introduction to LTE

eric m. gauthier – group fraud and revenue assurance

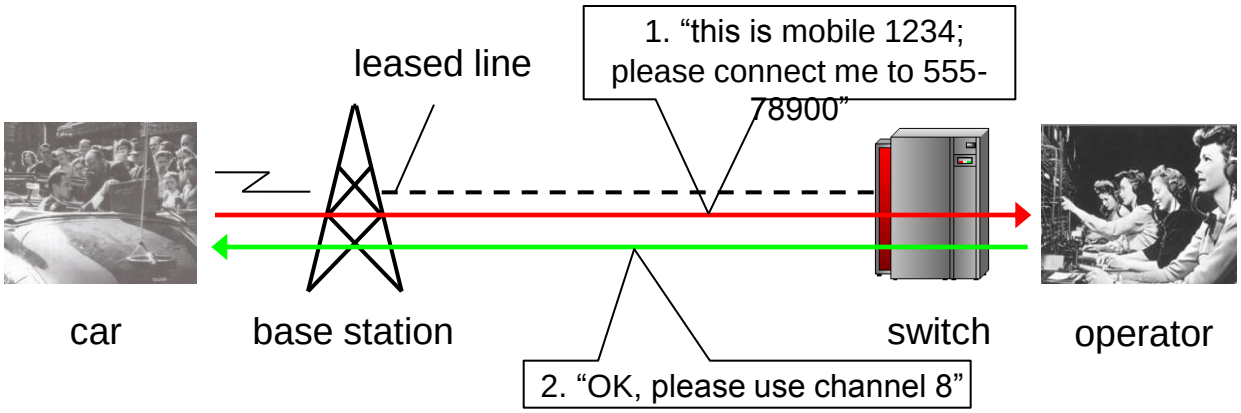
network security conference, may 2013

orange™

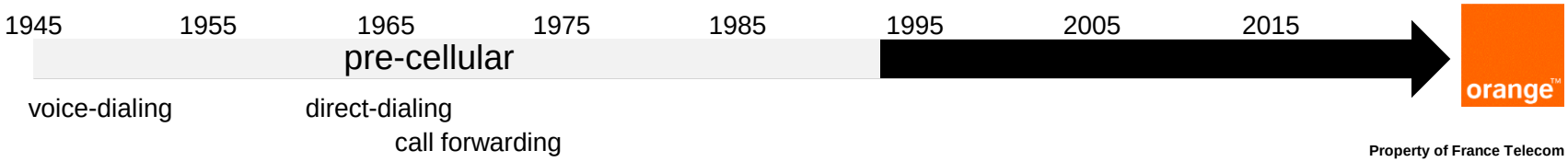
introduction

- LTE is considered a mobile technology of fourth generation (4G)
- every new generation introduces new security functions
- mobile security protects both customer privacy and billing integrity
- 2G, 3G and 4G mobile technologies are simultaneously in use today
- every new generation increases the number of mobiles on the network
- mobile devices support multiple technologies and security functions
- every new generation enables new services or replaces old services with better performing ones
- LTE provides broadband data access but requires a 2G, 3G or IMS network to support other services such as voice calls or messaging
- LTE provides a new interface for interconnection between operators

pre-cellular: radio telephony

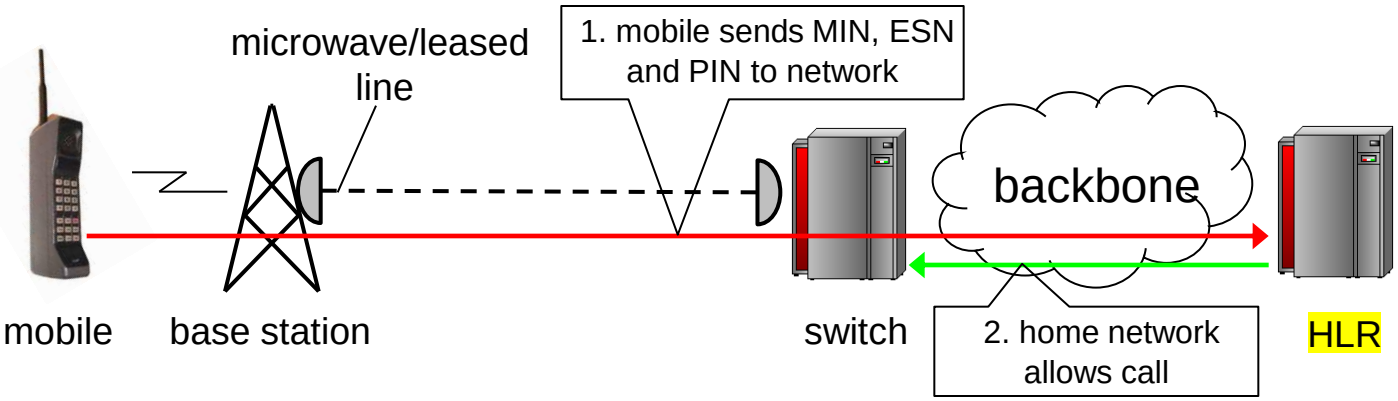


- calls could be eavesdropped
- fraudsters could guess or eavesdrop mobile numbers
- operators introduced PIN codes and assigned them to customers who were requested to provide them when dialing a number

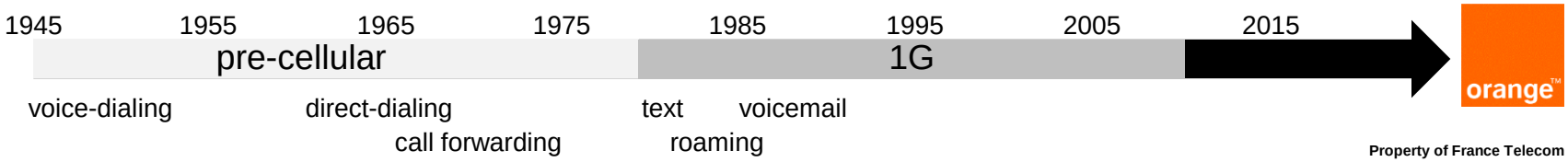


1G: analog cellular

HLR: Home Location Register

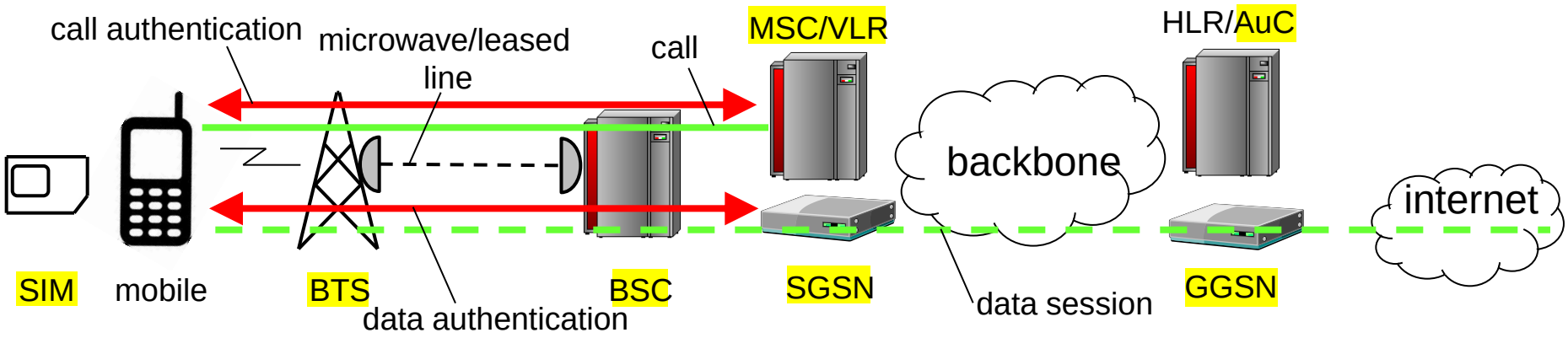


- mobile sends pair to network for automated billing
  - MIN: mobile number; can be changed by dealer
  - ESN: serial number; “burned” into mobile
- roaming introduced without realtime authentication
  - at first, roamers accepted by default, then caller had to dial a PIN code
  - operators reconciled billing after the fact
- fraudsters eavesdropped and resold list of MIN/ESN/PIN
- more than $600M of fraud losses in 1996 in North America (CTIA)

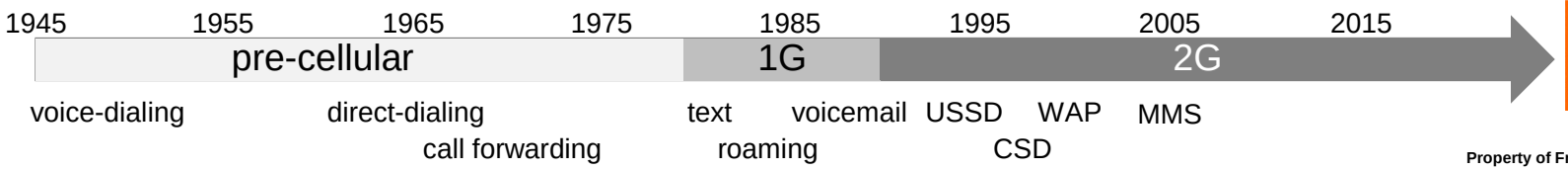


SIM: Subscriber Identity Module
BTS: Base Transmitter Station
BSC: Base Station Controller
MSC: Mobile Switching Center
VLR: Visiting Location Register
AuC: Authentication Center
SGSN: Support GPRS Serving Node
GGSN: Gateway GPRS Serving Node

2G: GSM and GPRS

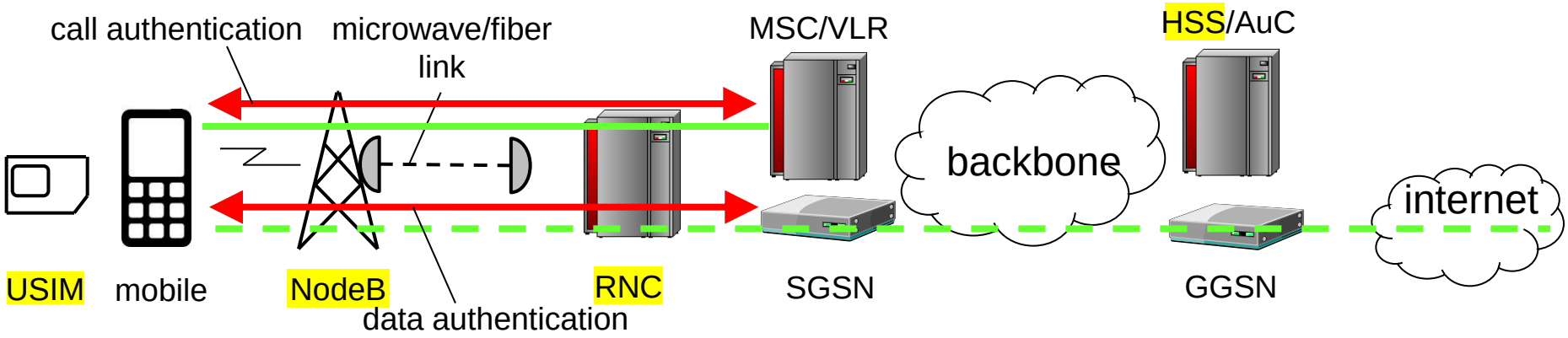


- secret key stored in SIM card is not sent over the air
- SIM uses key to compute a response to a challenge sent by network
- VLR and SGSN verify response received from mobile
- VLR and SGSN fetch authentication vectors in AuC
- authentication process produces an encryption key
- mobile encrypts call with base station and data with SGSN
- operators can use different flavors of encryption algorithm
- operators can choose their own authentication algorithm
- subscriber identity protected by temporary identities

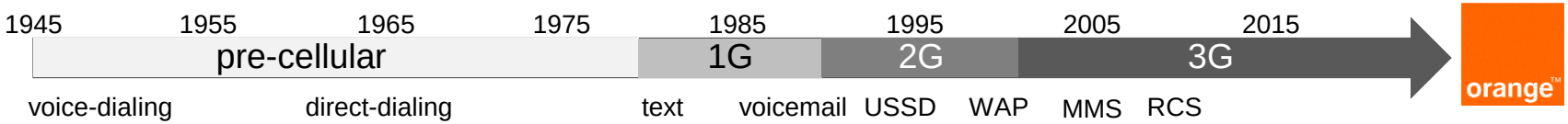


USIM: Universal SIM
RNC: Radio Network Controller
HSS: Home Subscriber Server

3G: UMTS

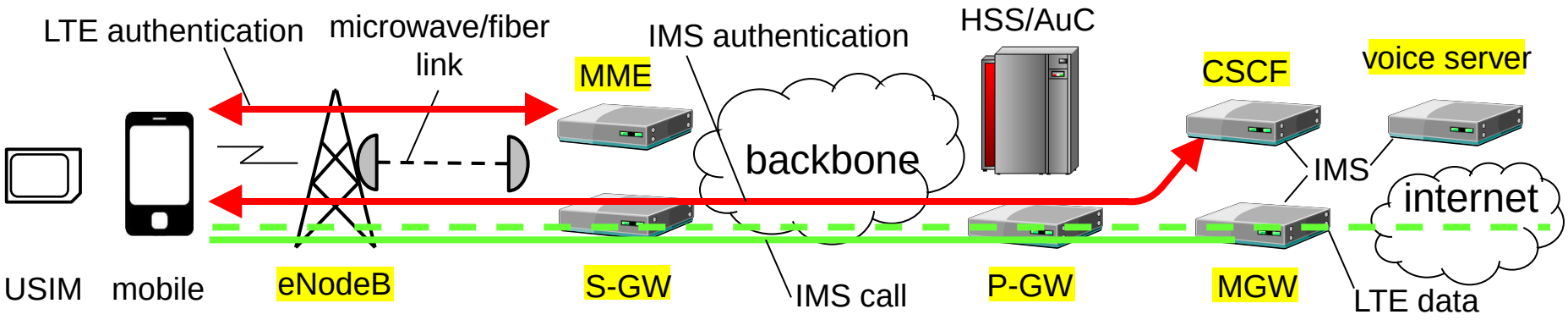


- USIM authenticates and verifies freshness of the challenge it receives
- authentication process produces an encryption and an integrity key
- mobile encrypts call and data with RNC
- UMTS introduces integrity protection.
- mobile, RNC, MSC and SGSN verify the integrity of communications
- UMTS doubles the length of encryption keys compared to GSM and GPRS.
- authentication and encryption algorithms different than 2G

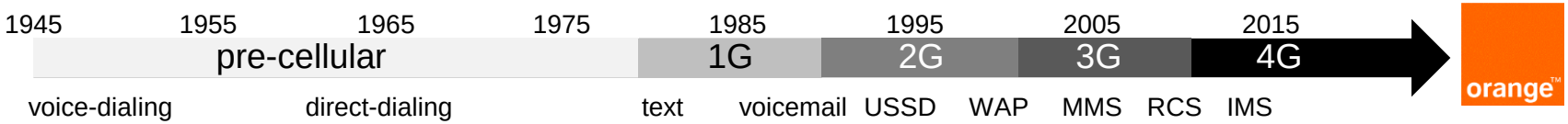


4G: LTE and IMS (1/2)

eNodeB: evolved NodeB
MME: Mobility Management Entity
S-GW: Serving Gateway
P-GW: Packet Data Network Gateway
CSCF: Call Session Control Function
MGW: Media Gateway



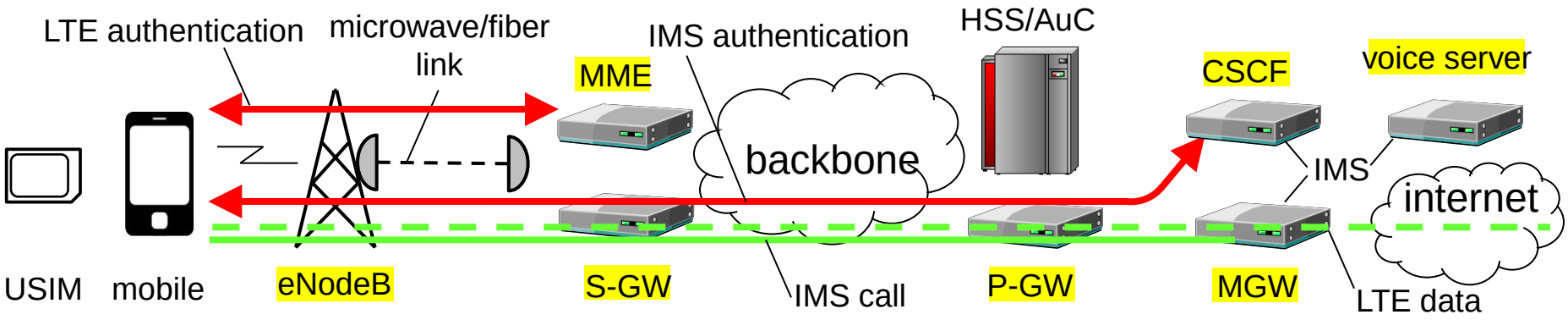
- fallback for calls to GSM or UMTS if no IMS call
- LTE and IMS reuse UMTS authentication scheme
- USIM and mobile can differentiate an LTE authentication from UMTS
- authentication performed by MME (LTE) and CSCF (IMS)
- MME and CSCF check integrity and prevent replay
- text sent over MME if no IMS messaging
- LTE reuses the UMTS encryption and integrity scheme
- user data encrypted between mobile and eNodeB



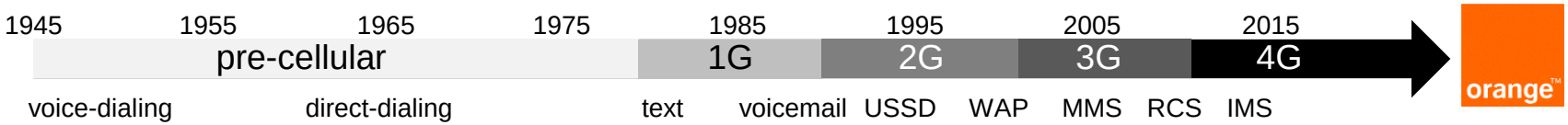
4G: LTE and IMS (2/2)

eNodeB: evolved NodeB
MME: Mobility Management Entity
S-GW: Serving Gateway

P-GW: Packet Data Network Gateway
CSCF: Call Session Control Function
MGW: Media Gateway



- LTE signaling encrypted and integrity protected from mobile to eNodeB and from mobile to MME
- IPSec from eNodeB to MME and from eNodeB to S-GW recommended by the standards
- IPSec protects IMS signaling between mobile and CSCF
- standard mandates integrity and anti-replay protection for IPSec
- encryption and integrity key length can be doubled compared to UMTS
- LTE introduces temporary identities valid across the network



conclusion

- LTE introduces a full packet-switched network
- LTE equipment more open to scrutiny because based on IP technology
- LTE introduces integrity protection between network equipment
- LTE signaling protection independent from user data protection
- LTE core network signaling protection independent from radio network.
- LTE reuses UMTS schemes but allows the mobile and the USIM to identify whether the service was requested on LTE or UMTS
- LTE can provide four times longer key length compared to current GSM
- LTE provides temporary identities valid accross the whole network
- IMS provides an additional authentication and integrity protection over LTE for services other than broadband data.

thanks