UNIK 4250 – Mobile Network Security

slides: (wi.unik.no/wiki/UNIK4250

↳ Mobile Network Security

Sindre

Tor

Iñaki

Seray

Nils

Andreas

Endre

Andre

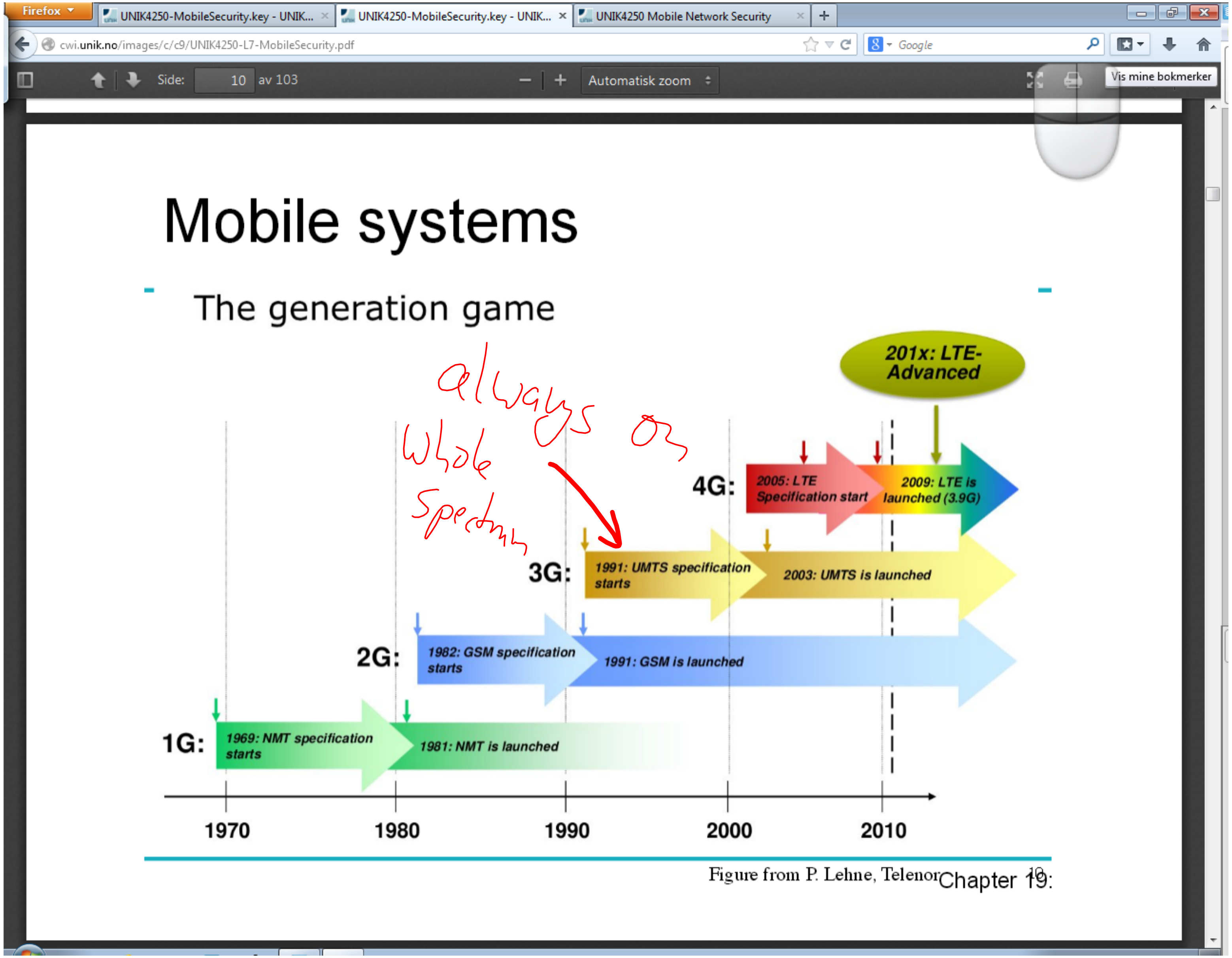
Erik

Josef

Polycom Real Presence Desktop

GSM : Cell size < 15km

UMTS : Cell size 3km → 1.5km


Firefox
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250 Mobile Network Security
cwi.unik.no/images/c/c9/UNIK4250-L7-MobileSecurity.pdf
Google
Side: 10 av 103
Automatisk zoom
Vis mine bokmerker

Mobile systems

The generation game

always on

whole Spectrum

201x: LTE-Advanced

4G: 2005: LTE Specification start → 2009: LTE is launched (3.9G)

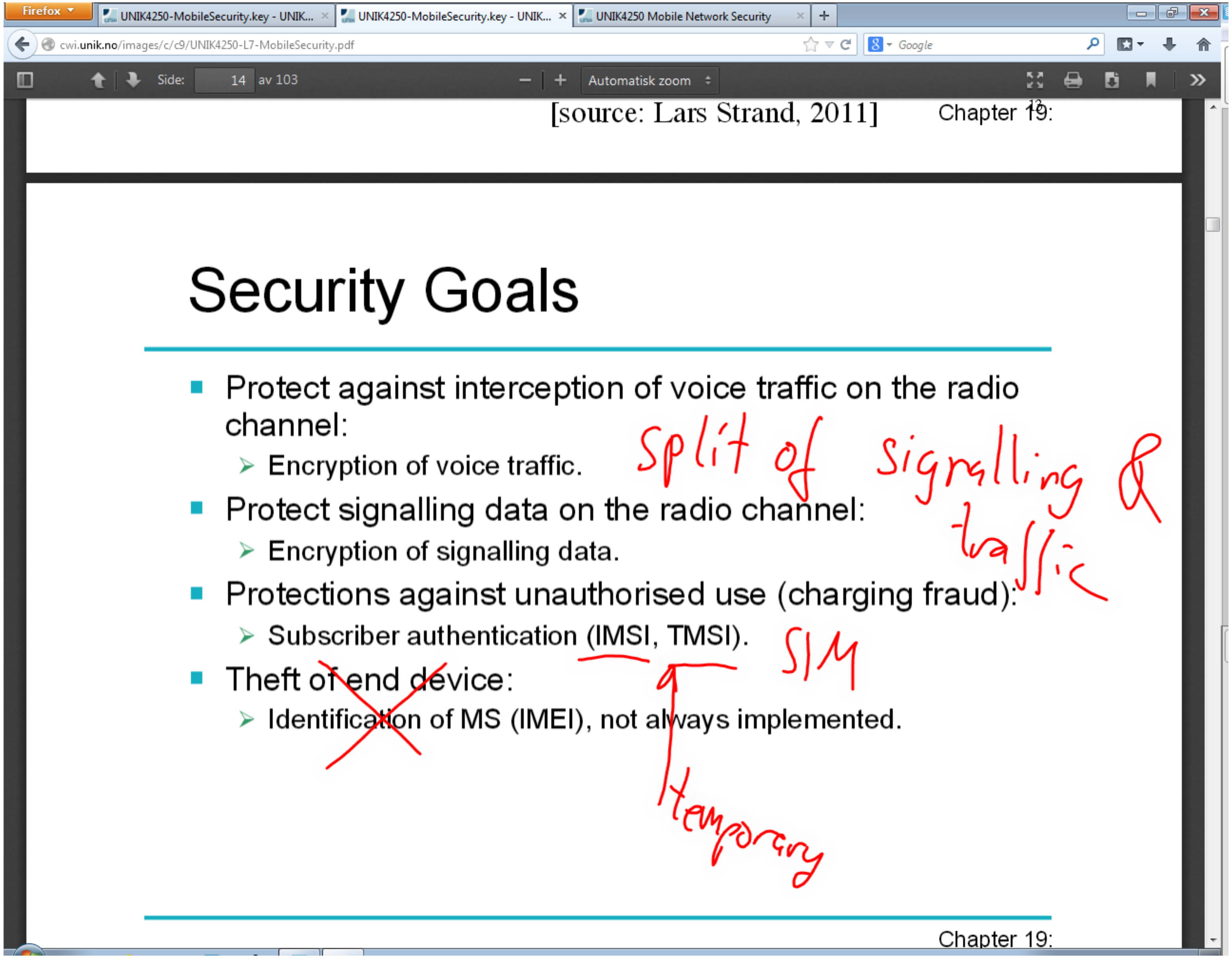
3G: 1991: UMTS specification starts → 2003: UMTS is launched

2G: 1982: GSM specification starts → 1991: GSM is launched

1G: 1969: NMT specification starts → 1981: NMT is launched

Figure from P. Lehne, Telenor

Chapter 19:


Firefox
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250 Mobile Network Security
cwi.unik.no/images/c/c9/UNIK4250-L7-MobileSecurity.pdf
Google
Side: 14 av 103
Automatisk zoom

[source: Lars Strand, 2011]

Chapter 19:

Security Goals

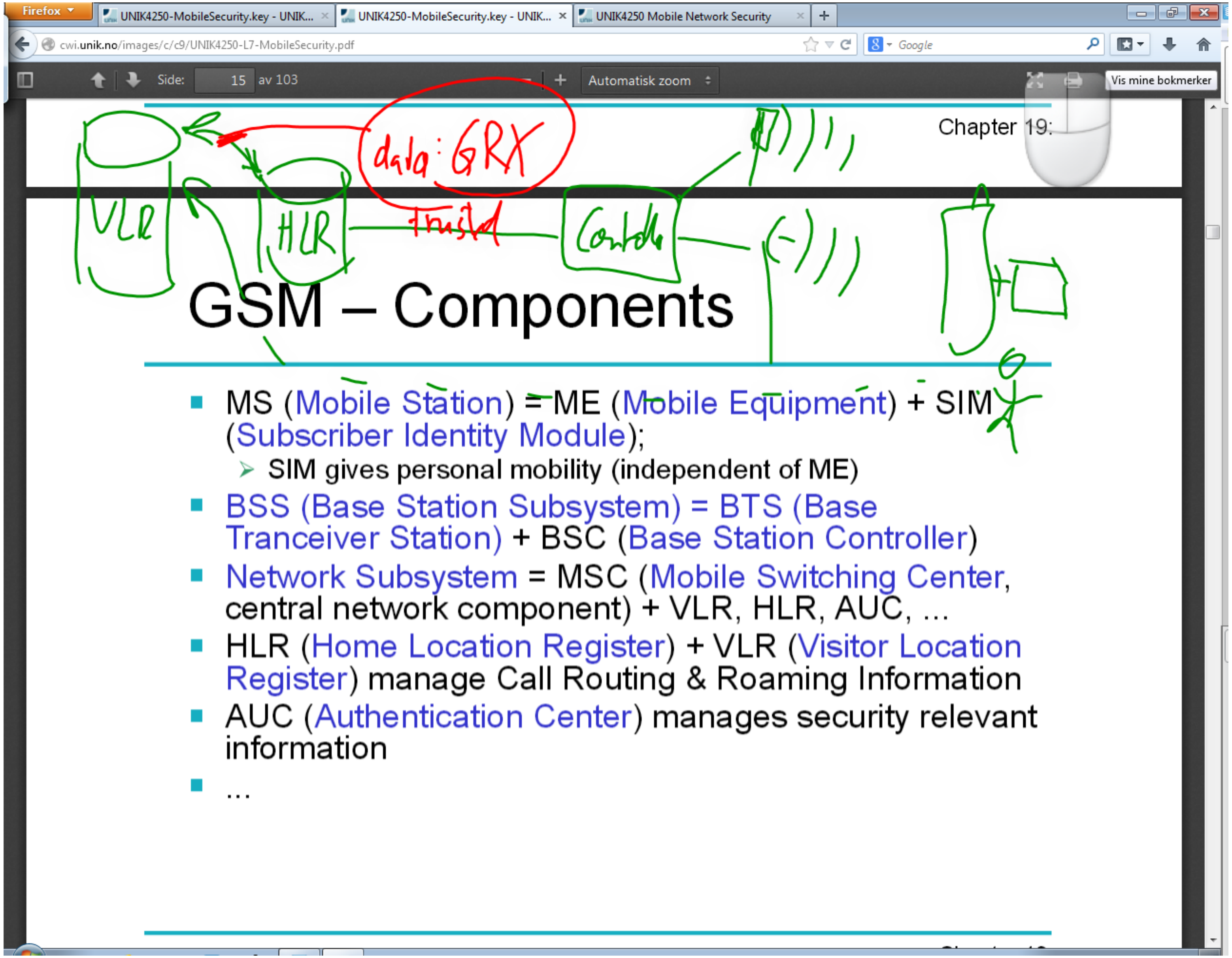
- Protect against interception of voice traffic on the radio channel:
  - Encryption of voice traffic.
- Protect signalling data on the radio channel:
  - Encryption of signalling data.
- Protections against unauthorised use (charging fraud):
  - Subscriber authentication (IMSI, TMSI).
- Theft ~~of end device~~:
  - ~~Identification~~ of MS (IMEI), not always implemented.

Split of signalling & traffic

SIM

temporary

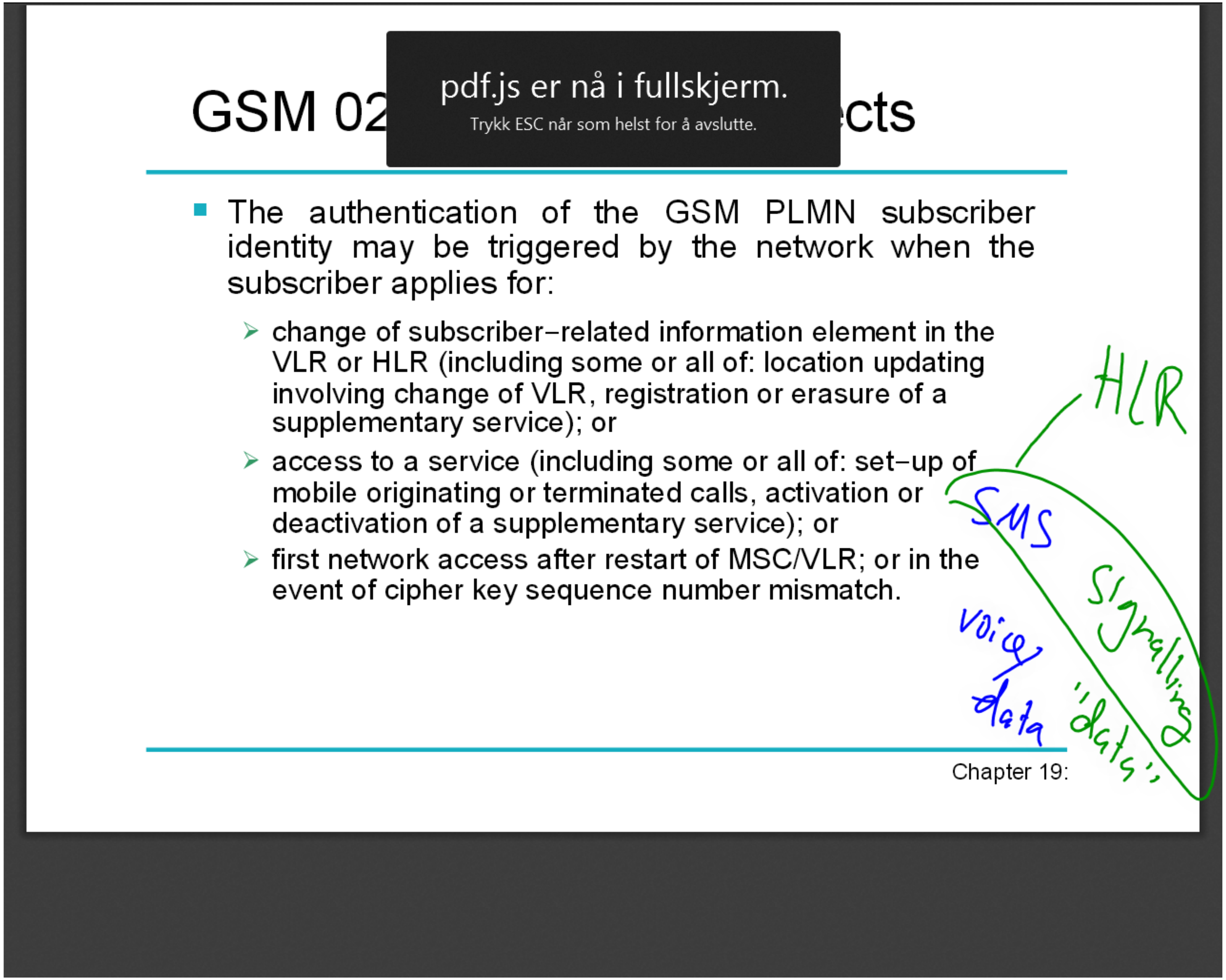
Chapter 19:


Firefox
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250-MobileSecurity.key - UNIK...
UNIK4250 Mobile Network Security
cwi.unik.no/images/c/c9/UNIK4250-L7-MobileSecurity.pdf
Google
Side: 15 av 103
Automatisk zoom
Vis mine bokmerker
VLR
HLR
data: GRX
Trusted
Controlle

Chapter 19:

GSM – Components

- MS (Mobile Station) = ME (Mobile Equipment) + SIM (Subscriber Identity Module);
  - SIM gives personal mobility (independent of ME)
- BSS (Base Station Subsystem) = BTS (Base Tranceiver Station) + BSC (Base Station Controller)
- Network Subsystem = MSC (Mobile Switching Center, central network component) + VLR, HLR, AUC, ...
- HLR (Home Location Register) + VLR (Visitor Location Register) manage Call Routing & Roaming Information
- AUC (Authentication Center) manages security relevant information
- ...



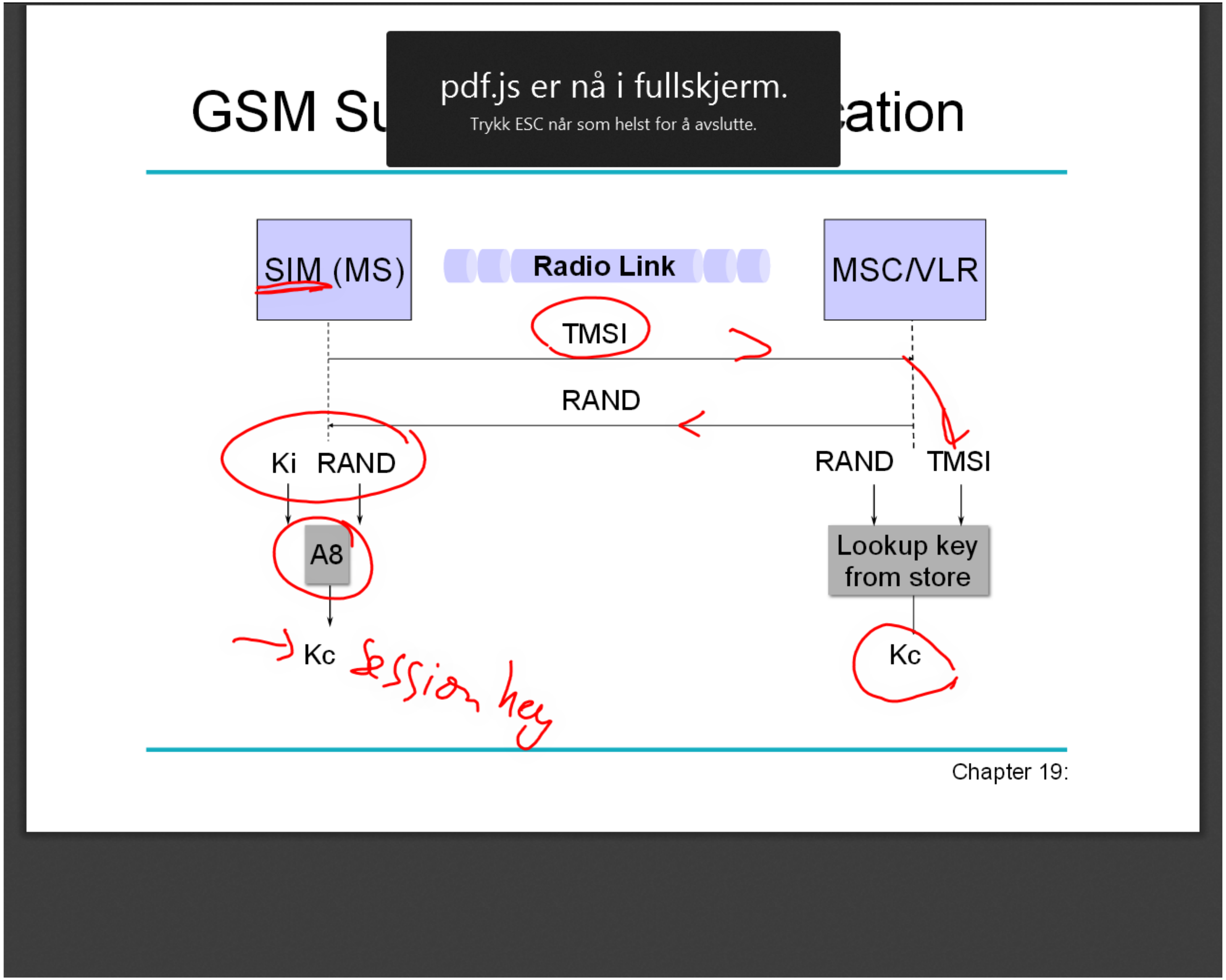
pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

GSM 02 cts

- The authentication of the GSM PLMN subscriber identity may be triggered by the network when the subscriber applies for:
  - change of subscriber–related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service); or
  - access to a service (including some or all of: set–up of mobile originating or terminated calls, activation or deactivation of a supplementary service); or
  - first network access after restart of MSC/VLR; or in the event of cipher key sequence number mismatch.

Chapter 19:



GSM Su

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

ation

SIM (MS)

Radio Link

MSC/VLR

TMSI

RAND

Ki RAND

A8

Kc

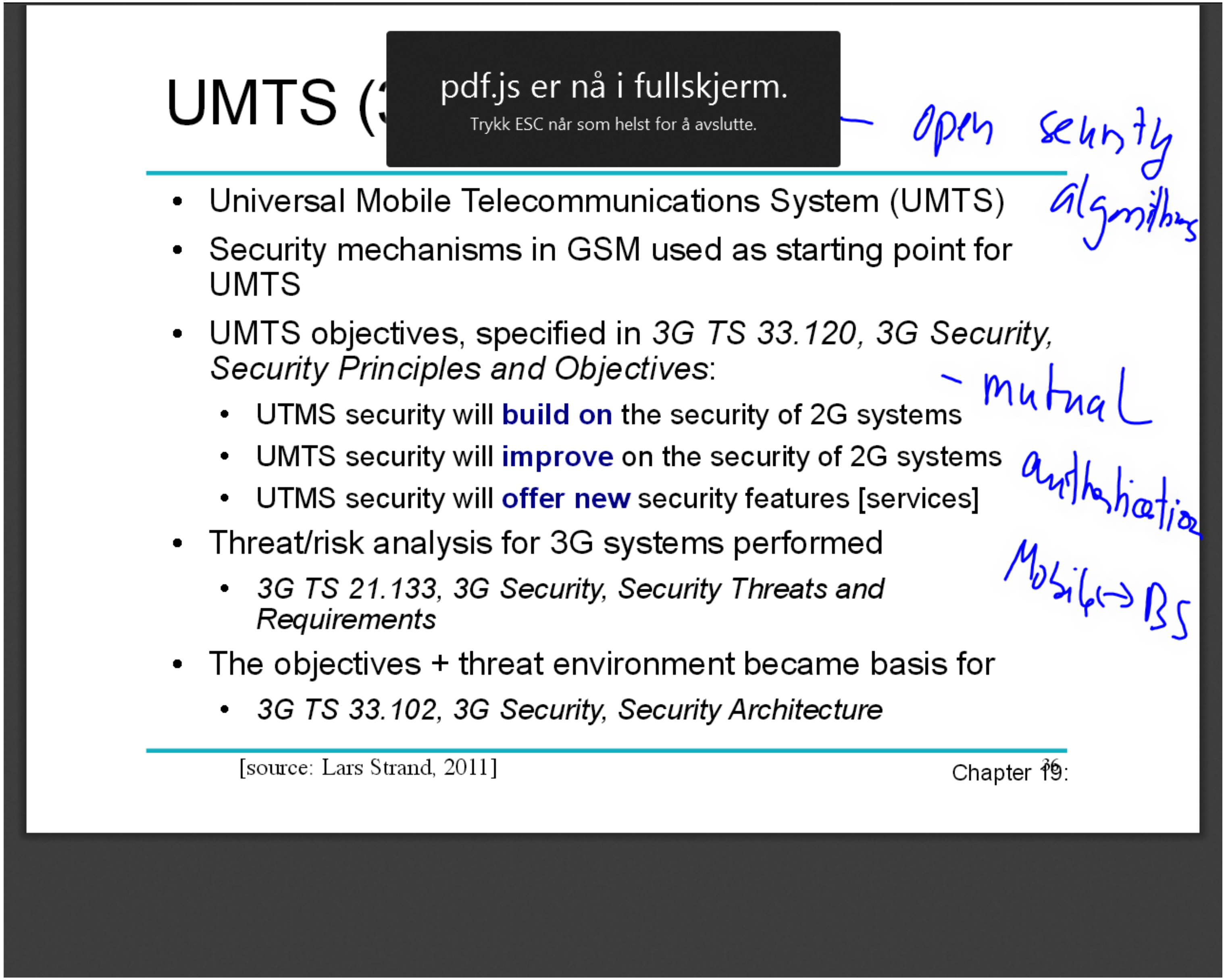
session key

RAND TMSI

Lookup key from store

Kc

Chapter 19:



pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

UMTS (3

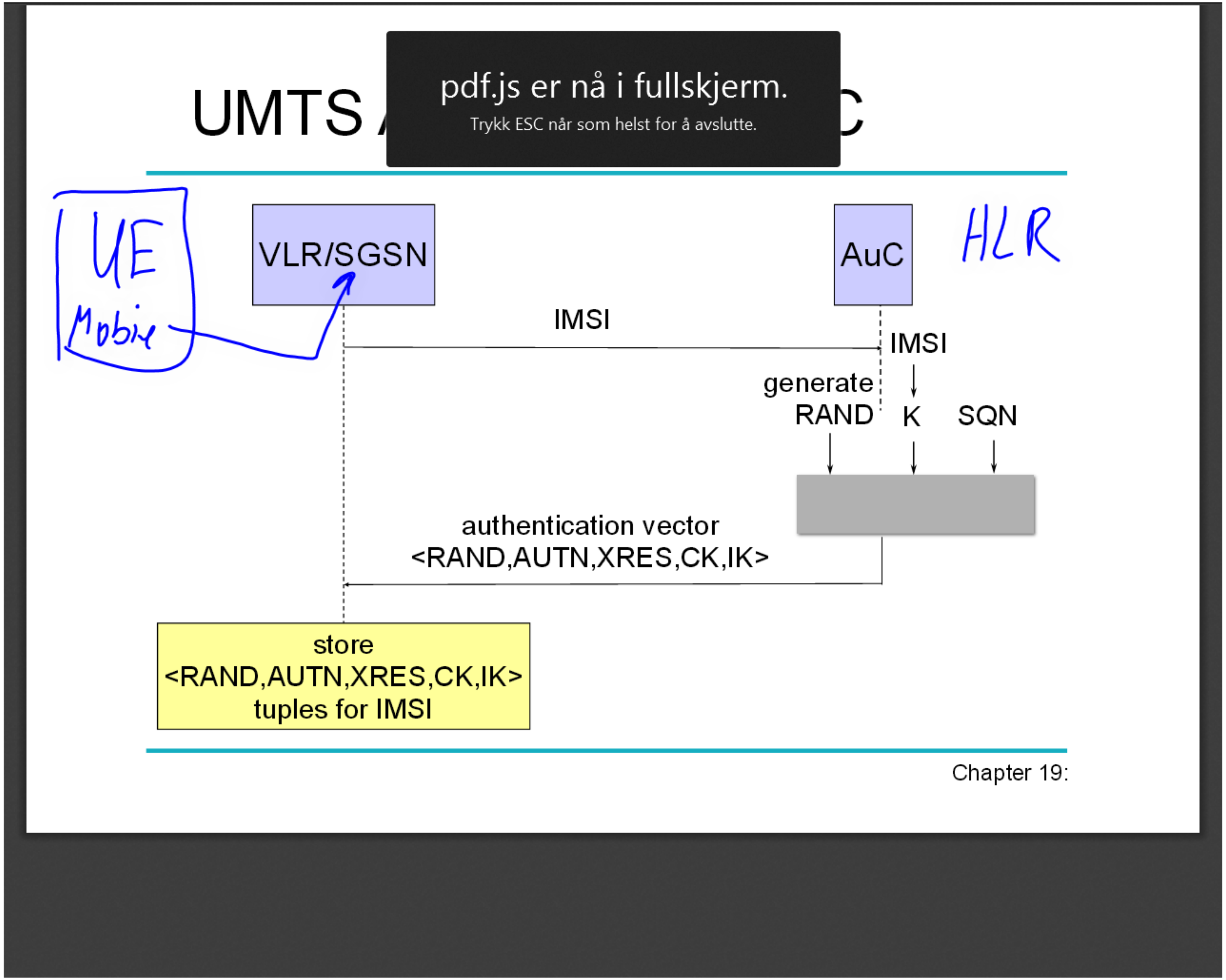
- open security algorithms

- Universal Mobile Telecommunications System (UMTS)
- Security mechanisms in GSM used as starting point for UMTS
- UMTS objectives, specified in *3G TS 33.120, 3G Security, Security Principles and Objectives*:
  - UTMS security will **build on** the security of 2G systems
  - UMTS security will **improve** on the security of 2G systems
  - UTMS security will **offer new** security features [services]
- Threat/risk analysis for 3G systems performed
  - *3G TS 21.133, 3G Security, Security Threats and Requirements*
- The objectives + threat environment became basis for
  - *3G TS 33.102, 3G Security, Security Architecture*

- mutual authentication Mobile ↔ BS

[source: Lars Strand, 2011]

Chapter 19: 36



UMTS C

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

UE

Mobile

VLR/SGSN

AuC

HLR

IMSI

IMSI

generate RAND

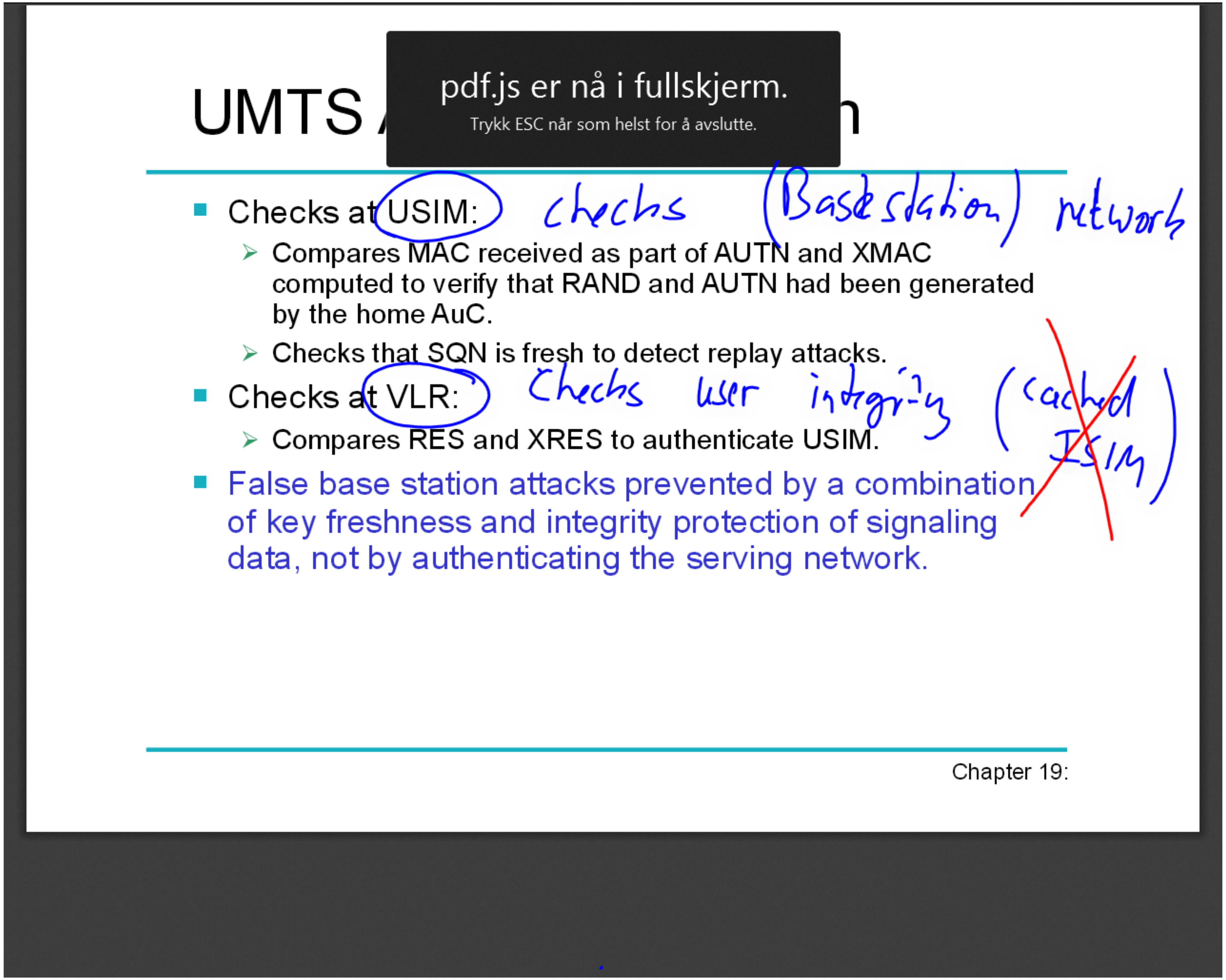
K

SQN

authentication vector <RAND,AUTN,XRES,CK,IK>

store <RAND,AUTN,XRES,CK,IK> tuples for IMSI

Chapter 19:



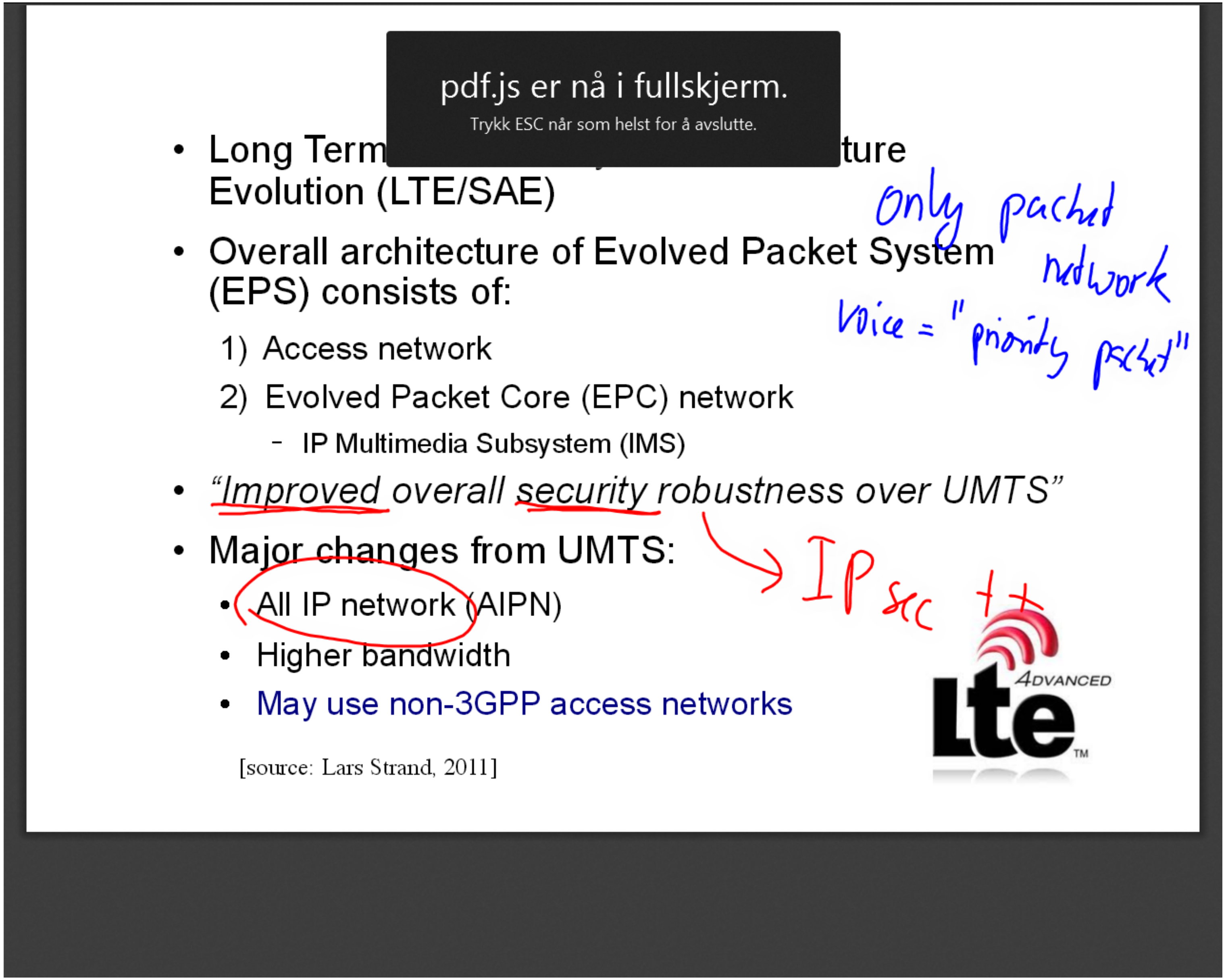
UMTS [illegible]n

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

- Checks at USIM: checks (Base station) network
  - Compares MAC received as part of AUTN and XMAC computed to verify that RAND and AUTN had been generated by the home AuC.
  - Checks that SQN is fresh to detect replay attacks.
- Checks at VLR: Checks user integrity (~~cached ISIM~~)
  - Compares RES and XRES to authenticate USIM.
- False base station attacks prevented by a combination of key freshness and integrity protection of signaling data, not by authenticating the serving network.

Chapter 19:



pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

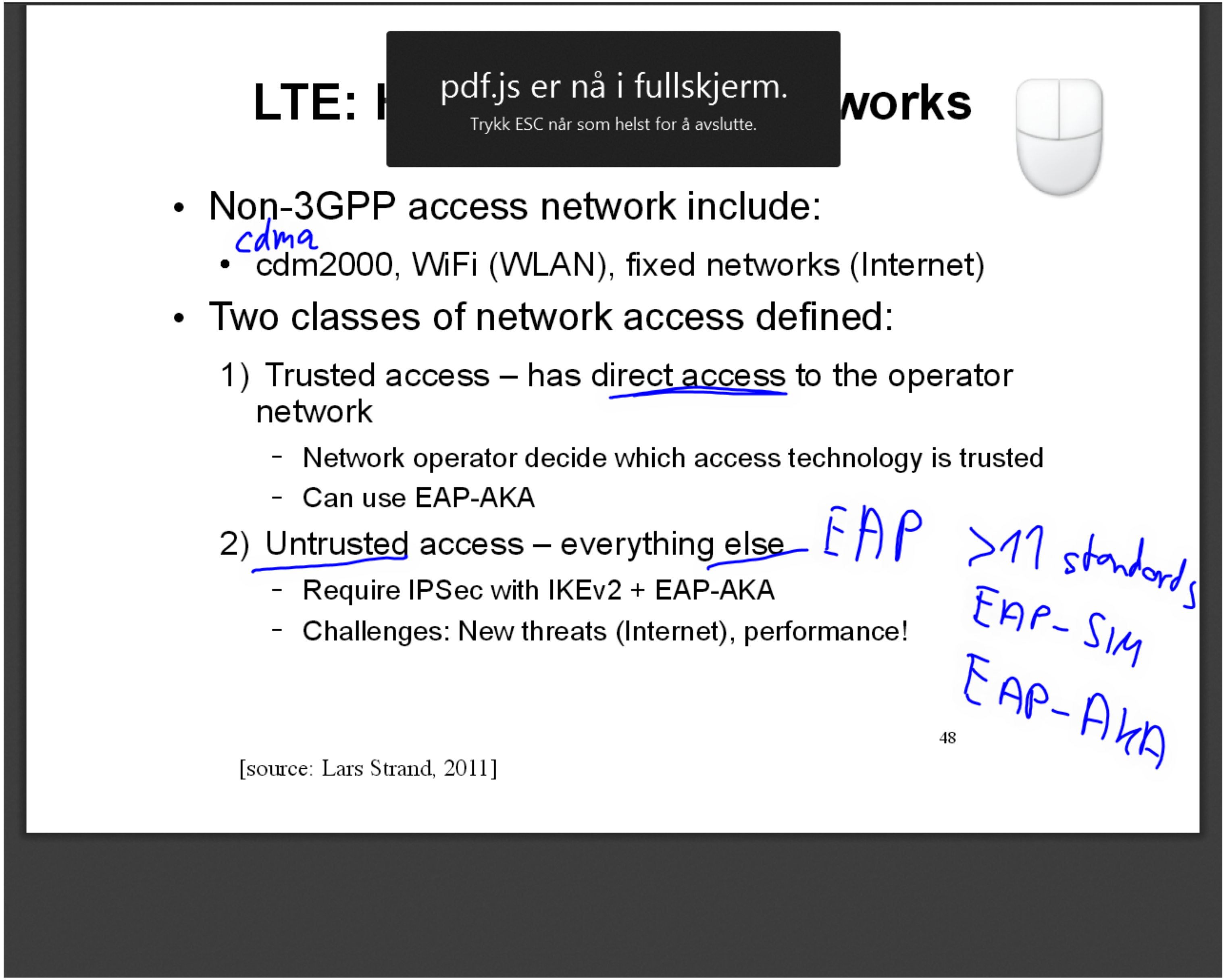
- Long Term ture Evolution (LTE/SAE)
- Overall architecture of Evolved Packet System (EPS) consists of:
  1) Access network
  2) Evolved Packet Core (EPC) network
     - IP Multimedia Subsystem (IMS)
- *"Improved overall security robustness over UMTS"*
- Major changes from UMTS:
  - All IP network (AIPN)
  - Higher bandwidth
  - May use non-3GPP access networks

[source: Lars Strand, 2011]

only packet network

Voice = "priority packet"

IPsec ++



LTE: I

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

works

- Non-3GPP access network include:
  - cdma
  - cdm2000, WiFi (WLAN), fixed networks (Internet)
- Two classes of network access defined:

1) Trusted access – has direct access to the operator network
   - Network operator decide which access technology is trusted
   - Can use EAP-AKA

2) Untrusted access – everything else EAP
   - Require IPSec with IKEv2 + EAP-AKA
   - Challenges: New threats (Internet), performance!

>11 standards

EAP-SIM

EAP-AKA

48

[source: Lars Strand, 2011]

EAP-SIM, EAP-AKA 1

<u>authenticator</u>

& federation between operators

m: +47 90838066 Telenor ⟹ Josef Noll

Signatur & encrypted email 2

Attach on GRX

GRX

- British Secret Service
- looked for people <u>Belgacom</u>
- "inject a virus" - faked LinkedIn
- captured http calls, inserted their LinkedIn

→ insert program on all mobiles

binary code update