Honors Option for NSSA 245

Alex Beaver

Cellular Cryptography

26 April 2023

alexbeaver.com

Topics

- What drove mobile network design?
- How does authentication/ authorization happen?
- How does transport-layer security work?

Constraints of a Mobile Network

- Radio roaming
- Access method and core are independent
- Billing and QoS

Structure

SIM Card (SIM)

User Endpoint (UE)

Base Station/Radio (eNB/ng-eNB)

Mobility Management Engine (MME)

Packet Core

Home Subscriber Server (HSS)

SIM Card (SIM)

- Chip for Network Authentication
- Inside of the User Endpoint
- Cryptographic Operations, Data Storage
- Data about the subscriber
- TPM to store keys
- Duplicate of data on HSS

SIM Card (SIM)

User Endpoint (UE)

Base Station/Radio (eNB/ng-eNB)

Mobility Management Engine (MME)

Packet Core

Home Subscriber Server (HSS)

User Endpoint (UE)

- Device that a user interacts with
- Phone, Laptop, Car, Vending Machine
- Contains the SIM Card
- Radios to connect to the network

SIM Card (SIM)

User Endpoint (UE)

Base Station/Radio (eNB/ng-eNB)

Mobility Management Engine (MME)

Packet Core

Home Subscriber Server (HSS)

Mobility Management Engine (MME)

- Per Region
- Part of the EPC
- Owned by Serving Network
- Manages connection to the network

SIM Card (SIM)

User Endpoint (UE)

Base Station/Radio (eNB/ng-eNB)

Mobility Management Engine (MME)

Packet Core

Home Subscriber Server (HSS)

Home Subscriber Server (HSS)

- Part of Packet Core
- Owned by home carrier
- Stores data about customers and SIM cards
- Manages authentication, QoS, Billing, etc.

SIM Card (SIM)

User Endpoint (UE)

Base Station/Radio (eNB/ng-eNB)

Mobility Management Engine (MME)

Packet Core

Home Subscriber Server (HSS)

AAA

Authentication vs Authorization

Authentication

- Who is a SIM card assigned to?
- Is this a legitimate device?
- Is this device on a legitimate network?

Authorization

- Is a user allowed to roam on this network?
- Can a user access certain carrier resources?
- What QoS should this device expect?

Authentication and Authorization

- Challenge/Response
- SIM/UE initiates a connection to MME
- MME forwards SIM data to HSS
- HSS gives a random value to the SIM, and tells MME what to expect as output

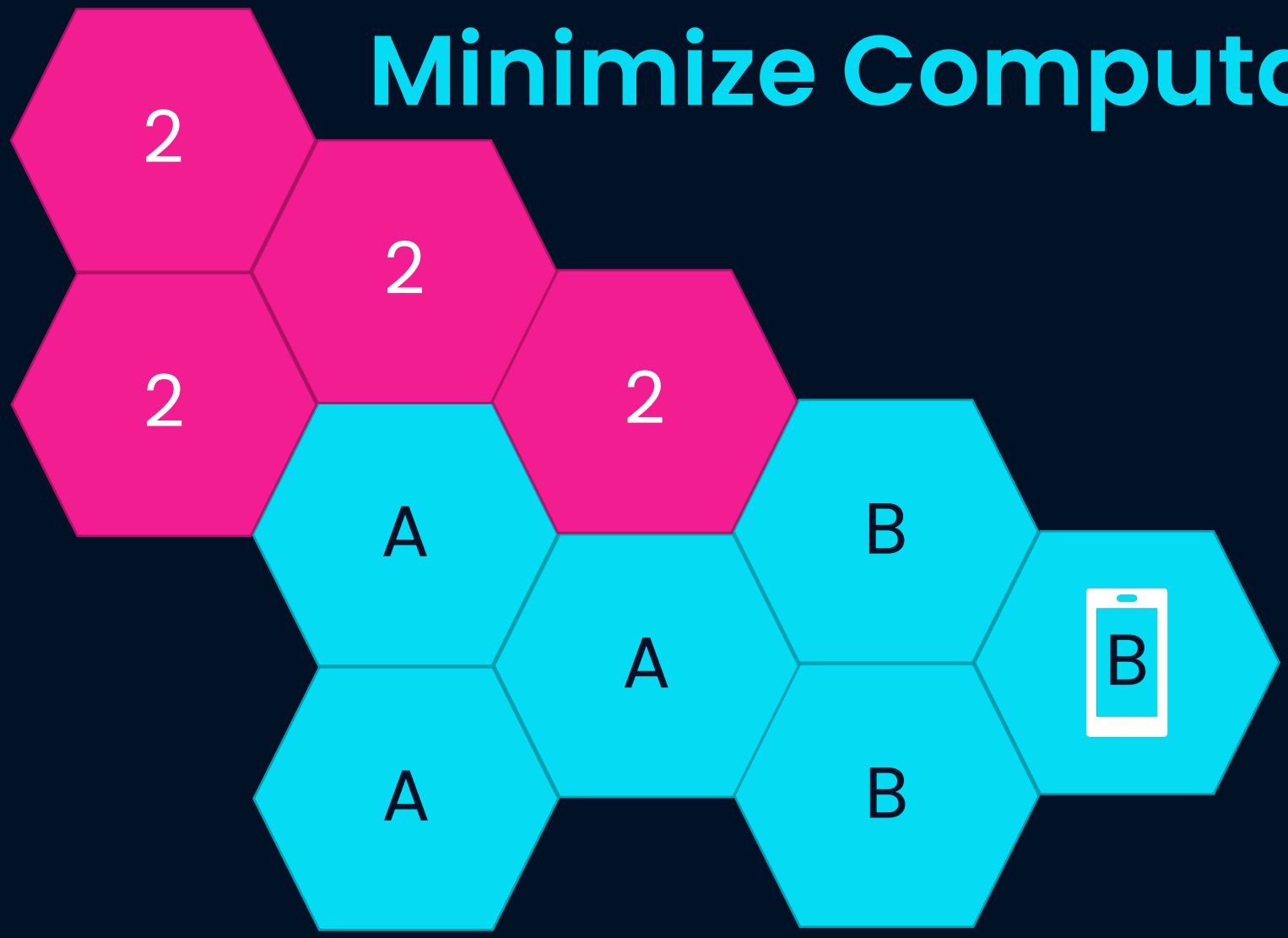
Keys

- Root is stored on HSS and derived on SIM
- Derive down
- Limit scope
  - Add parameter at each step, cannot reverse upwards
- HSS is a relay

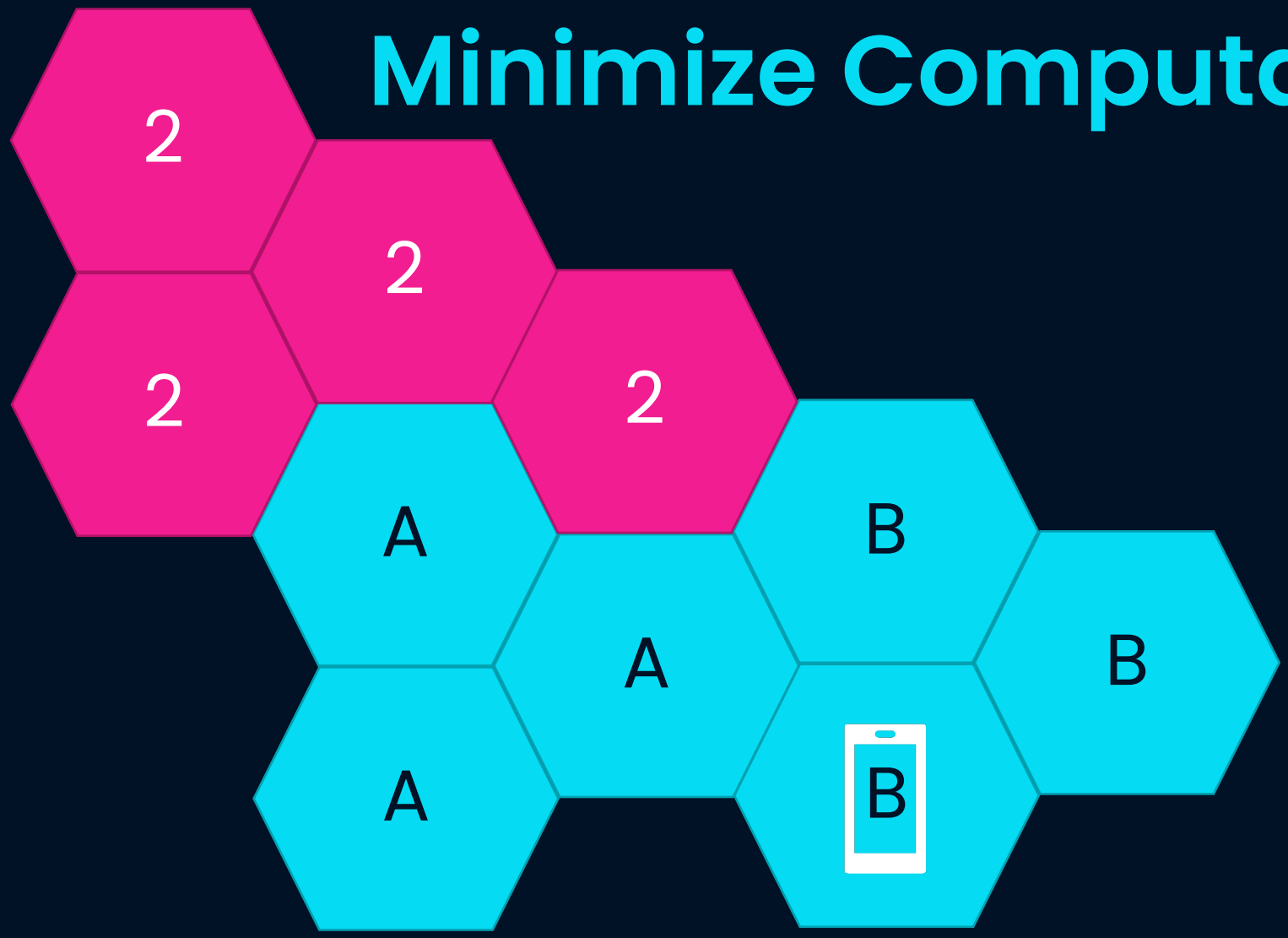
Keys

- K is stored on SIM
- Cipher Key, Integrity Key on HSS
  - Derivation is Carrier-Specific
- K_{ASME} is per SN/SEQ, on MME
- K_{eNB} adds COUNT, at eNodeB

Minimize Computation



Minimize Computation



Change eNodeB

K

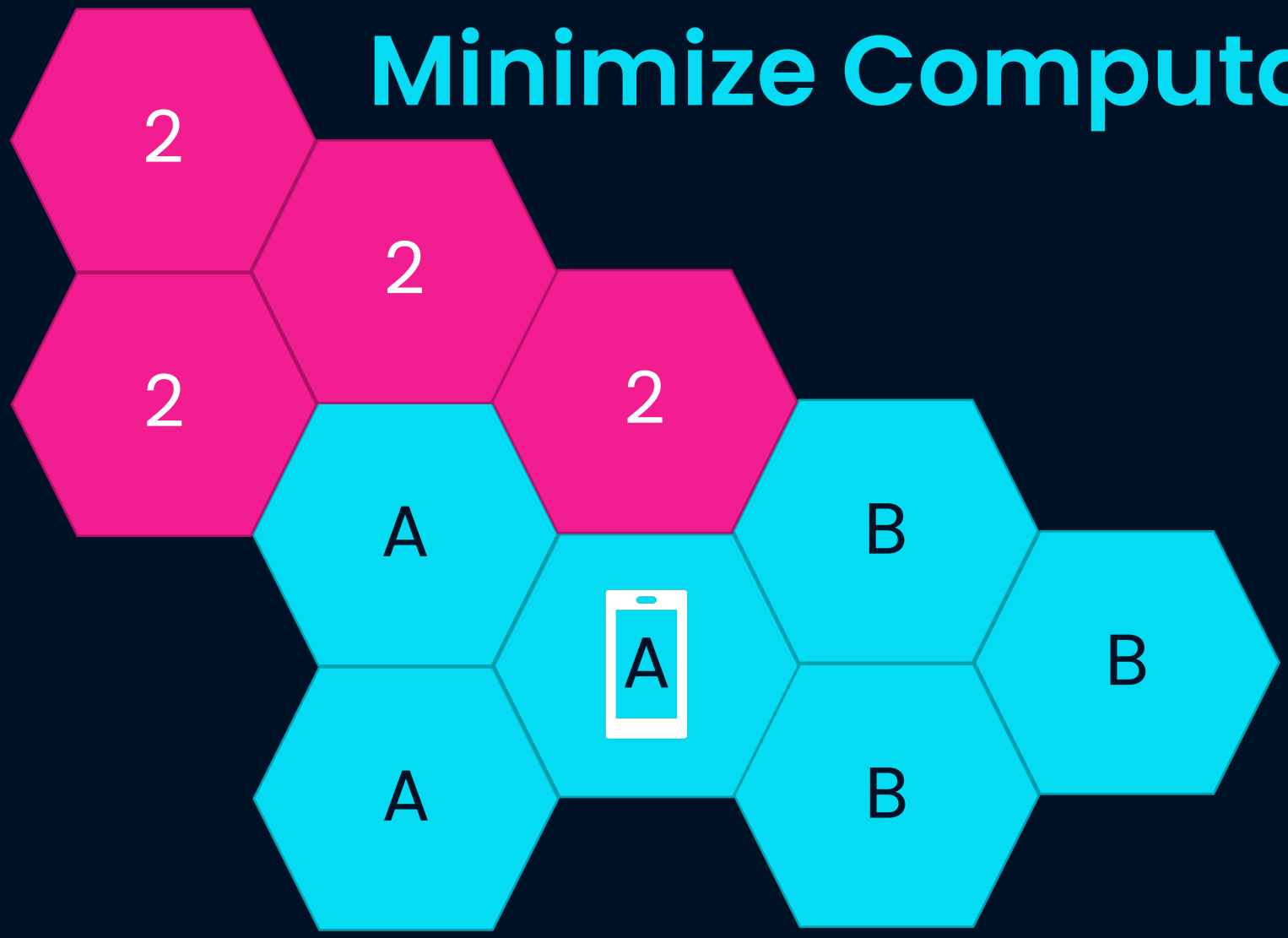
CK, IK

SEQ

K_{ASME}

K_{eNB}

Minimize Computation



Change MME

K

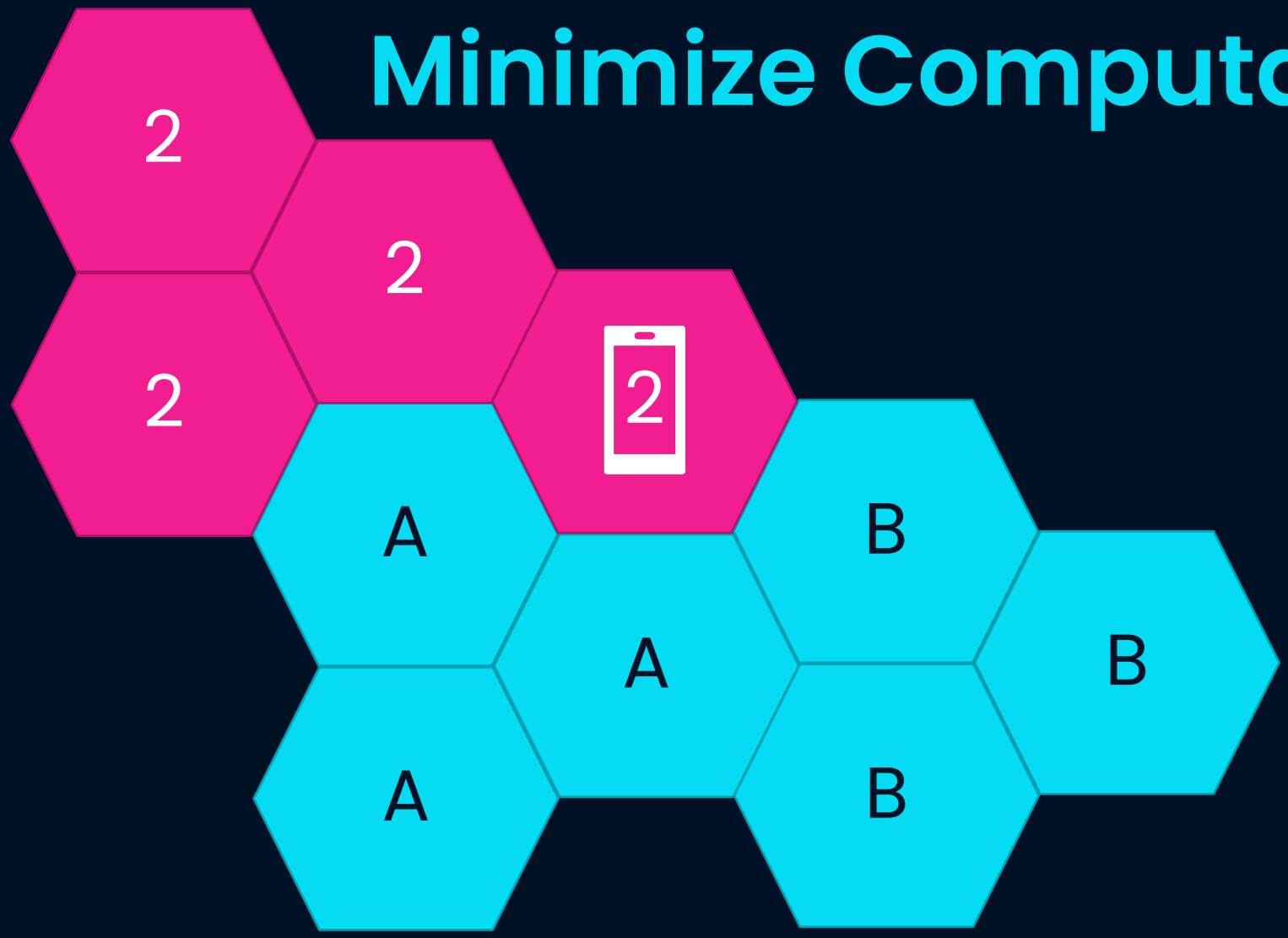
CK, IK

SEQ

K_{ASME}

K_{eNB}

Minimize Computation



Change SN

K

CK, IK

SEQ

K_{ASME}

K_{eNB}

Opportunities for Failure

- Incorrect MAC
- SEQ Synchronization Failure
- Incorrect AV type
- Invalid Authentication (XRES ≠ RES)
- Retransmission of (RAND, AUTN)

Evolution Over Time

5G: Authenticate with Home Network

4G (LTE): Serving-Network-Specific Keys

3G (UMTS/CDMA2000): Mutual Authentication

2G (GSM/GPRS): Phone Authenticated by Network

Downgrade Attack

Broadcast 2G at super strong signal

5G: Authenticate with Home Network

4G (LTE): Serving-Network-Specific Keys

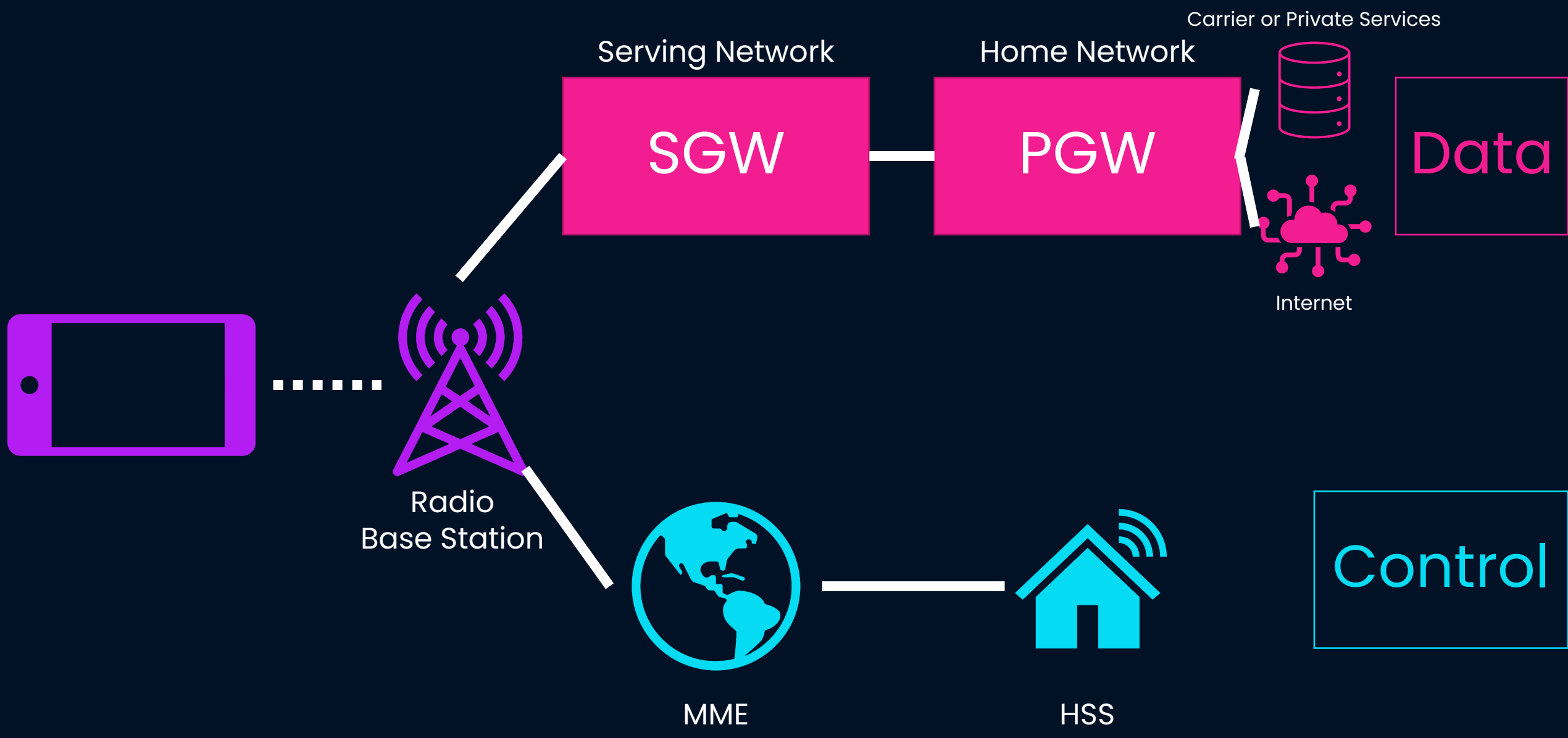
3G (UMTS/CDMA2000): Mutual Authentication

2G (GSM/GPRS): Phone Authenticated by Network

Network Components

26 April 2023

alexbeaver.com


Carrier or Private Services
Serving Network
Home Network
SGW
PGW
Data
Internet
Radio
Base Station
Control
MME
HSS

Strata

Access Stratum

- Layer 2
- Between UE and Base Station

Non-Access Stratum

- Layer 3
- Between UE and MME

K_{RRCint}	COUNT	BEARER	Direction
128	32	5	1

AS

- Radio Resource Control (RRC) Protocol for signaling
- Some unencrypted comm before encrypted
- Packet Data Convergence Protocol for RRC & User Data

NAS

- All communication is integrity checked
- After establishing algorithm, all communication encrypted
- Key derived from HSS
- IMEI always secret

Algorithm-Independent

26 April 2023

alexbeaver.com