IT security

Monday 8th April
Course day #9

Theme D (ii)
Wireless security
Case: The wired equivalent privacy (WEP) protocol and the credit card theft at TJ Maxx

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

Theme D: Network security

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

Wireless means

- no wires (cables connections)
- Wi-Fi
  - wireless LANs
  - normally connected to the Internet
  - Wi-Fi is a trademark used by IEEE 801.11 “family”
  - not an abbreviation
  - designed to resemble “Hi-Fi”
- GSM/mobile (“cellular”)
- bluetooth, ..

← Wireless security (Ch. 24)

Literature and exam questions for today

Stallings & Brown:
- 24.1+24.2: Wireless network security

Additional mandatory literature:
- *T.J. Maxx Data Theft Likely Due to Wireless 'Wardriving'.* (3-4 pages)
- *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.* (Maple et al, 2006). (8 pages)

Exam questions
- Q17: “What are the main security challenges of wireless networks?”
- Q18: “What are the main security countermeasures to wireless security threats?”

Plan for today

Challenges of wireless networks

- Article on the *TJ Maxx* credit card numbers theft

Security countermeasures to wireless security threats

- Paper on *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.*

Course evaluation

- please fill out written form - results to be discussed next time

Practical exercise: the *wireshark* network analysis tool

Business case: DriveGreen start-up

“Drive green”
- start up company
- started 1st Januar 2019

Service provided:
- customers rent electric cars
- customers drive themselves
- to find and rent a car, customers use laptops and mobiles to connect to website

Graphics: based on image by Henrik Kiær / Berlingske Grafik

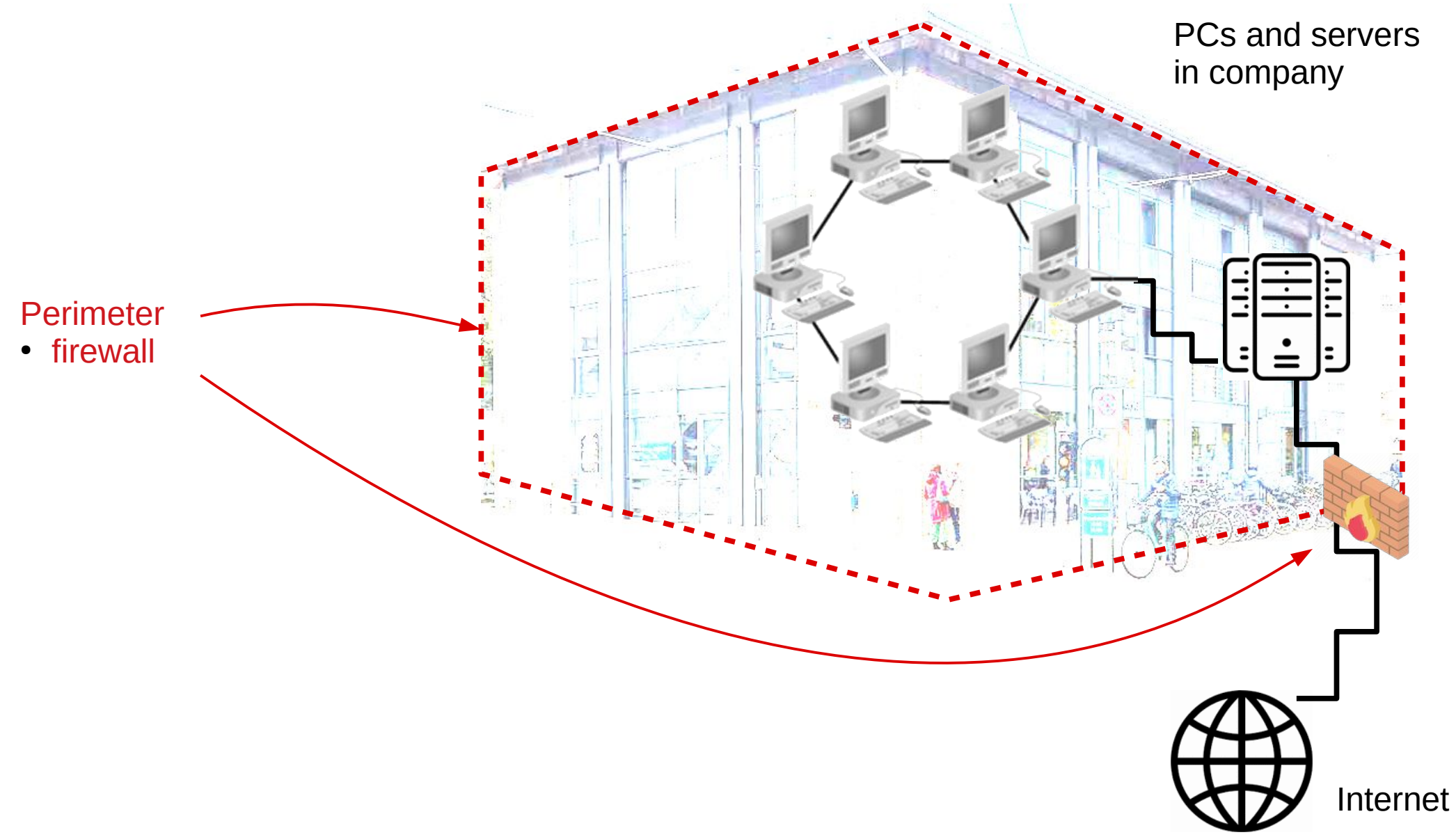
Business case: organization

10 people in office premises
- of which 5 it-people
- web development, ..
- *define wireless security policy*

In-house servers with
- customer credit card data
- mail, business plans, ..
- (possibly with cloud support)

All employees have
- company laptops
- company mobiles
- connect to server using Wi-Fi
  - though in the field, mobiles use GSM

DriveGreen *wired* LAN (20th century)



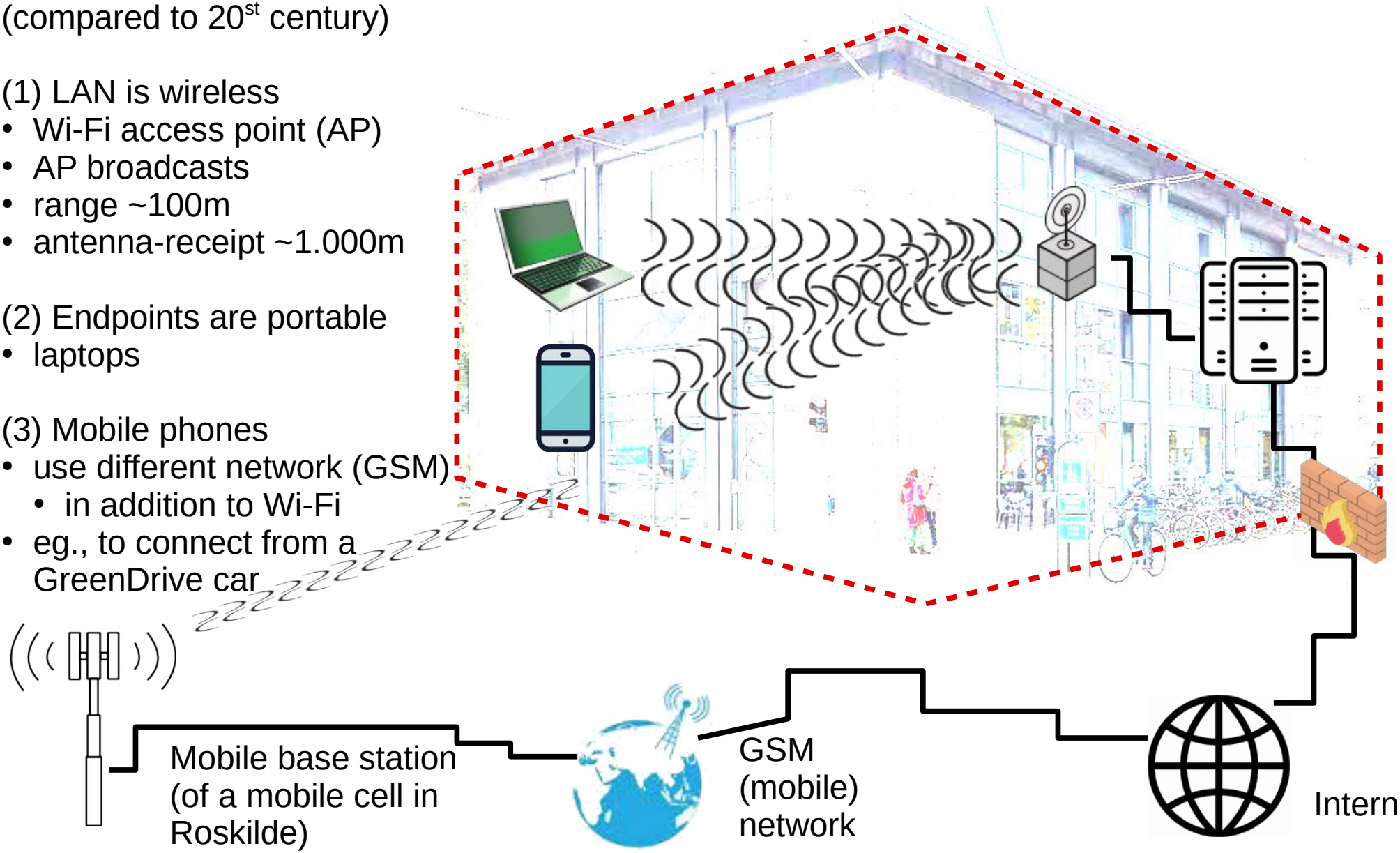
DriveGreen wireless LAN (+ GSM)

Three major changes
(compared to 20st century)

(1) LAN is wireless
- Wi-Fi access point (AP)
- AP broadcasts
- range ~100m
- antenna-receipt ~1.000m

(2) Endpoints are portable
- laptops

(3) Mobile phones
- use different network (GSM)
  - in addition to Wi-Fi
- eg., to connect from a GreenDrive car



Plan for today

Challenges of wireless networks

- Article on the *TJ Maxx* credit card numbers theft

Security countermeasures to wireless security threats

- Paper on *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.*

Course evaluation

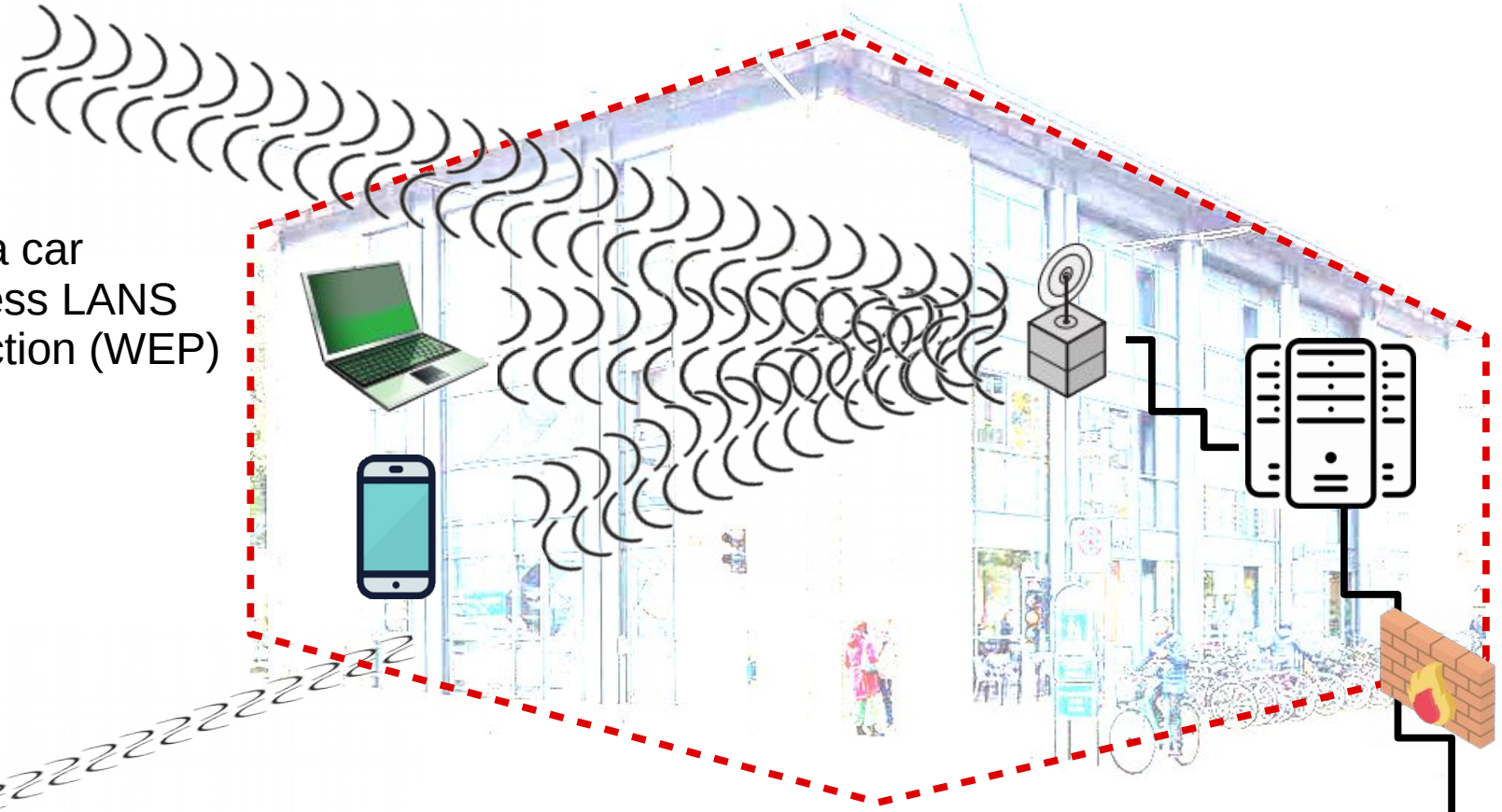
- please fill out written form - results to be discussed next time

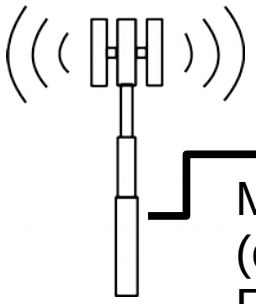
Practical exercise: the *wireshark* network analysis tool

TJ Max: wardriving

Wardriving

- drive around in a car
- search for wireless LANS with weak protection (WEP) or no protection
- eavesdrop
- logon





Mobile base station (of a mobile cell in Roskilde)

GSM (mobile) network

Internet

Other TJ Maxx key points

Theft of data of 45+ mill. credit/debit cards
- sold on to others

Targetted retail store
- Miami, Florida
- from a parking lot
- once inside, they hacked/downloaded via ordinary internet (not Wi-Fi)

Court sentences included -
- Albert Gonzales, 20 years (US court)
  - a hacker working as an informant for a US agency
- Maksym Yastremskiy, 30 years (Turkish court - for other hacks)
  - profit estimated to 11 mill. USD

Learning point
- upgrade to most recent version (WPA2)
- even though expensive
- 2.300 stores worldwide

Exercise

Define three main threats X, Y, Z
- to be prioritized in the DriveGreen wireless security policy

Hint: Use list p724 in Stallings & Browns
- no 100% correct answer
- feel free to include other threats
- note p723 (list of risks)

(Countermeasures)
- (to be discussed later today)

Is it *mandatory* in DK for a private enterprise to have a security policy in writing?
- no, but good idea
- however, concerning privacy/GDPR, a (written) policy is required
- about storing of customer data

DriveGreen wireless security policy

Threat #1: X
Countermeasures
- ..

Threat #2: Y
Countermeasures
- ..

Threat #3: Z
Countermeasures
- ..

Other threats/c.measures/policies/..
- ..

Exercise solution

DriveGreen wireless security policy

Threat #1: Rouge endpoints (eavesdropping, logon)
Countermeasures
- ..

Threat #2: Rouge access point (steal passwords)
Countermeasures
- ..

Threat #3: Employees' mobile phones (protection may be weak)
Countermeasures
- ..

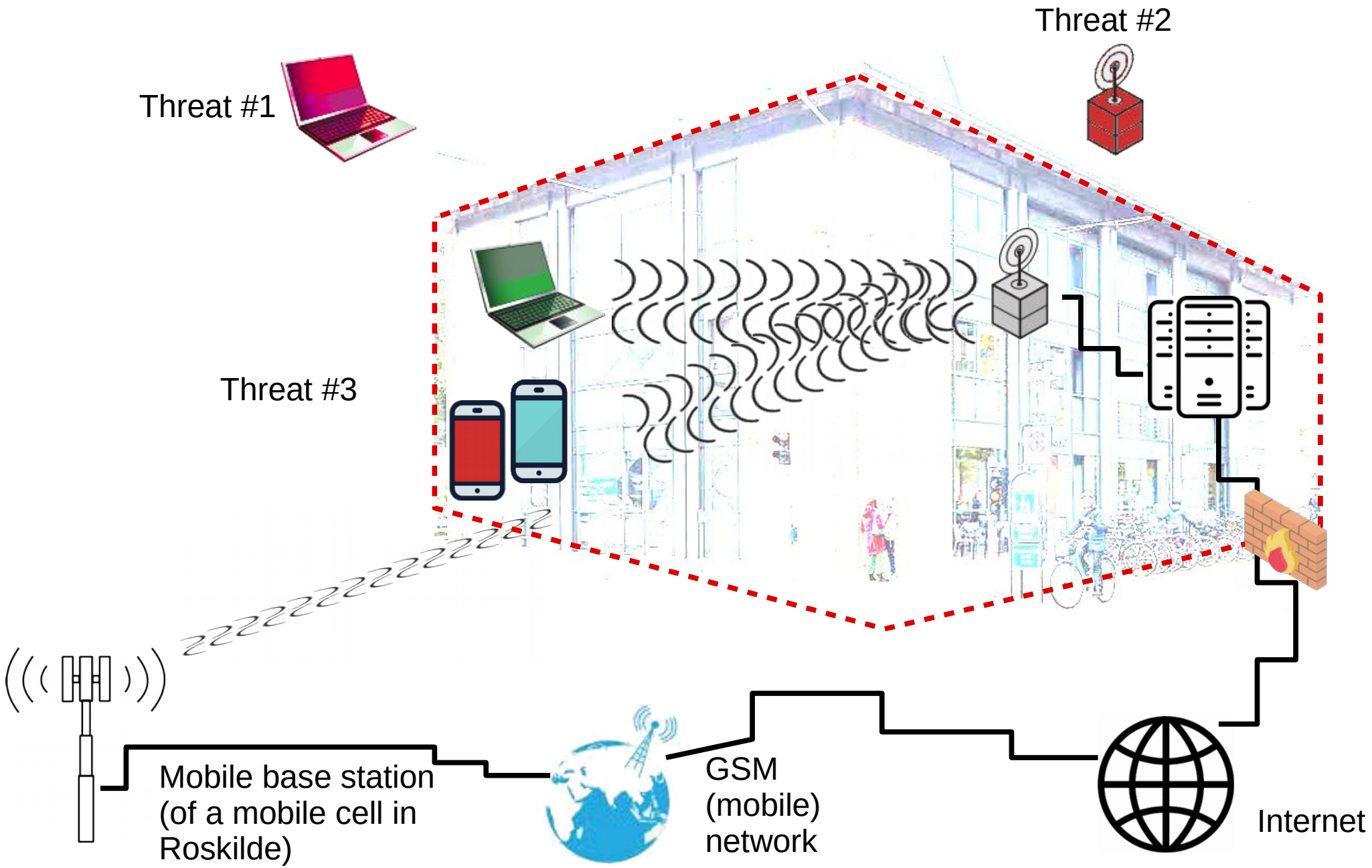
Other threats/c.measures/policies/..
- WPA2/WPA3
- upgrade policy

Please note:

There are also other important threats (mention them)

Threats can also be grouped according to which CIA++ goal they concern:
- *Threats to Confi..*
- *Threats to Integri..*
- *..*

DriveGreen wireless threats #1-3



Assignment

Hand-in May 1st at 12.00

- mandatory
- (though oral exam is by far the most important basis for grading)

4.800 - 48.000 characters

- 2-20 pages
- you are strongly encouraged to limit the lenght of your assignment to approximately 2-5 pages
- for example, three pages provide space for 6-7 questions per page

Assignment example

Question 17: “What are the main security challenges of wireless networks?”

“I will explain the challenges using the fictive example of GreenDrive (provided in Niels J’s lecture). Company network includes laptops and mobiles which are connected by wi-fi to servers and internet. Challenges include rouge endpoints, rouge access points, and employees’ mobile phones that are weakened and possibly compromised. The challenges should be be identified in a written security policy”.

In your oral presentation, you may explain, for instance
- why is a wireless network used in the first place?
- what are the threats related to rouge endpoints, access points and mobiles?
- perhaps also mention some countermeasures (Q18)

In the Q/A section of the oral exam
- we will mainly ask questions about the selected exam question
- we may also ask questions about other exam questions
- and your assignment

Assignment, alternatives

Question 17: “What are the main security challenges of wireless networks?”

Alternative topics: in your assignment you may emphasize, for instance:
- The CIA++ goals
- The Wi-Fi standards
- ..

Alternative style: you may use a style with keywords/headlines, for instance:

“Fictive example of GreenDrive (Niels J’s lecture). Company network: laptops + mobiles, connected by wi-fi to servers and internet. Challenges: rouge endpoints + rouge access points + weakened employees’ mobile phones. Written security policy”.

Thus, a short-hand style is ok
- of course the keywords you provide must make sense
- use your own words - the usual plagiarism rules apply

Plan for today

Challenges of wireless networks

- Article on the *TJ Maxx* credit card numbers theft

Security countermeasures to wireless security threats

- Paper on *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.*

Course evaluation

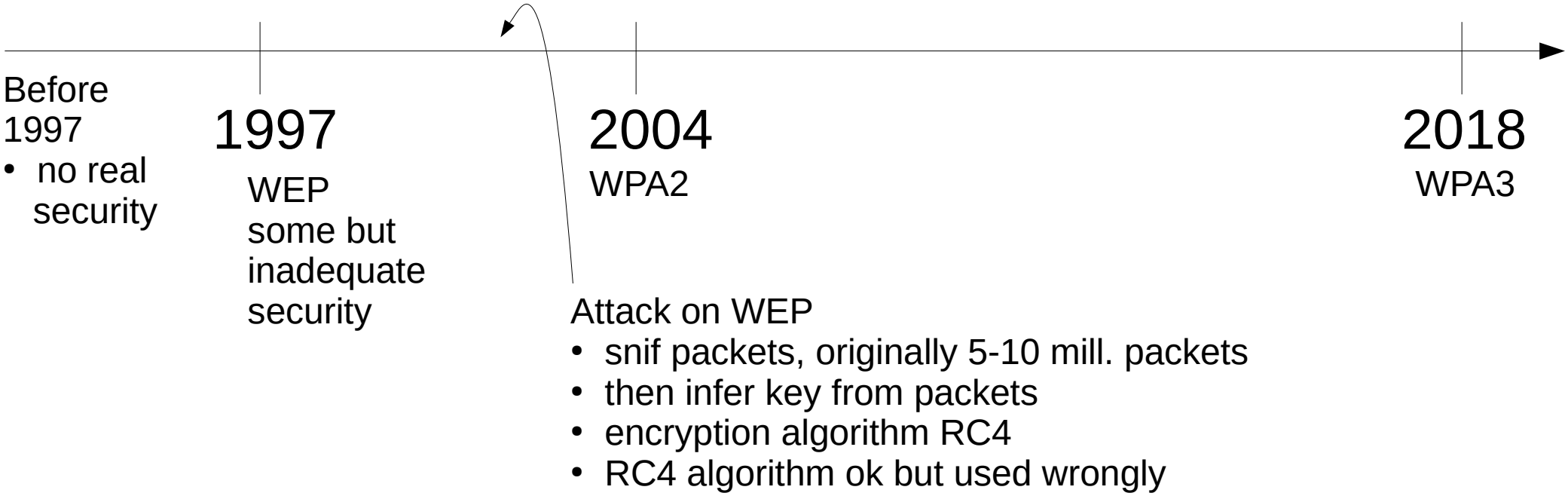
- please fill out written form - results to be discussed next time

Practical exercise: the *wireshark* network analysis tool

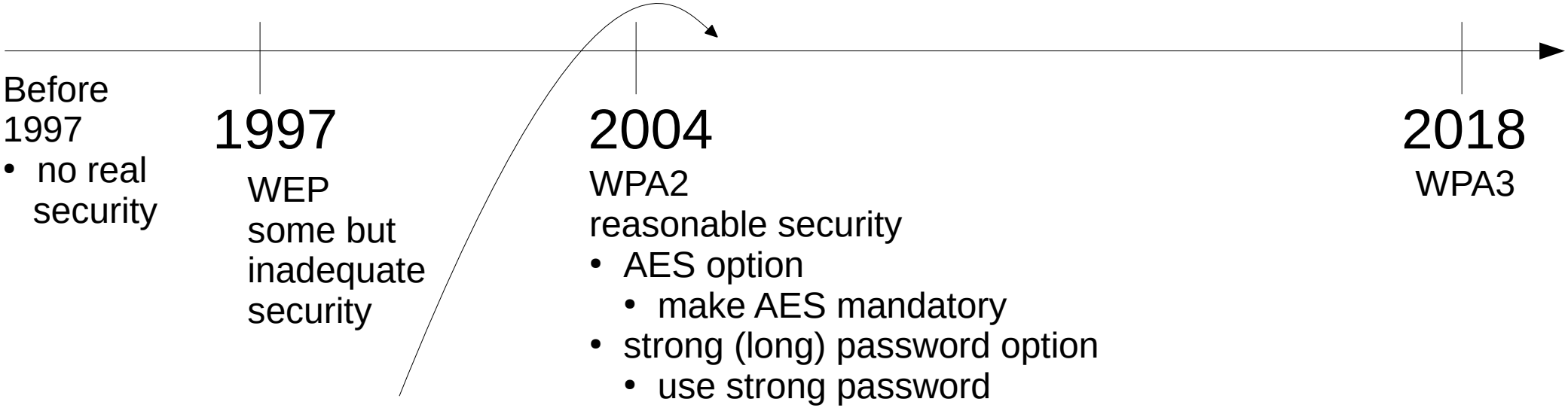
Countermeasures in general

Upgrade
- WPA2, instead of WEP, or no security
- WPA3 when equipment available

Timeline of wireless networks compliant with the IEEE 802.11 family of standards



Countermeasures in general (cont.)



Before 1997
- no real security

1997
WEP
some but inadequate security

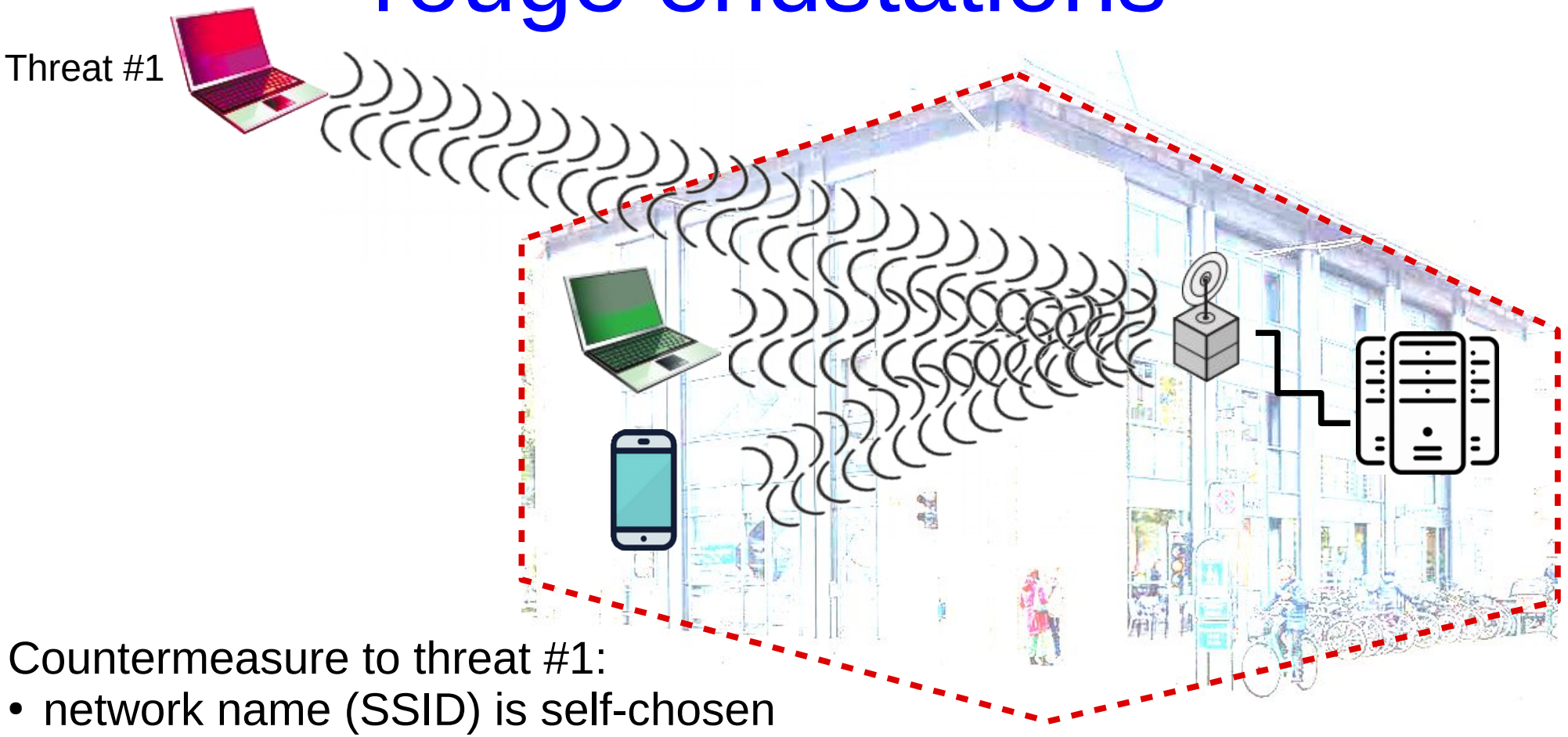
2004
WPA2
reasonable security
- AES option
  - make AES mandatory
- strong (long) password option
  - use strong password
- though there are weaknesses
  - including password brute-forcing

2018
WPA3

Maple et al. business survey 2005
- 51% no encryption
- 25% default name (SSID)
  - and therefore probably also defaut password

There is a WPA standard preceding WPA2 and WPA3
- but insufficient and never widely used

Countermeasures to threat #1: rouge endstations

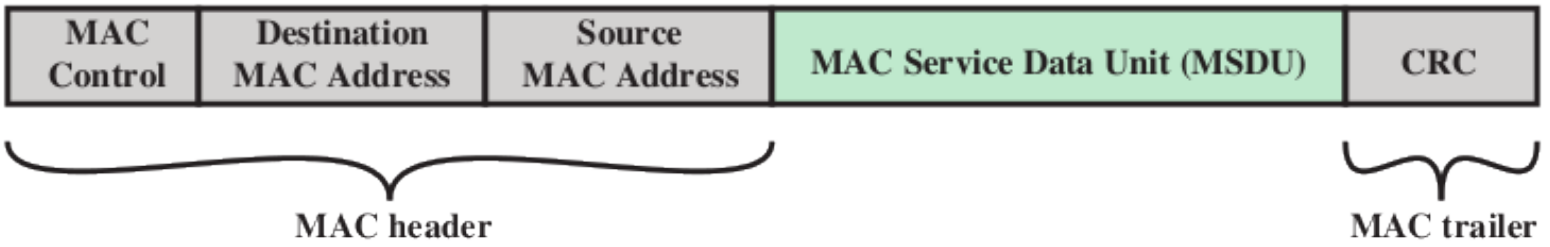


Countermeasure to threat #1:

- network name (SSID) is self-chosen
- do not broadcast network name
- network name might be “GreenDriveWiFi”
- or “GWiFi” to conceal location

(In addition to using WPA2/WPA3)

“MAC frame” (Fig. 24.4)



“MAC frame” = MAC protocol data unit = MPDU

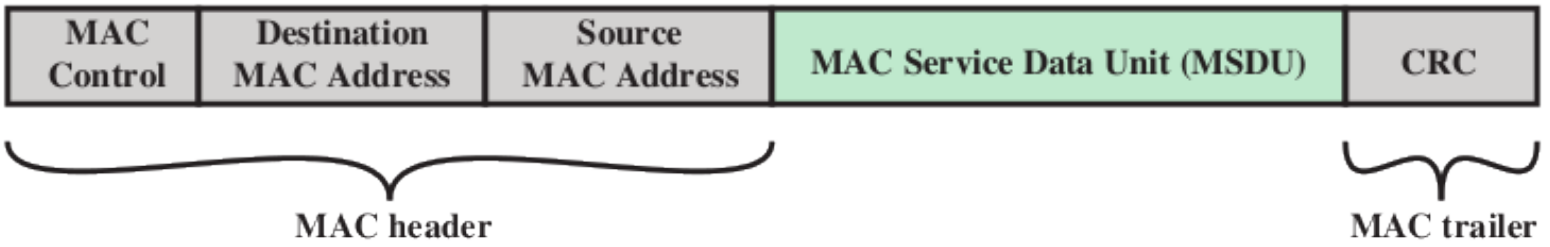
MAC = Medium Access Control

MAC address
- by intension, uniquely identifies each device (endpoint or access point)

Find your MAC address
- mac/linux: “ifconfig” (then search for en0); windows: “ipconfig /all”

MAC address caveat: you have multiple MAC addresses
- one MAC address per network card (selected by manufacturer)
  - one wireless MAC address + one wired MAC address + ..
- as an intruder, your may spoof your MAC address
- also as a privacy aware user
- since your device periodically sends out MAC packets, searching for networks

MAC frame (cont.)



MAC header:
- destination, source are local
- not final destination (eg., a webserver)

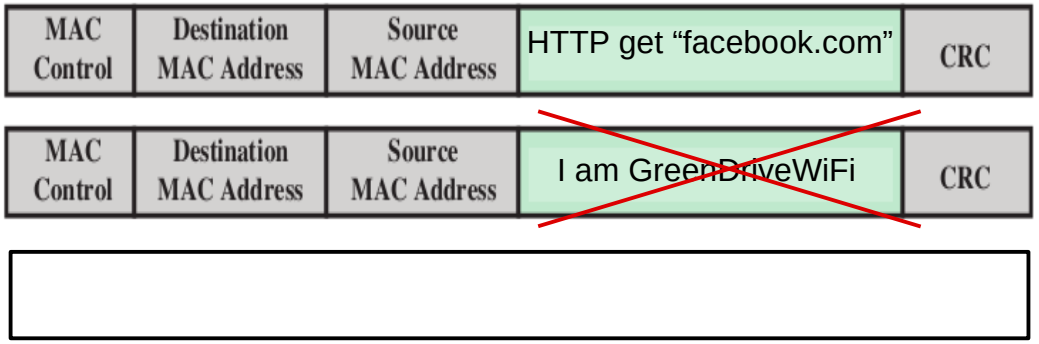
MAC service data:
- up to approx. 2KB
- eg., an HTTP get “facebook.com”
- MAC frames belong to OSI layer 2: the data link layer
- IP packets belong to OSI layer 3: the transport layer

} *Knowledge of OSI model/layers not required*

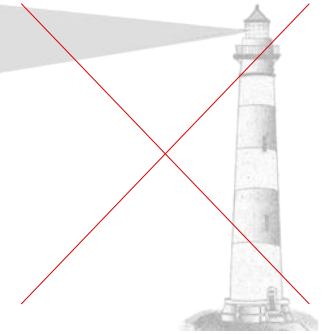
MAC trailer
- an error detecting code, to ensure integrity of header + service data
- similar to a hash
- but a checksum, not a cryptographic hash

Countermeasure to threat #1: conceal network name

Three types of MAC frames
1. data frames
2. management frames
   - for authentication + more
3. control frames
   - for confirmation of receipt + more



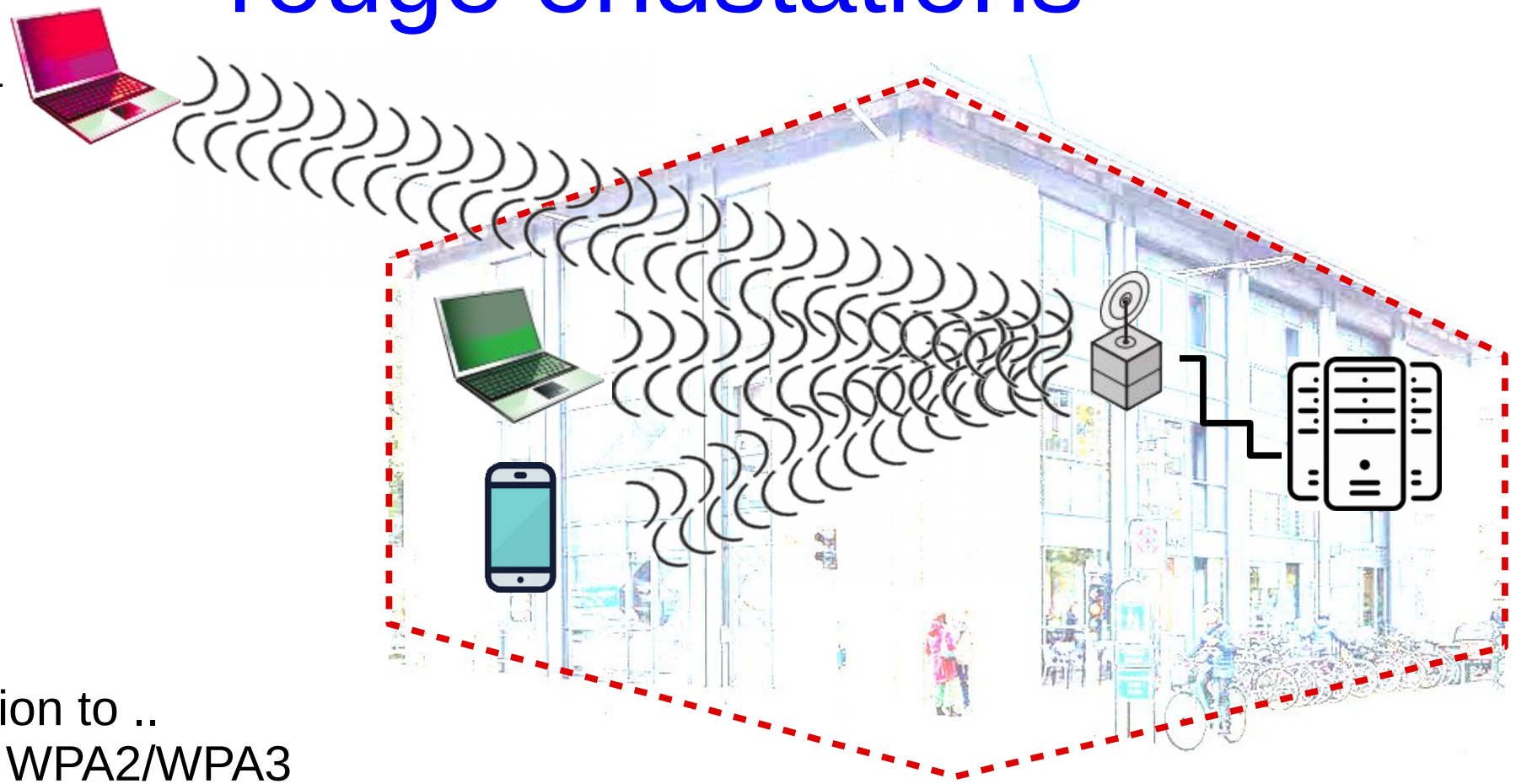
To logon, an endpoint must provide network name (SSID)
- access point can be configured to “closed mode”
- in “closed mode”, no management frames with SSID are sent
- so client must know SSID by other means
- otherwise access point regularly sends out SSID (in “beacon frames”)



Thus, if GreenDrive does not need to provide Wi-Fi access to guests
- then configure access point to run in “closed mode”
- as a small, extra protection against rouge endpoints
- small because there are other ways to eavesdrop the name

Countermeasures to threat #1: rouge endstations

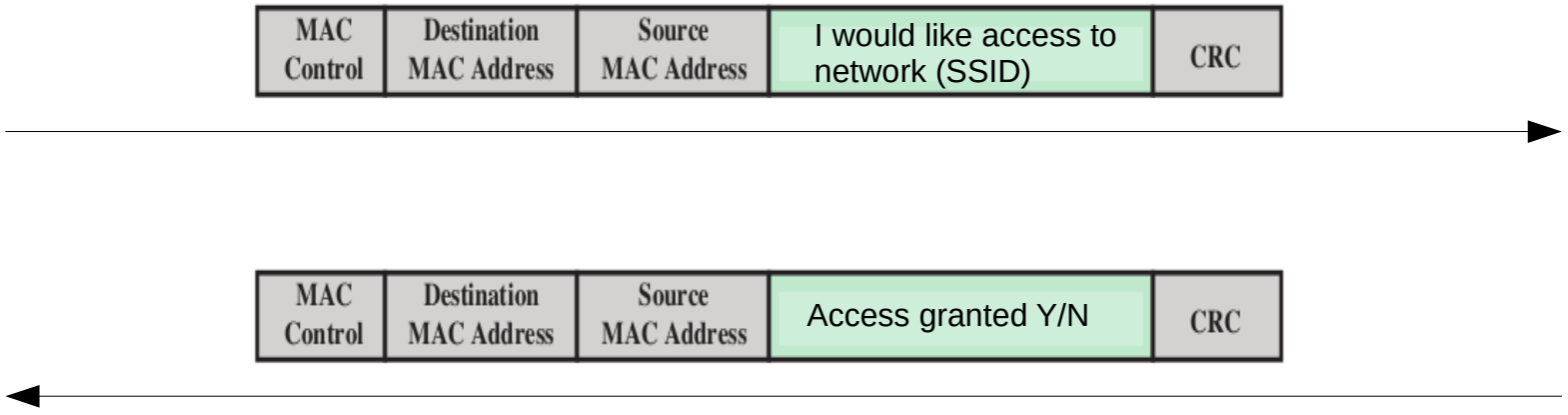
Threat #1



In addition to ..
- using WPA2/WPA3
- not broadcasting network name

.. access point may be configured
- to accept only clients with certain MAC addresses
- .. again there are ways of sniffing legitimate MAC addresses

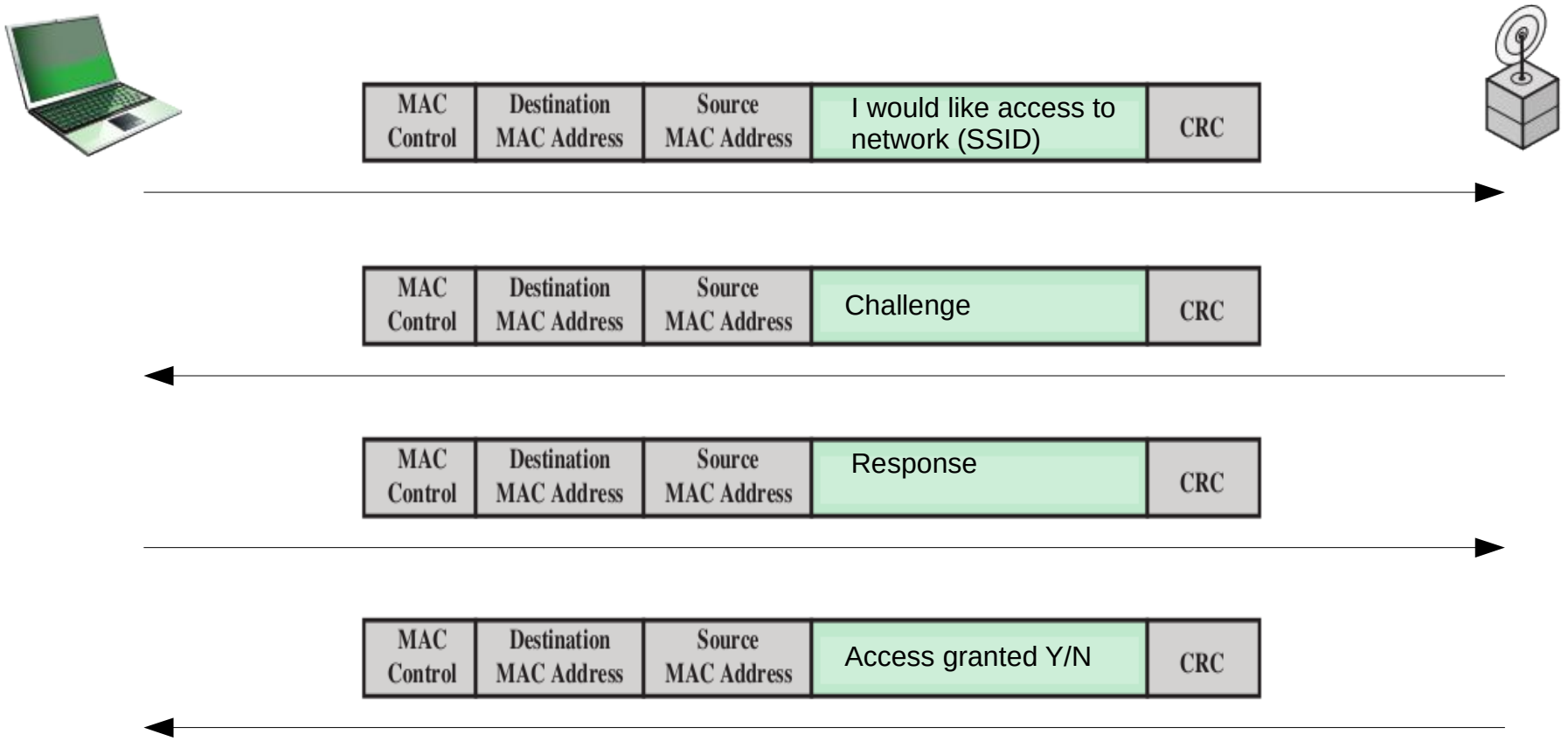
Exercise: problem 24.1



The problem concerns a 802.11 Wi-Fi network without WEP/WPA

Authentication is by means of two management MAC frames

Exercise: problem 24.2



The problem concerns authentication in WEP.
(STA = endpoint).
Please note: Not enough information to solve question 24.2c properly.

Exercise solution: 24.1

a. Benefits

Simple to implement.
Excludes endpoints believed to be rouge.
If there is also a “positive list” (clients/endpoints allowed),
then the approach excludes accidental logons (eg., from a neighbor).

b. Vulnerabilites

MAC address spooing.
So the approach relies on endpoints being honest.

Exercise solution: 24.2

a. Benefits

Authenticates the client/endpoint
(proves possession of the shared, secret key).

b. Incomplete

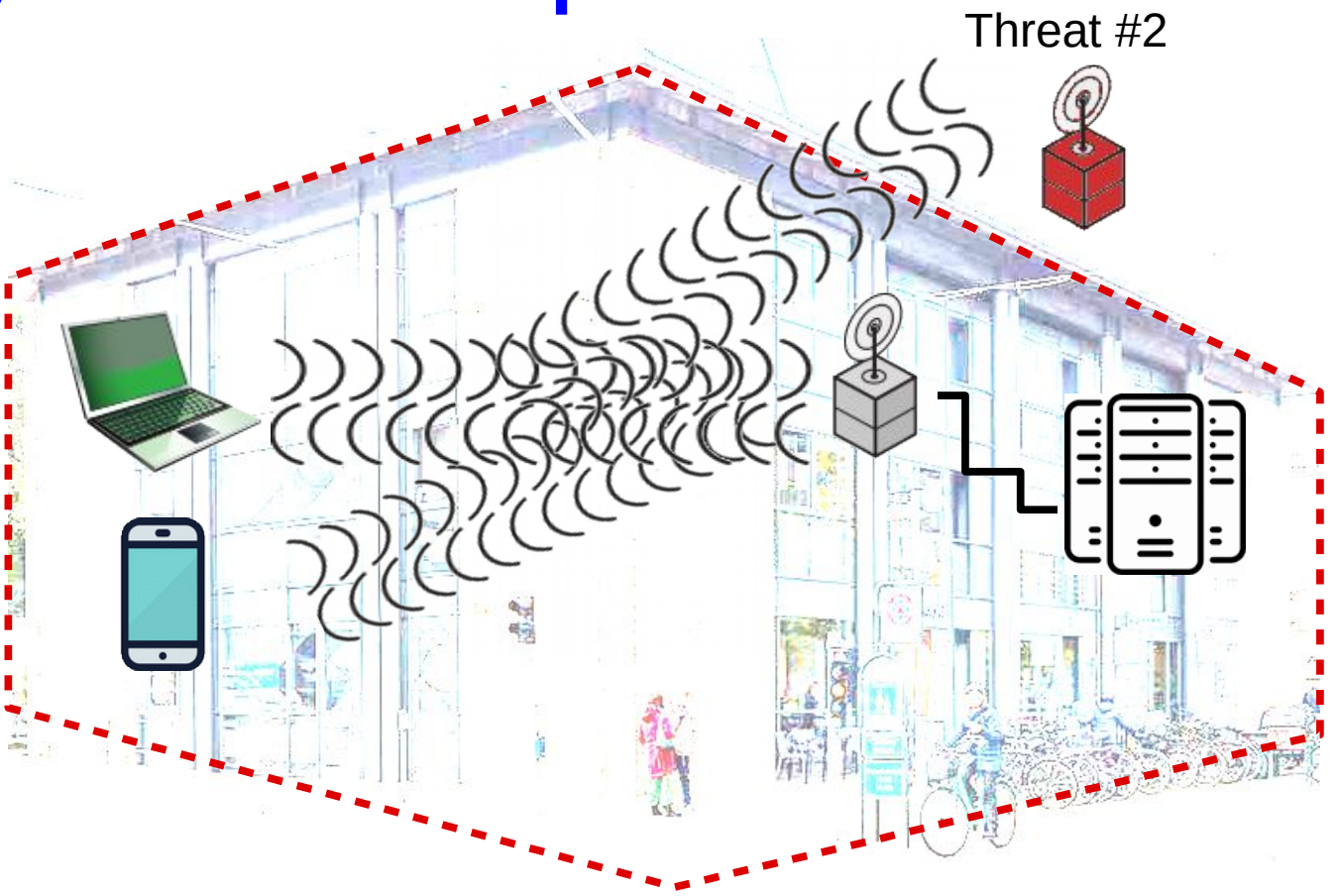
Does not authenticate the access point.

c. Weakness

An eavesdropper can store pairs of plantext/ciphertext:

- <challenge, E1(key, challenge)>
- in theory, if there are enough pairs, an attacker can guess the key
- in practice, this attack is not feasible, due to the large 128 bit challenge
- however, the attack is feasible against WEP because of other weaknesses

Countermeasures to threat #2: rouge access points

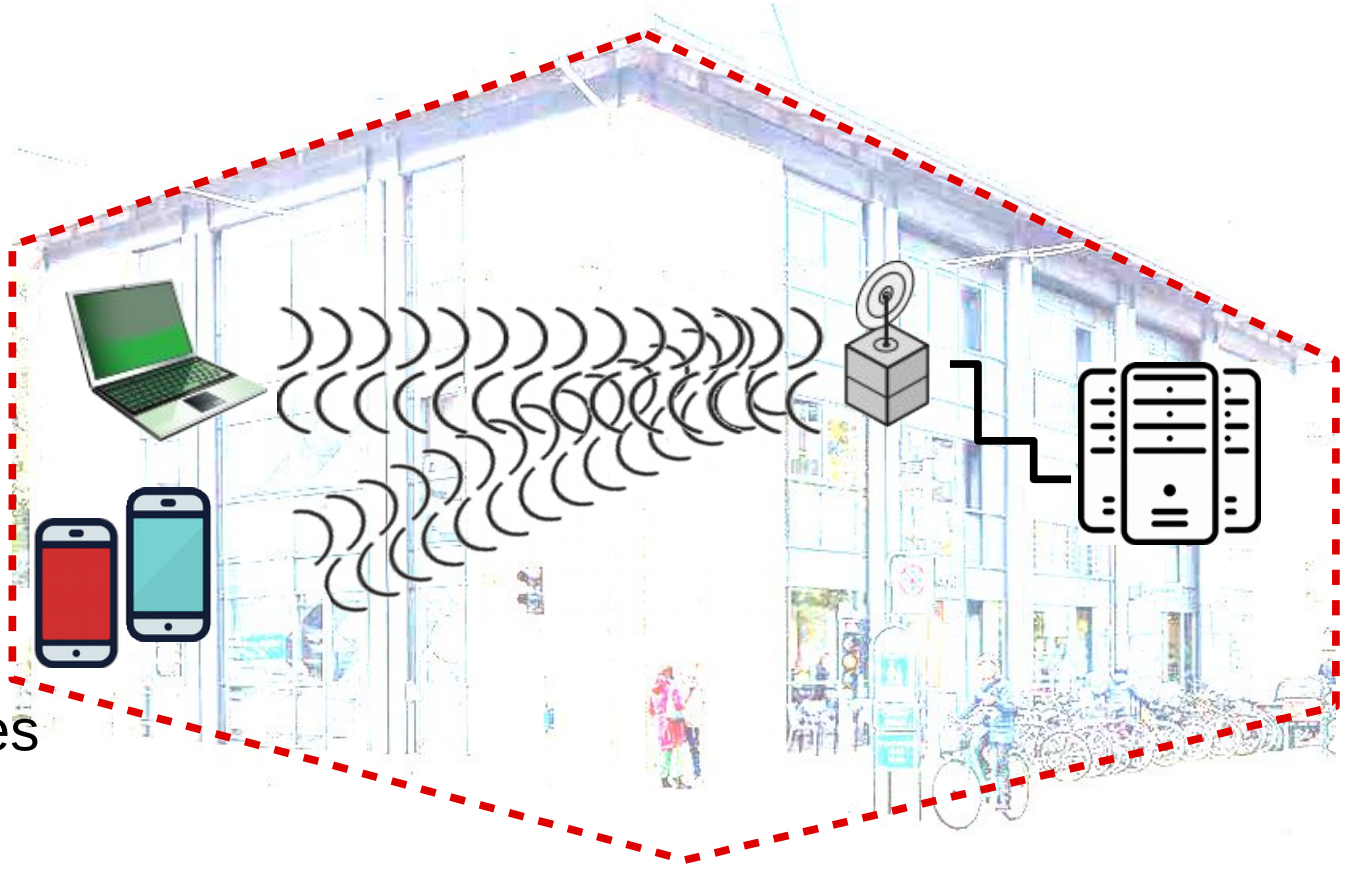


All clients should be configured with PKI

- require authentication of access point with certificate + proof of private key possession

Countermeasures to threat #3: employees' mobile phones

Threat #3



Employees' mobile phones
- may be compromised
- eg. by malicious apps

Exercise: is "Mobile device security strategy" of Stallings & Brown (p729-730, 13 bullits) ..
- .. appropriate?
- .. for company or private (BYOD) mobiles?

Exercise: solution (?)

Exercise: is “Mobile device security strategy”
of Stallings & Brown (p729-730, 13 bullits) ..

- .. appropriate?
- .. for company or private (BYOD) mobiles?

Strategy contains elements that many would perceive as invasive

- *eg., “IT staff should also have the ability to remotely access devices..”*
- *probably not acceptable to employees’ private phones (if at all)*

Summary of wireless security policy

DriveGreen wireless security policy

Threat #1: Rouge endpoints
(eavesdropping, logon)
Countermeasures
- no name broadcast; allow only certain MACs

Threat #2: Rouge access point
(steal passwords)
Countermeasures
- authenticate AP with PKI

Threat #3: Employees' mobile phones
(protection may be weak)
Countermeasures
- restricted mobile phones provided by company

Other threats/c.measures/policies/..
- WPA2
- upgrade policy

Also many alternatives
- *SMS codes at login*

- as on RUC Hotspot
- user proves possession of a mobile with a certain phone number
- two factor-authentication

Plan for today

Challenges of wireless networks

- Article on the *TJ Maxx* credit card numbers theft

Security countermeasures to wireless security threats

- Paper on *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.*

Course evaluation

- please fill out written form - results to be discussed next time

Practical exercise: the *wireshark* network analysis tool

Course evaluation

Please fill out the evaluation form on moodle

Answers are anonymous (to us teachers)

On the final course day

- evaluation will be continued
- Niels Chr. and I will be present, and reflect on, main results of written feedback

Plan for today

Challenges of wireless networks

- Article on the *TJ Maxx* credit card numbers theft

Security countermeasures to wireless security threats

- Paper on *Choosing the Right Wireless LAN Security Protocol for the Home and Business User.*

Course evaluation

- please fill out written form - results to be discussed next time

Practical exercise: the *wireshark* network analysis tool

Wireshark

Please download and install wireshark
- wireshark.org

Captures all network traffic visible to your computer
- not merely the traffic sent to your MAC address
- puts network card in “promiscuous mode” (sees, reads, .. everything)
- analysis is *passive*
- unlike nmap which is *active* (eg., sends TCP SYN packets)

Note that many parts of the wireshark program
run with admin/superuser privileges
- security risks if parts of wireshark is compromised
- so make sure to close/remove wireshark after use

Wireshark

To capture wireless data
- select Capture -> Options
- select/accept Input
- select WiFi
- select start, then select “Continue without saving”

Suppose you want to know what wireless packets are sent from your computer
- for example, is malware secretly sending data?
- type ip.src == <IP address>
  - in the form at top of window (“Apply a display filter”)
  - (using your own IP address on the local network)

Alternatively, suppose you want to know what packets are sent from another computer on the network
- type wlan.sa == <MAC-adress>
- wlan = wireless local area network
- sa = source address

Find IP address and MAC address using ifconfig/ipconfig

Monday 15th April

Main topics
- course evaluation (cont.)
- oral exam Q/A

Case
- Ethical codes - of ACM and IEEE - and our own at the IT Security course

Literature
- ACM and IEEE codes in Stallings & Brown p 621-622

Presentation
- *The five biggest security breaches of 21st century.* (Niels J.)