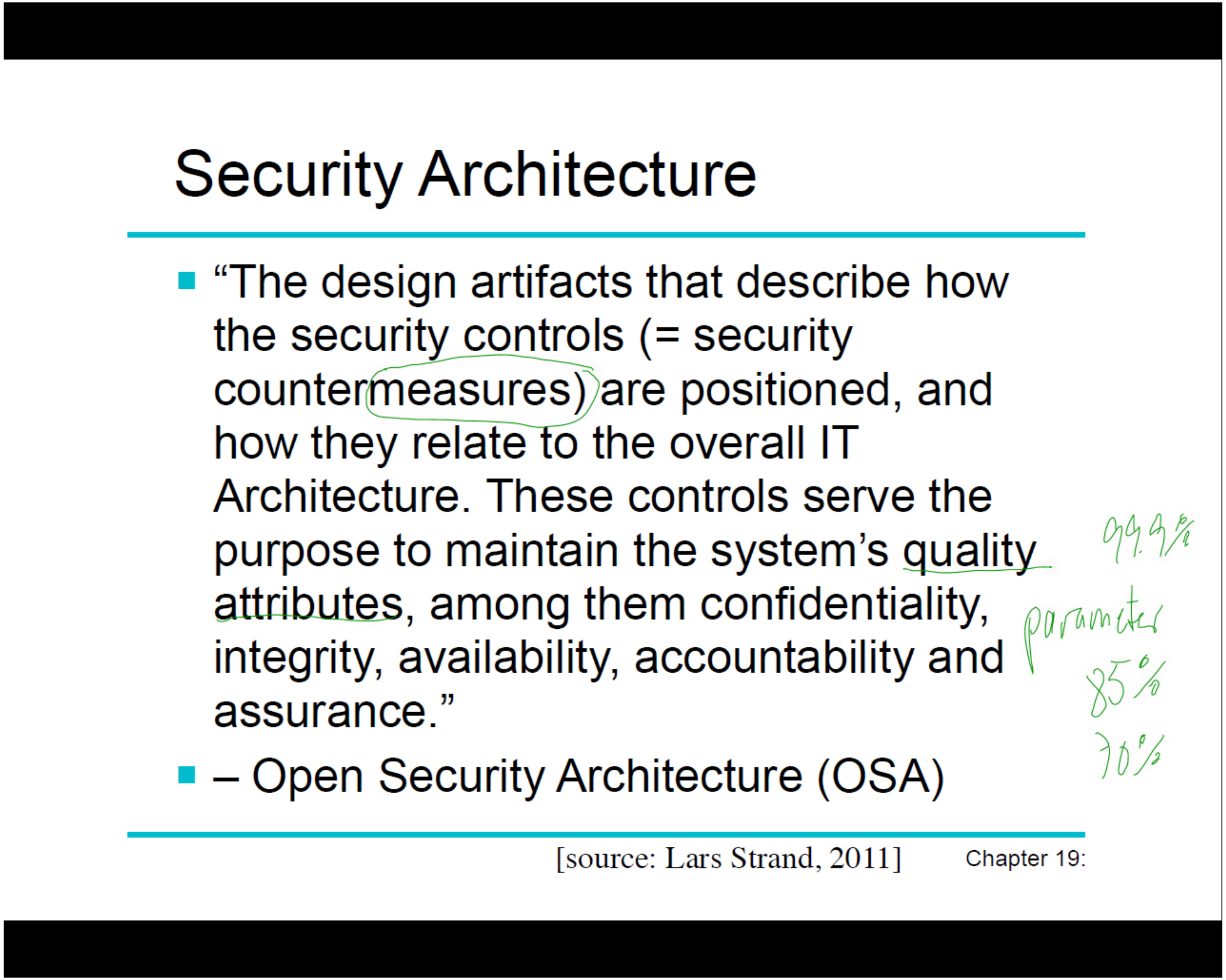
Cwi.unik.no/wiki/UNIK4250



Security Architecture

- “The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes, among them confidentiality, integrity, availability, accountability and assurance.”
- – Open Security Architecture (OSA)

99.9%

parameter

85%

70%

[source: Lars Strand, 2011]

Chapter 19:

Mobile systems: GSM

- Developed in the late 1980s, deployed 1992.
  - Norway a key developer and inventor
- Today: Cover 80% of world population (5+ billion users!), gsmworld.com.
- GSM security goal: “as secure as the wire”
- GSM network consists of several network elements
  - Radio Subsystem (RSS)
    - Base station Subsystem (BSS)
    - Mobile Equipment (ME) (cell phone/handset)
  - Network and Switching Subsystem (NSS) – core network
  - Operation Subsystem (OSS)

Telecom
"plain"

[source: Lars Strand, 2011]

Security

architecture

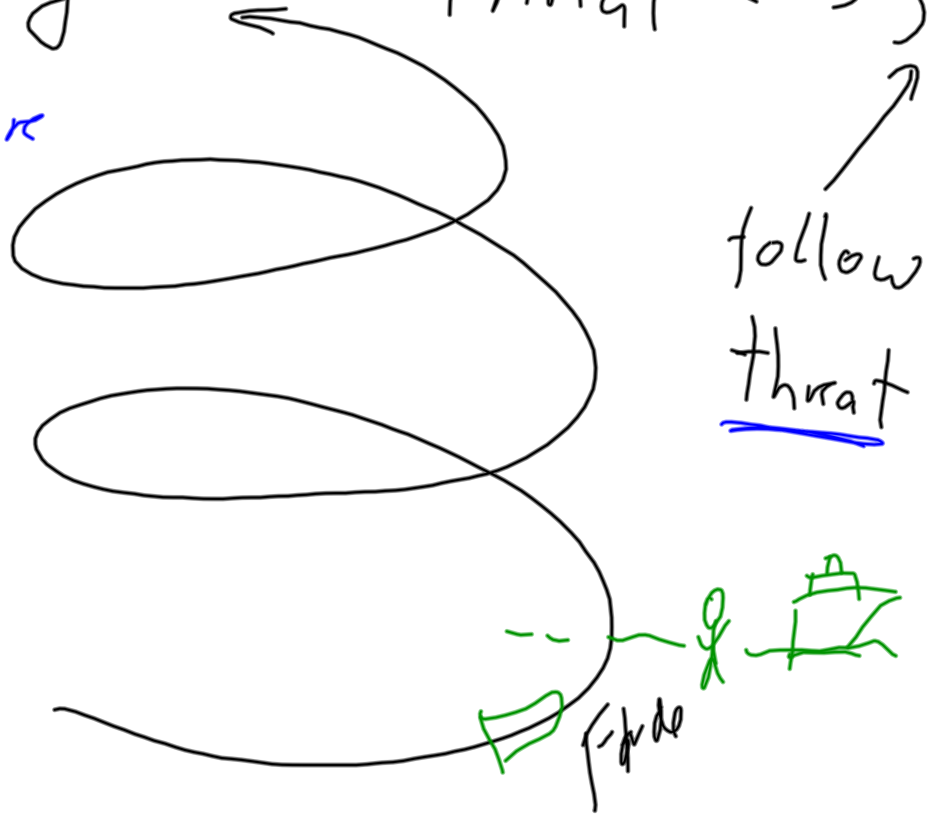
Threat ↔ System

2

follow

threat

1



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): Western Europe
  - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
  - Identification of MS (IMEI), not always implemented.

Security Goals

signalling

- Protect against interception of voice traffic on the radio channel: 8 tidsluker
  - ➢ Encryption of voice traffic.

- Protect signalling data on the radio channel: egen kanal
  - ➢ Encryption of signalling data.
- Protections against unauthorised use (charging fraud): (SMS)
  - ➢ Subscriber authentication (IMSI, TMSI).

credential

- Theft of end device:
  - ➢ Identification of MS (IMEI), not always implemented.

mobilnummer

2G ⟷ GSM, IS95

IMT 3G ⟷ UMTS

3.9G . . . . — LTE, Wimax, 802.16e

= 4G "sales"

IMT-A 4G

100 MBit/s high mobility

1 GBit/s low mobility, stadionairy

ITU

Brand

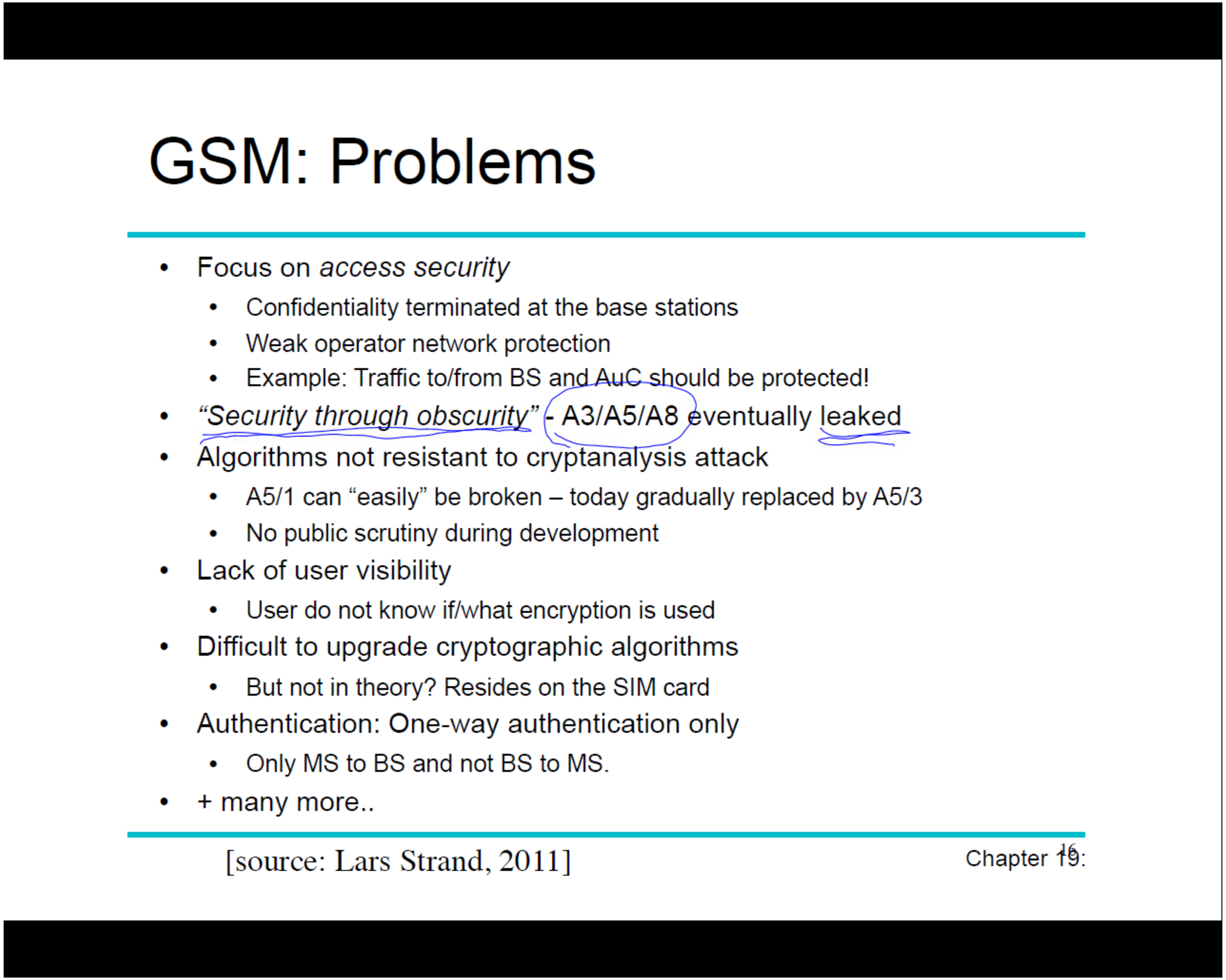
Family of radio interfaces

GSM – Components

Trusted Element
nano SIM
virtual SIM

- 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
- …

utlandet



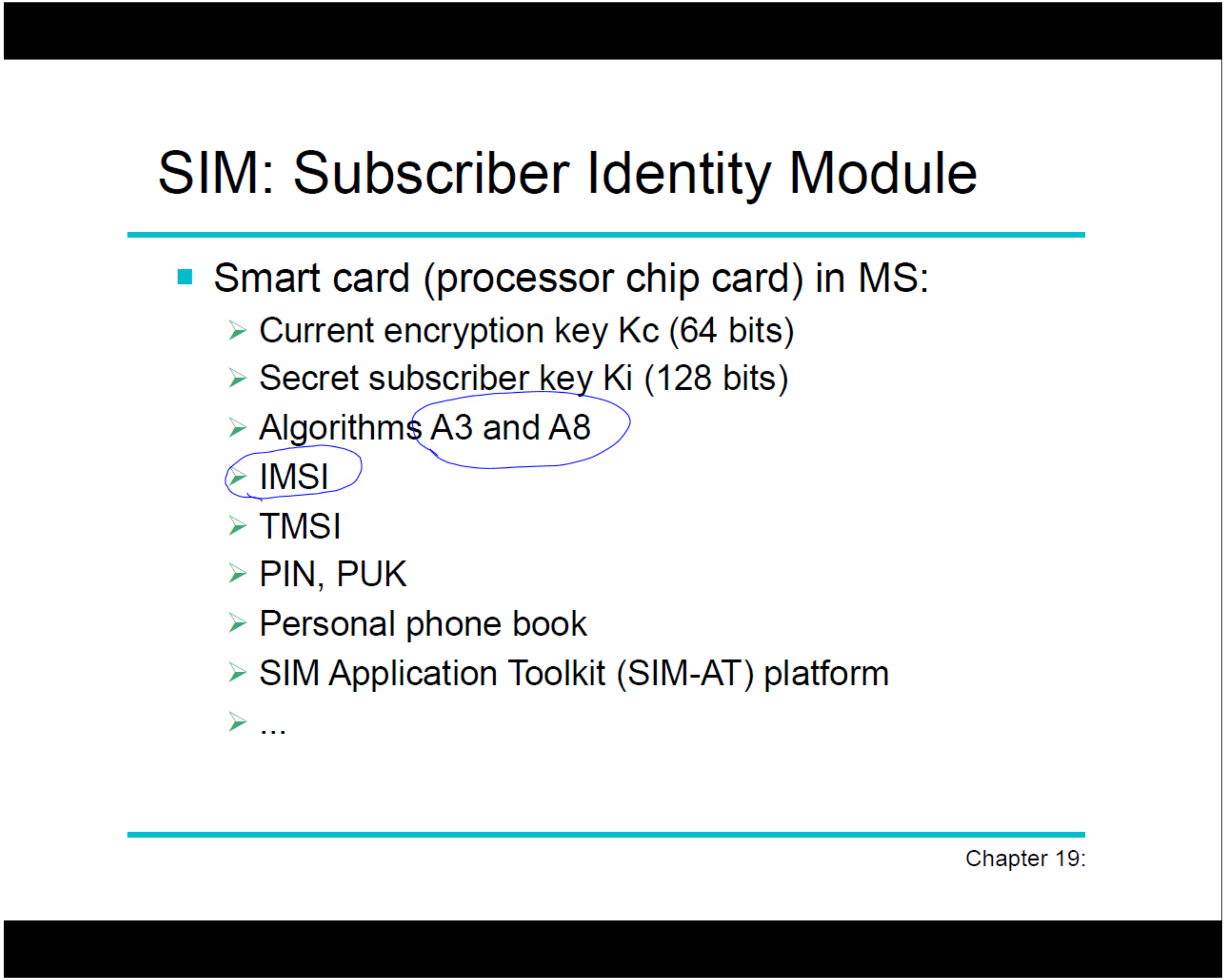
GSM: Problems

- Focus on *access security*
  - Confidentiality terminated at the base stations
  - Weak operator network protection
  - Example: Traffic to/from BS and AuC should be protected!
- *"Security through obscurity"* - A3/A5/A8 eventually leaked
- Algorithms not resistant to cryptanalysis attack
  - A5/1 can "easily" be broken – today gradually replaced by A5/3
  - No public scrutiny during development
- Lack of user visibility
  - User do not know if/what encryption is used
- Difficult to upgrade cryptographic algorithms
  - But not in theory? Resides on the SIM card
- Authentication: One-way authentication only
  - Only MS to BS and not BS to MS.
- + many more..

[source: Lars Strand, 2011]

16

Chapter 19:

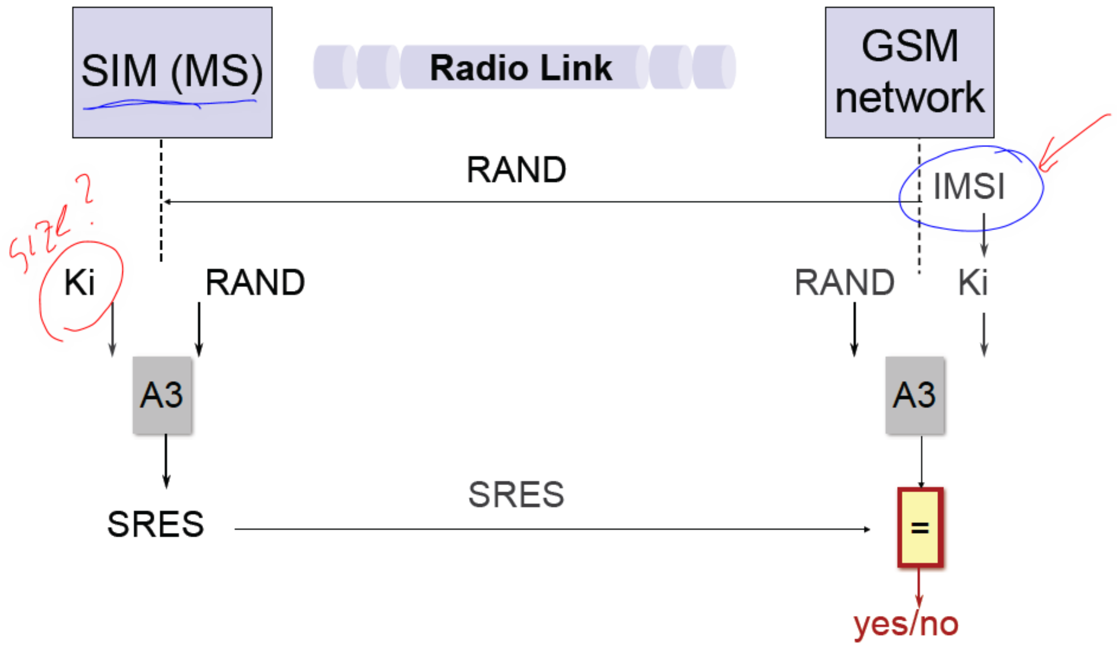


SIM: Subscriber Identity Module

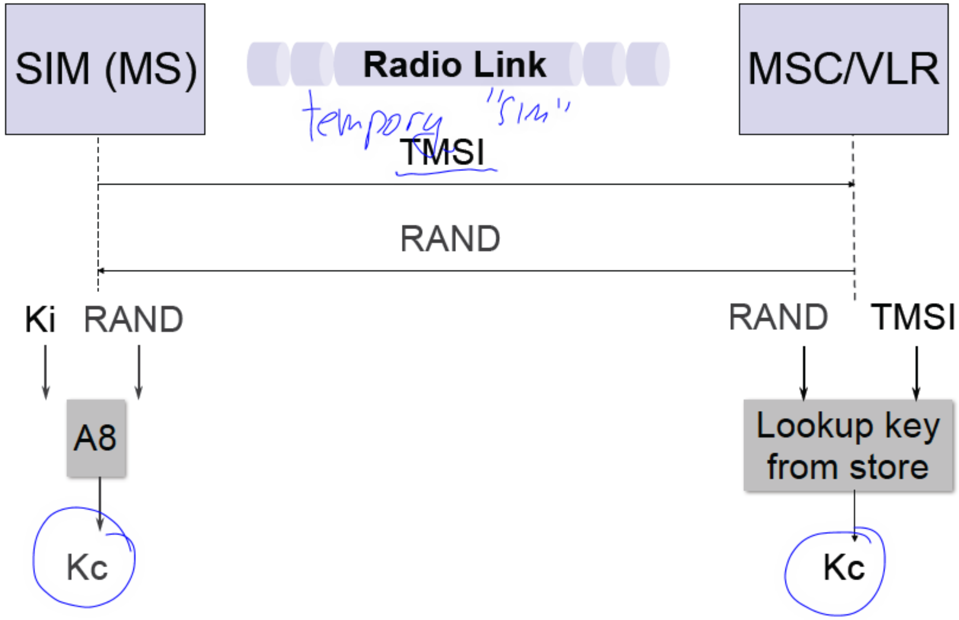
- Smart card (processor chip card) in MS:
  - Current encryption key Kc (64 bits)
  - Secret subscriber key Ki (128 bits)
  - Algorithms A3 and A8
  - IMSI
  - TMSI
  - PIN, PUK
  - Personal phone book
  - SIM Application Toolkit (SIM-AT) platform
  - ...

GSM Subscriber Authentication

Trusted



GSM Subscriber Authentication



SIM (MS)

Radio Link

MSC/VLR

tempory "sim"

TMSI

RAND

Ki RAND

A8

Kc

RAND TMSI

Lookup key from store

Kc

Cryptographic Algorithms: A3/A8

- Algorithms A3 and A8 shared between subscriber and home network; thus each network could choose its own algorithms.
  - Algorithms A3 and A8 at each PLMN operator’s discretion.
  - GSM 03.20 specifies only the formats of their inputs and outputs; processing times should remain below a maximum value (A8: 500 msec).
- COMP128: one choice for A3/A8; attack to retrieve Ki from the SIM (→ cloning) possible; not used by many European providers.

standard

MS/BSC Encryption

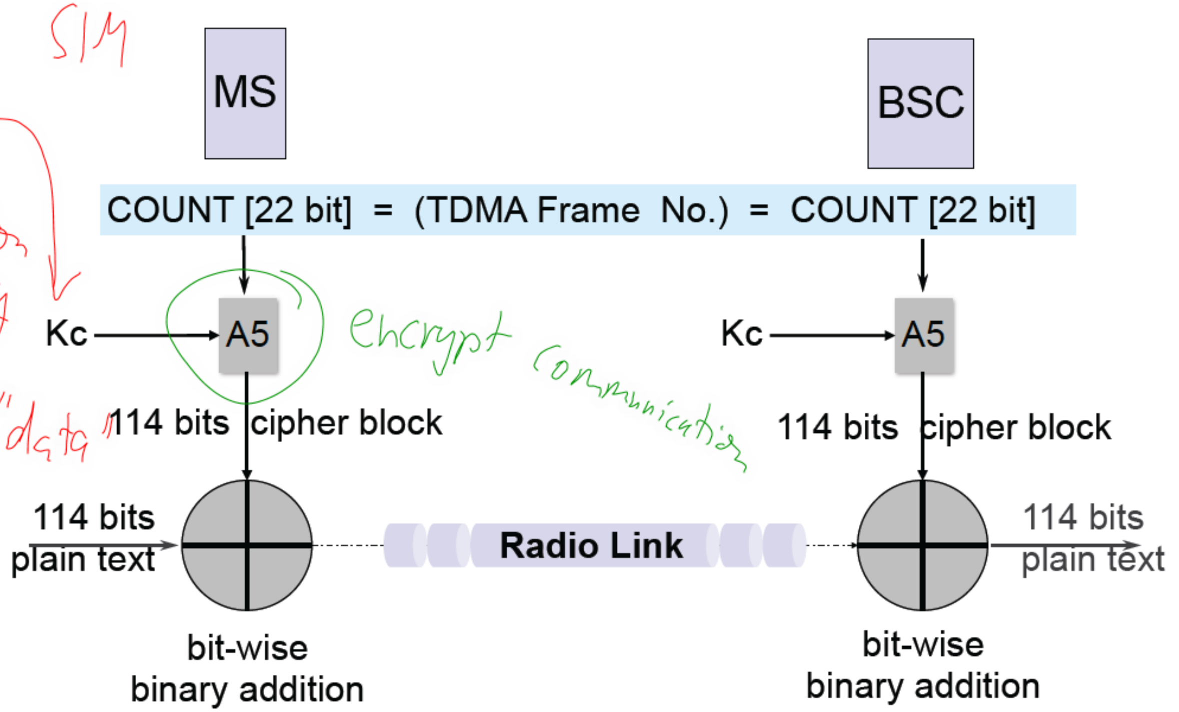
A3: SIM

A8

session key

A5 "data"

A5.1, 5.2, 5.3, 5.4



Chapter 19:

Biometric passport

"legal"
= papir

RFID

lev1: passport data
text

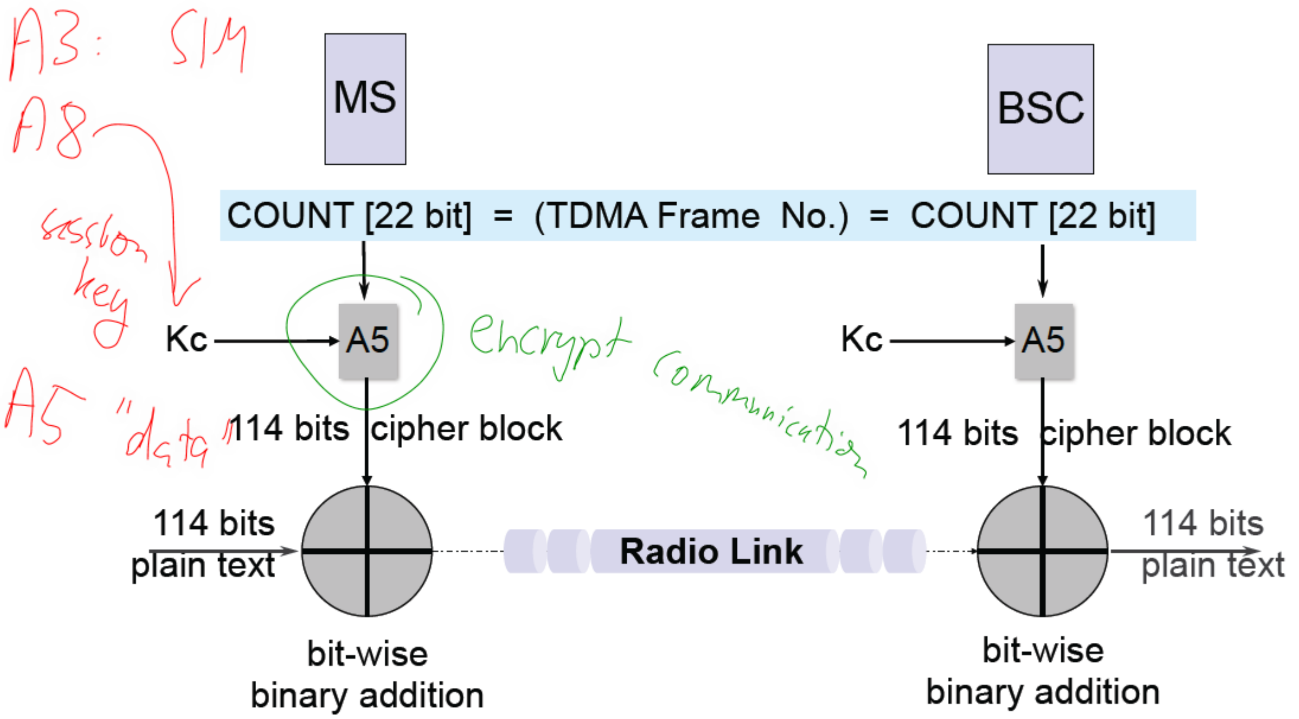
pass nr + utløpsdato + fødselsdato

lev2: biometric (fingerprint)

ingen enighet!

- personvern

MS/BSC Encryption



A3: SIM

A8

session key

A5 "data"

encrypt communication

MS

BSC

COUNT [22 bit] = (TDMA Frame No.) = COUNT [22 bit]

Kc → A5

Kc → A5

114 bits cipher block

114 bits cipher block

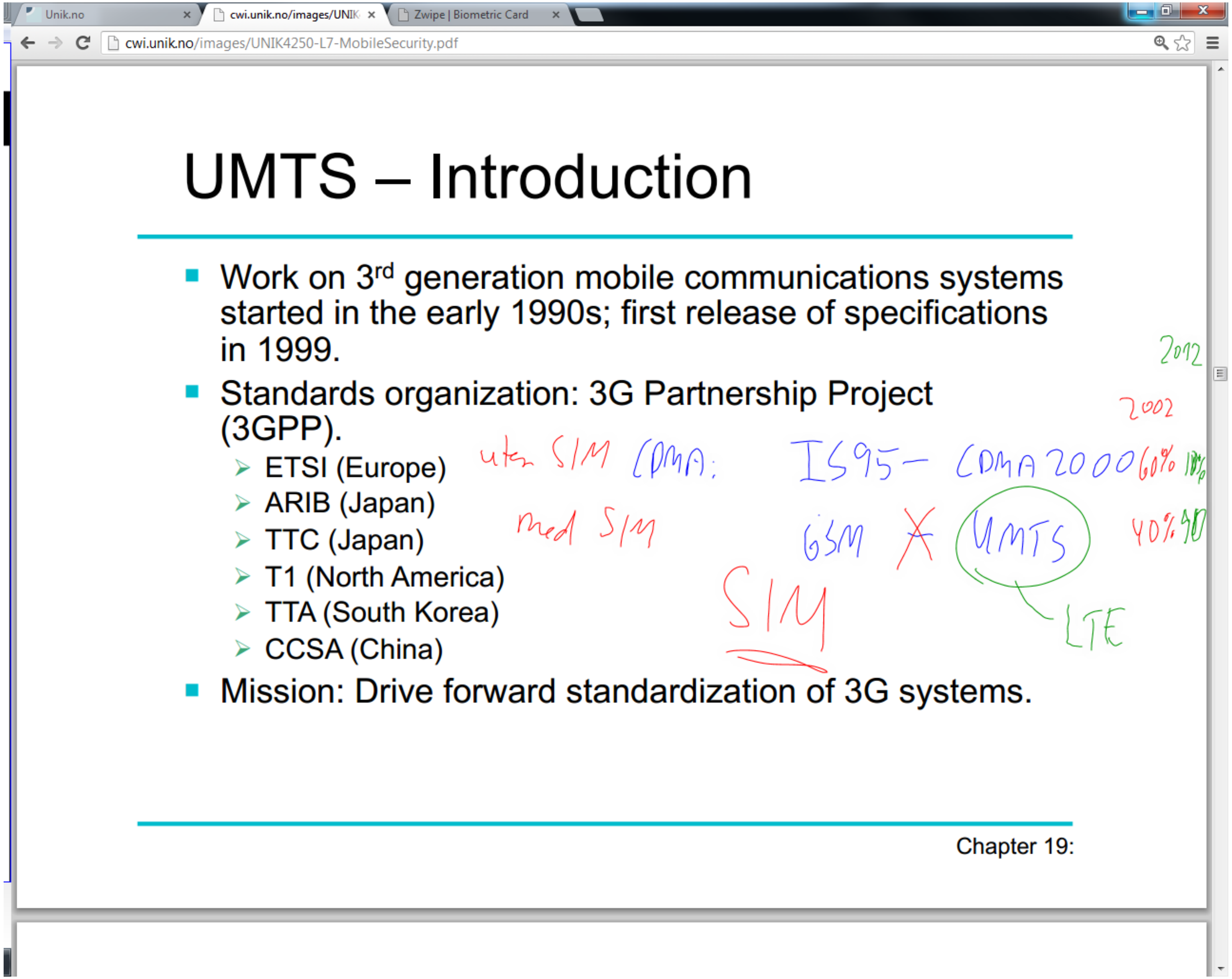
114 bits plain text

Radio Link

114 bits plain text

bit-wise binary addition

bit-wise binary addition



UMTS – Introduction

- Work on 3rd generation mobile communications systems started in the early 1990s; first release of specifications in 1999.
- Standards organization: 3G Partnership Project (3GPP).
  - ETSI (Europe)
  - ARIB (Japan)
  - TTC (Japan)
  - T1 (North America)
  - TTA (South Korea)
  - CCSA (China)
- Mission: Drive forward standardization of 3G systems.

2012

2002

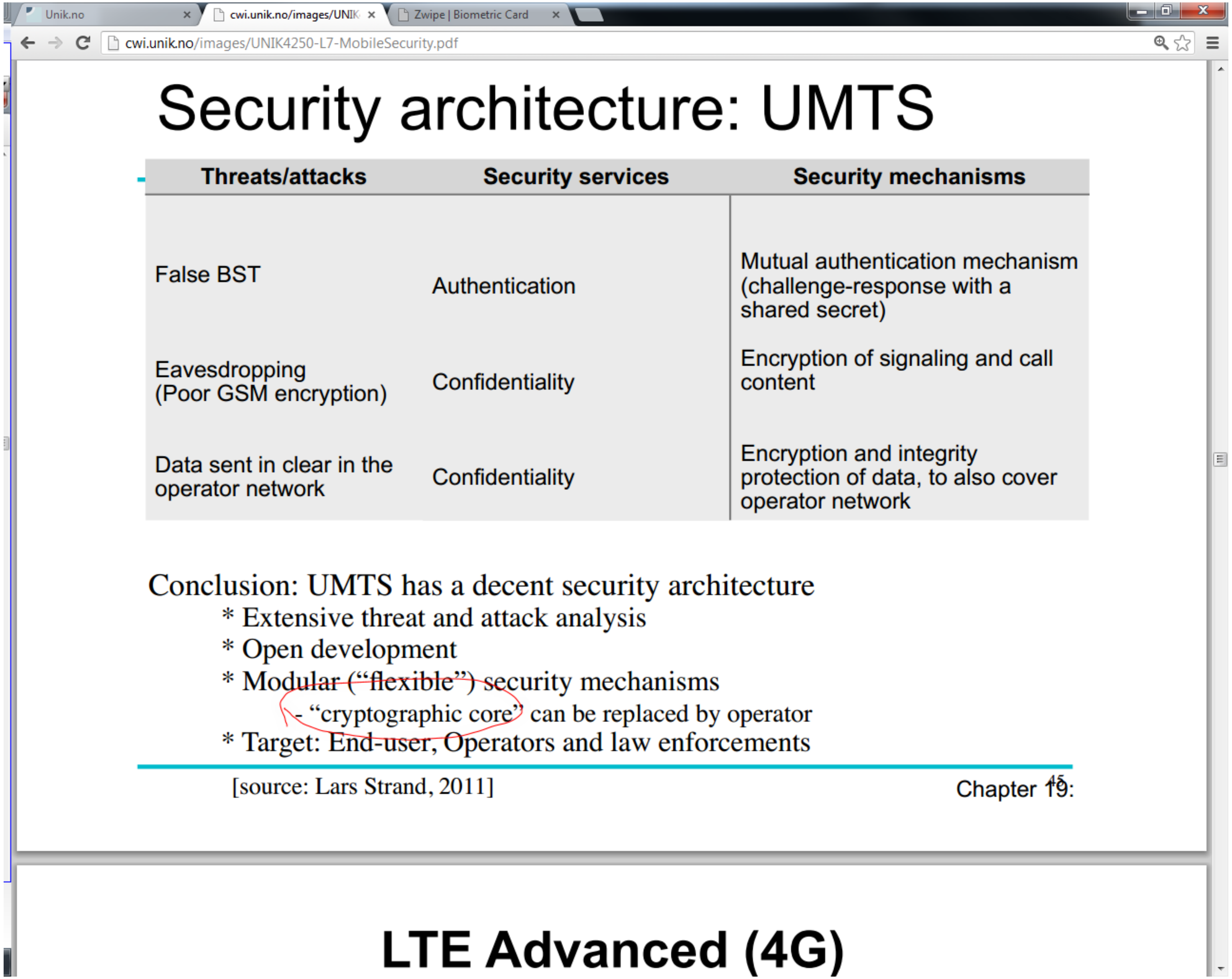
uten SIM CDMA: IS95– CDMA2000 60% 10%

med SIM GSM ✗ UMTS 40% 90

SIM

LTE

Chapter 19:



Security architecture: UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

Conclusion: UMTS has a decent security architecture

* Extensive threat and attack analysis
* Open development
* Modular (“flexible”) security mechanisms
  - “cryptographic core” can be replaced by operator
* Target: End-user, Operators and law enforcements

[source: Lars Strand, 2011]

Chapter 19:

45

LTE Advanced (4G)

(2G | 3G)

GSM & UMTS

WCDMA ≠ TDCDMA i UMTS

støy

sender

dårlig sikkerhet

nå

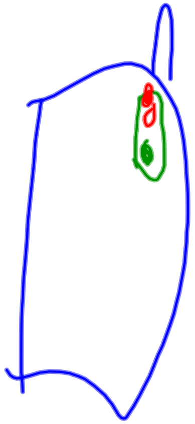
MHz

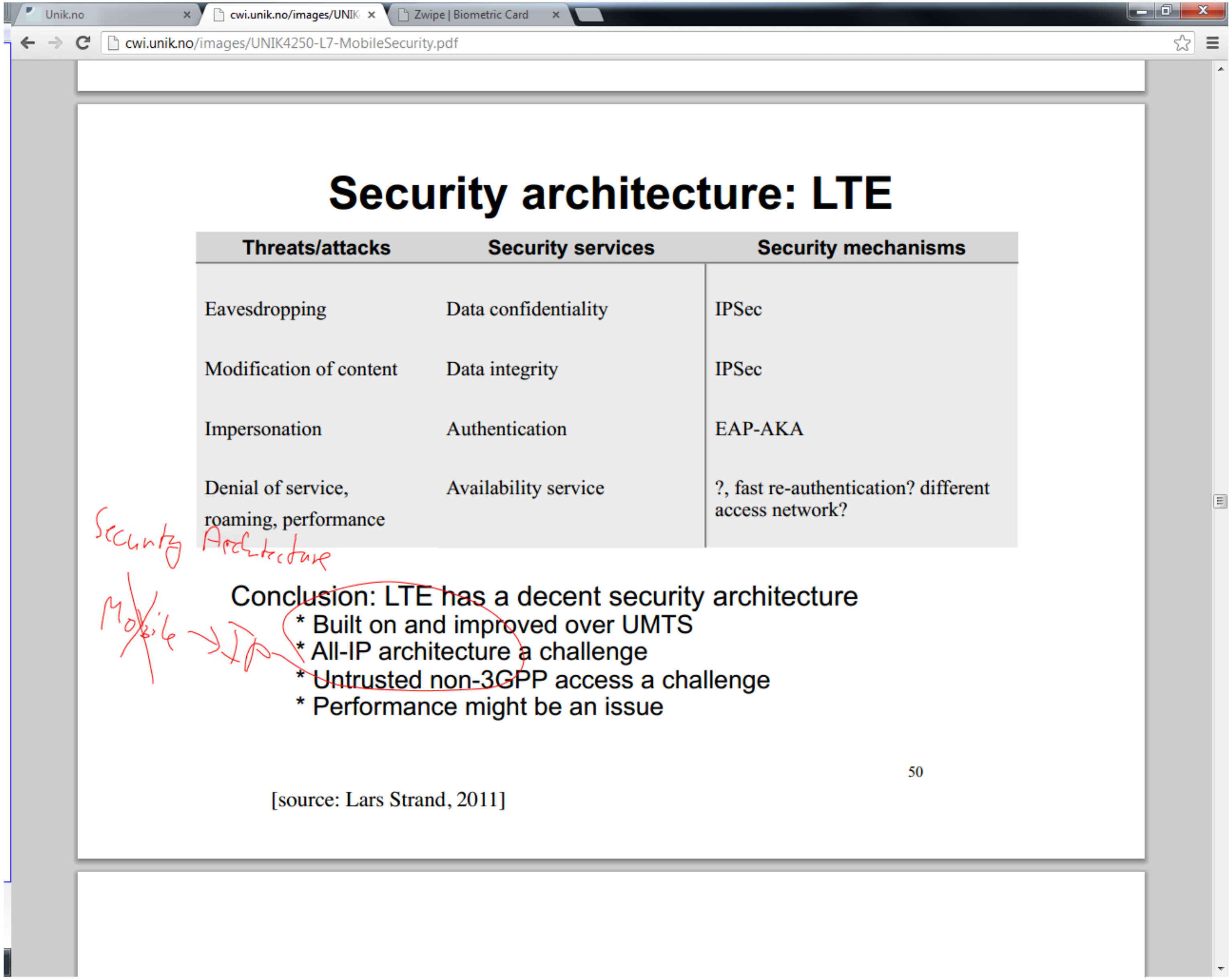
UMTS 900

GSM: 900, 1800

UMTS: 1900, 2100

LTE: 2600





Security architecture: LTE

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	?, fast re-authentication? different access network?

Security Architecture

Mobile → IP

Conclusion: LTE has a decent security architecture
- Built on and improved over UMTS
- All-IP architecture a challenge
- Untrusted non-3GPP access a challenge
- Performance might be an issue

50

[source: Lars Strand, 2011]