Department of Computer Science

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

CSE 4820: Wireless and Mobile Security

21. Cellular Networks Ctd

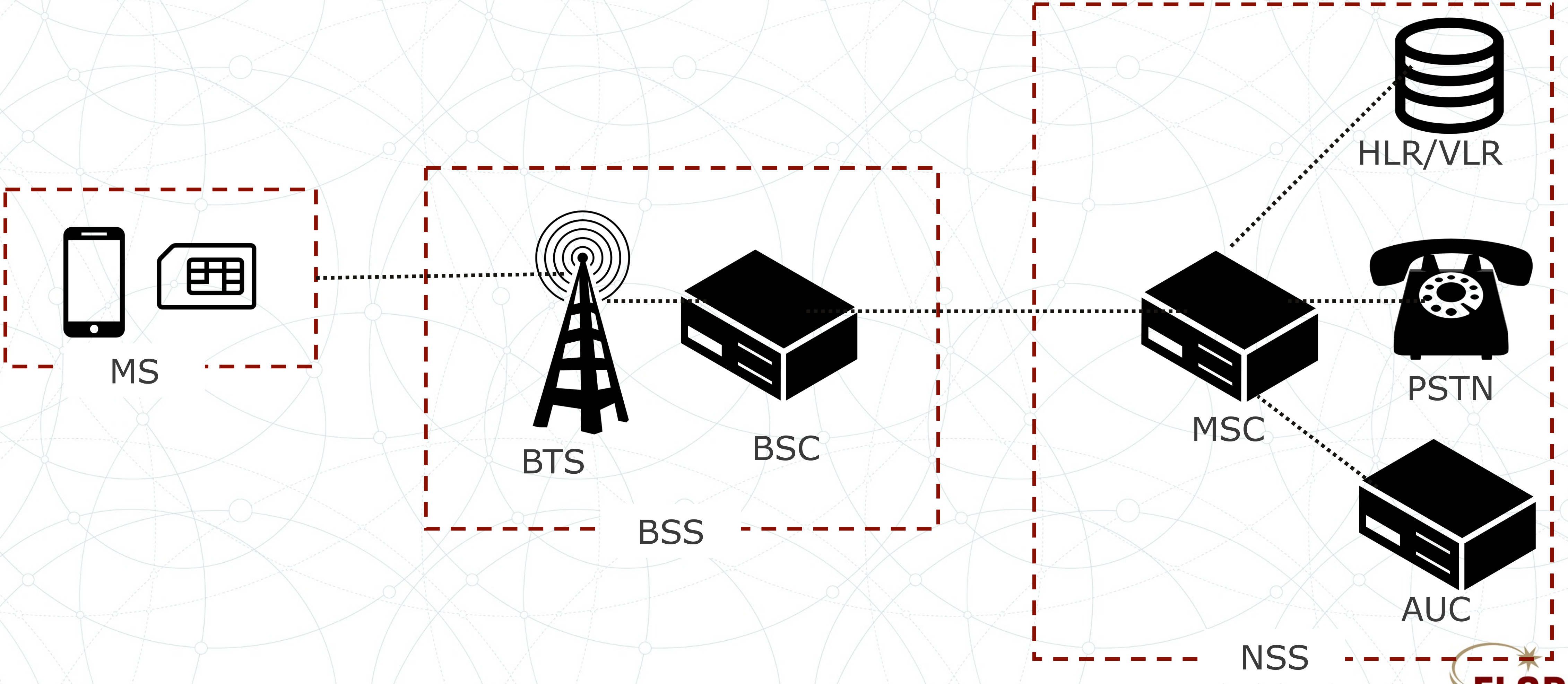
Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

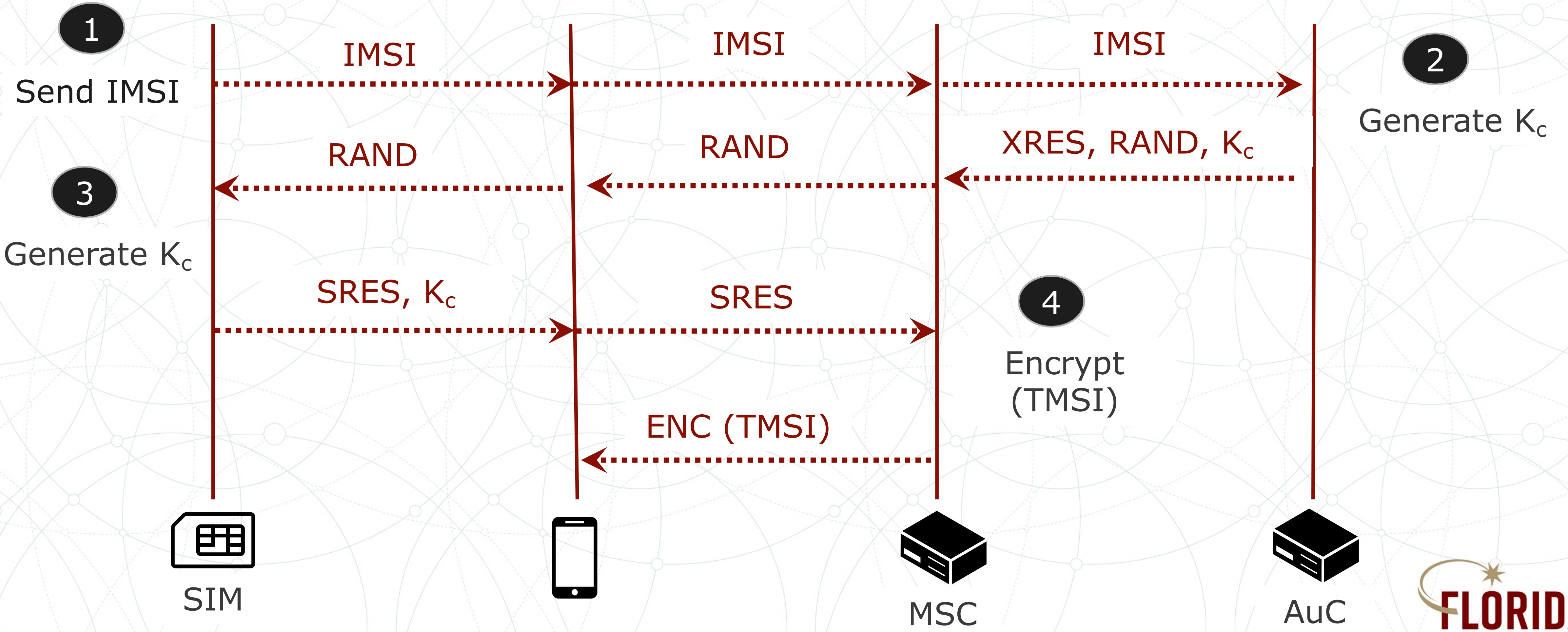
Cellular Networks

- Femtocell
- 4G/LTE

Recall: GSM Network Model



Recall: GSM Authentication



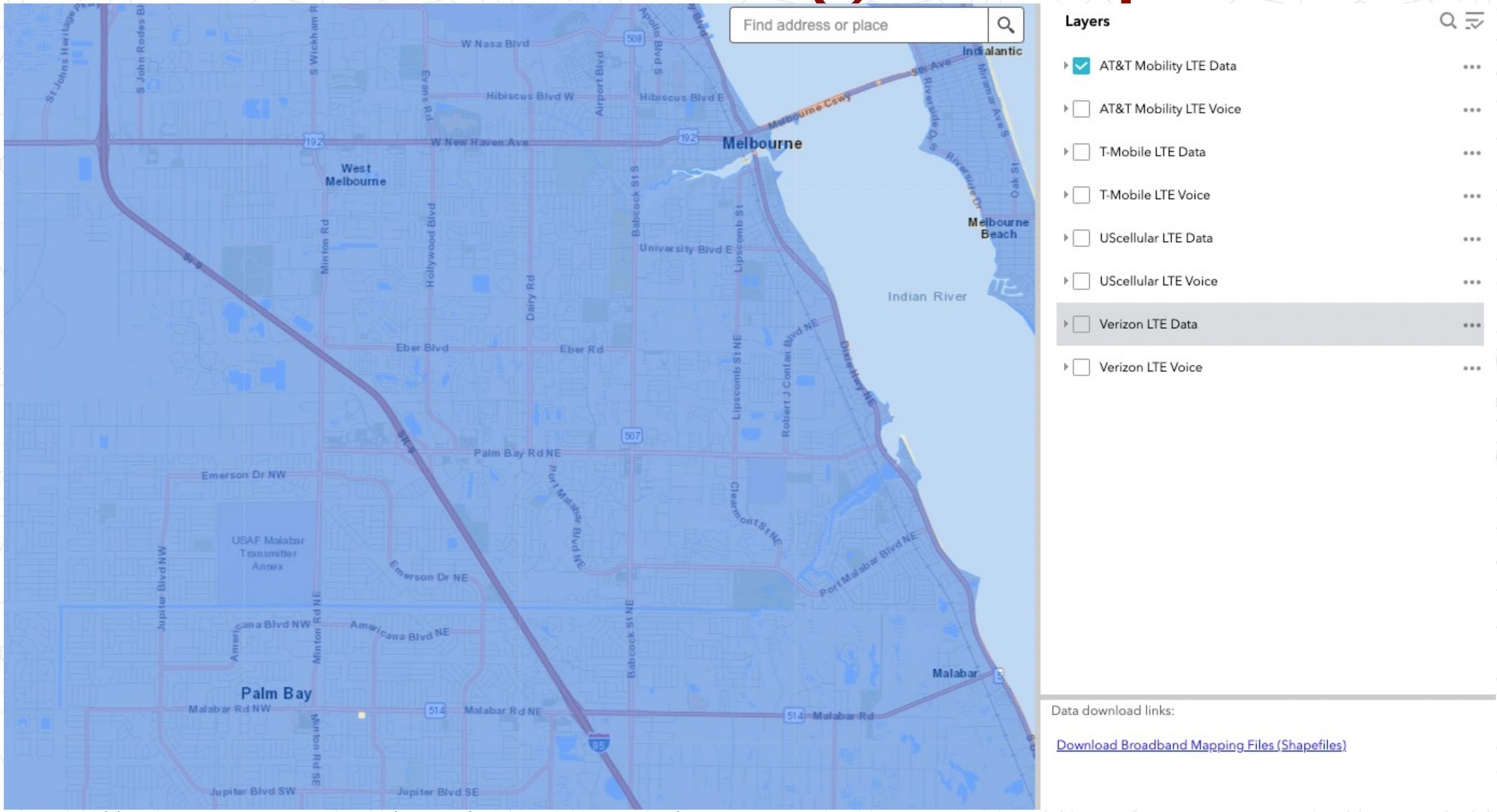
Recall: A5/1 Key Recovery

- 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

GSM Attacks: IMSI Catcher

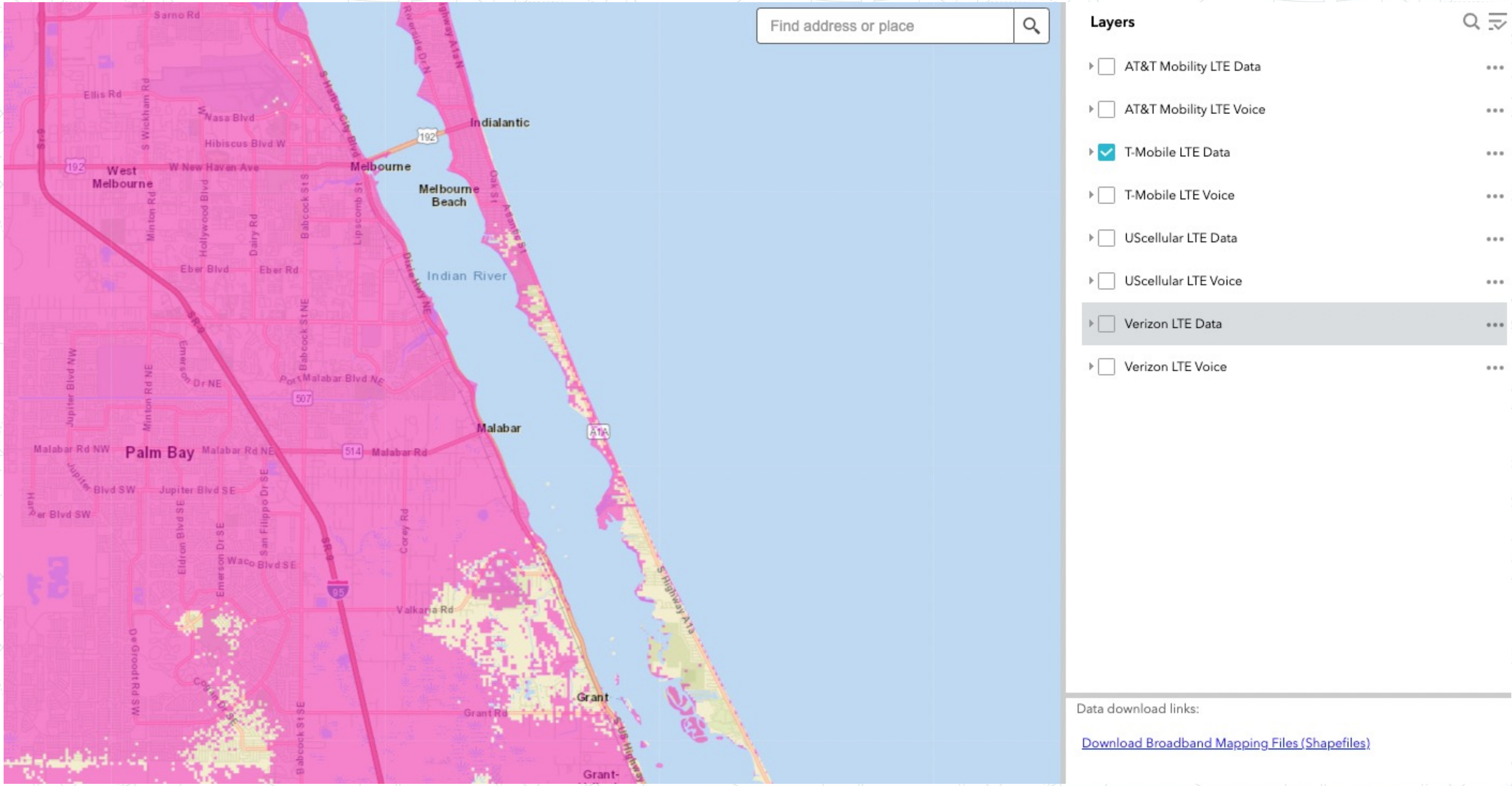
- An IMSI Catcher is a fake cell phone tower used to surreptitiously eavesdrop on mobile phones
- Sting-Ray phone tracker, manufactured by L3 Harris, is an example of an IMSI catcher distributed to law-enforcement/military
- IMSI Catchers can work passively (by advertising MCC/MNC) or actively by (disrupting channel and forcing disconnect)

Network Coverage Map: AT&T

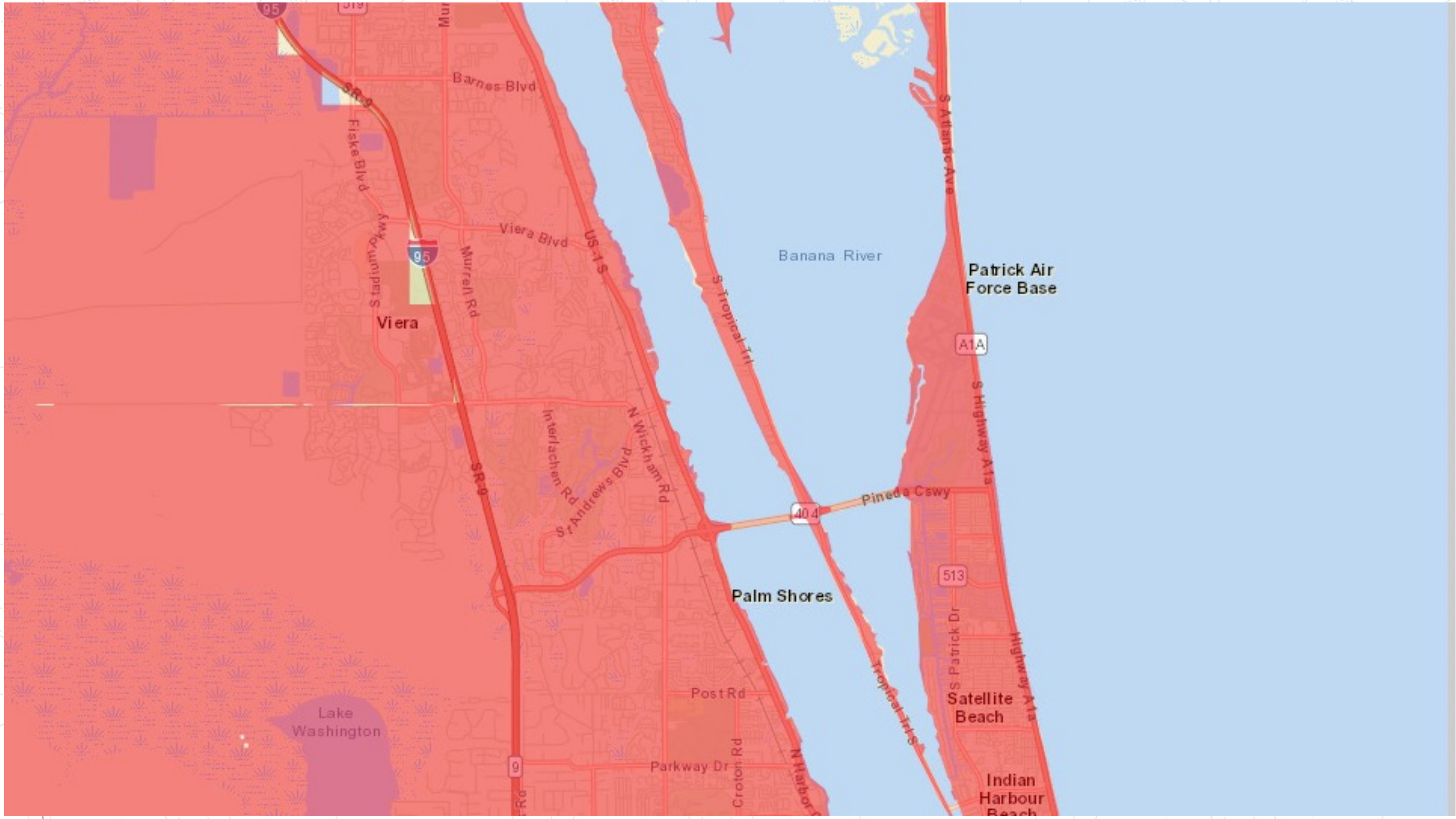


https://fcc.maps.arcgis.com/apps/webappviewer/index.html?id=6c1b2e73d9d749cdb7bc88a0d1bdd25b

Network Coverage Map: T-Mobile



Network Coverage Map: Verizon



- AT&T Mobility LTE Voice
- T-Mobile LTE Data
- T-Mobile LTE Voice
- UScellular LTE Data
- UScellular LTE Voice
- [x] Verizon LTE Data
- Verizon LTE Voice

Femtocell

- Extend the carrier network, leveraging the consumer's broadband connection for uplink connectivity
- Femtocell devices (e.g., Home NodeB or HNB) allow consumers to establish a relatively short-range extension of the carrier network that provides similar connectivity services (e.g., voice, data, SMS/MMS)
  - Also offers attackers new opportunities to attack the carrier infrastructure, as well as User Equipment devices

Femtocell

- HNB devices use IPsec to connect to the carrier network and provides strong confidentiality and integrity support over the untrusted broadband connection
- UE is responsible for encrypting/decrypting the 3G voice, data, and messaging services locally before forwarding to the UE or to the carrier over IPsec
  - The opportunity to mount attacks against unsuspecting UE devices

Femtocell Attack

- HNB is authorized device on the carrier network and has access to dynamic key information used to encrypt/decrypt the 3G connection
  - MiTM to manipulate and intercept phone calls
- They found a way to have root access to femtocell device and run their codes in them to sniff the traffic
  - Presented at Defcon 21

https://www.youtube.com/watch?v=gfcq8clu1RI

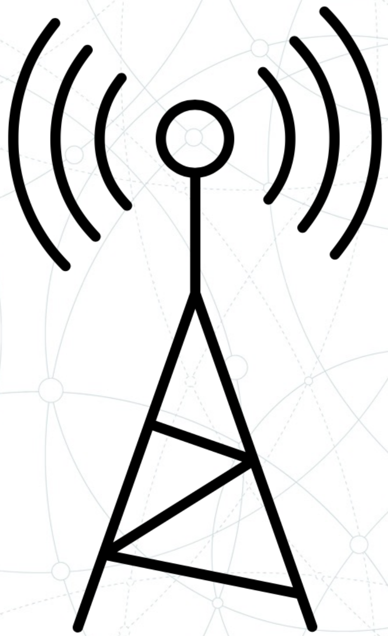
WiFi Based IMSI Catcher

- Features
  - Tracking: IMSI, Location
- Operates in unlicensed ISM Bands: WiFi
  - Fake Access Points
  - Redirect/Spoofs mobile packet data gateway
  - Exploits protocol & configuration weaknesses
- Based on two separate techniques [3GPP TS33.234]
  - WiFi Network Authentication ('WLAN direct IP access')
  - WiFi-Calling Authentication ('WLAN 3GPP IP access')

https://www.youtube.com/watch?v=7ZBDfxSdnD4

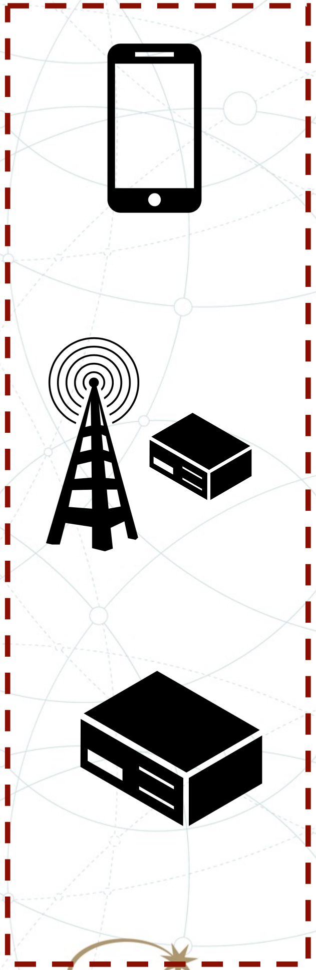
4G/LTE

- Long-Term Evaluation (LTE) Protocol
- Predecessor to GSM
- Marketed as 4G LTE or Advanced 4G
- In addition to higher speeds
  - Offers improvements for privacy
  - Introduces new encryption schemes



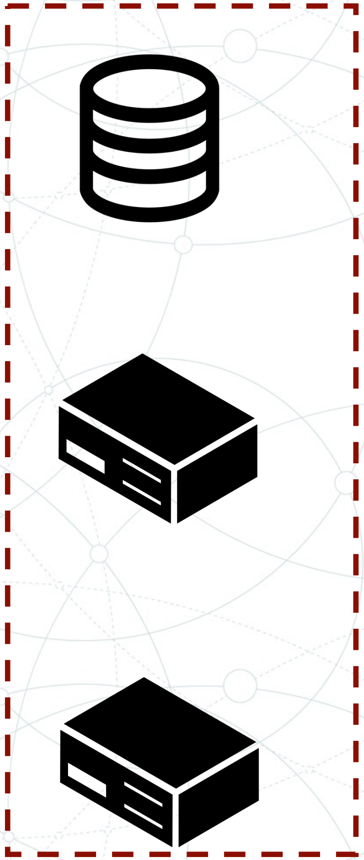
LTE Network Elements

- Universal Subscriber Identity Mobile (USIM):
  - An application that resides within the mobile devices;
  - Implements mutual authentication, encryption, and the address book functionality
- Evolved Node B (eNodeB):
  - Provides the radio element access mechanism for the network
- Mobile Management Entity (MME):
  - Key-control node for LTE access network;
  - Responsible for encryption/decryption of network traffic after mutual authentication and key setup/exchange

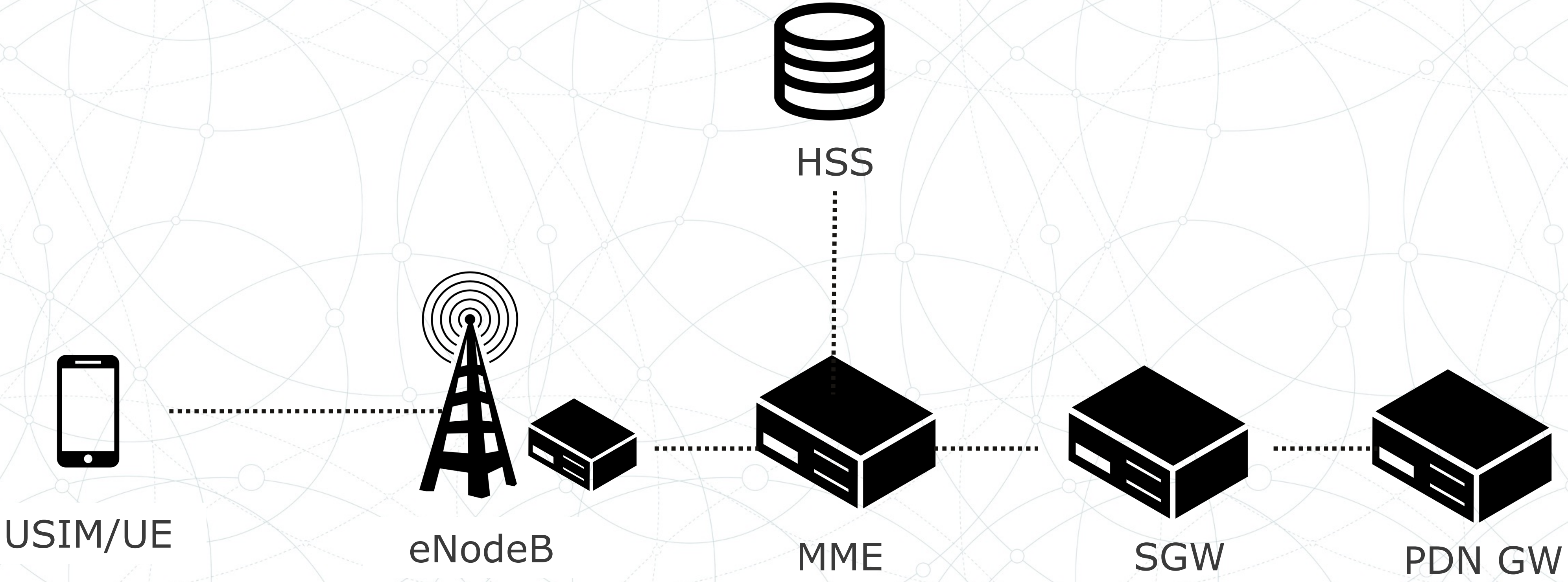


LTE Network Elements

- Home Subscriber Server (HSS):
  - Subscriber database that provides MME with records to establish mutual authentication between USIM and MME
- Serving Gateway (SGW):
  - Establishes routing and packet forwarding within network
  - Interacts with MME to grant/deny access to the UE
- Packet Data Network Gateway (PDN-GW):
  - Provides connectivity to external packet networks

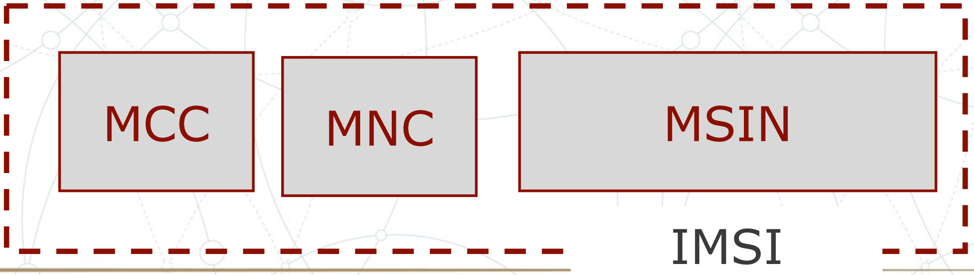


LTE Network Model



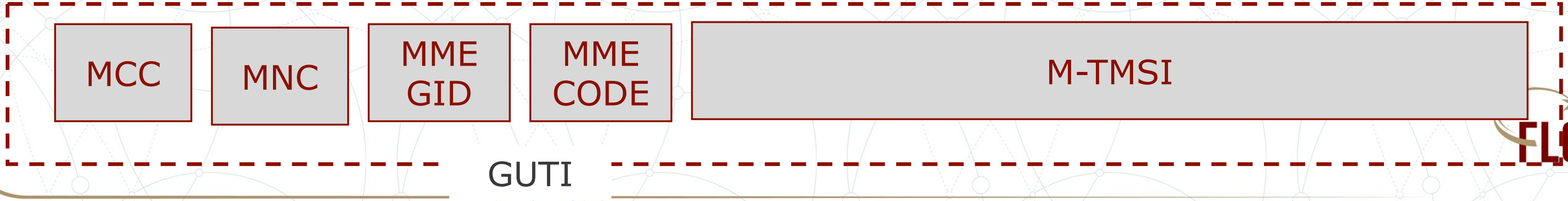
LTE Addressing Scheme for IMSI

- IMSI is made up of three components:
  - MCC: Mobile Country Code, identifying the country of the end-user
  - MNC: Mobile Network Code, identifying the home network
  - MSIN: Mobile Subscriber Identification Number, identifying the user within MCC and MNC context



LTE Addressing Scheme for IMSI

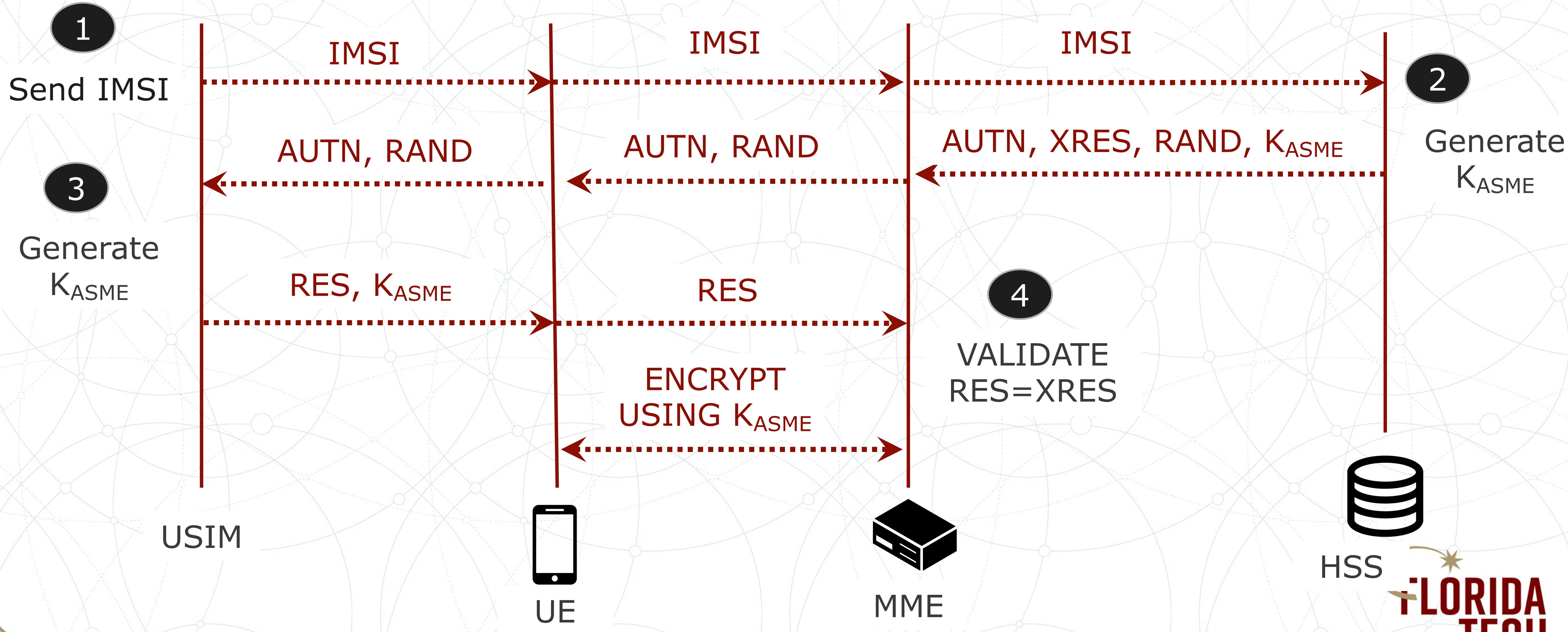
- IMSI value is stored on the USIM and a fixed value
  - Acts as a shared identifier for UE (e.g., LTE phone) and the HSS for the associated authentication key ”K”
- To ensure privacy of the unique handset (such as identifying an IMSI to an individual), LTE introduces a Globally Unique Temporary ID (GUTI) which consists of the MCC, MNC MME info and the Temporary Mobile Subscriber ID (TMSI)



LTE Authentication

- Mutual auth of the handset and the network infrastructure through the Evolved Packet System Authentication and Key Agreement (EPS-AKA)
- Similar to GSM/3G, authentication in LTE relies on the identification function and shared key content provided by the IMSI (International Mobile Subscriber Identity)

LTE Authentication



LTE Authentication Steps

- 1. USIM shares IMSI with the UE
  - USIM never discloses the secret key K to the UE or over any network interface
- 2. UE forwards IMSI to the MME
- 3. MME forwards IMSI to the HHS
  - With IMSI, HSS can identify the secret key K (that is never shared with MME)
  - With secret key K, HHS selects a random value (RAND) and derives the Access Secure Management Entity Key (K_{ASME}), an authentication value (AUTN), and the Expected Response (XRES) values

LTE Authentication Steps

- 4. HHS shares K_{ASME}, AUTN, XRES, and RAND values with the MME
  - HHS is finished with the exchange at this point, leaving identity validation to the MME
- 5. MME retains the K_{ASME} and XRES values as local secrets, sharing the AUTN and RAND values with the UE
- 6. UE shares the AUTN and RAND with the USIM

LTE Authentication Steps

- 7. The USIM, who, like the HHS, knows the secret key K, calculates its own AUTN value, comparing it to that of AUTN originally from the HSS
  - If the AUTN values match, the USIM has validated the identity of the HSS as having the same shared key K
  - Next, USIM calculated its own response value (RES) and intermediate key values ultimately used to derive the K_{ASME} sent to the UE
- 8. The UE saves the K_{ASME} for later use, forwarding the RES value to the MME

LTE Authentication Steps

- 9. The MME compares the RES to the XRES previously delivered from the HHS
  - By comparing them, MME validates that the USIM has the correct secret key K
  - Mutually authenticated
- 10. Using the derived K_{ASME} values, UE an MME can encrypt and decrypt traffic over the wireless medium

LTE Authentication Vulnerability

- The IMSI is sent in plaintext
  - Rogue LTE network can get IMSI
  - Privacy threat to IMSI
- Yet, the secret K never is disclosed to the UE from USIM, preventing rogue applications from stealing the value and limiting attacker's ability to clone the value onto another USIM

LTE Encryption

- LTE supports algorithm flexibility
- 3GPP systems were limited to a handful algorithms and these could not be replaced without changes to the network infrastructure
- Yet, LTE networks could adapt to new algorithm option to mitigate any flow
  - Let's say there is a flaw found in AES

LTE Supported Encryption Algorithms

- NULL Algorithm:
  - Does not provide confidentiality of network traffic
  - In some cases, need to provide service outweighs the desire for security in LTE
  - Provides network access for devices lacking USIM card for situations such as emergency services (e.g., 911 in US)
  - May create opportunity for attacker to impersonate a legitimate carrier network without the need for cryptographic attacks

LTE Supported Encryption Algorithms

- The Kasumi Algorithm:
  - The first ciphering algorithm for the LTE standard, the Kasumi algorithm, is mainly a block cipher algorithm that uses a key size of 128 bits
  - The algorithm utilizes two mapping functions to produce the ciphertext, which are called S-boxes
  - Kasumi was specifically designed as a building block for the UMTS encryption algorithms (UEA1) and integrity algorithms (UIA1)

LTE Supported Encryption Algorithms

- SNOW 3G (128-EEA1):
  - Word-based synchronous stream ciphers implemented with a LFSR and Finite State Machine
  - Brought forward from 3G networks and reintroduced as a well-known option for carriers that have used the algorithm for many years prior
  - Helped LTE by reusing an algorithm well understood and readily available

LTE Supported Encryption Algorithms

- Milenage:
  - AES-128-bit Based algorithm in CTR (Counter) mode
  - AES encryption can be accelerated in hardware using parallelism and has already been proven in other well-known deployment scenarios (e.g., 802.11/WPA2 security)

LTE Supported Encryption Algorithms

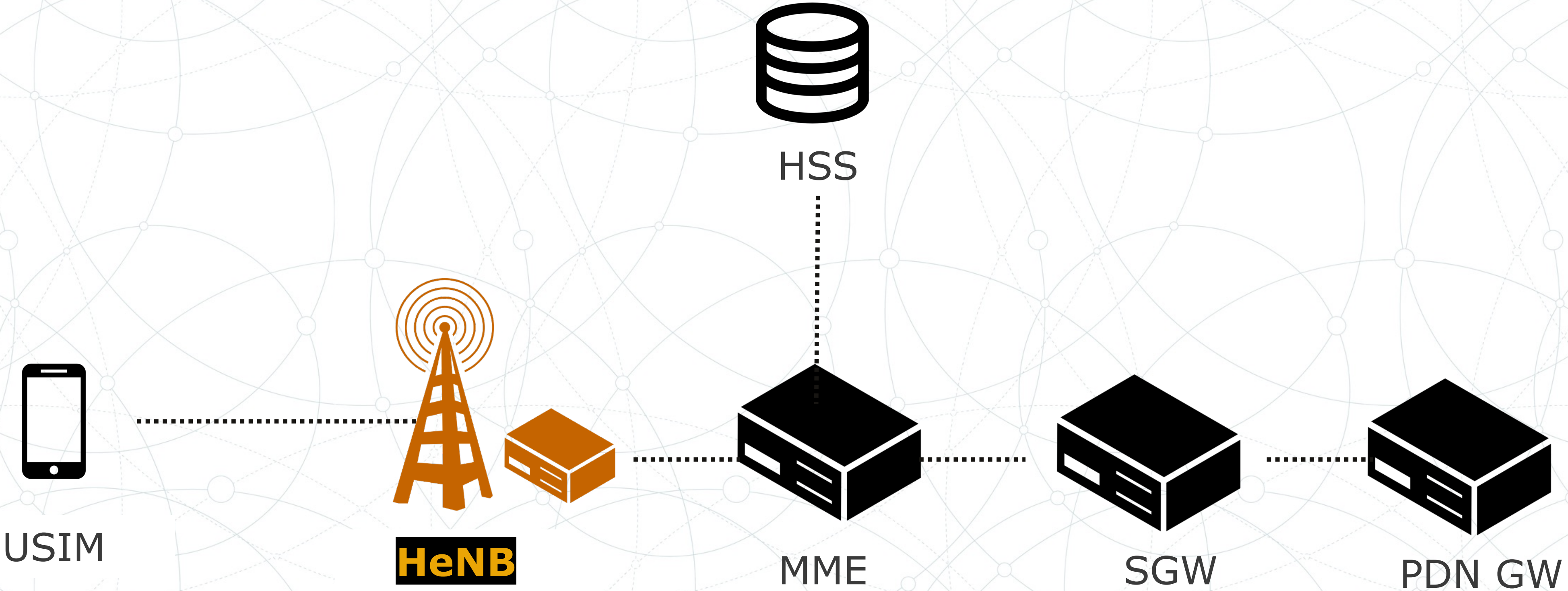
- ZUC:
  - Cryptographic algorithm for LTE
  - Combines block + steam cipher approaches, using:
    - Non-Linear Function (e.g., S-Boxes)
    - Linear Feedback Shift Register (LFSR)
  - Uses Bit Reorganization (BR)
  - Strong resistance to algebraic attacks

```
void GenerateKeystream(u32*
pKeystream, int KeystreamLen)
{
int i; {
BitReorganization();
F(); /* discard the output of F */
LFSRWithWorkMode();
}
   for (i = 0; i < KeystreamLen; i ++)
   {
      BitReorganization();
      pKeystream[i] = F() ^ BRC_X3;
      LFSRWithWorkMode();
}
}
```

LTE Encryption Algorithm Tradeoffs

Scheme	Advantages	Disadvantages
Kasumi	Offers strong encryption via 128-bit keys Optimized for hardware implementation Offers resistance to block cipher attacks	Vulnerable to algebraic attacks
SNOW 3G	Fits 3G security requirements Offers protection against algebraic attacks	Computationally complicated
Milenage	Fits 3G security requirements Offers strong encryption via 128-bit keys Protects against side-channel attacks	Does not require standard algorithm Some interoperability issues
ZUC	**Fits 3G security requirements** **Offers strong encryption via 128-bit keys** **Built on sound design principles**	**Still under scrutiny**

Home eNodeB: AKA Femtocell



HeNB Device Requirements

- Physical security requirements
- Root of trust and Trusted Execution Environment:
  - Utilize root of trust that is subsequently used to verify the Trusted Execution Environment (TEE)
  - Through this mechanism, all code must pass signature validation tests based on the root of trust to thwart malicious code attacks
  - Specifically, TEE must extend the boot process and all OS and other executables used on the HeNB

HeNB Device Requirements

- Device and data integrity check:
  - Must provide these check functionalities to identify tampering attacks that could threaten the security of the HeNB, user data, and the carrier network
- Geolocation:
  - To make sure it is using the frequency that it is allowed to in a given location that is obtained by GPS receiver
- Time synchronization
  - Maintain an accurate clock system to ensure validity of certificate expiration used by IPsec

Thank you.
Questions?

Dr. Abdullah Aydeger