
- changes operating system's system calls
- gives attacker control over computer



# Exercises

See Stallings & Brown, p 243.

Review questions

- 6.6
- 6.8
- 6.11

Problems

- 6.10

# Exercise answers

## Review questions

- 6.6
  - Worm: Program; standalone; (self-)replicating
  - Zombie: Computer; contains bot/malware; bot “sleeps”, remote controlled, for targetting other computers
- 6.8
  - Drive-by-download: spreads from webserver to browser during visit, exploiting weaknesses in browser plugins (eg. Java, Flash Player)
  - Worm: see 6.6.
- 6.11
  - backdoor: a second, hidden entry;
  - bot: see 6.6
  - keylogger: senses keystrokes and sends them to remote computer
  - spyware: general term, includes keylogger, also software that reads passwords, usernames, webaddresses etc.

# Exercise answers

## Problems

- 6.10

## Type of malware:

- Trojan Horse (apparently useful)
- Malvertising (malicious + advertising)
  - send positive product reviews to your friends
- Ransomware (delete files from phone; send ransom message to friends)
- ..

## Type of threat:

- a threat to your privacy (confidentiality)
- a threat to your normal use of the mobile (availability)
- ..

# Countermeasures: on host (6.10)

An anti-virus program is run on the host computer

- 1<sup>st</sup> generation:
  - scanned for viruses
  - scanned files for “signatures” (bit patterns) of known malware
- 2<sup>nd</sup> generation:
  - check hashvalues to determine if programs have been altered
- 3<sup>rd</sup> generation:
  - monitor activities (rather than files)
- 4<sup>th</sup> generation:
  - combination of many approaches



Sandbox analysis is conducted on a protected computer

- experimental approach
- observe *behavior* of suspected software
- made difficult by dormant malware (“time bombs”)



# Countermeasures: on perimeter

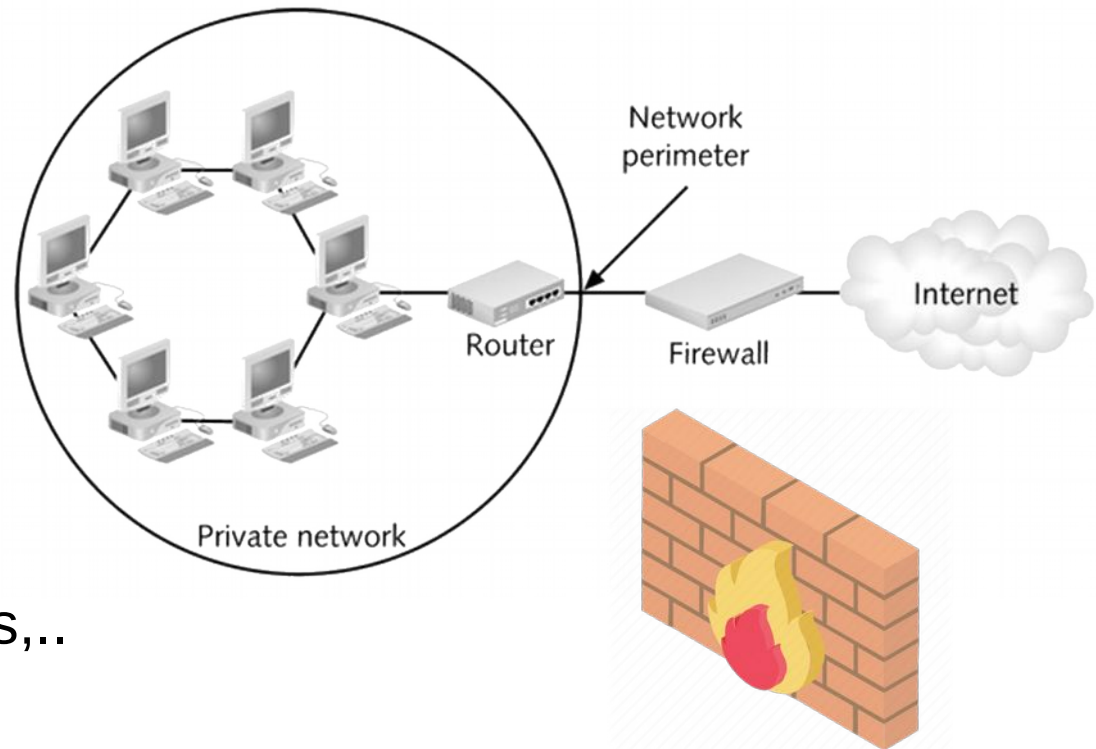
## On the perimeter

### Ingress monitoring, filtering

- incoming network traffic
- spam
- dos attacks
- ..

### Egress monitoring, filtering

- outgoing network traffic
- signs of worms, network scanners,..
- ..





# Plan for today

The Petya attack (NJ)

Taxonomy of ransomware (Niels)

Malware (Chapter 6) (NJ)

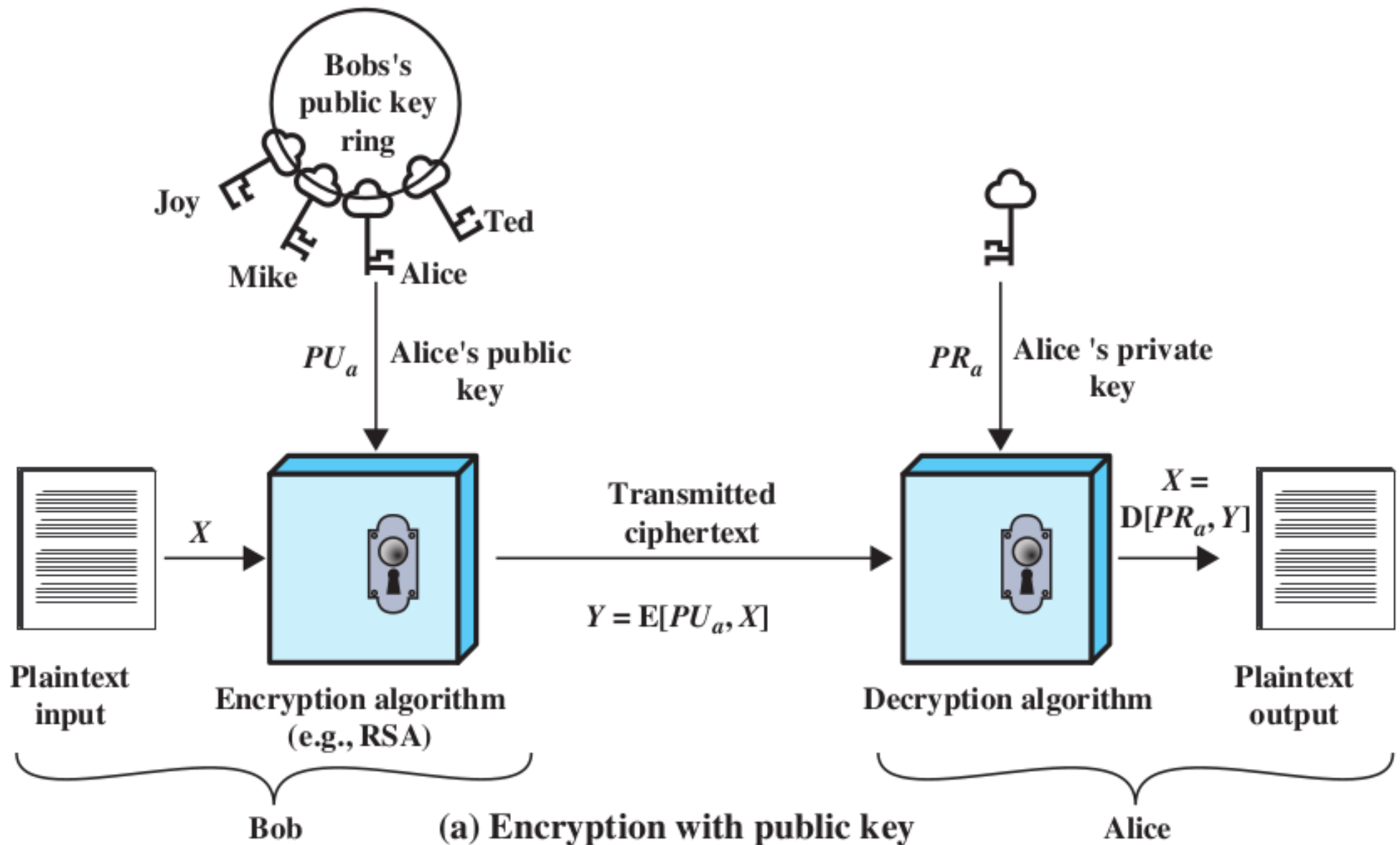


Asymmetric encryption (Chapter 2.3) (NJ)

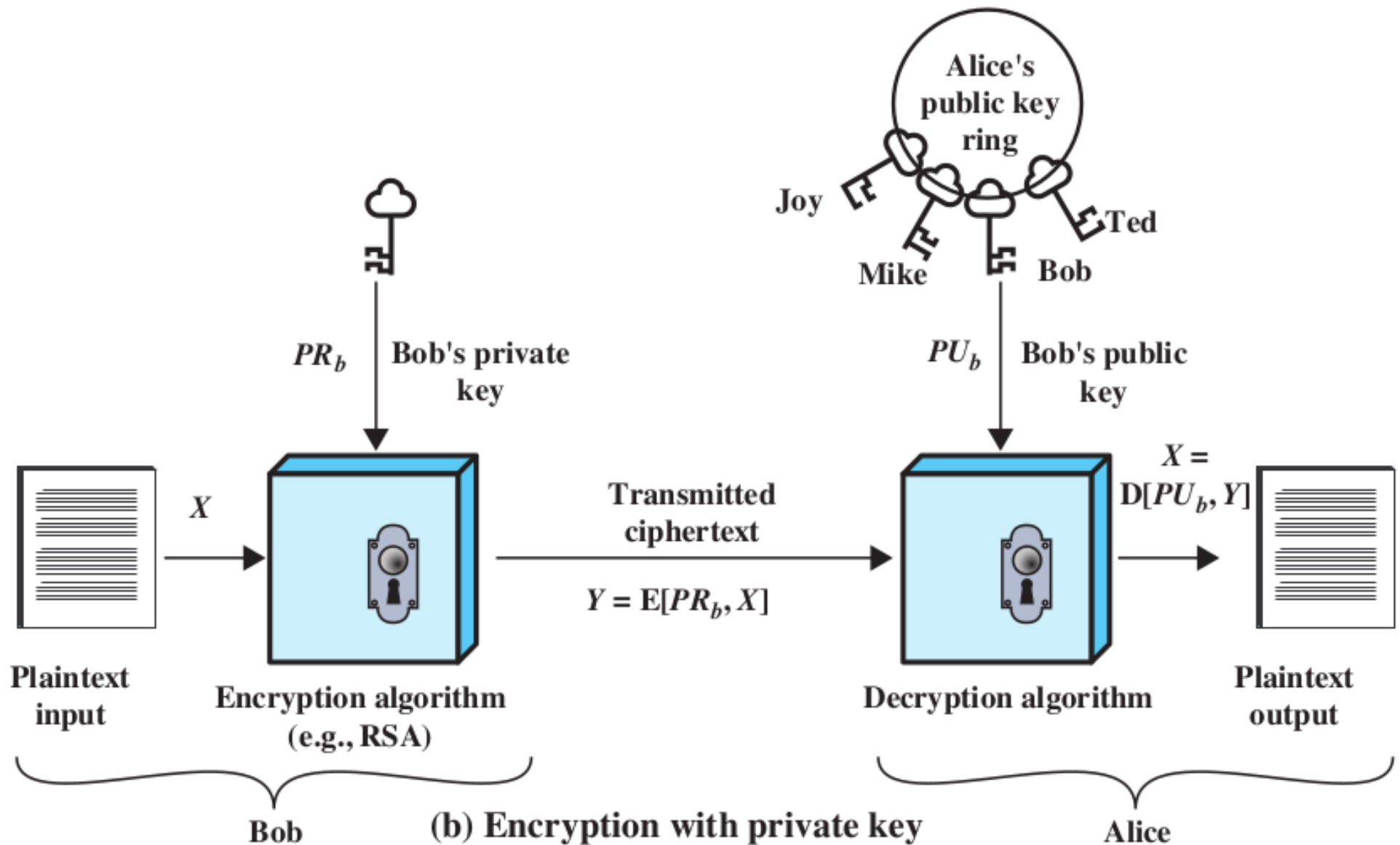
“Hybrid encryption model” of ransomware (Johannes)

Introduction to course day #3

# Figure 6a



# Figure 6b



# 6a versus 6b

In both cases, the ciphertext Y

- is encrypted
- so cannot be read, except if decrypted

In Figure 6a:

- Y could have been encrypted by anyone (since Bob's public is ... public)
- Y can only be decrypted by Alice (using Alice's private key)

In Figure 6b:

- Y must have been encrypted by Bob (using Bob's private key)
- Y can be decrypted by anyone (since Bob's public key is .. public)

# Exercise

(1) Provide a reason that

- $X = D[PR_a, Y]$  (Figure 6a)
- $X = D[PU_b, Y]$  (Figure 6b)

(X is the original plaintext)

(2) Suppose you, Bob, are designing ransomware to encrypt files on Alice's computer, using a randomly generated symmetric key, K.

Suppose you want the ransomware on Alice's computer to send K to you, in an encrypted form, so that neither Alice nor anybody else can read K (except you).

For encrypting K, would you use:

- $PR_a$
- $PU_a$
- $PR_b$
- $PU_b$

# Exercise answers

(1) Provide a reason that

- $X = D[PR_a, Y]$  (Figure 6a)
- $X = D[PU_b, Y]$  (Figure 6b)

Note that  $X$  is the original plaintext.

Stated informally, the reason is that a pair of keys (a corresponding public and private key) can be used for decrypting an encrypted message.

The equation  $X = D[PR_a, Y]$  (Figure 6a) relies on requirement 3 (p 70), since if one replaces  $Y$  by  $E[PU_a, X]$ , one obtains  $X = D[PR_a, E(PU_a, X)]$ , which is the same as requirement 3 (except that it is stated for  $a$ /Alice), so we may conclude the equation holds.

The equation from Figure 6b relies on requirement 6 (p 71), which says that given a pair of public and private keys, one may interchange their roles, that is, either one may be used for encryption as long as the other is used for decryption.

# Exercise answers

(2) Suppose you, Bob, are designing ransomware to encrypt files on Alice's computer, using a randomly generated symmetric key,  $K$ .

Suppose you want the ransomware on Alice's computer to send  $K$  to you, in an encrypted form, so that neither Alice nor anybody else can read  $K$  (except you).

For encrypting  $K$ , would you use:

- $PR_a$ 
  - no, because anybody could decrypt  $K$  using  $PU_a$
- $PU_a$ 
  - no, because it could only be decrypted using  $PR_a$
- $PR_b$ 
  - no, because anybody could decrypt  $K$  using  $PU_b$
- $PU_b$ 
  - yes, because only you can decrypt  $K$  using  $PR_b$

# Plan for today

The Petya attack (NJ)

Taxonomy of ransomware (Niels)

Malware (Chapter 6) (NJ)

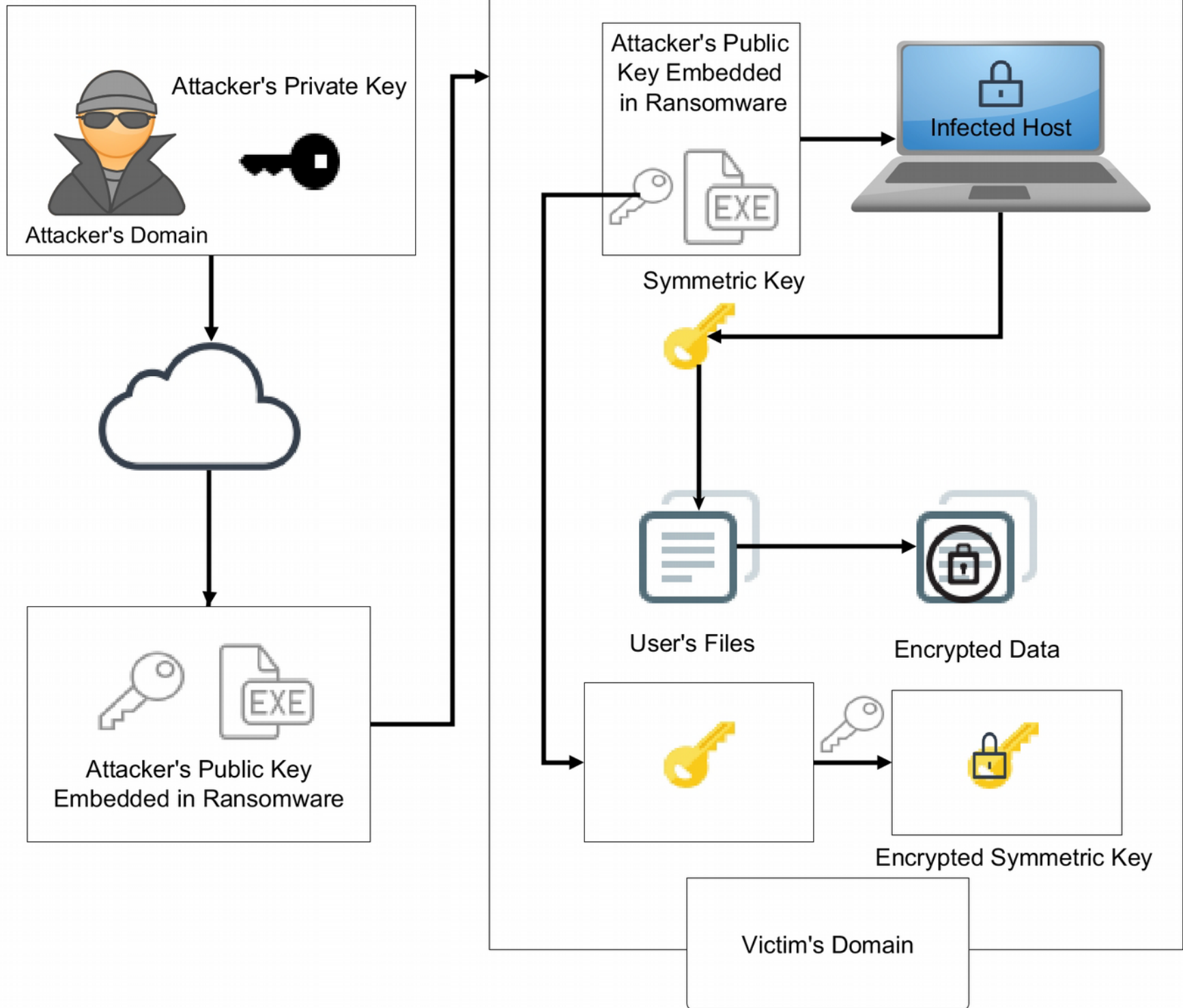
Asymmetric encryption (Chapter 2.3) (NJ)



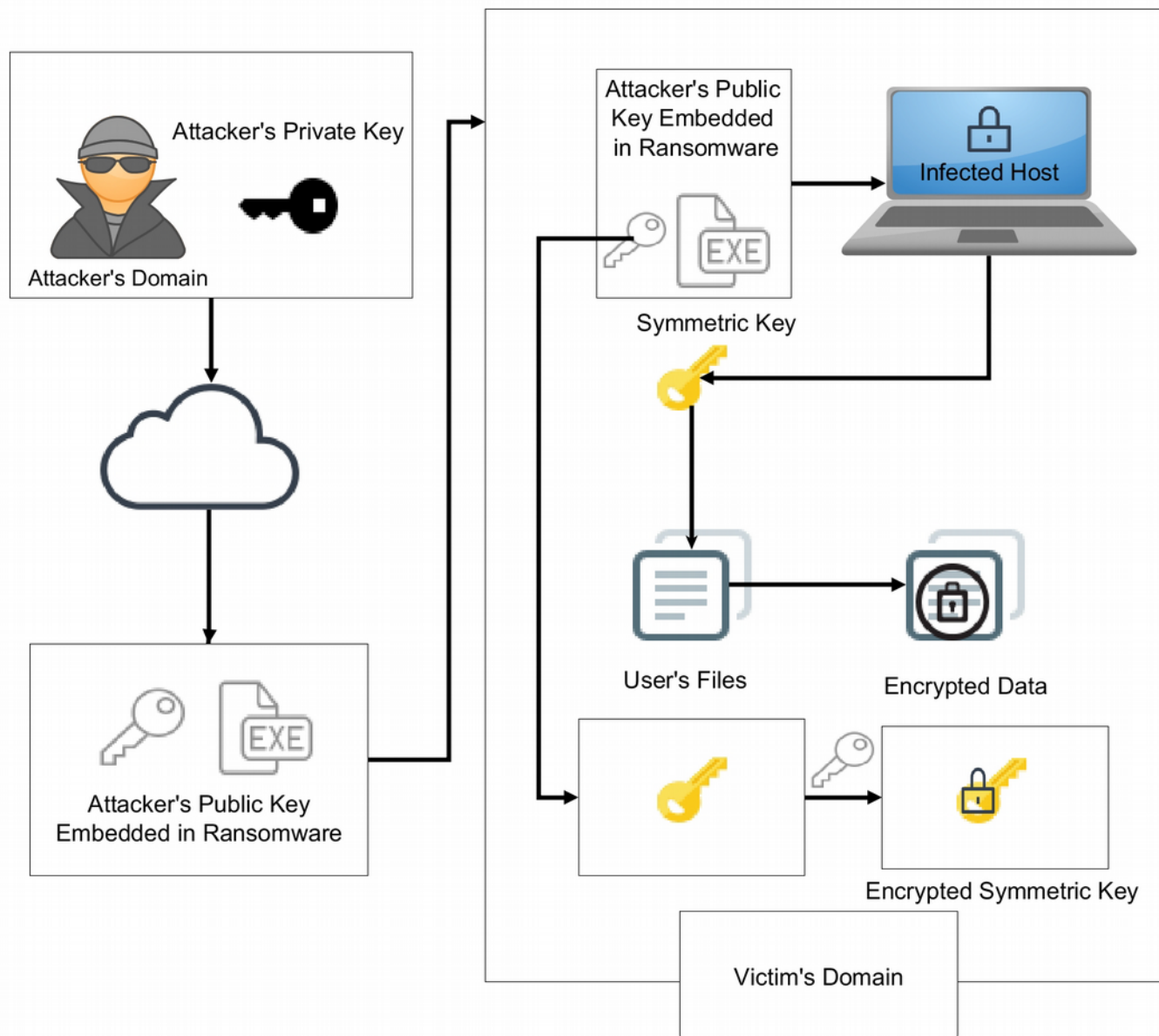
“Hybrid encryption model” of ransomware (Johannes)

Introduction to course day #3





# “Hybrid model”



## Communication:

1. Attacker sends/injects ransomware to victim.
2. Ransomware sends encrypted symmetric key from victim's computer to some public space, where attacker reads it anonymously.
3. Attacker decrypts key.
4. Attacker sends key to victim, via a C&C/bot

# Plan for today

The Petya attack (NJ)

Taxonomy of ransomware (Niels)

Malware (Chapter 6) (NJ)

Asymmetric encryption (Chapter 2.3) (NJ)

“Hybrid encryption model” of ransomware (Johannes)



Introduction to course day #3

# Digital passports

EU passports contain digital fingerprints

- in Denmark from 2012 onwards
- however, fingerprints not used

Governments want a method for establish authenticity of passport holder

- fingerprints preferred over photos
- prevent “look-alike” from using passport of other person



# February 25<sup>th</sup>: course day #3

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

Case: The EU digital passport.

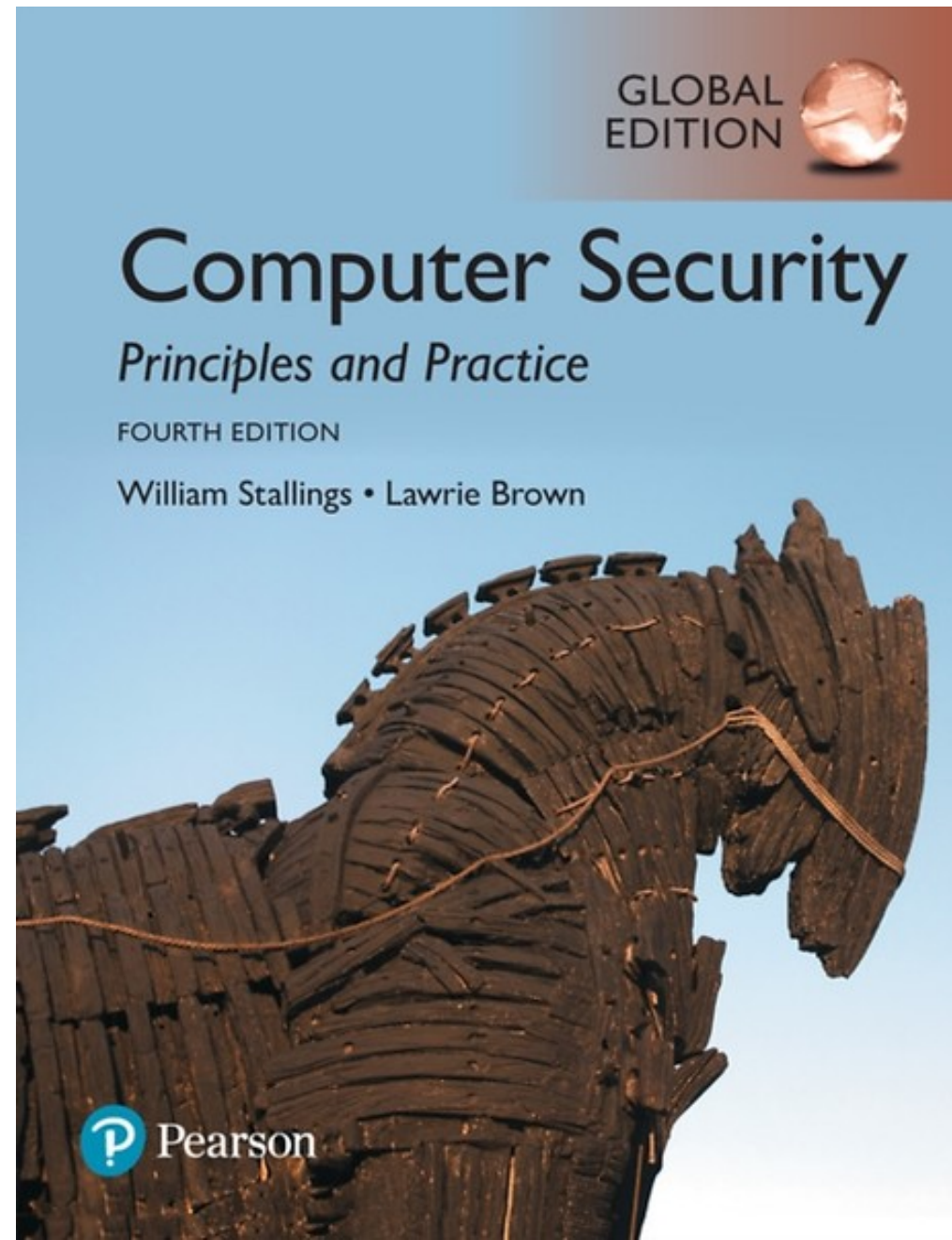
Digital signatures and user authentication.

Stallings & Brown

- Chapter 2 (2.4-2.7)
- Chapter 3 (3.1-3.6 + 3.8-3.9). (OK to read the section about the Bloom filter (p 102-104) extensively)
- Chapter 23 (only 23.2)

Additional literature:

- Jaap-Henk Hoepman et al. Crossing Borders. Security and privacy issues of the European e-Passport (2006).



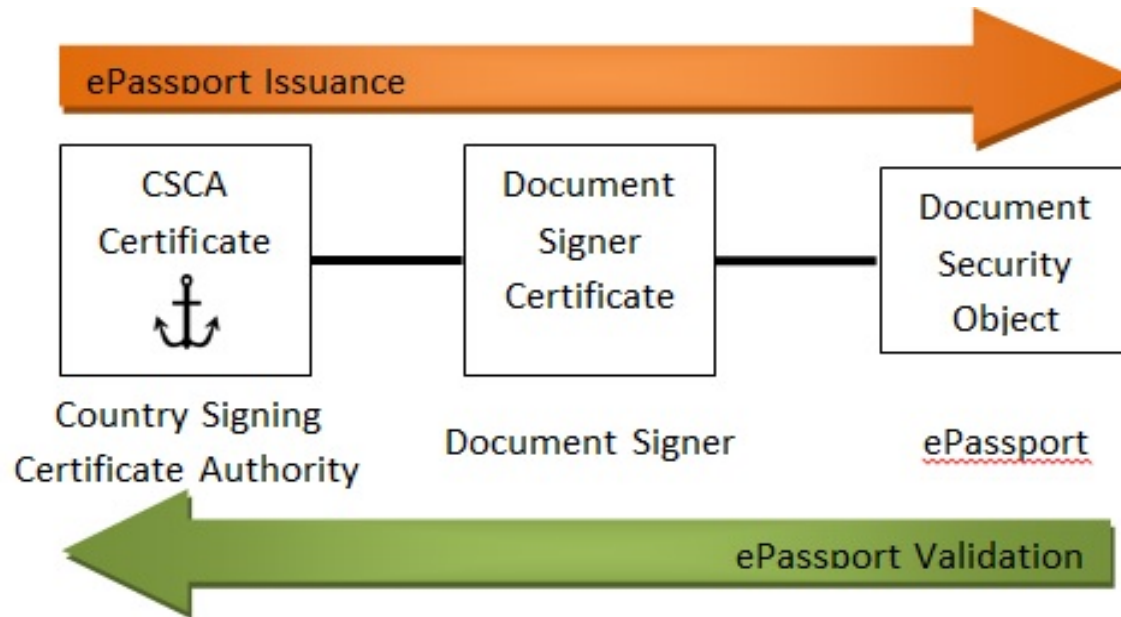
# Student presentations

## 25<sup>th</sup> February

Presentation 1. Explain digital signatures (using Figure 2.7) and digital certificates (using Figure 2.8).

Presentation 2. Based on Stallings & Brown (Section 3.4), what are the main advantages and disadvantages of biometric authentication?

# Tips for reading Hoepman et al: Crossing Borders



Citizens want: privacy of data

- “Basic Access Control”
  - terminal proves it has read MRZ (Machine Readable Zone)
- “Extended Access Control”
  - terminal’s certificate verified by passport