FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

20. Cellular Networks

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

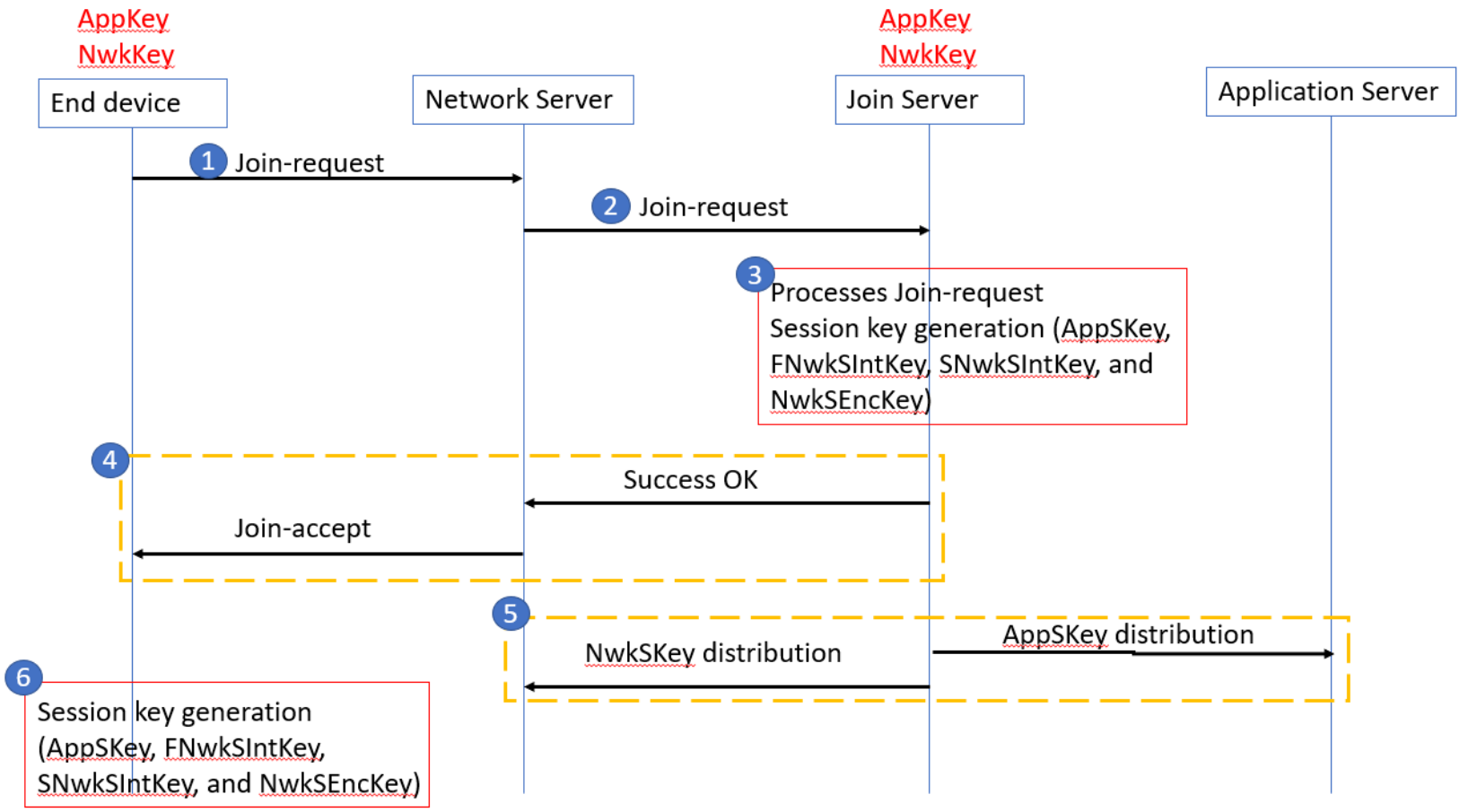
Outline

Cellular Networks

2G - Edge

Recall: OTAA

- The join procedure is always initiated by the end device
- The end device sends the Join-request message to the network that is going to be joined



Recall: LoRaWAN: Frame Counters

- Anyone will be able to capture and store messages
  - It's not possible to read these messages without the AppSKey, because they're encrypted
  - Nor is it possible to tamper with them without the NwkSKey, because this will make the MIC check fail
  - It is however possible to re-transmit the messages
- These so-called replay attacks can be detected and blocked using frame counters

Cellular Network Radio Frequencies

- Modern cell phones use a number of different frequencies to transmit data
  - Depends on the country and mobile operator network
- Some countries provide government-owned cellular services
  - Some lease spectrum to mobile operators to provide cellular access

Cellular Network Standards

- Responsible body for defining global cellular standards is 3GPP;
  - Composed of Association of Radio Industries and Businesses, Japan
  - The Alliance for Telecommunications Industry Solutions, US
  - Standards Association, China
  - The European Telecommunications Standards Institute, EU
  - Telecommunications Technology Association, Korea
  - Telecommunication Technology Committee, Japan

Cellular Network Standards

- “Release 98” comprising the majority of 3G
- “Release 8” in 2008 -> the first 4G LTE
- ”Release 10” in 2011 -> advanced LTE
- 3GPP defines radio interfaces and backend network infrastructure components and protocols used

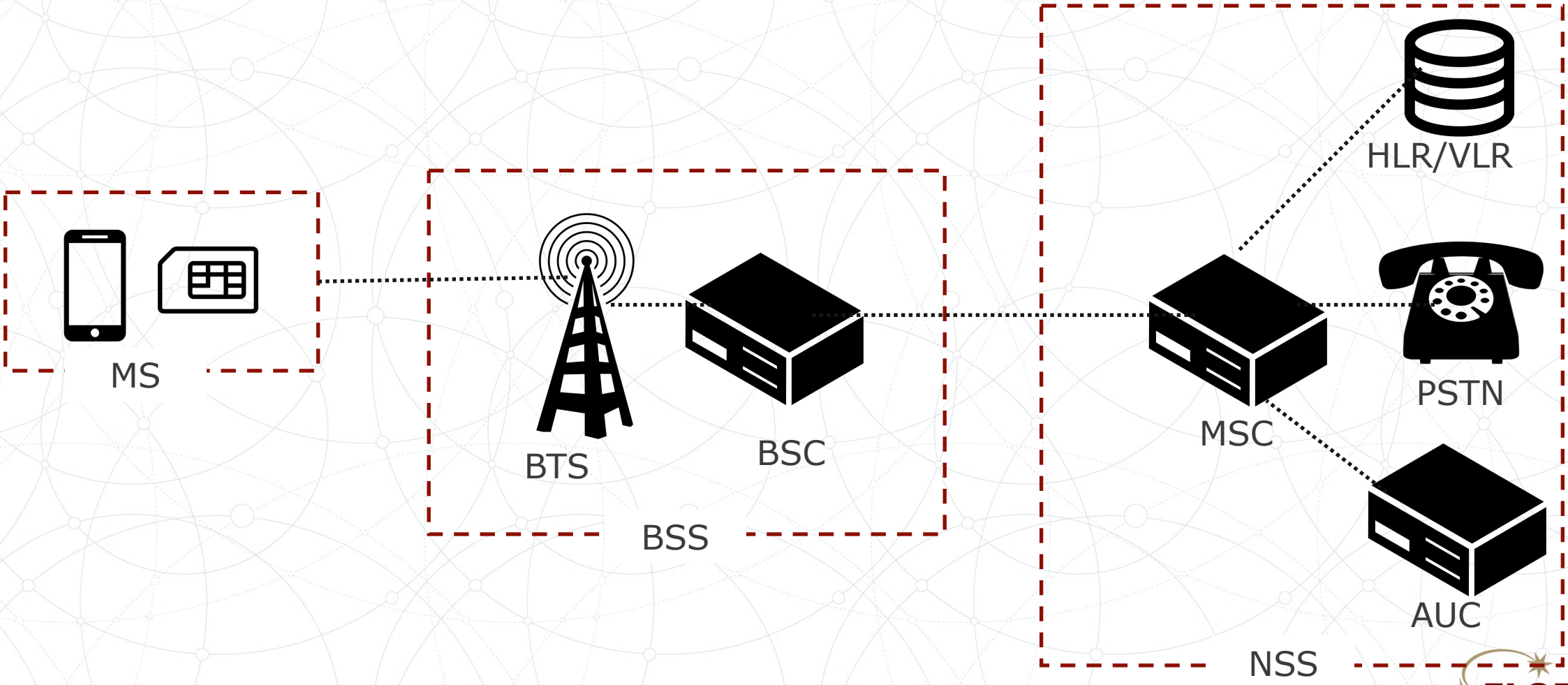
2G

- 2.5G Global System for Mobile (GSM), 2.75G General Packet Radio Service (GPRS), and Enhanced Data Rates for GSM Evolution (EDGE)
- Has been the most widespread cellular protocol used worldwide
  - Some devices still use it for backward-compatibility or back-up connection in the absence of other access opportunities

GSM Protocol

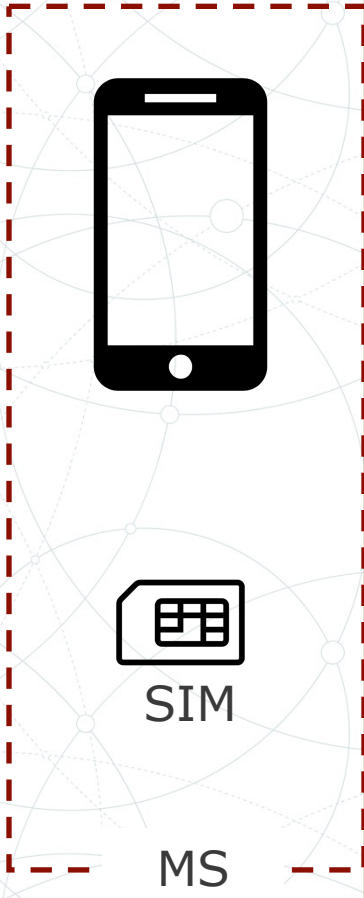
- Global System for Mobile Communications (GSM)
- First digital, circuit-switched network for carrying voice
- Expanded for carrying data (GPRS)
- Implemented cryptographic algorithms for security
- By mid-2010s, had over 90% of market share
- Obsoleted by LTE (4G); reached end-of-life for AT&T in 2017

GSM Network Model



GSM Mobile Station

- Mobile Station (MS):
  - User handset/device that connects to the GSM network
- Subscriber Identity Mobile (SIM):
  - Removable media that identifies the unique International Mobile Subscriber Identifier (IMSI) for the mobile station and the 128-bit Authentication Key (K_i)
- International Mobile Subscriber Identifier (IMSI):
  - Unique identifier consisting of Mobile Country Code (3 digits), Mobile Network Code (2 | 3 digits), Mobile Subscriber Identification (10 | 15 digits)

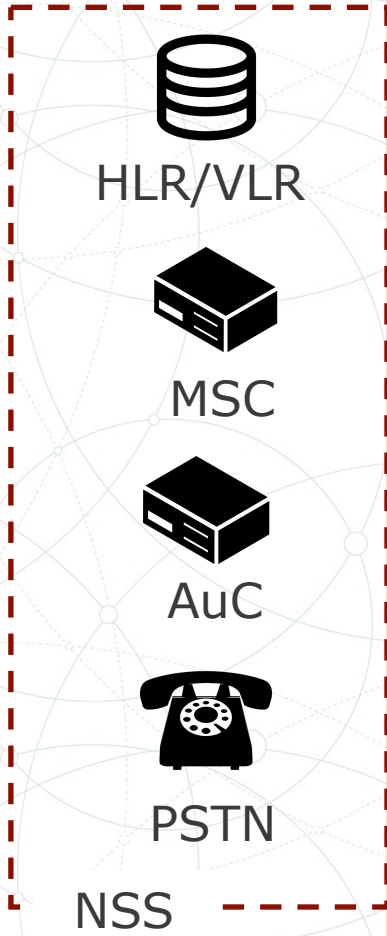


GSM Base Station Subsystem

- Base Transceiver Station (BTS):
  - Devices that facilitates radio connectivity for the mobile station (e.g., cell tower)
- Base Station Controller (BSC):
  - Facilitates the management of several BTSs;
  - Handles radio allocation, BTS handovers, etc.
- Base Station Subsystem (BSS):
  - Consists of BTS/BSC;
  - GSM network component that connects mobile station and network switching system

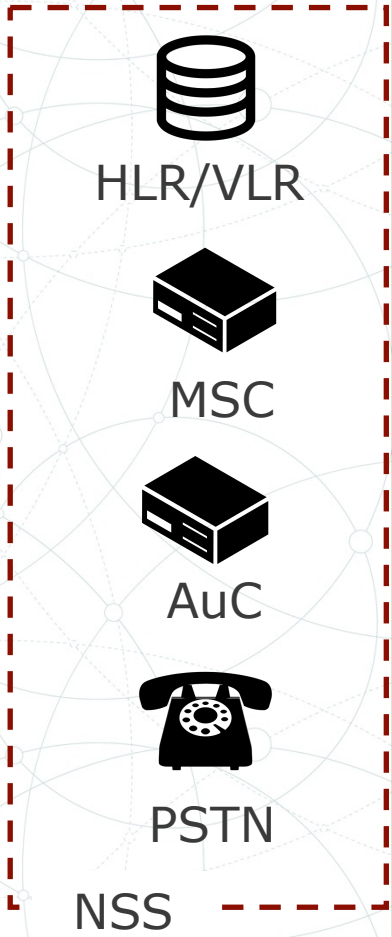
GSM Network Switching Subystem

- Network Switching Subsystem (NSS):
  - Back-end network for GSM provider and services
- Home Location Register (HLR):
  - Database that contains the IMSI for each MS on the network
- Visitor Location Register (VLR):
  - Database that facilitates roaming operations for MS devices

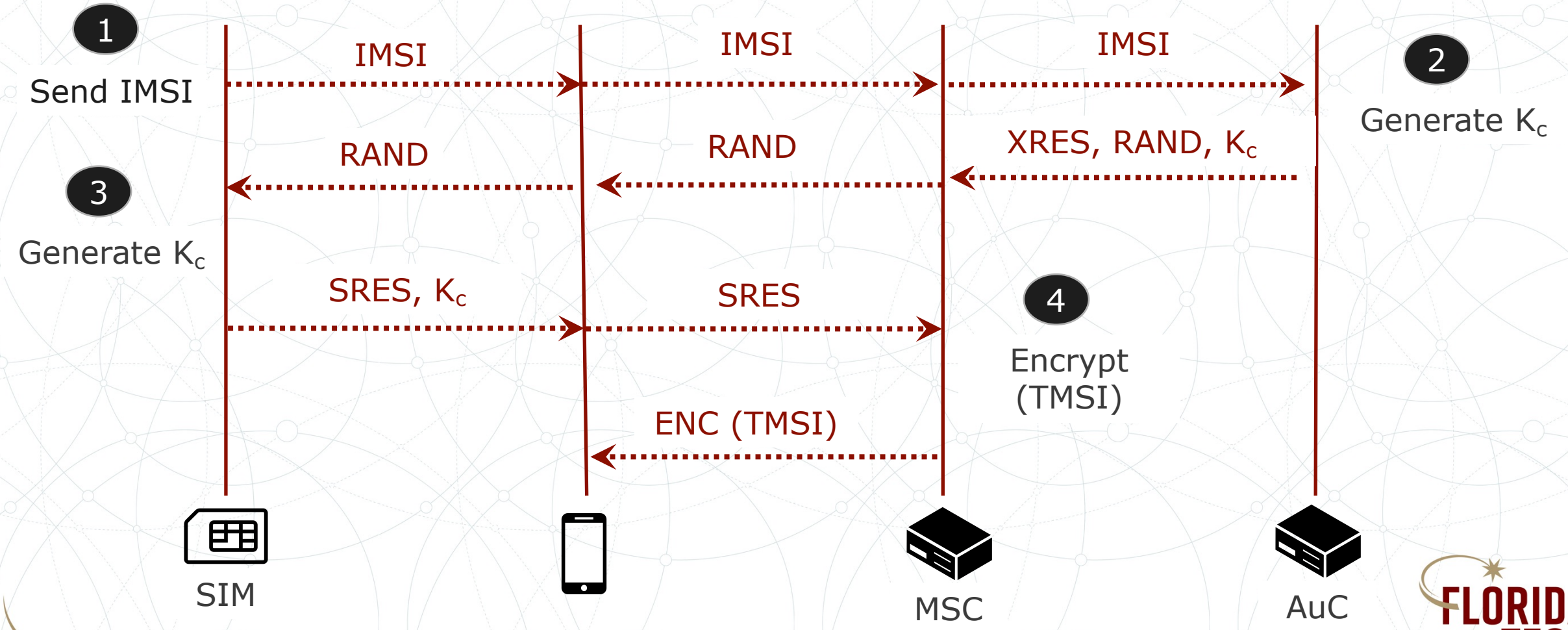


GSM Network Switching Subystem

- Mobile Switching Center (MSC):
  - Responsible for routing
- Authentication Center (AuC):
  - Facilitates user identification and authentication for SIM cards
- Public Switched Telephone Network (PSTN):
  - Public interface to GSM network and other network providers



GSM Authentication



GSM Authentication

- Exchange validates the identity of the subscriber through the use of the IMSI and the associated subscriber key, K_i, stored on the SIM card
  - Involves the SIM, the MS, the MSC, and the AuC
- AuC and SIM have knowledge of IMSI and Ki as part of the device registration process
  - When the MS connects to network, SIM shares IMSI info which is forwarded to AuC

GSM Authentication

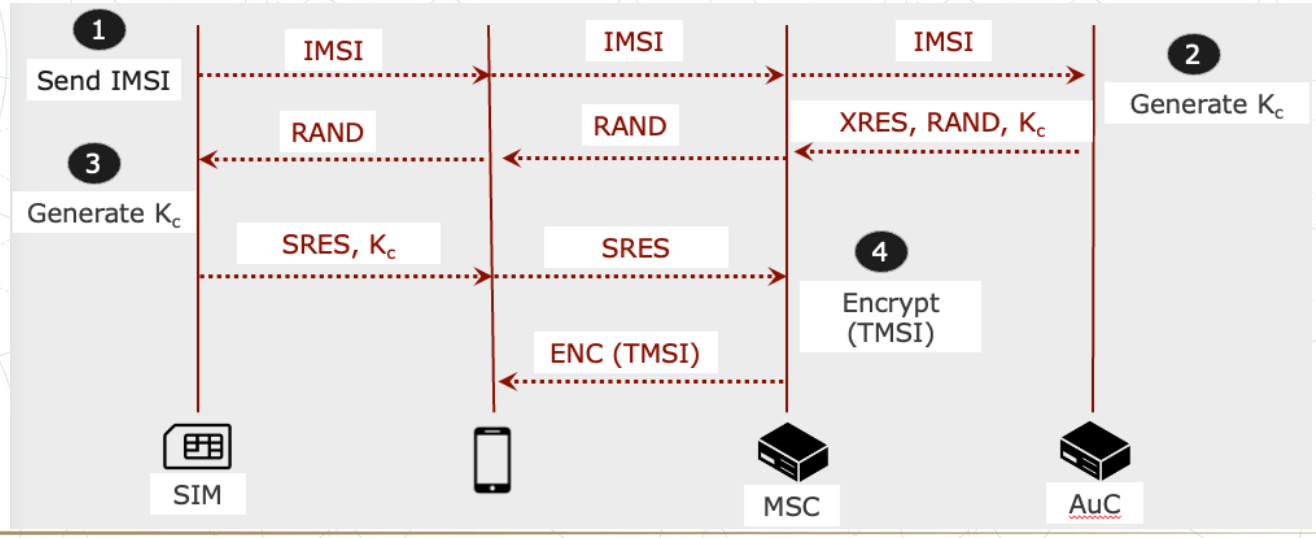
- The AuC retrieves K_i linked to IMSI and selects a random value RAND
- The RAND is used with two algorithms, A3 and A8, with the subscriber key K_i to generate the temporary cipher key K_c and the expected response (XRES)
- AuC shares K_c, RAND and XRES with the MSC, ending its role in the authentication process

GSM Authentication

- Next, MSC shares the RAND with the MS, which sends it to the SIM
  - Similar to AuC, the SIM uses the RAND to generate Kc and signed response SRES
  - SRES is delivered to MS, which forwards it over the air interface to the MSC for validation

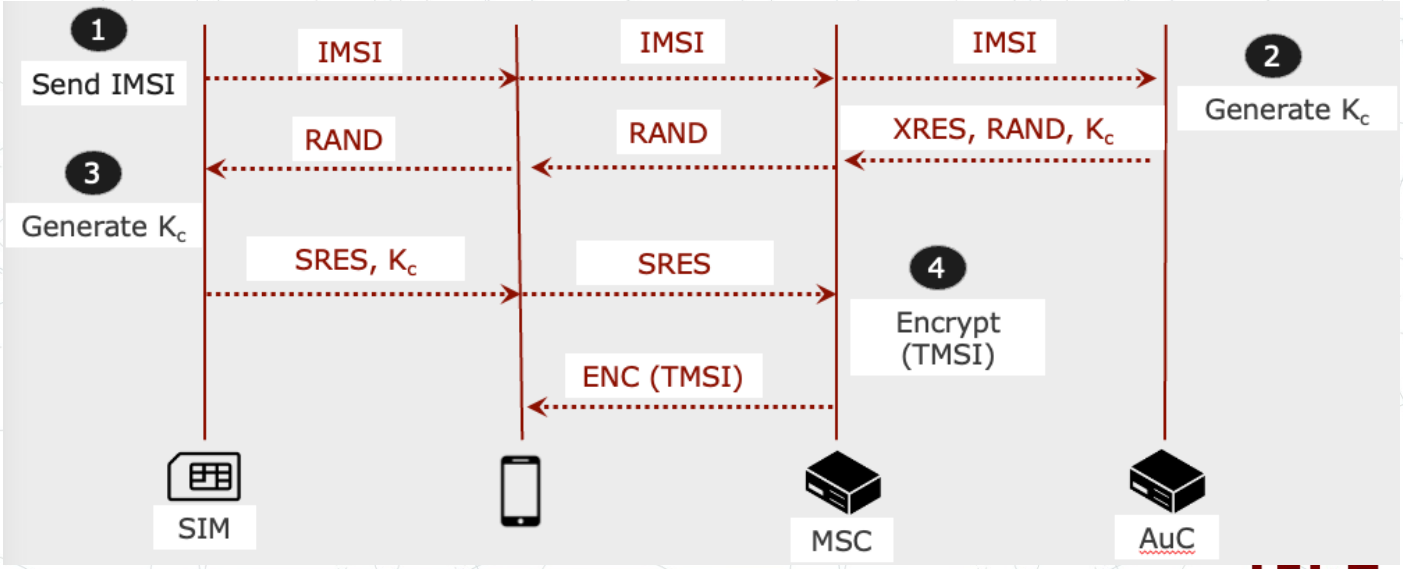
GSM Authentication

- The MSC compares SRES to XRES;
  - If match, validating the ME's identity
  - Then, MSC generates and encrypts TMSI for the ME to use and delivers it over the air interface



GSM Authentication: Vulnerability

- SIM card (and so the ME) is authenticated to the AuC
  - Prevent unauthorized devices accessing network services
- The authentication exchange does not validate the identity of the provider to the ME

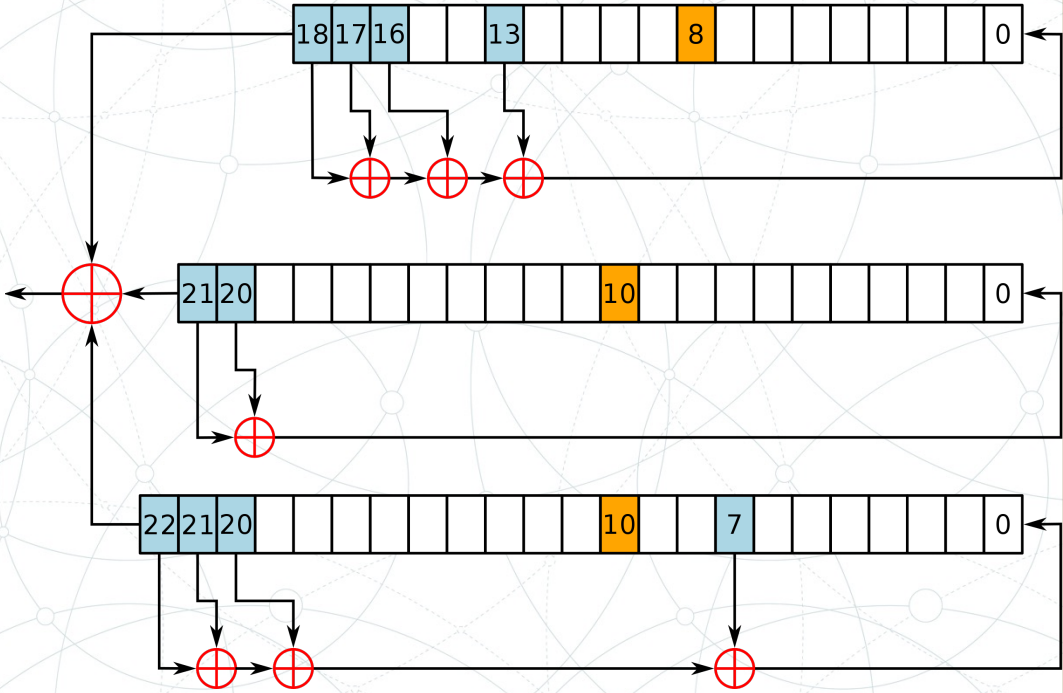


GSM Encryption

- Use the A5/1 cipher to provide confidentiality controls of traffic delivered over the GSM air interface between MS and BSC
- A5/1 is a stream cipher implemented using a Linear Feedback Shift Register (LFSR) mechanism
- Temporary cipher key Kc is used as the A5/1 input to generate keystream data
  - Ease of implementation in hardware and reduced implementation cost

A5/1

- Developed in 1987 (before GSM)
- 114 bits of GSM are XORd with 114 bits of Keystream material to produce encrypted data
- Uses three Linear Feedback Shift Registers (LFSR)



GSM Encryption

- The plaintext data is XOR'd with the keystream data to generate ciphertext
- Ciphertext is similarly XOR'd with matching keystream data at the recipient to decrypt

GSM Attacks

- Privacy attacks;
  - Leading to the disclosure of IMSI
- Confidentiality attacks;
  - Disclosure of voice and data communications over the GSM
- Integrity attacks;
  - Adversary manipulates or impersonates back-end GSM services to modify the content being delivered

GSM Eavesdropping

- Commercial tools are expensive
  - But, you can build your own GSM sniffer using inexpensive hardware
  - For ex. RTL-SDR
- GSM packet captures disclose basic information about the network, but do not reveal the contents of phone call/SMS etc. due to being encrypted

A5/1 Key Recovery

- Precomputed reference attack for full key recovery
- In 2008, gsm-tvoid; keystream data to known keystream state information in lookup tables
  - Using set of precomputed 288 quadrillion possible entries (apprx 2tb storage), adversary recovers K_i in approx. 30mins
  - It was taken offline without explanation
  - Possible government intervention

A5/1 Key Recovery

- In 2009, A5/1 cracking project reproduced the work previously published
  - As a plus, they distribute key recovery lookup tables through peer-to-peer networks to prevent them from being taken offline
- In 2011, 'Kraken', practical tool that integrates with AirProbe for effective capture and decryption of GSM traffic with the A5/1 tables
  - Later, 'Pytacle' tool improved features of the tool by adding play back capabilities for full and simple passive GSM decryption attack

https://github.com/0xh4di/kraken

Running Pytacle Requirements

- RTL/SDR with AirProbe software for GSM capture
- Kraken software
- Pytacle software
- A5/1 tables on a temporary storage drive, apprx 1.6tb
- A5/1 tables written to one or more lookup drives, apprx 3tb

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger