LTE Security – How Good Is It?

Michael Bartock
IT Specialist (Security)
National Institute of Standards & Technology

Jeffrey Cichonski
IT Specialist (Security)
National Institute of Standards & Technology

Joshua Franklin
IT Specialist (Security)
National Institute of Standards & Technology
Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
Agenda

◆ Discussion of LTE standards
◆ Description of LTE technology
◆ Exploration of LTE's protection mechanisms
  ◆ In-depth discussion of applied backhaul security research
◆ Enumeration of threats to LTE
◆ How good is LTE security?
Context of Research

- The Public Safety Communications Research (PSCR) program is a joint effort between NTIA & NIST
- Located in Boulder, CO
- PSCR investigates methods to make public safety communications systems interoperable, secure, and to ensure it meets the needs of US public safety personnel
- Researching the applicability of LTE in public safety communications
What is LTE

- LTE – Long Term Evolution
  - Evolutionary step from GSM to UMTS
- 4th generation cellular technology standard from the 3rd Generation Partnership Project (3GPP)
- Deployed worldwide and installations are rapidly increasing
- LTE is completely packet-switched
- Technology to provide increased data rates
Cybersecurity Research Objectives

- Led by the Information Technology Laboratory’s Computer Security Division with support from Software and System Division and Information Access Division
- Kicked off at the PSCR stakeholder meeting in June 2013
- Takes a holistic approach to cybersecurity for public safety communications
- Leverages existing mobile cybersecurity efforts within the government and industry
- Conduct research to fill gaps in cybersecurity
Cybersecurity Research Objectives

- LTE architecture, standards, and security (NISTIR)
- Identity management for public safety (NISTIR 8014)
- Mobile application security for public safety
- Enabling cybersecurity features in the PSCR demonstration network
- Mapping public safety communication network requirements to standard cybersecurity controls and frameworks (NISTIR)
- Usable cybersecurity for public safety
3GPP Standards & Evolution

Note: Simplified for brevity
LTE Technology Overview
The Basics

- A device (UE) connects to a network of base stations (E-UTRAN)
- The E-UTRAN connects to a core network (Core)
- The Core connects to the internet (IP network).
Mobile Device

- **User equipment (UE):** Cellular device containing the following
  - **Mobile equipment (ME):** The physical cellular device
  - **UICC:** Known as SIM card
    - Responsible for running the SIM and USIM Applications
    - Can store personal info (e.g., contacts) & even play video games!
  - **IMEI:** Equipment Identifier
  - **IMSI:** Subscriber Identifier
The Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

- **eNodeB**: Radio component of LTE network
  - De-modulates RF signals & transmits IP packets to core network
  - Modulates IP packets & transmits RF signals to UE
- **E-UTRAN**: mesh network of eNodeBs
- **X2 Interface**: connection between eNodeBs
Evolved Packet Core (EPC)

- **Mobility Management Entity (MME)**
  - Primary signaling node - does not interact with user traffic
  - Functions include managing & storing UE contexts, creating temporary IDs, sending pages, controlling authentication functions, & selecting the S-GW and P-GWs

- **Serving Gateway (S-GW)**
  - Router of information between the P-GW and the E-UTRAN
  - Carries user plane data, anchors UEs for intra-eNodeB handoffs

- **Packet Data Gateway (P-GW)**
  - Allocates IP addresses and routes packets
  - Interconnects with non 3GPP networks

- **Home Subscriber Server (HSS)**
  - Houses subscriber identifiers and critical security information
LTE Network
Communications Planes

- LTE uses multiple planes of communication
- Different logical planes are multiplexed into same RF signal
- Routed to different end points
TCP/IP sits on top of the cellular protocol stack:

- **Radio Resource Control (RRC):** Transfers NAS messages, AS information may be included, signaling, and ECM

- **Packet Data Convergence Protocol (PDCP):** header compression, radio encryption

- **Radio Link Control (RLC):** Readies packets to be transferred over the air interface

- **Medium Access Control (MAC):** Multiplexing, QoS
Subscriber Identity (IMSI)

- International Mobile Subscriber Identity (IMSI)
  
  - LTE uses a unique ID for every subscriber
  
  - 15 digit number stored on the UICC
  
  - Consists of 3 values: MCC, MNC, and MSIN
  
  - Distinct from the subscriber’s phone number
LTE Security Architecture
LTE Security Architecture

- We will explore several LTE defenses:
  - SIM cards and UICC tokens
  - Device and network authentication
  - Air interface protection (Uu)
  - Backhaul and network protection (S1-MME, S1-U)
- LTE's security architecture is defined by 3GPP's TS 33.401
  - There are many, many, many references to other standards within
UICC Token

- Hardware storage location for sensitive information
  - Stores pre-shared key K
  - Stores IMSI
- Limited access to the UICC via a restricted API
- Performs cryptographic operations for authentication

**TS 33.401 - 6.1.1:** Access to E-UTRAN with a 2G SIM or a SIM application on a UICC shall not be granted.
Device & Network Authentication

- Authentication and Key Agreement (AKA) is the protocol used for devices to authenticate with the carrier to gain network access.
- The cryptographic keys needed to encrypt calls are generated upon completion of the AKA protocol.

3GPP 33.401 - 6.1.1: EPS AKA is the authentication and key agreement procedure that shall be used over E-UTRAN.
AKA Packet Capture

Sending Temporary Identity

Authentication Vectors

Authentication Response
Cryptographic Key Usage

- **K**: 128-bit master key. Put into USIM and HSS by carrier
- **CK & IK**: 128-bit Cipher key and Integrity key
- **KASME**: 256-bit local master, derived from CK & IK
- **KeNB**: 256-bit key used to derive additional keys
- **NASenc & NASint**: 256/128-bit key protecting NAS
- **RRCenc & RRCint**: 256/128-bit key protecting RRC
- **UPenc**: 256/128-bit key protecting UP traffic
Air Interface Protection

- The connection between the UE and the eNodeB is referred to as the air interface.
- 3 algorithms exist to protect the LTE air interface:
  - SNOW 3G = stream cipher designed by Lund University (Sweden)
  - AES = Block cipher standardized by NIST (USA)
  - ZUC = stream cipher designed by the Chinese Academy of Sciences (China)
- Each algorithm can be used for confidentiality protection, integrity protection, or to protect both.

3GPP 33.401- 5.1.3.1: User plane confidentiality protection shall be done at PDCP layer and is an operator option.
Backhaul Protection

- Confidentiality protection of traffic running over S1 Interface (Backhaul)
- Hardware security appliances are used to implement this standard
- Security Gateways (SEG)
- IPSEC tunnel created between eNodeB and SEG

3GPP TS 33.401 - 13: NOTE: In case the S1 management plane interfaces are trusted (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is not needed.
PSCR Applied Research
PSCR Applied Research

- Our Focus is on communication from the cell site to core network.
Our Focus is on communication from the cell site to core network.
Initial Research Goal

- Enable data encryption on the backhaul connection.
- Verify data is encrypted.
- Analyze impact on networks performance.
- Encourage the default use of backhaul encryption.
Why Encrypt the Backhaul

- User data travels over the backhaul.
- The backhaul may or may not be trusted.
  - Example: Operator A uses Operators B’s fiber trunk to connect remote cell sites to its core network.
- An adversary could be listening in on this connection.
Implementation

- Use Internet Protocol Security (IPSEC) to encrypt this communication.
  - Provides encryption at the Internet layer of the IP protocol stack
  - Commercial base stations support IPSEC

- Use public key infrastructure (PKI) certificates to provide strong authentication.
  - Base station and core network authenticate each other.
Current State of Research

- Collaborating with CRADA partners to identify commercial grade solutions
- Implemented backhaul protection on part of PSCR Demonstration Network
- Testing impacts on network performance
- Working to verify interoperability & scalability
Non Encrypted Traffic
## Encrypted Traffic

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200</td>
<td>14:274680000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1201</td>
<td>14:275690000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1202</td>
<td>14:276180000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>150</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1203</td>
<td>14:285995000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>358</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1204</td>
<td>14:286010000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>150</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1205</td>
<td>14:286015000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1206</td>
<td>14:286017000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>150</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1207</td>
<td>14:286019000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>158</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1208</td>
<td>14:286920000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>438</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1209</td>
<td>14:286941000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>278</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1210</td>
<td>14:286943000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>1510</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1211</td>
<td>14:287040000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>118</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1212</td>
<td>14:287045000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>182</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1213</td>
<td>14:287046000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>1510</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1214</td>
<td>14:287049000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>118</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1215</td>
<td>14:287051000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1216</td>
<td>14:287052000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1217</td>
<td>14:292855000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>214</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1218</td>
<td>14:301919000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1219</td>
<td>14:303757000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>198</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1220</td>
<td>14:308218000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>390</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1221</td>
<td>14:308250000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>150</td>
<td>ESP (SPI=0x81d74104)</td>
</tr>
<tr>
<td>1222</td>
<td>14:308805000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>1510</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1223</td>
<td>14:308802000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>118</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
<tr>
<td>1224</td>
<td>14:308801000</td>
<td>10.98.98.98</td>
<td>10.98.98.98</td>
<td>ESP</td>
<td>230</td>
<td>ESP (SPI=0x9e5e27)</td>
</tr>
</tbody>
</table>

- Encapsulating Security Payload
  ESP SPI: 0x9e5e27 (3386901207)
  ESP Sequence: 613
Initial Performance Results

UDP Downlink

Mega Bits per Second

UDP Downlink IPSEC Off

UDP Downlink IPSEC On

39.47

39.39
Initial Performance Results

UDP Uplink

Mega Bits per Second

UDP Uplink IPSEC Off - 12.12
UDP Uplink IPSEC On - 11.06
Next Steps

- Identify additional more tests to better simulate real world deployments.
  - Simulate multiple base stations connecting to one security gateway
  - Interoperability tests
- Identify other vulnerable network interfaces to secure.
  - Uu
Threats to LTE Networks
General Computer Security Threats

- **Threat:** LTE infrastructure runs off of commodity hardware & software.
- **Mitigation:** Security engineering and a secure system development lifecycle.

- With great commodity, comes great responsibility.
- Susceptible to software and hardware flaws pervasive in any general purpose operating system or application.

---

**Threat:** LTE infrastructure runs off of commodity hardware & software.

**Mitigation:** Security engineering and a secure system development lifecycle.

---

**Search Results (Refine Search)**

**CVE-2015-1414**

**Summary:** Integer overflow in FreeBSD before 8.4-p16, 9.x before 9.3-p10, 10.0 before p3p, and 10.1 before p2p allows remote attackers to cause a denial of service (crash) via a crafted ICMP packet, which triggers an incorrect size calculation and allocation of insufficient memory.

**Published:** 2/27/2015 10:59:00 AM

**CVSS Severity:** 2.8 HIGH

**CVE-2014-6413**

**Summary:** The ioctl module in FreeBSD 10.1 before p5, 10.2 before p2p, 10.3 before p2p, and 10.4 before p2p allows remote attackers to cause a denial of service (NULL pointer dereference and kernel panic) via a crafted RE_CONFIG chunk.

**Published:** 2/2/2015 11:56:02 AM

**CVSS Severity:** 2.8 HIGH

---

**Exploit Index**

**CVE-2013-6821**

**Summary:** Pseudo random number generator (PRNG) in the STREAMS virtual network interface (VIF) in FreeBSD 9.0, 9.1, 9.2, 9.3 before p10, and 9.4 before p23 allows local users to (1) gain privileges via the stream sio to the sandbox function, when setting the SCTP_SS_ALLOC option, or (2) read arbitrary kernel memory via the stream sio to the sandbox function, when getting the SCTP_SS_PRIORITY option.

**Published:** 2/2/2013 11:59:01 AM

**CVSS Severity:** 6.6 MEDIAN
Renegotiation Attacks

- **Threat:** Rogue base stations can force a user to downgrade to GSM or UMTS.
- Significant weaknesses exist in GSM cryptographic algorithms.

- **Mitigation:**
  - Ensure LTE network connection. Most current mobile devices do not provide the ability to ensure a user's mobile device is connected to an LTE network.
  - A ‘Use LTE only’ option is available to the user
  - Use a rogue base station detector
Device & Identity Tracking

**Threat:** The IMEI and IMSI can be intercepted and used to track a phone and/or user.

- Rogue base stations can perform a MiM attack by forcing UEs to connect to it by transmitting at a high power level
- The phone may transmit its IMEI or IMSI while attaching or authenticating.

**Mitigation:**

- UEs should use temporary identities and not transmit them in over unencrypted connections.
- IMSI-catcher-catcher
Call Interception

- **Threat:** Renegotiation attacks may also allow MitM attacks to establish an unencrypted connection to a device making a phone call
  - Attacker may be able to listen to the phone call

- **Mitigation:** The ciphering indicator feature discussed in 3GPP TS 22.101 would alert the user if calls are made over an unencrypted connection
Jamming UE Radio Interface

- **Threat:** Jamming the LTE radio prevents the phone from successfully transmitting information.
  - Jamming decreases the signal to noise ratio by transmitting static and/or noise at high power levels across a given frequency band.
  - Research suggests that, due to the small amount of control signaling in LTE, this attack is possible.
  - Prevents emergency calls

- **Mitigation:** Unclear. Further research is required and may require changes to 3GPP standards to mitigate this attack.
Attacks Against the Secret Key (K)

**Threat:** Attackers may be able to steal K from the carrier's HSS/AuC or obtain it from the UICC manufacturer:

- Card manufacturers may keep a database of these keys within their internal network

**Mitigation(s):**

- Physical security measures from UICC manufacturer
- Network security measures from carrier
Physical Base Station Attacks

- **Threat:** The radio equipment and other electronics required to operate a base station may be physically destroyed

- **Mitigation:** Provide adequate physical security measures such as video surveillance, gates, and various tamper detection mechanisms
Availability Attacks on eNodeB & Core

- **Threat:** A large number of simultaneous requests may prevent eNodeBs and core network components (e.g., HSS) from functioning properly.
  - Simulating large numbers of fake handsets
- **Mitigation:** Unclear
Apply What You Learned Today

- Following this talk:
  - Take notice when you’re connected to non-LTE networks (e.g., EDGE, GPRS, UMTS, HSPA, WiFi)
  - Understand protections are offered by LTE – and what isn’t
  - Don’t send sensitive information over untrusted or non-LTE networks
  - LTE helps mitigate rogue base station attacks
Summary – How Good is it?

- LTE security is markedly more secure than its predecessors
- Strong security mechanisms are baked-in
  - Unfortunately, many of them are optional or may not be on by default
  - Although integrity protection mechanisms are required
  - Call your friendly neighborhood wireless carrier today
- Unaddressed threats exist (e.g., jamming)
  - Some are outside the purview of the carriers & standards bodies, such as SoC manufacturers
- LTE is always evolving
  - Today's defenses are not etched in stone
  - Upgrades are in the works via 3GPP Working Groups
Questions?
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AuC</td>
<td>Authentication Center</td>
</tr>
<tr>
<td>AS</td>
<td>Access Stratum</td>
</tr>
<tr>
<td>AUTN</td>
<td>Authentication token</td>
</tr>
<tr>
<td>CP</td>
<td>Control Plane</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data Rates for GSM Evolution</td>
</tr>
<tr>
<td>eNB</td>
<td>eNodeB, Evolved Node B</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packet Core</td>
</tr>
<tr>
<td>EPS</td>
<td>Evolved Packet System</td>
</tr>
<tr>
<td>E-UTRAN</td>
<td>Evolved Universal Terrestrial Radio Access Network</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GUTI</td>
<td>Globally Unique Temporary UE Identity</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identifier</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>K</td>
<td>Secret Key K</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>MME</td>
<td>Mobility Management Entity</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Access Stratum</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards &amp; Technology</td>
</tr>
<tr>
<td>PDCP</td>
<td>Packet Data Convergence Protocol</td>
</tr>
<tr>
<td>P-GW</td>
<td>Packet Gateway</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>PSCR</td>
<td>Public Safety Communications Research</td>
</tr>
<tr>
<td>RAND</td>
<td>Random</td>
</tr>
<tr>
<td>RES</td>
<td>Response</td>
</tr>
<tr>
<td>RLC</td>
<td>Radio Link Control</td>
</tr>
<tr>
<td>RRC</td>
<td>Radio Resource Control</td>
</tr>
<tr>
<td>S-GW</td>
<td>Serving Gateway</td>
</tr>
<tr>
<td>SQN</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary Mobile Subscriber Identity</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>XRES</td>
<td>Expected result</td>
</tr>
</tbody>
</table>
References

- 3GPP TS 33.102: “3G security; Security architecture”
- 3GPP TS 22.101: “Service aspects; Service principles”
- 3GPP TS 33.210: “3G security; Network Domain Security (NDS); IP network layer security”
- 3GPP TS 33.401: “3GPP System Architecture Evolution (SAE); Security architecture”
- 3GPP TR 33.821: “Rationale and track of security decisions in LTE”
- Schneider, Peter, “How to secure an LTE-network: Just applying the 3GPP security standards and that's it?”, Nokia, 2012.