IT security

Monday 11th February
Course day #1

Introduction to the course
Theme A (i)

Case: The NotPetya attack

Chapter 1 + parts of Chapter 2

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

Plan for today

Welcome to the course ! (NJ)

The NotPetya case (NJ)

Chapter 1 (NCJ)

Chapter 2 (NJ)

Case revisited
- management aspects (NCJ)
- technical aspects (NJ)

IT security

Protection of IT infrastructure
- NotPetya attack (2017)
- Maersk lost 200-300 USD

Protection of privacy
- “Se og Hør” scandal (2016)

Four themes (A-D)

A. Computer security technology and principles

(Part One in Stallings & Brown)

B. Software and system security

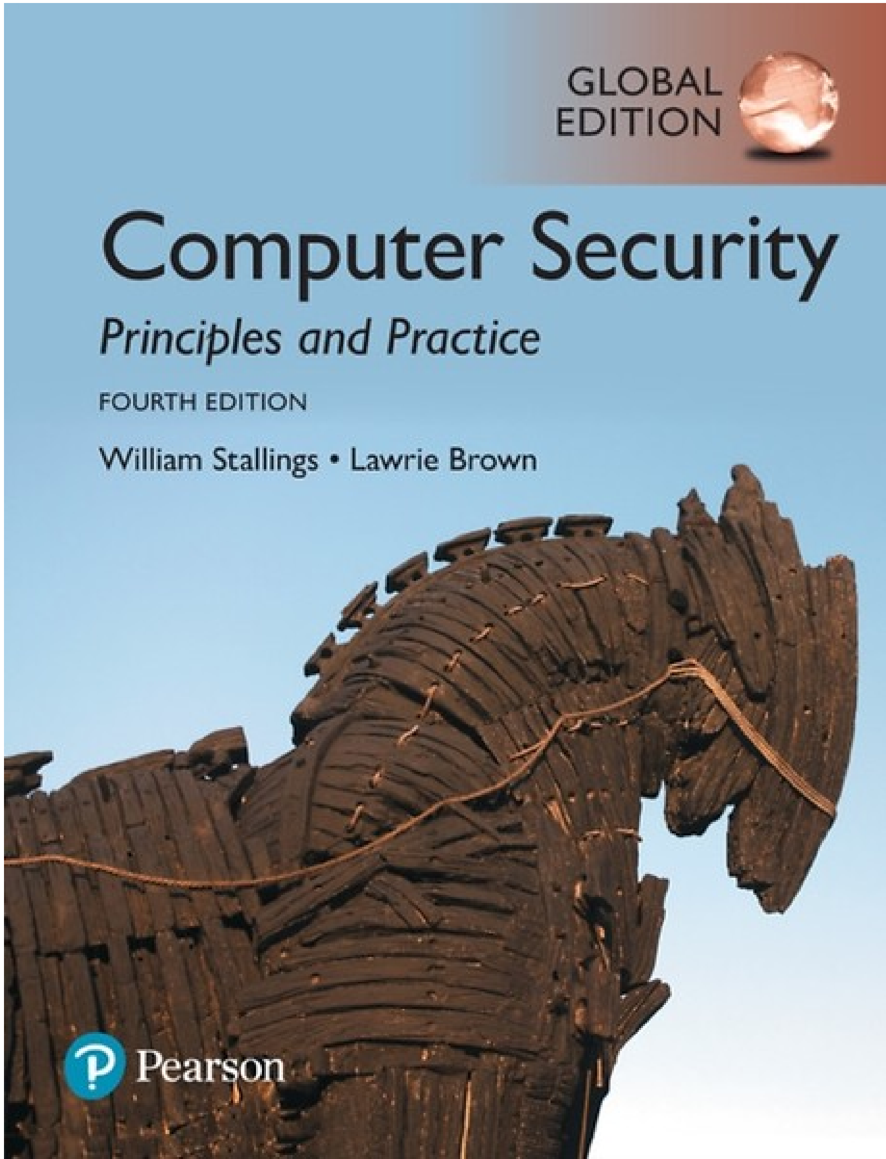
(Part Two)

C. Management issues

(Part Three)

D. Network security

(Part Five)



Course themes

A. Computer security technology and principles (Part One in Stallings & Brown)	- cryptography, user auth., viruses, worms, ..
B. Software and system security (Part Two)	- design to prevent .. - .. buffer overflow attacks, IoT attacks
C. Management issues (Part Three)	- implement routines and standards (GRPR, ISO 27000) - risk analysis - human resources, social engineering, ..
D. Network security (Part Five)	- cases - credit card systems, mobile payment, ..

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

“Anatomi” of secure software

Implement guidelines!

In-depth analysis of actual designs

Ten consecutive Mondays

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

Themes A-D covered

- in alphabetical order
- corresponding to Brown & Stallings

Except:

- course day #4 is "prematurely" about C

Course day 10

- topics defined later

Cases

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

- NotPetya
- Petya ransomware
- The EU digital passport

Example course day: Monday 18th Feb

Theme A: Computer security technology and principles (ii)

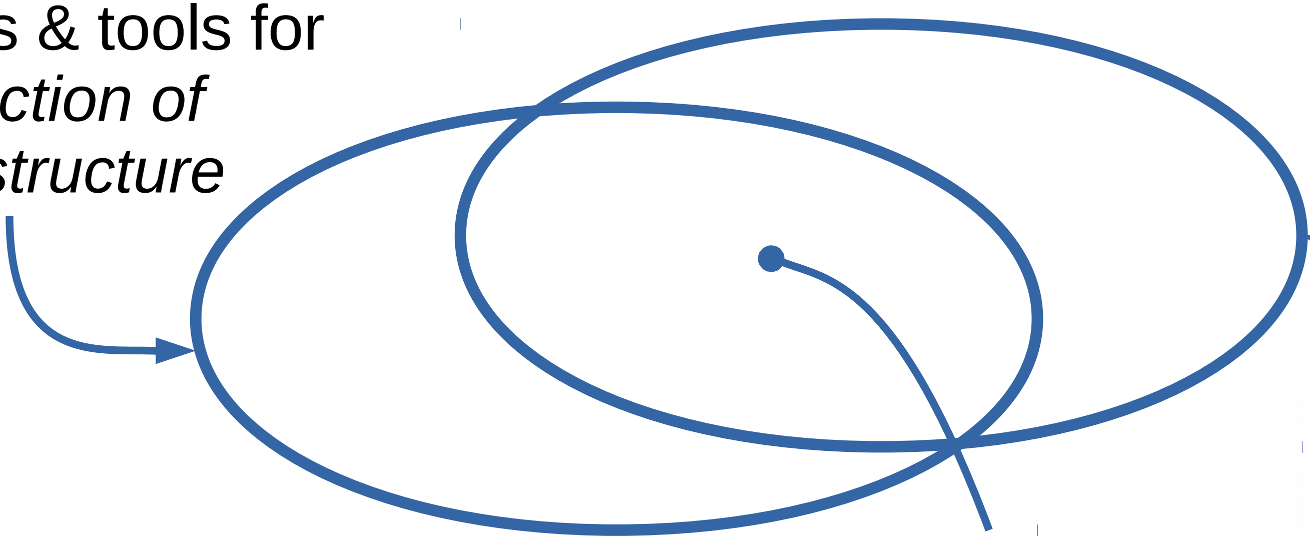
Case:
- Petya attack

Teacher presentation

Two short student presentations (5-10 minutes per presentation)

Exercises

Two types of security
- are they the same?



Goals & tools for *protection of infrastructure*

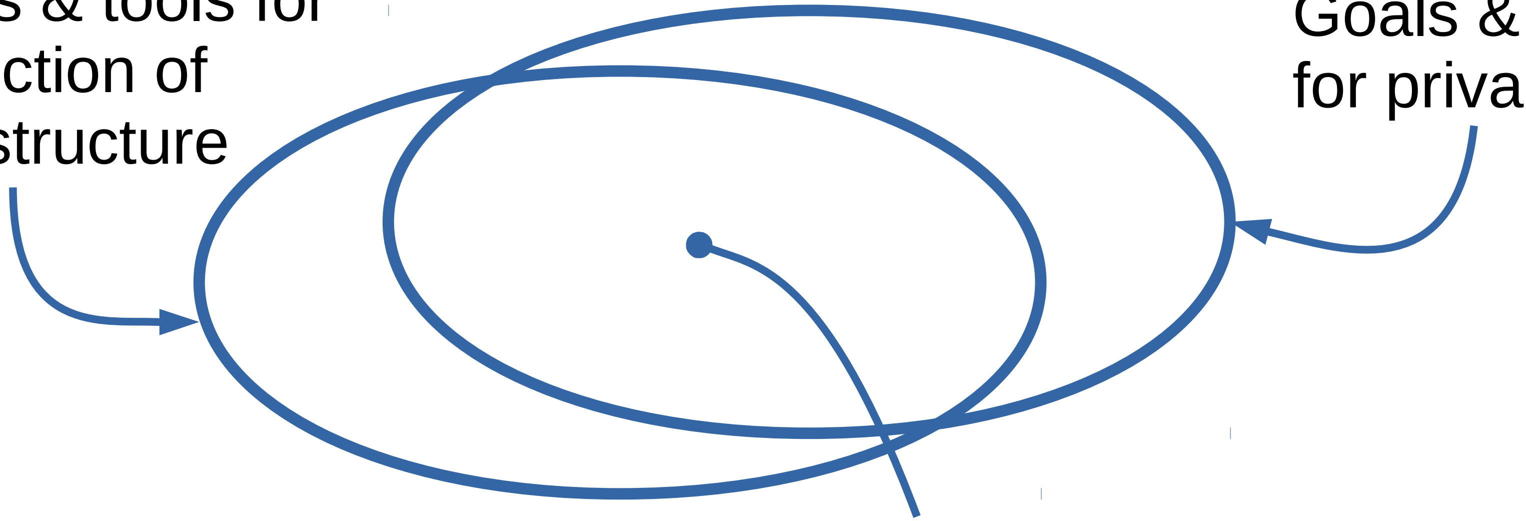
Goals & tools for *privacy*

Goals & tools that are shared

- confidentiality
- encryption

Exercise

1. Provide another example of a goal or tool.
2. What type of security is it? (privacy or protection of infrastructure or both?)



Goals & tools for protection of infrastructure

Goals & tools for privacy

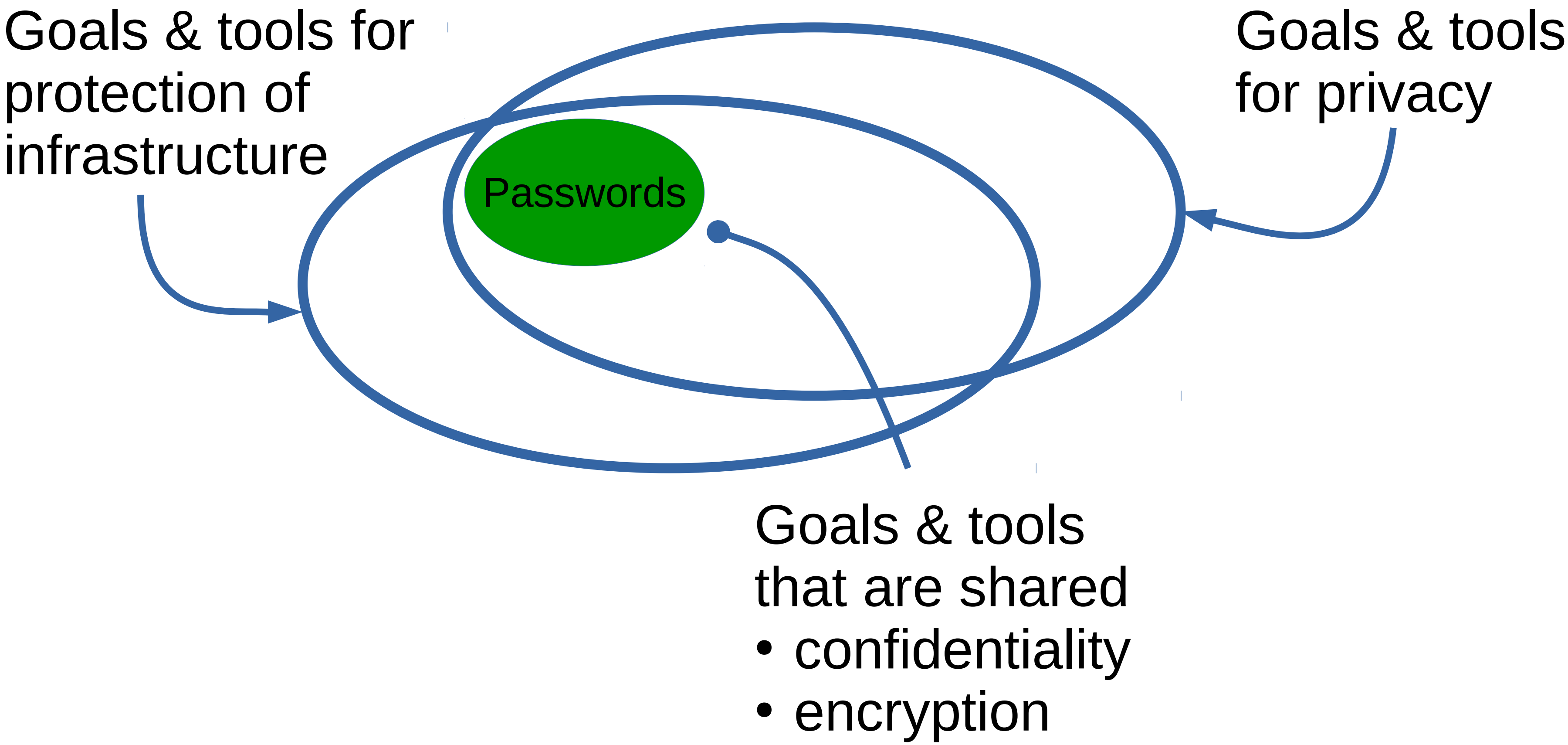
Goals & tools that are shared

- confidentiality
- encryption

Exercise - answer

1. Provide another example of a goals or a tool.
- *passwords for user-authentication*

2. What type of security is it?
- *both types (most are)*



Passwords

Goals & tools for protection of infrastructure

Goals & tools for privacy

Goals & tools that are shared
- confidentiality
- encryption

Stallings & Brown

Privacy is not prioritized

- privacy has seven pages
- section in “Legal and ethical aspects”

GDPR barely mentioned

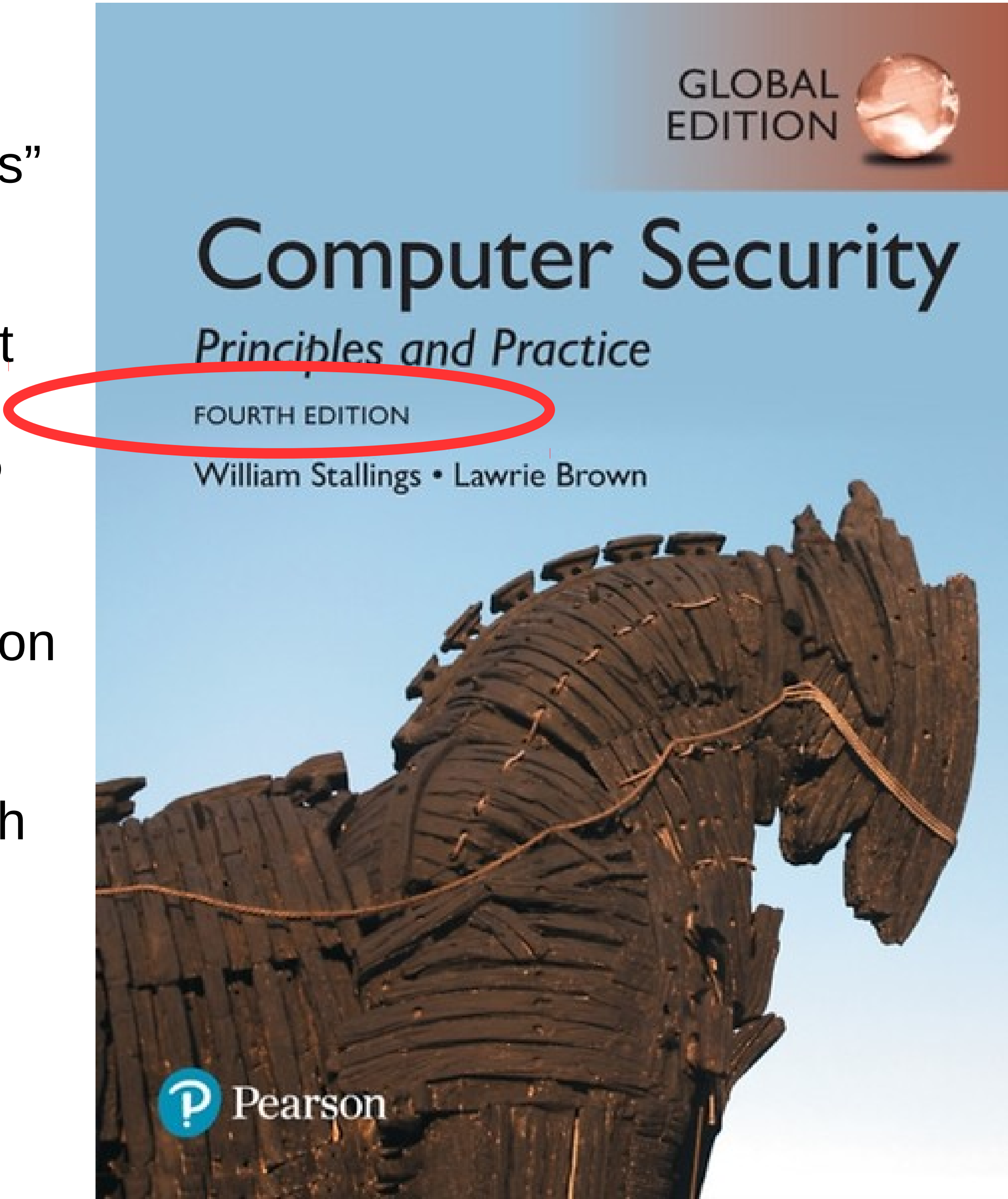
- no mention of the most recent, most important version
- = the version passed by EP in 2016

Assets

- privacy focus suggests more focus on data than hw+sw (p29)

Elements of an authoritarian approach

- attacks are seen as “illegal”, “unauthorized” (eg., p31)
- what about privacy violations authored by government or management?



Plan for today

Welcome to the course ! (NJ)

The NotPetya case (NJ)

Chapter 1 (NCJ)

Chapter 2 (NJ)

Case revisited
- management aspects (NCJ)
- technical aspects (NJ)

Later today:
- *Exam*
- *written assignment*
- *oral exam*

Two student presentations on course day #2

Plan for today

Welcome to the course ! (NJ)

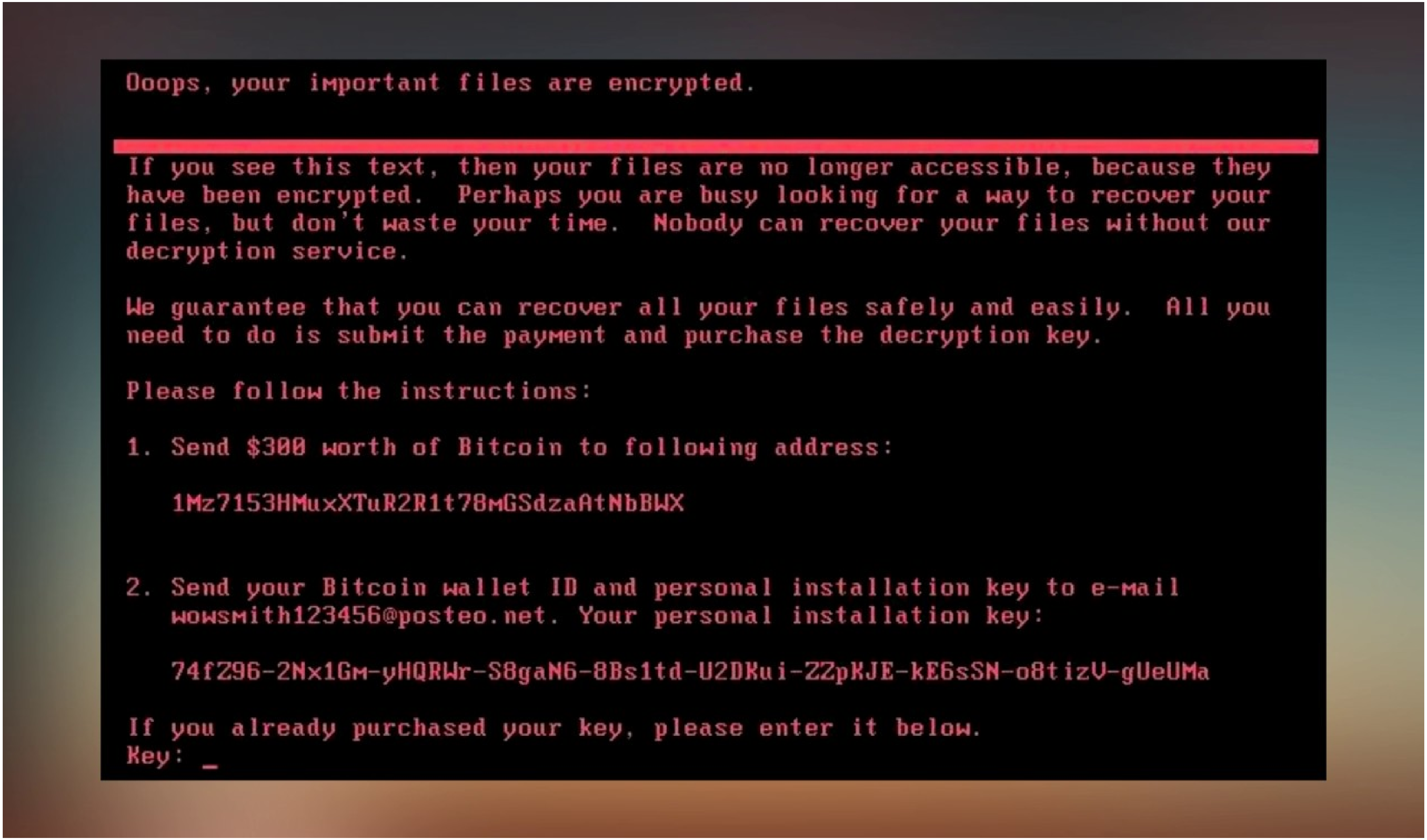
The NotPetya case (NJ)

Chapter 1 (NCJ)

Chapter 2 (NJ)

Case revisited
- management aspects (NCJ)
- technical aspects (NJ)

NotPetya: impact



```
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
   wowsmith123456@posteo.net. Your personal installation key:

   74fZ96-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

Impact of NotPetya June 22nd onwards

Ransom message appeared on screen

- “PC files encrypted”
- bitcoin address for ransom
- email adress for exchange of key

Shut down most computers in Maersk

- in Ukraine
- and spread to Maersk all over the world
- though not the computers onboard of ships

Infected also Maersk’s so-called domain controllers

- required to run Maersk’s internal network
- all 150 domain controllers in different countries
- except 1 machine in Ghana

Costs

Maersk’s costs

- claimed loss of USD 200-300 mill

Costs for other companies

- FedEX: USD 400 mill (including TNT/Europe)
- Merck: USD 840 mill (a pharmaceutical company)
- companies world-wide: estimated at USD 10 bill (70 mia. DKR)

Impact on Ukraine

- shut down 10% of all computers

Maersk’s reaction

During infection period

- people would try to disconnect PCs before/during infection

Crisis management and “Rebuilding” effort

- two-three weeks
- HQ in Maidenhead, UK
- 600 people

Rebuilding effort included

- installed new software on individual PCs (45.000)
- at total of 4.000 servers rebuilt
- used the domain controller in Ghana as a basis for copying data to new domain controllers
- rebuilt data about business
  - including containers’ and ships’ destinations
  - using data from the onboard computers?

Exercise

1) Discuss what assets were affected by NotPetya

- use the four categories suggested by Stallings & Brown (p29)
  - hardware
  - ..

2) Discuss NotPetya’s type of attack and origin

- use the two types of attacks (p31)
- and the classicification into two types of origin (p31)

Exercise answers

1) Discuss what assets were affected by NotPetya

- use the four categories suggested by Stallings & Brown (p29)
  - hardware
  - ..

NotPetya affected all four categories of assets

- *it directly affected data*
- *indirectly it rendered hardware, software, and communication useless*
- *difficult to define distinctions between, eg. attack on sw/data*

2) Discuss NotPetya's type of attack and origin

- use the two types of attacks (p31)
- and the classicification into two types of origin (p31)

NotPetya was

- *active attack*
- *outside attack*

NotPetya vs Petya

“Payload”

- appeared similar to Petya
- ransomware attack from 2016

However, “Not Petya” was

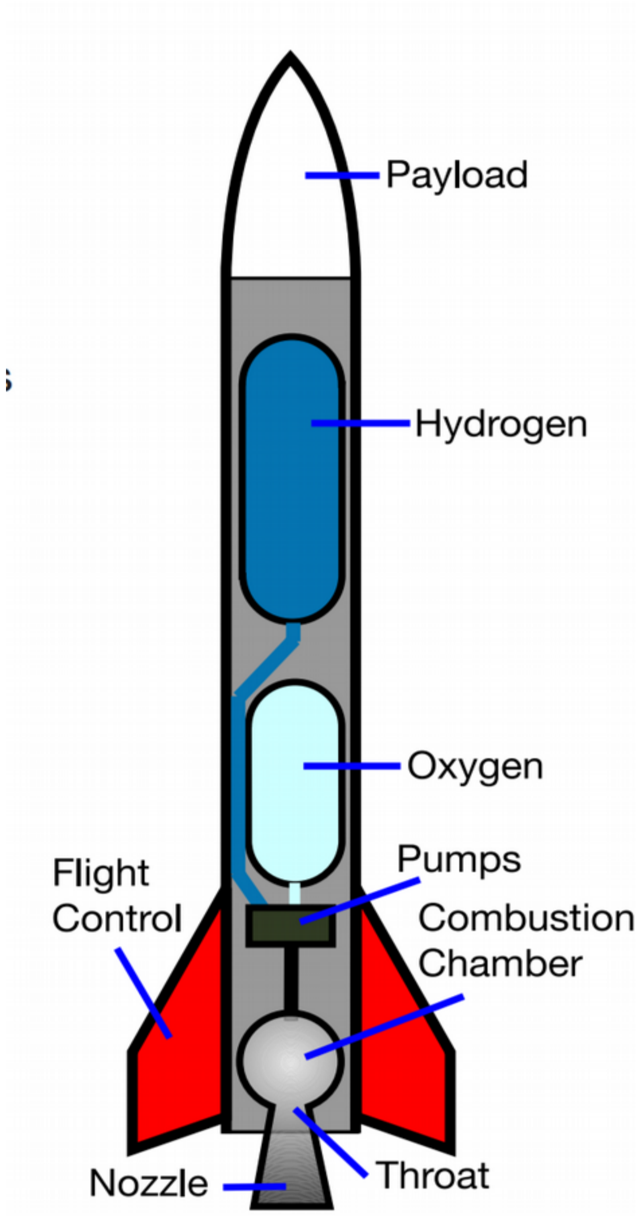
- not identical to Petya
- merely destructive
  - no recovery
- 300 USD ransom
- a single bitcoin address
- a single email address

payload

- *impact on computer*

propulsion

- *method of propagation to (infection of) other computers*
- *exploits a sw vulnerability*


Payload
Hydrogen
Oxygen
Pumps
Flight Control
Combustion Chamber
Nozzle
Throat