Fixing Insecure Cellular System Information Broadcasts For Good

Alexander J. Ross
North Carolina State University
Raleigh, NC, USA
ajross6@ncsu.edu

Bradley Reaves
North Carolina State University
Raleigh, NC, USA
bgreaves@ncsu.edu

Yomna Nasser
Google
San Francisco, CA, USA
yomna@google.com

Gil Cukierman
Google
New York City, NY, USA
cukie@google.com

Roger Piqueras Jover
Google
New York City, NY, USA
rogerpiqueras@google.com

ABSTRACT

Cellular networks are essential everywhere, and securing them is increasingly important as attacks against them become more prevalent and powerful. All cellular network generations bootstrap new radio connections with unauthenticated System Information Blocks (SIBs), which provide critical parameters needed to identify and connect to the network. Many cellular network attacks require exploiting SIBs. Authenticating these messages would eliminate whole classes of attack, from spoofed emergency alerts to fake base stations.

This paper presents Broadcast But Verify, an efficient backwards-compatible mechanism for SIB authentication. Broadcast But Verify specifies a new signing SIB that encodes authentication signatures and hashes for all other SIBs while building on a standard cellular PKI. We identify the security and functional requirements for such a system, define a scalable and flexible mechanism to meet those requirements, and demonstrate negligible common-case connection latency overhead of 3.220ms in a 4G LTE testbed. We also demonstrate that unmodified mobile devices successfully connect to networks deploying Broadcast But Verify. In contrast to prior proposals, Broadcast But Verify authenticates every SIB broadcasted by a cell. By demonstrating that even 4G LTE has the capacity to authenticate SIBs, we argue that future network generations can and should mandate authenticated SIBs.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; *Security protocols*; *Authentication*; • **Networks** → *Session protocols*; *Signaling protocols*.

KEYWORDS

Cellular Networks, Cellular Network Defenses, Cellular Network Security, Connection Bootstrapping

ACM Reference Format:
Alexander J. Ross, Bradley Reaves, Yomna Nasser, Gil Cukierman, and Roger Piqueras Jover. 2024. Fixing Insecure Cellular System Information Broadcasts For Good. In *The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024), September 30–October 02, 2024, Padua, Italy.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3678890.3678924

RAID 2024, September 30–October 02, 2024, Padua, Italy

ACM ISBN 979-8-4007-0959-3/24/09
https://doi.org/10.1145/3678890.3678924

1 INTRODUCTION

Cellular connectivity has woven itself into the fabric of modern life, becoming an indispensable tool for individuals and critical sectors like healthcare, finance, and transportation. The evolution of cellular technology from analog voice to near-gigabit data rates has facilitated its transformation into an essential utility.

While cellular networks lead in development and deployment of advanced wireless techniques, they lag in security posture. As other computing and communications domains increase security, cellular networks are becoming lower-hanging fruit for attackers. Sophisticated adversaries still use "cell-site simulators" for dragnet surveillance [38], spyware sideloading [1], and electronic warfare [10]. Less sophisticated adversaries increasingly leverage cellular network attacks to distribute spam and phishing messages in Europe [28, 29] and Asia [23].

The aforementioned attacks and others [20, 33, 35] all rely on the fact that the "beacon" messages in cellular networks cannot be authenticated by mobile devices, so an attacker can mislead a device into connecting to malicious infrastructure. Prior work has even declared that these unauthenticated messages are the "root of all evil" in cellular networks [19].

4G LTE and 5G NR term these beacons "System Information Blocks (SIBs)," and they broadcast connection bootstrapping information for mobile devices to find cell sites and configure themselves to attach to the network. The lack of integrity protection in SIB broadcast messages enables adversaries to tamper with neighboring cell information, luring devices to connect to cell-site simulators instead of legitimate base stations. These messages are also the network layer transport medium for Wireless Emergency Alert (WEA) broadcast messages, and this lack of integrity protection permits spoofing of most critical broadcast emergency notifications in cellular networks [6, 22]. While 3G and later networks allow mobile devices to authenticate networks during the attach process, malicious SIBs can specify advantageous parameters that allow attackers to evade protections later.

This paper introduces a new proof-of-concept system, Broadcast But Verify (BBV), that augments the existing 4th generation Long Term Evolution (4G-LTE) cellular protocols with constructs that

enable devices to validate the legitimacy of SIBs and thus cellular base stations. In particular, Broadcast But Verify uses a series of signed hashes to provide integrity protection for SIBs that carry critical connection setup and neighboring cell information as well as the particular SIBs used to transport WEA payloads. These signed hashes are authenticated by a certificate chain with the root of trust centered at each mobile network operator. This chain of trust guarantees integrity and authenticity of all SIBs broadcasted by the cell while still permitting roaming between authorized networks.

In contrast to prior work, Broadcast But Verify adds a dedicated SIB, known as the "signing SIB", to transport signed hashes for other SIBs. This signing SIB protects *every* SIB broadcasted in the cell while simultaneously providing deployment flexibility. We provide an extensive comparison to prior work in the discussion section (6.1) after we have described our approach.

Broadcast But Verify was designed to support incremental deployment, so it supports full backwards compatibility with existing networks and user equipment (UEs). We verified that unmodified UEs will successfully attach to a cell implementing Broadcast But Verify and modified UEs can attach to traditional networks if its BBV security policy permits. While we prototype on LTE networks and devices due to the availability of LTE-based implementation tools, our proposal can be applied to 5G by simply accounting for different SIB types. Moreover, we believe that Broadcast But Verify serves as a design template and positive argument for mandatory SIB authentication in 6G.

This paper makes the following contributions:

- We define the security model of a commercially-deployable SIB authentication system.
- We design Broadcast But Verify, a lightweight system that guarantees SIB unforgeability by enabling UEs to verify the authenticity of any and all SIBs.
- We demonstrate that BBV UEs correctly identify tampered or spoofed SIBs. We further demonstrate that legacy UEs remain fully compatible with BBV networks.
- We evaluate the performance overhead of Broadcast But Verify in the connection setup process and observed an average latency of 3.220ms, which is less than the standard deviation for traditional attaches (40.73ms).

SIB security enables a tradeoff between availability and integrity of infrastructure. Different users and networks will want to make differing policy decisions based on their threat models. Average users may want to prioritize availability and use unauthenticated network parameters with notice that their security may be reduced. Individuals like heads of government may prefer to lose availability to prevent the potential harm of adversarial infrastructure. In many cases, there is no obviously correct choice between avoiding malicious infrastructure or maintaining availability. Nevertheless, Broadcast But Verify provides a mechanism for subscribers and network operators to make informed decisions.

The remainder of this paper proceeds as follows. Section 2 will cover the technical background of LTE networks. Section 3 highlights design constraints and security goals our system must meet. Section 4 describes the design of the Broadcast But Verify system. Section 5 evaluates the performance of BBV. Section 6 provides a discussion of the limitations of BBV, security policy for commercial deployment, compares it with prior work, and implementation in future generations. Section 7 surveys related works in cellular security. Section 8 concludes.

2 TECHNICAL BACKGROUND

In this section, we will provide a brief overview of the upgradeability of LTE/5G cellular networks and then dive into the network architecture, paying particular attention to cellular public key infrastructure, mechanisms for delivering system information, and procedures UEs use to establish a new radio connection with a cell.

2.1 Upgrading Cellular Network Protocols

Cellular network protocols are updated more frequently than advertised. All cellular network generations are designed to evolve to meet the needs of providers and subscribers over their multi-decades long deployment lifetime without requiring a major generational upgrade (e.g., LTE → 5G). The 3GPP (3rd Generation Partnership Project) collects and publishes changes to these standards in "releases" which may cover multiple generations.

With rare exceptions, 3GPP releases are by design fully backwards compatible with user equipment and base stations of differing releases within the same generation, even if the user equipment or base station cannot support all of the features of a newer release. Modifications to existing cellular protocols happen through the use of non-critical extensions of these protocols. Devices that do not understand how to decode non-critical extensions from newer releases simply ignore them.

2.2 LTE Cellular Network Overview

In all LTE networks, there are two main components that provide wireless connectivity: the eNodeB and the User Equipment (UE).
eNodeB: eNodeBs are wireless base station transceivers that provide connectivity between mobile devices and the Evolved Packet Core (EPC). The eNodeB transmits and receives multiple control & data channels that, when multiplexed together, form the Radio Access Network (RAN). The eNodeB also transmits several synchronization signals and broadcasts system information to help UEs find the cell, synchronize with it, and establish a connection.
UE: The User Equipment (UE) is the mobile device that a subscriber uses to access the cellular network. It communicates with the eNodeB to access voice and data services provided by the EPC. The UE uses a Subscriber Identity Module (SIM) card that contains a long-term identifier known as the International Mobile Subscriber Identity (IMSI) along with other long-term symmetric cryptographic keys to authenticate itself to the network. These same cryptographic keys are also stored in the Home Subscriber Server (HSS) located within the EPC of the subscriber's provider.

2.3 Provider Networks

Cellular providers use different terms to describe the network that a subscriber receives connectivity from and pays for service.
Home Network Provider (HN): The HN is the mobile network operator (MNO) that the subscriber pays for cellular service. HNs are responsible for allocating telephone numbers, setting usage policies, authenticating subscribers and for provisioning a Subscriber

Identity Module (SIM) card that UEs use to connect.

A special subclass of MNOs are the so-called mobile virtual network operators (MVNOs). Like MNOs, MVNOs operate a cellular core but they do not operate wireless infrastructure like eNodeBs. Instead, they rely on *serving network providers* to provide wireless coverage for their subscribers.

Serving Network Provide(SN): The SN is the provider that is currently providing wireless service to a particular UE. In many cases, the HN will also serve as the SN when a subscriber is covered by the HN's wireless infrastructure. All serving network providers are identified by their Public Land Mobile Network (PLMN) ID.

Roaming Provider: Most providers do not have global coverage. To permit their subscribers to access cellular network services while out of coverage range of the home network, such as when they are abroad, providers engage in roaming agreements with each other. Roaming agreements are substantial business relationships that rely on mutual trust between roaming partners to transit the traffic of subscribers roaming on their network. When a subscriber roams on a roaming partner's network, that network will reach out to the home network operator to obtain authentication information and route voice and data traffic back to the home network provider.

2.4 System Information Blocks (SIBs)

In LTE and 5G networks, system information blocks (SIBs) are used to quickly and efficiently broadcast information to all UEs within a cell simultaneously. To ensure that a UE entering the cell will be able to quickly configure itself to access the network, all SIBs are broadcasted at regular intervals. Additionally, SIBs are designed to be compact and are broadcast without integrity protection.

In both LTE and 5G, SIBs are encoded into ASN.1 structures. The maximum size of a SIB for traditional LTE may be as low as 217 bytes [4]. 5G increases the maximum SIB size to 372 bytes [2].

As of Release 17, there are 31 defined SIBs for standard LTE and 21 defined SIBs for 5G. Some SIBs, such as SIBtype1 in both LTE and 5G and SIBtype2 in LTE, are essential to bootstrap the UE to access the network. Other SIB types may be used to inform the UE of neighboring cells, apply cell-specific configurations, or quickly disseminate time-sensitive safety alert broadcasts.

In practice, not all SIB types are used in every cell. Only the SIBs that are needed for a particular cell will be broadcasted. Further, some SIBs will only be scheduled on demand. For example, LTE SIBtype12 and 5G SIBtype8, both of which carry Wireless Emergency Alerts (WEA) messages (e.g., severe weather alerts), will only be scheduled if there is an active alert in the cell's serving area.

SIBtype1 is broadcasted on a dedicated transmission with a fixed interval, known as the periodicity, of 80ms with additional repetitions made every 20ms [4]. Cells group and broadcast the remaining SIBs into one or more System Information (SI) broadcast messages. These SI broadcast messages can have different periodicities, permitting the carrier to adjust the transmission frequency for each SIB. SIBtype1 contains scheduling information for other SI messages.

2.5 Network Attach and Handover Procedures

UEs can use several different procedures to set up a radio connection with a cell. The procedure used depends on whether the UE is currently idle to save power or is actively exchanging data with another cell. The descriptions of these procedures presented in this paper focus only on how SIBs facilitate completion of these procedures and thus how introducing Broadcast But Verify might impact their operation.

Attach and Service Requests: Whenever a UE is switched on for the first time, it sends an attach request to register itself with the network. Registration informs the network of the UEs current location and establishes a security context between both parties. From then on, whenever the UE needs to access the network to access voice, SMS, or data services, it will "resume" the connection by sending a service request to the network.

Before the UE can establish a radio connection with the cell, it must obtain the Master Information Block (MIB) and SIBs type 1 and 2 as they contain critical configuration parameters required to access the cell. After receiving the MIB and SIBs type 1 and 2, the UE will execute the random access procedure and then proceed with either the attach or service request.

Handover: The handover procedure is used whenever the cellular network needs to move the UE from one eNodeB to another to facilitate mobility or to load balance between cells. One key difference that set handovers apart from attach and service requests is that the UE is actively exchanging data with another eNodeB in the network. This eNodeB is known as the source eNodeB in this procedure. To permit a mobile device to quickly switch cells while keeping voice and data sessions functional, the network prepares a target eNodeB to accept the UE and forwards traffic to this eNodeB from the source eNodeB while the UE is switching cells. The network prepares the UE with all of the system information required to access the target cell, allowing the UE to immediately start the random access procedure after synchronizing with the target cell.

2.6 Cellular Public Key Infrastructure

With the introduction of 3G, the 3GPP released Technical Specification (TS) 33.310 which standardizes an authentication framework based on public key infrastructure in cellular networks [5]. This standards document provides an overview of public key infrastructure, defines two certificate cross-signing strategies, introduces certificate management and revocation procedures, and describes the architecture of the network domain security and authentication framework (NDS/AF). While the PKI infrastructure described in 3GPP TS 33.310 is standardized, not all features may be deployed yet by providers. In this paper, we focus on the public key infrastructure components that are applicable to Broadcast But Verify.

Certificates: At the heart of all PKI systems is asymmetric cryptography. Private keys are kept secret while public keys are distributed inside of certificates. The purpose of the certificate is to bind a public key to an entity's identity. To ensure that only an authorized party can generate a certificate, the certificate is signed by the issuer, a certificate authority (CA). All certificates have a finite validity period before they expire.

Certificate Chains: Most PKI systems are structured to have multiple certificates chained together to represent trust relationships between different entities. Trust of a particular certificate can be checked by verifying each signature in the certificate chain back to the root certificate. Each certificate must have a valid path back to a trusted root certificate for it to be trusted.

Cross-Signing Certificates: In some situations, it may be necessary to establish trust between different certificate chains. In the context of cellular, this could mean establishing trust between different providers where each provider has its own certificate chain. To establish these trust relationships, certificates are cross-signed. Cross-signing establishes an alternate certificate chain path to the root certificate of a different certificate chain. There are two ways to cross-sign certificates, manual cross-certification and cross-certification with a bridge CA.

Manual Cross-Certification: In this cross-signing strategy, providers directly cross-sign certificates with other providers. A key advantage of this approach is that each provider has complete control over which external certificates and entities they trust.

Cross-Certification with a Bridge CA: In this cross-signing strategy, a third-party CA becomes the bridge between different providers. Unlike manual cross-certification, providers do directly cross-sign certificates of other providers to form trust relationships. Instead, they establish trust with a bridge CA by cross-signing the certificate of this CA. One key advantage of this approach is that a single certificate can be used to trust all providers that the bridge CA trusts. However, a major drawback of this approach is that trust decisions are now delegated to the bridge CA. The provider must trust that the bridge CA is making the right trust decisions for them as they are no longer in full control.

Certificate Revocation: In some situations, such as when a private key is compromised, a certificate may need to be revoked and replaced. Several mechanisms exist to check whether a certificate has been revoked such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP). All certificates except for root certificates can be distributed over insecure channels as the authenticity and integrity of these certificates can be checked by evaluating the certificate chain. Root certificate updates must be distributed over secure channels.

3 PROBLEM STATEMENT

In this section, we describe the constraints, challenges, and requirements associated with securing system information blocks.

3.1 Stakeholders and Adversaries

The cellular ecosystem involves various stakeholders with distinct roles and interests, including mobile network operators and subscribers. Each group's goals and actions are outlined below:

Mobile (Virtual) Network Operators: MNOs and MVNOs provide wireless voice, text, and data services for a subscription fee. They process and route calls, text messages, and data in the EPC between UEs, the PSTN, and the Internet. MNOs additionally operate wireless base stations that UEs use to access the EPC. Their priorities include efficient operation of their network, authentication of subscribers, enforcement of quality of service based on the subscriber's plan, and prevention of theft of service by both malicious subscribers and third parties.

Subscribers: Subscribers access cellular network services provided by MNOs/MVNOs for a fee. They make calls, send text messages, and use data services provided by the cellular network. Subscribers prioritize reliable service from providers and expect location privacy as well as confidentiality and authenticity for all calls, text messages, metadata, and Internet traffic they generate.

Adversaries: Our system defines the attack surface for adversaries as the air interface. We assume a Dolev-Yao style adversary where anyone capable of both transmitting and receiving arbitrary radio signals on cellular frequencies can stand up a fake base station or attempt to broadcast over SIBs or other cellular traffic [11]. Our adversaries include malicious subscribers, intelligence agencies, nation states, and organized criminal groups. We further assume that our adversaries are external to the core network because if they had internal core access, they would not need to execute the attacks we defend against.

Our adversaries may try to inject new SIBs, modify existing SIBs, or erase them entirely to directly attack the UE or prepare it for a second-stage attack. Some examples of attacks against the UE include forcing it to show fake warning messages [6, 19, 22], degrading or preventing connection setup [19, 20, 35], or convincing it to connect to a fake base station to intercept or alter phone calls, text messages, or data traffic [1, 10, 19, 20, 23, 28, 29, 33, 35, 38]. It is important to note that we do not protect against passive relays that simply retransmit traffic without modification, but we do protect against active relays that tamper with the system information before retransmitting it. To do so would likely require authenticating the location of a transmission which is an orthogonal open problem.

3.2 System and Security Requirements

System information blocks are used to convey cell-wide configuration information. Some of these SIBs (e.g., SIBtype1 and SIBtype2) are critical to bootstrapping the connection to the network. Without these SIBs, a UE cannot configure the radio to access the cell. Other SIBs convey information about neighboring cells or carry cell-wide broadcasts. While they are not critical to connection setup, they are still sensitive as tampering with these SIBs could make a UE show fake warning messages [6, 19, 22], degrade or prevent connection setup [19, 20, 35], or convince it to connect to a fake base station [19, 20, 23, 33, 35]. Therefore, it is imperative to protect all broadcasted SIBs from a wide range of attacks, including insertion of new SIBs or modification or erasure of existing SIBs.

3.2.1 Security Requirements. To protect a SIB, we need to both protect the integrity of the transmitted data and authenticate that the SIB originated from an authorized network provider. We therefore stipulate that a secure SIB signing system should meet, at a minimum, the following security requirements:

- **S1** *SIB Unforgeability:* Valid SIBs can only originate from an authorized serving network. No one else can fabricate, replay, modify, or drop a SIB without detection.
- **S2** *SIB Authenticity:* A UE must be able to verify *all* received SIBs were generated by an authorized serving network.
- **S3** *SIB Freshness:* A UE should not accept a SIB transmitted after a specified validity period.

The principle behind these security requirements is that only authorized serving networks should be able to broadcast SIBs that UEs will accept. Adversaries should not be able to broadcast new SIBs or alter existing ones and have them be accepted by UEs.

3.2.2 Functional Requirements. These security requirements are crucial but are not the only factors that affect deployment of our

system. Broadcast But Verify must be designed to be deployable in existing networks while enabling BBV UEs to take appropriate action if they detect an invalid SIB. We therefore stipulate that Broadcast But Verify should meet, at a minimum, the following functional and compatibility requirements:

- **F1** UEs should detect and take action if a critical bootstrapping SIB is altered.
- **F2** UEs should detect and take appropriate action if a non-critical SIB is altered.
- **F3** Legacy UEs should still connect to BBV eNodeBs.
- **F4** BBV UEs should support connecting to legacy eNodeBs.
- **F5** BBV UEs should enforce strict SIB security.

The insight into these functional requirements is that the system must appropriately handle violations of the security properties listed above while maintaining required backwards compatibility with legacy devices and networks.

Every SIB broadcasted by a BBV network should be integrity protected and attested for by a signature. BBV UEs should take appropriate action if they encounter a SIB that fails verification or is not attested for by the network. This action could range from attempting to reacquire the SIB to rejecting the cell and restarting the cell search procedure. The exact action that a BBV UE takes if it finds an invalid SIB is defined by the current BBV security policy specified by the subscriber and the provider.

Any system we develop needs to maintain compatibility with legacy UEs and networks for it to be commercially deployable. We cannot expect universal updates for all devices, especially obsolete devices that no longer receive regular software updates. Additionally, network upgrades will occur incrementally over a span of several months to several years. Therefore, any modification we make to the network and UE must be implemented in a 3GPP-compliant manner such that backwards compatibility is maintained.

Supporting legacy networks introduces a fundamental tradeoff between security and availability. On one hand, allowing legacy networks may seem counter-intuitive as an adversary could set up a fake base station claiming to be "legacy" equipment. On the otherhand, not supporting legacy networks will harm availability, especially for providers with a partial deployment of Broadcast But Verify. Therefore, to provide maximum flexibility, BBV UEs will remain compatible with legacy infrastructure, but the choice to connect to this infrastructure should be left to the user or the provider to decide.

Additionally, to help mitigate risk in partial deployment scenarios, the UE can track which cells have been upgraded. Our system is modeled after the design principles of HTTP Strict Transport Security [16]. When a UE visits a cell for the first time and successfully attaches to it, the network can inform the UE via dedicated signaling if it should strictly require SIB authentication to access the cell in the future. From then on, whenever the UE visits the cell, it will always check for SIB authentication data. If this data is missing or has been tampered with, the UE will refuse to attach.

3.2.3 eNodeB Relays. All wireless systems rely on an open medium to transmit information which makes verification of origin particularly difficult. The physical layer in cellular cannot be authenticated by higher layers.[1] This means that if an adversary wants to transmit, they can and physical layer hardware cannot differentiate between a legitimate signal and a signal broadcasted by an adversary.

An adversary could take advantage of this issue to perform a relay attack or a wormhole attack against our system. Relay and wormhole attacks are physical layer attacks that rebroadcast a received signal, but differ in where the signal is rebroadcasted. Relay attacks rebroadcast the cell locally (the transmitter and receiver are in the same device) whereas a wormhole attack separates the transmitter and receiver, enabling the cell to be rebroadcasted at a distant transmitter. Further advantage is gained from protocol flaws in higher layers. Attacks such as the AdaptOver and SigOver attack have demonstrated that it is possible to inject, modify, or jam signals at the symbol level [12, 37]. Previous malicious relay attacks such as the aLTEr attack have demonstrated that an adversary can take advantage of missing data-plane integrity protection to manipulate user data transmissions [33].

The previously mentioned attacks happen *after* network attach, and they can be mitigated by control- and data-plane integrity mechanisms like MACs. With data integrity protection in place, adversary cannot manipulate traffic after the UE has attached, even when connected through a relay. Adding SIB authentication further prevents an adversary from controlling connection parameters and other information. Even with SIB authentication, an adversary can still rebroadcast authenticated SIBs within their validity period. Doing so could convince a UE to send/receive their traffic through the adversary, but with data integrity the adversary can only read and jam/drop encrypted packets — the same capability any Dolev-Yao adversary is assumed to always have in wireless systems [11].

4 OUR APPROACH

To solve the issue of insecure system information in LTE and, by extension, the overarching threat of fake base stations in current and future cellular networks, we introduce Broadcast But Verify. Broadcast But Verify enables implementing UEs to verify the authenticity, integrity, and freshness of SIBs broadcasted by implementing eNodeBs before they connect to the cell.

Broadcast But Verify is implemented using two new dedicated system information blocks and a certificate chain. The first new system information block is the Signing SIB which contains signed hashes of all other SIBs broadcasted by the eNodeB. A second system information block is used to carry a portion of the full certificate chain that is used to verify the signature of the Signing SIB and, by extension, all SIBs in the cell.

The amount of free space in existing SIBs is extremely limited. The SI message that carries these SIBs has a maximum size that may be as small as 217 bytes if Downlink Control Information (DCI) format 1C is used [4]. We chose to use dedicated system information blocks rather than appending authentication data onto existing system information blocks to maximize deployment flexibility and futureproof our system to support newer SIBs and cipher suites. Constraining ourselves to the free space available on existing SIBs would compromise the flexibility and upgradeability of our system.

We will begin by describing the signing SIB that provides integrity protection for all SIBs in the cell, and then follow with the

[1] As far as we know, every other wireless system suffers from this flaw.

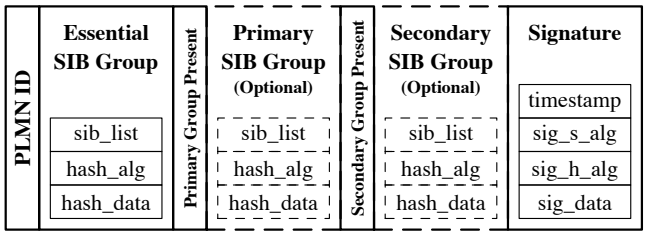

Figure 1: Our new signing SIB structure is flexible and supports many different deployment configurations.

certificate chain of trust that permits a UE to verify the integrity and authenticity of the signing SIB. Finally, we discuss potential implications on handovers and legacy network support.

4.1 Signing SIB

The first component in our system is a new system information block, the signing SIB. The signing SIB contains several fields to permit UEs to verify the integrity and authenticity of all broadcasted SIBs, as shown in Figure 1. The first field in the signing SIB is the Public Land Mobile Network (PLMN) ID of the serving cell. The PLMN ID is a unique identifier that identifies the network operator of the cell. In the event that there are multiple PLMN IDs in the cell, the first PLMN ID in the PLMN ID list, the primary cell PLMN ID, is the one used. This field serves two purposes, it identifies the certificate chain required to later verify the signing SIB and allows the UE to detect if a signing SIB from a different network is being replayed in this network.

Immediately following the PLMN ID are three SIB groups. Every protected SIB is hashed and the combined hash is placed into a designated hash group. Each SIB group structure contains a list of all SIB IDs that are included within the group, the selected hash algorithm *hash_alg*, and the hash *hash_data*. The SIBs included in the group are assembled in ascending SIB type number and packed into the ASN.1 byte array *sibs_packed*. The hash for each group is generated by computing $hash\_data = \text{HASH}(sibs\_packed, hash\_alg)$.

The first SIB group is known as the essential SIB group and it is used to protect critical SIBs. Recall that critical SIBs contain system information that the UE requires to configure itself to access the cell. In LTE, SIBtype1 and SIBtype2 are required to bootstrap a connection and thus these SIBs will always be included in this group. An operator may also choose to add additional SIBs to this group that it deems as critical. All SIBs included in this group must pass verification before the random access procedure can start.

To allow for deployment flexibility, two optional SIB groups, known as the primary and secondary groups, follow the essential SIB group. The mobile network operator can choose whether to use these additional groups and what action the UE should take if either or both of these SIB groups fail verification. From a technical standpoint, there is no difference between these groups other than the policy the carrier applies to these groups. All SIBs broadcasted by a BBV network should be a member of at least one of these groups. We suggest that the primary SIB group should be used for all regularly scheduled SIBs (e.g., neighboring cell lists in SIBs 3-8 and 24) and the secondary SIB group be used for temporarily scheduled SIBs (e.g., CMAS Alert in SIBtype12) as it minimizes the number of SIBs in the essential SIB group while simultaneously permitting the carrier to add temporarily scheduled SIB(s) to the cell without requiring a full re-evaluation of every SIB group.

Certain messages conveyed by SIBs (e.g., Wireless Emergency Alerts) may exceed the maximum transmission size of a single SI message. If this occurs, that message may be segmented into multiple SIBs. Each SIB segment carries a different segment of the message and the full message is reconstructed at the UE. If multiple SIB segments are broadcasted, all SIB segments will be packed in ascending order at the eNodeB and all SIB segments must be received by the UE it to verify the message.

All SIBs (and SIB segments) currently being broadcasted by the cell must be included in at least one SIB hash group. Any SIB except for SIBtype1 and SIBtype2 can be a member of multiple hash groups, though we see no benefit to including a SIB in more than one group. SIBtype1 and SIBtype2 are implicitly scheduled in the essential SIB hash group and thus cannot be added to the primary or secondary groups.

The last block in the signing SIB is the signature which provides integrity protection and authenticity for all group hashes as well as the signing SIB itself. The signature structure contains a 64-bit time of generation timestamp, indications for the desired hashing and signature algorithm, and the signature itself. The signature is generated by first populating the timestamp with the current time and then packing every field in the signing SIB into *sib_packed* except for the signature data. We then obtain the hash by computing $sig\_hash = \text{HASH}(sib\_packed, sig\_h\_alg)$. The signing SIB is then signed by calling $\text{SIGN}(sig\_hash, sig\_s\_alg, K^{-})$. Finally, the *sig_data* field is populated.

The SIB group hashes cannot be modified without also changing the signature, which the adversary cannot compute unless they are in possession of the correct signing key. Only a legitimate serving network should be in possession of the signing key. Since the group hashes can no longer be changed by the adversary, the adversary is also now unable to forge any SIBs that are part of one of these groups. These SIBs, through the use of the group hash and the signing SIB signature, can now be checked for data authenticity and integrity. Therefore, the Broadcast But Verify signing SIB provides security requirements **S1** and **S2**.

The timestamp in the signature is used to bind the signing SIB generation time so that the signing SIB cannot be replayed hours or days later. SIB updates happen relatively infrequently so a timestamp validity duration may be as large as a few minutes with minimal risk. The exact validity time is up to the mobile network operator to specify. Since the timestamp is mixed into the signature and the adversary cannot forge a new signature without the key, the signing SIB provides a guarantee of freshness, thus providing security requirement **S3**.

Ideally, the carrier will schedule all system information changes to coincide with the expiration of the signing SIB so that an adversary cannot broadcast old system information. If the carrier had to update the system information early (e.g., add a time-sensitive SIBtype12 warning message), the most an adversary could do is delay the delivery of the new system information by the remaining validity time of the old signing SIB. When carriers select the max validity time of the signing SIB, they will need to balance their risk tolerance to replay, relay, and wormhole attacks with overhead of

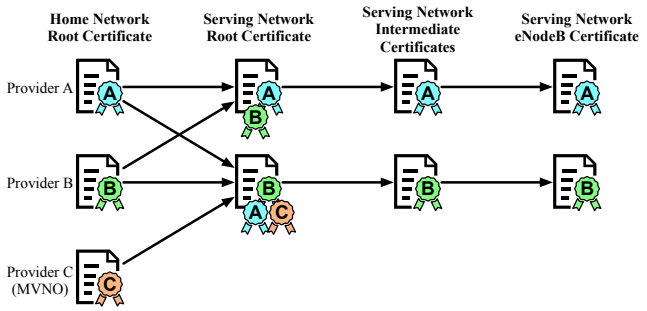

Figure 2: Providers cross-sign certificates to form links of trust with roaming providers. In this example, Providers A and B have established a roaming agreement with each other. Provider C is an MVNO that relies on Provider B to provide wireless connectivity for their subscribers. The certificate chain terminates at the eNodeB.

signing new signing SIBs on their infrastructure (we discuss these attacks further in Section 3.2).

The signing SIB was designed to impose minimal additional load on the eNodeB. When an eNodeB switches on, the eNodeB will automatically generate the signing SIB after it packs all of the other SIBs. From then on, the signing SIB is only regenerated when a SIB is added, updated, or removed, or whenever the validity period of the signing SIB expires.

4.2 Certificate Chain of Trust

The Broadcast But Verify signing SIB relies on public key cryptography to provide integrity protection and ensure authenticity of all SIBs broadcasted in BBV networks. Broadcast But Verify builds on top of cellular public key infrastructure standardized in 3GPP TS 33.310 [5]. This document standardizes the use of PKI in cellular networks by providing a foundational overview of PKI architecture, cross signing strategies, and certificate management and revocation procedures. For more information, please see Section 2.6.

While this document provides a solid foundation, it does not prescribe a specific PKI system or certificate chain style. For Broadcast But Verify to provide SIB security, a certificate chain is used to verify the integrity and authenticity of the signing SIB, and thus the SIBs in the cell. In the following subsections, we will describe the structure of the certificate chain and cover how certificates are stored, transmitted, and revoked in Broadcast But Verify.

4.2.1 Certificate Chain. The certificate chain in Broadcast But Verify establishes trust between different network entities in the provider's core and access networks. Broadcast But Verify uses this certificate chain to verify the integrity and authenticity of the signing SIB which is then able to extend these protections to SIBs broadcasted in the cell. In designing the certificate chain, we made each network operator a so-called self-sovereign network. The proposed certificate chain is shown in Figure 2.

The chain starts with the home network root certificate and terminates with the signature in the signing SIB. All cellular providers will possess a root home network certificate. Every provider that operates a radio access network also possesses a root serving network certificate that is signed by their home network certificate. If the provider has engaged in roaming agreements with other providers, the root serving network certificate is also cross-signed by each roaming partner. Since roaming agreements are substantial business relationships, cross-signing serving network certificates should not be a significant impediment to implementation of this system. The serving network certificate chain can contain additional layers for other network entities (e.g., Mobility Management Entity (MME) certificates), but will ultimately terminate at the eNodeB. The eNodeB uses the private key corresponding with the public key in the eNodeB certificate to sign the signing SIB.

This certificate chain style has several advantages. First, by making each network a self-sovereign network, providers are in complete control over trust decisions for roaming providers. By introducing the serving network root certificate as the cross-signing point, we maintain deployment flexibility while simultaneously reducing the number of certificates that need to be cross-signed. Finally, this chain style also limits the impact should any of the serving network certificates be compromised.

4.2.2 Certificate Storage and Broadcasts. The long-term root certificates are preloaded into the certificate repository within the SIM card or the eSIM provisioning profile. At least two long-term home network root certificates should be preloaded to permit failover should one of these certificates require replacement. The serving network root certificates are also preloaded into the certificate repository as they are cross-signed by the home network root CA.

Serving network certificates are signaled to the UE via a dedicated certificate SIB. This SIB contains the certificate chain from the eNodeB to the certificate immediately before the serving network root certificate. If the certificate chain is too large to fit in a single certificate SIB, multiple certificate SIBs may be scheduled, each carrying a portion of the chain. Before the UE can use certificates in the certificate SIB, it must validate the certificates with the root home network certificate.

4.2.3 Certificate Revocation. If a certificate needs to be revoked, the certificate will be added to the provider's certificate revocation list. Short-term serving network certificates can be replaced by updating the certificates in the certificate chain SIB; they are not stored on the UE. Replacement of long-term root certificates requires the certificate repository in the SIM card or eSIM profile to be updated. They could be delivered via binary SMS messages or carrier configuration updates the next time the UE attaches to the network. The UE will still be able to attach even if one of the long-term home or serving network root certificates is revoked as both the UE and the network can switch to the backup certificate already preloaded on the UE.

4.3 SIB Verification Procedure

When the UE selects a cell and receives the signing SIB, the UE will first verify the data authenticity of the signing SIB before proceeding to verify each SIB group. The SIB verification pipeline steps are shown in Figure 3. A detailed diagram of the BBV connection setup procedure is shown in Figure 5 in the Appendix.

Upon reception of the signing SIB, the UE will first check that the Public Land Mobile Network (PLMN) ID of the signing SIB and SIBtype1 match. This check is performed to detect early whether

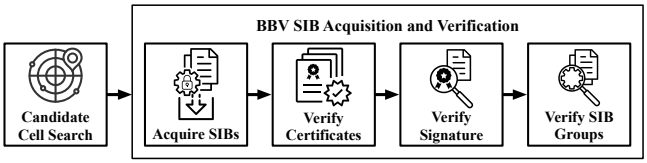

Figure 3: The signing SIB verification procedure is a multi-step process that verifies the integrity and authenticity of transmitted SIBs.

a signing SIB from another network is being replayed in this cell. If the PLMNs match, the UE then evaluates the freshness of the signing SIB by checking that the elapsed time since the SIB was generated is within the maximum allowed validity period as defined in the BBV security policy. If the signing SIB has expired, the UE will attempt to acquire a new signing SIB before continuing with this procedure. Provided that the SIB is deemed to be fresh, the UE will then retrieve the corresponding serving network certificates as identified by the PLMN and verify the certificate chain.

To validate the signature, the signing SIB is first re-packed into *sib_packed* with the signature data field excluded. The UE then computes $sig\_hash = \text{HASH}(sib\_packed, sig\_h\_alg)$ and finally verifies it by calling $\text{VERIFY\_SIG}(sig\_data, sig\_hash, sig\_s\_alg, K^{+})$. If signature verification fails, the UE should consider the signing SIB as invalid. The action that the UE takes from this point depends on the UE's BBV policy, and the UE could attempt to reacquire the signing SIB or abandon the cell and restart the cell search procedure.

After verifying the signing SIB signature, the UE will validate all three hash groups. For each group, the UE will first acquire any missing SIBs from that group. Next, the UE will pack all SIBs in the group into *sibs_packed* in ascending order. Finally, we obtain the hash by computing $computed\_hash = \text{HASH}(sibs\_packed, hash\_alg)$ and compare it to the expected hash in the signing SIB.

If hash verification succeeds for the essential group, the UE can proceed to process all SIBs that are part of the group and start the attach procedure. However, if hash verification fails, the UE should consider the SIBs as invalid. Depending on the current Broadcast But Verify security policy, the UE could attempt to reacquire all invalid SIBs, ignore the SIBs, accept them anyway, or abandon the cell and restart the cell search procedure.

For the primary and/or secondary groups, the UE will process SIBs that are part of these groups only if the group is verified successfully. If the primary or secondary SIB group fails verification, the UE should consider the SIBs within the affected group(s) as invalid. Depending on the current Broadcast But Verify policy, the UE may attempt to reacquire all invalid SIBs, ignore the SIBs, accept them anyway, or abandon the cell. Different resolution actions may be specified in the Broadcast But Verify security policy for the primary and secondary SIB groups.

4.4 Impact on Handovers

One important consideration of Broadcast But Verify is the potential impact on handovers. Handovers need to be completed quickly or an ongoing voice or data session will be interrupted. There are three main types of handovers: "blind", "UE assisted", and "Radio Link Failure" handovers.

In "blind" and "UE assisted" handovers, the network is in control of the handover procedure and decides when the UE should move from one cell to another. The source eNodeB initiates the handover by transmitting an `RRCConnectionReconfiguration` message to the UE. This message informs the UE of the target frequency of the new cell, its identity in the new cell, and provides all required system information to access the cell [3, 4]. Upon executing the cell switch procedure, the UE will synchronize with the cell and obtain the Master Information Block (MIB) before initiating the random access procedure. The UE does not acquire SIBs before connecting; it already received all system information required to access the cell in the `RRCConnectionReconfiguration` message. SIB acquisition, and thus Broadcast But Verify evaluation, will only execute after the handover has been completed, not during the handover. Therefore, Broadcast But Verify will have no impact on the performance of "blind" and "UE assisted" handovers. The BBV handover procedure is shown in Figure 6 in the Appendix.

In contrast to "blind" and "UE assisted" handovers, "Radio Link Failure" (RLF) handovers are performed only in exceptional cases where the UE loses connection with the original cell and must reestablish a connection with a different cell. It is important to note that a RLF handover will always result in an interruption to any ongoing voice or data sessions. Therefore, the goal of this procedure is to establish a new connection as quickly as possible, not to guarantee a seamless transition between cells. Since recovering from radio link failure requires the UE to search for a new cell and thus receiving SIBs before establishing a connection to that cell, BBV could impact the recovery speed. Just like a traditional network attach or service request, the UE would need to at minimum receive and verify the signing SIB along with all SIBs in the essential SIB group before it can begin the random access procedure. Therefore, the performance penalty would be identical to that of a traditional network attach or service request to a new cell.

One edge case of concern is what happens if the UE completes a "blind" and "UE assisted" handover but is unable to verify the signing SIB or the essential hash group. In traditional LTE, UEs will replace the system information received from the source eNodeB with the system information broadcasted by the target eNodeB as soon as it is received. We do not prescribe the behavior the UE must take, instead, we provide a mechanism to allow the carrier to specify the action the UE takes upon encountering this condition. The UE could, for example, remain connected but continue to use the system information provided by the source eNodeB, accept the broadcasted system information anyway, or disconnect from this cell, either immediately or after a predetermined condition occurs (e.g., current call ends). Ultimately, the UE will choose the action that was specified by the current BBV security policy. Please see our discussion on policy in Section 6.2 for more information.

4.5 Optional Legacy Network Support

Broadcast But Verify was designed with flexibility in mind and supports a wide range of deployment scenarios. To allow for incremental deployability, carriers and/or OEMs can enable or disable legacy network compatibility mode in the BBV security policy. Hardened deployments can immediately switch on strict SIB verification while carriers rolling out the signing SIB to their network

can permit the UE to connect to legacy networks. This setting could also be defined by the user, opting in or out of Broadcast But Verify via a user toggle.

The only situation where support for connecting to legacy networks is mandatory is when the UE must emergency attach to any available network. Emergency attaches, by definition, are a last-resort procedure to establish connectivity to emergency services when home or roaming network access is unavailable. This is an opt-in procedure. If a subscriber dials emergency services and the UE initiates an emergency attach, then they are consciously forfeiting *all* security protections including ciphering and integrity protection for availability of the phone network. To facilitate availability, Broadcast But Verify will also be disabled completely for the duration of the emergency connection.

Legacy network support may also be required to support roaming, even if the home network operator has completely rolled out Broadcast But Verify across their entire network. Therefore, if the UE needs to roam on an authorized roaming network that does not support Broadcast But Verify, it must fall back to legacy mode. The UE will decide whether to roam on networks based on the current BBV security policy.

Adding support for legacy networks does introduce the potential for bidding down attacks adversaries could try to convince the UE that they are "legacy" equipment. To mitigate this issue, UEs can keep track of cells that have been updated to support Broadcast But Verify. Whenever the UE successfully attaches to a BBV cell, it will mark that cell as supporting strict SIB security in an internal database. This is analogous to HTTP Strict Transport Security. Network operators can also push a list containing the cell IDs of all upgraded cells to the UE through an over-the-air update. If an attacker attempts to erase the signing SIB from the cell, BBV UEs that already have the cell marked as supporting strict SIB security can refuse to attach, thus providing functional requirement **F5**.

5 EXPERIMENTAL EVALUATION

In this section, we evaluate the performance of Broadcast But Verify. We first built BBV on top of srsRAN, an open-source LTE network stack [15]. srsENB was modified to support generating and transmitting the new signing SIB while srsUE was modified to support receiving and verifying the signing SIB. The modified copies of srsENB and srsUE will be referred to as bbvENB and bbvUE, respectively, for the remainder of this section.

We start our evaluation by verifying that our Broadcast But Verify implementation meets all of the functional, security, and backwards compatibility requirements as described in our problem statement. We then analyze the performance implications of running BBV SIB verification compared to a traditional network attach. Finally, we perform a case study where we subject Broadcast But Verify to a Presidential Alert Spoofing Attack.

5.1 Research LTE Network

A modified copy of srsRAN that implements Broadcast But Verify was run on a desktop equipped with an Intel Core i9-13900K processor and 128 GB of RAM. A USRP B210 SDR served as the radio for the BBV eNodeB to broadcast our LTE network [13]. A second USRP served as the radio for the BBV UE.

Figure 4: We performed all experiments in a Faraday cage

All experiments were performed in a Ramsey Electronics STE3500 Faraday cage. For experiments that required a commercial off-the-shelf (COTS) UE, we used a Google Pixel 6 running Android 13 build TP1A.221105.002. Our setup is depicted in Figure 4.

5.2 Broadcast But Verify Functional Testing

In these experiments, we verify that several of the security requirements outlined in Section 3.2 function correctly in our implementation of Broadcast But Verify. To perform these experiments, test cases were added to bbvENB that alter certain fields in the signing SIB to intentionally corrupt the signing SIB.

In all of our experiments, we configured the BBV security policy to strictly validate the signing SIB and the essential SIB group. If the signature is invalid or the essential SIB group fails verification, bbvUE will reject the cell and restart the cell search procedure. If the primary or secondary SIB groups fails verification, the SIBs in those groups are ignored but we do not abandon the cell.

We first verified that bbvUE correctly accepts a valid signing SIB. bbvENB was configured to broadcast a valid signing SIB for the current network configuration. We observed that bbvUE correctly accepted all SIBs and attached to the cell.

We then tested functional requirement **F1** which requires bbvUE to detect and take appropriate action if it receives an invalid critical bootstrapping SIB. In Broadcast But Verify, the signing SIB is used to authenticate critical bootstrapping SIBs so a signature verification error on this SIB should invalidate it. Additionally, the UE should take action as specified by the Broadcast But Verify security policy if the essential SIB group is found to be invalid.

To test whether bbvUE correctly implements this functional requirement, we performed two experiments. The first experiment examines whether bbvUE would reject the cell if it received an

invalid signing SIB signature. In our setup, we corrupted the signature by adding "1" to the last block of the signature. We observed that bbvUE correctly flagged the signature as invalid and rejected the cell by refusing to start the attach procedure as required by our applied BBV security policy.

Next, we tested whether bbvUE would reject the cell if it received an invalid essential SIB group hash. In our setup, we corrupted the essential SIB group hash by adding "1" to the last block of the hash. We observed that bbvUE correctly flagged the essential SIB group as invalid and rejected the cell by refusing to start the attach procedure as required by our applied BBV security policy. Since both of these experiments pass, bbvUE meets functional requirement **F1**.

Finally, we tested functional requirement **F2** which requires bbvUE to detect and take appropriate action if it received an invalid non-critical SIB. Recall that a non-critical SIB is any SIB that is not required to set up the connection and is not part of the essential SIB group. In Broadcast But Verify, non-critical SIBs can be protected by either the primary or secondary SIB group hash.

In our implementation, bbvUE will ignore all SIBs in the primary or secondary SIB group if it receives an invalid SIB in either of these groups. We performed the experiment twice, with the primary hash group corrupted in the first run and the secondary hash group corrupted for the second run. Both the primary and secondary SIB group hashes were corrupted by adding "1" to the last block of the hash. We observed that when the primary SIB group is corrupted, bbvUE still attaches but correctly flagged the primary SIB group as invalid. We repeated this experiment with the secondary SIB group and also observed that bbvUE correctly flagged the secondary SIB group as invalid. Since both of these experiments pass, bbvUE meets functional requirement **F2**.

5.3 BBV Backwards Compatibility

We next verified that Broadcast But Verify maintains backwards compatibility with legacy UEs and networks as outlined in our system requirements in Section 3.2.

To examine whether Broadcast But Verify maintains backwards compatibility with legacy UEs and thus meets functional requirement **F3**, we experimentally tested whether a COTS UE could connect to a BBV network. Specifically, we connected a Google Pixel 6 running a Google internal development version of Android to bbvENB and examined the modem logs.

As a control, we first configured an unmodified version of srsENB to broadcast only SIBs 1, 2, and 3. We observed that the Google Pixel 6 successfully attached to the network. The modem diagnostic log from this experiment was saved for later comparison.

Next, we configured bbvENB to broadcast the signing SIB with SIBtype3 added to the primary SIB group. We observed that the Google Pixel 6 successfully attached to the network and that there was no appreciable difference in attach time or network responsiveness. We also examined the modem diagnostic log and found only two additional diagnostic messages indicating that the signing SIB was detected and ignored. We did not observe any errors or abnormal behavior compared to the control. Therefore, bbvENB meets compatibility requirement **F3**.

Finally, we examined whether Broadcast But Verify maintains backwards compatibility with legacy networks and thus meets functional requirement **F4**. We reconfigured bbvUE to permit connecting to legacy networks and used the same copy of srsENB used earlier. We observed that bbvUE displayed a warning indicating that the network could not be authenticated, but that it still permitted the network attach to take place. Therefore, bbvUE meets compatibility requirement **F4**.

5.4 BBV Performance Evaluation

In these experiments, we aim to characterize the time overhead experienced by both the eNodeB and the UE. To evaluate the overhead, we measured the amount of time required for bbvENB to generate the signing SIB and for bbvUE to acquire this SIB and use it to verify all other SIBs.

Broadcast But Verify permits the signing SIB to be broadcast standalone or together with other SIBs. Choosing when to broadcast the signing SIB is critically important to optimize the performance of BBV. Specifically, the SI periodicity or the amount of time between SI broadcasts, directly impacts the performance of BBV. A higher interval between broadcasts will negatively impact the average connection setup time as the UE on average has to wait longer to receive the BBV SIB. Real-world deployments will need to balance data transmission overhead with the average connection setup overhead from waiting for the SI message carrying the signing SIB to be transmitted. In our setup, we chose to broadcast this SI message every 160ms or 16 radio frames, the same as the default configuration for SIBtype2 which is a critical connection setup SIB.

The signing SIB was configured to broadcast with all three signatures present. The essential hash group contained the hash for SIBtype1 and SIBtype2 while both the primary and secondary hash groups contained the hash for SIBtype3. This configuration resulted in a data overhead of 191 bytes every 160ms. It is important to note that the size of the signing SIB is variable and will be dependent on the number of SIBs, whether the primary and/or secondary hash groups are present, and the cryptographic algorithms used.

As a control, we first measured the amount of time required for a UE to switch on and complete the attach procedure. We then evaluated the amount of additional time required for the UE to complete the attach procedure while verifying all SIBs. Each scenario was repeated 100 times to obtain an average attach time. The results of this experiment are shown in Table 1.

At the eNodeB, we observed minimal overhead during the generation of the signing SIB. The BBV SIB generation procedure took around 0.75ms to complete, regardless of whether the SIB was scheduled in a dedicated SI message or broadcasted alongside SIBtype2. Bear in mind that the BBV SIB generation procedure is called infrequently, only whenever a system information update occurs, the timestamp expires, or one of the certificates in the certificate chain expires or is replaced.

At the UE, we first evaluated the amount of overhead processing the signing SIB. We anticipate that the processing overhead delay should be constant, regardless of where the signing SIB is scheduled. As expected, verification takes approximately 1.36ms in both cases.

When the signing SIB was combined with SIBtype2, the connection setup time increased to 201.71ms, a modest 1.62% increase over the control. The 3.220ms difference in average connection time between BBV and the control is dwarfed by the 40+ms standard

Table 1: Connection and Processing Times compared with Standard LTE

Signing SIB Location	eNodeB Signing SIB Generation		UE SIB Verification		UE Connection Setup Time	
	Average (ms)	STDEV (ms)	Average (ms)	STDEV (ms)	Average (ms)	STDEV (ms)
Standard LTE	N/A	N/A	N/A	N/A	198.49	40.73
BBV: Combined SI Message	0.751	0.015	1.367	0.029	201.71	48.91
BBV: Dedicated SI Message[1]	0.750	0.015	1.363	0.022	370.66	49.04

[1]In practice, a dedicated SI message may never actually be needed but we include it to demonstrate the worst case scenario performance of Broadcast But Verify.

deviation, so we argue that the cost of BBV is insignificant in this scenario. However, when the signing SIB was scheduled in its own SI message, the connection setup time increased to 370.66ms, almost double the control. Almost all (99.21%) of the added delay was spent acquiring the signing SIB.

We examined the srsUE source code and determined that the overhead we observed can be attributed to the way srsUE handles SI broadcast acquisition. For each SI broadcast signaled in SIBtype1, srsUE launches an independent SI acquisition process to receive that SI broadcast. Only a single SI acquisition process is active at once; additional SI acquisition processes must wait until the current one has finished. When the signing SIB is scheduled in a dedicated SI message, srsUE has to receive two SI messages instead of just one. We examined a network trace captured at srsENB and found that the SI message carrying the signing SIB was broadcasted immediately after the first SI broadcast. Therefore, we attribute the increased overhead to srsUE waiting approximately 160ms for the second SI broadcast to repeat as it missed the first instance because the first SI acquisition procedure is taking too long to complete.

While we anticipate that a commercial baseband will perform significantly better at acquiring multiple SI broadcasts compared to srsUE, this experiment demonstrates that providers need to carefully choose when SIBs are scheduled. Since SI messages are fairly large (minimum 217 bytes for traditional LTE and 372 bytes for 5G), we anticipate that the need to schedule the signing SIB separately from other critical connection setup SIBs should be exceptionally rare. However, even in the worst-case scenario presented above, an unoptimized UE implementation still completes the entire SI acquisition and attach procedure in less than half a second. Subscribers are highly unlikely to notice this delay.

Battery-powered UEs have a finite amount of available power. To verify all SIBs, the UE must consume some of this power. Therefore, the BBV SIB verification procedure must execute quickly to ensure that the maximum amount of available power can be used by the subscriber. Given that acquiring the BBV SIB and verifying all SIBs takes only a fraction of the total connection setup time and that connection establishment occurs infrequently, the power impact of this procedure is minimal. Subscribers are highly unlikely to notice any additional battery drain when connected to cells that implement BBV compared to legacy cells.

Although we are unable to test handovers because srsRAN has only basic support for this procedure, we examined whether BBV SIB verification would impact the outcome of the handover procedure. For both "blind" and "UE assisted" handovers, the UE is provided with the system information for the target cell before it leaves the source cell. This permits the UE to completely skip SIB acquisition and start the random access procedure as soon as it has synchronized with the cell. Therefore, Broadcast But Verify will have no impact on these handovers because the UE does not acquire SIBs before completing the handover procedure.

"Radio Link Failure" (RLF) handovers, on the other hand, will be impacted by BBV procedure. When a UE performs a RLF handover, it must acquire SIBs before it is able to attach to a new cell. Therefore, BBV will have the same impact on this procedure as it does during a traditional network attach.

5.5 Case Study: Presidential Alert Spoofing Attack

The wireless emergency alert (WEA) system utilizes the commercial mobile alerting system (CMAS) to broadcast alert messages quickly to all mobile subscribers. However, this system is vulnerable to SIB spoofing attacks such as the presidential alert spoofing attack as there is integrity protection or authentication for the SIBtype12 that carries these alerts [22]. Broadcast But Verify provides a mechanism to authenticate the source of these alerts and should only deliver legitimate ones to the subscriber. In this experiment, we examine whether bbvUE correctly identifies whether a CMAS alert is valid.

To perform this experiment, we first added support for SIBtype12 to bbvENB and bbvUE. We used the same SIB verification policy configuration as in the functional experiments. We also configured bbvUE to show an alert if SIBtype12 is found to be invalid. It is important to note that bbvUE, just like a legacy UE, will only show the SIBtype12 warning message payload once. The same applies to the invalid SIB warning message as Broadcast But Verify will not show the warning message again unless the SIB contents change.

Legitimate CMAS Alert: To evaluate whether a legitimate CMAS alert will be accepted by bbvUE, we configured bbvENB to broadcast SIBtype12 and added the SIB to the secondary hash group in the signing SIB. We observed that after the signing SIB verification procedure completed the UE correctly displayed the presidential alert. We also attached a Google Pixel 6 to the network and observed that the presidential alert was immediately displayed after taking the phone out of airplane mode.

Spoofed CMAS Alert: To evaluate whether a spoofed CMAS alert will be correctly rejected by bbvUE, we removed SIBtype12 from the secondary hash group to simulate a SIB fabrication attack. We observed that the spoofed presidential alert was correctly rejected by bbvUE and that a SIB integrity verification error was displayed to the user. We also observed that the Google Pixel 6 still displayed the alert, which is expected because it does not have any mechanism to verify the authenticity of the CMAS alert.

6 DISCUSSION

In this section, we compare Broadcast But Verify to prior work and discuss defining a security policy for deployment, limitations

of BBV, applicability to future cellular generations, and potential implications to availability and lawful interception.

6.1 Comparing BBV to Alternate Proposals

Prior work has investigated enabling UEs to verify system information blocks and/or the validity of the current serving cell. One closely related work authenticated SIBtype1 and SIBtype2 by attaching signatures and a certificate chain directly onto these SIBs [19]. Another closely related work attached the signature directly to SIBtype1 and used a pre-shared key to authenticate these signatures [36]. A third related work takes a different approach and uses an authentication token to verify the authenticity of the serving base station [25]. While these approaches share common goals, they each have drawbacks that limit their ability to adequately protect all SIBs broadcasted by the cell. We demonstrate a different approach that provides superior operational and security guarantees.

Two of the prior works proposed attaching a signature directly onto existing SIBs. [19, 36]. A key design constraint for both of these approaches is the amount of remaining spare space available on existing SIB messages. SI broadcast messages have a maximum size limit that may be as small as 217 bytes if DCI format 1C is used [4]. Since the amount of free space is thus extremely limited, the size of the signature and any supplementary data (e.g., certificate chain) must be minimized.

By constraining themselves in the way they have, the alternative approaches only provide limited protection for other broadcasted SIBs. Although both systems prevent the modification of SIBtype1, this only provides protection against fabrication of new SIBs. If another SIB, such as SIBtype12, is already scheduled, an attacker can modify these SIBs without invalidating the signature. This could permit the attacker to add false base stations and/or remove existing cells from the neighboring cell list, change the type and text of an already scheduled emergency alert, or disrupt connectivity to the network by deliberately misconfiguring sidelinks or the multimedia broadcast multicast service (MBMS).

A third closely related work implemented an efficient authentication scheme that enables the UE to verify the validity of the serving base station [25]. In this system, the UE transmits an encrypted authentication challenge, known as an authentication token, to the network during a handover or the initial access to the network. The network forwards this token to a trusted entity which decrypts it, performs a transformation on it, and then re-encrypts it. This encrypted authentication response is then transmitted back to the UE from the current serving eNodeB (the target eNodeB in a handover) which the UE then verifies to authenticate the eNodeB. While this approach permits the UE to verify the authenticity of the current serving cell and thus eliminate a wide range of pre-authentication attacks, it provides no protection for system information blocks. An adversary can still tamper with any SIB broadcasted by these cells without invalidating the authentication token.

In contrast to prior work, Broadcast But Verify was implemented by adding dedicated system information blocks to transport the signed hashes and certificate chain. Adding new SIBs to LTE is practical and can be done in a standards-compliant manner that maintains backwards compatibility with existing UEs and networks. By using a dedicated signing SIB, we have room to include multiple signed hashes, thus permitting Broadcast But Verify to protect *every* SIB broadcasted in the cell. The signing SIB was designed with flexibility to support multiple hashing and signature algorithms. Broadcast But Verify natively supports many different cipher suites today including post-quantum safe algorithms.

Our system uses a similar PKI-scheme to one of the existing approaches with one important difference. In the previously proposed work, the certificates or public keys for all roaming providers would be provisioned onto the SIM card of the UE [19]. We, however, reuse already existing PKI schemes in cellular network standards to simplify certificate management, enabling easy onboarding of new roaming providers, and easy revocation and updates to existing certificates from all authorized serving networks.

6.2 Broadcast But Verify Security Policy

When a UE encounters a tampered or spoofed SIB, it is presented with a dilemma. The UE needs to choose between integrity or availability in deciding whether to accept the SIB or not. Previously, the decision was always for "availability." The UE had no choice as it had no way of knowing if a particular SIB is legitimate or not.

Broadcast But Verify was designed to enable subscribers and carriers to be in full control of whether the UE accepts a particular SIB or not. We intentionally designed flexibility into the system to meet the needs of different deployment scenarios. Some deployment scenarios may still want to enforce integrity and strictly drop all SIBs while others may want to make different choices based on the SIB type and importance for a particular UE, subscriber, or application. Broadcast But Verify enables UEs to now make this decision, but they are responsible for defining a Broadcast But Verify security policy that meets their deployment goals and needs.

6.3 Broadcast But Verify Limitations

Although Broadcast But Verify significantly reduces the pre-authentication attack surface, it does not eliminate it entirely. Broadcast But Verify was designed to provide protection only to system information blocks. It does not protect against attacks other pre-authentication traffic and signals such as 2G downgrade attacks via spoofed attach reject messages.

Broadcast But Verify only protects SIBs when both the UE and the eNodeB implement Broadcast But Verify. UEs without BBV support can still use networks that implement the Broadcast But Verify signing SIB, but they will not benefit from the additional security that the signing SIB provides. Similarly, a BBV UE connecting to legacy networks will still be vulnerable to SIB tampering and spoofing attacks. However, in this case, we have the option to strictly require the UE to only connect to BBV networks, trading availability for security in the process.

6.4 Availability Implications in BBV Networks

In wireless, spectrum is always shared with the adversary. An active adversary can impact the availability of the network by transmitting on the same frequency as the eNodeB to add, modify, or jam entire wireless frames or a portion within them. While it may seem like Broadcast But Verify increases the risk for denial of service attacks as an adversary could corrupt SIBs to prevent Broadcast But Verify UEs from connecting, an adversary can already mount this

same attack in currently deployed networks by corrupting SIBs 1-2. Therefore, there is no effective increase in attack surface in BBV networks versus traditional LTE networks.

An edge case of particular concern is availability of the phone network for emergency calls. Emergency attaches are a last resort procedure to establish connectivity to emergency services when a traditional attach is not possible. This is an opt-in procedure as a subscriber must dial emergency services to initiate an emergency attach. If the UE proceeds with an emergency attach, then it is forfeiting all security protections to prioritize availability. When it attaches to the network, it does not perform traditional authentication and key agreement and a security context is not established. To ensure that the UE will connect to an available network, Broadcast But Verify will be disabled completely for the duration of the emergency connection.

Another edge case of concern is the broadcast of time-sensitive wireless emergency alerts. Broadcast But Verify introduces a viable way to integrity-protect the SIBs that carry these messages. However, it is important to highlight that such notifications and the protocols transporting them were intentionally designed to prioritize availability above all else. BBV UEs will need to decide between displaying a potentially invalid alert or suppressing the alert based on the BBV security policy.

6.5 Lawful Interception

Despite being a controversial aspect of cell-site simulators, they are commonly used by law enforcement agencies for lawful and approved applications, such as locating criminals or abducted children. Historically, cell-site simulators were used to provide access to metadata such as real-time location pings and IMSI catching that traditional CALEA taps within the core network could not provide. Today, cell-site simulators are used by law enforcement agencies with no technical means to ensure accountability.

Our system will prevent cell-site simulators from being used without cooperation of the mobile network provider. Unlawful operation of cell-site simulators will not be possible as adversaries will not have access to valid keys to sign SIBs for the target cell. Lawful use of cell-site simulators will require MNO cooperation, creating a capability for independent oversight.

6.6 5G and Future Generations

Although our work primarily targets fourth generation LTE cellular networks, the same techniques can be applied to fifth generation and later networks. Currently, 5G cellular networks transmit equivalent SIBs also without authentication. Because we successfully add SIB authentication to LTE while maintaining full backwards compatibility with existing devices, it should be trivial to port Broadcast But Verify to operate in a 5G environment.

6G is fertile ground for us to re-examine SIB transmission. Secure SIBs should be the default, not the exception for this generation. Broadcast But Verify provides a roadmap for a secure SIB mandate.

7 RELATED WORK

SIBs are not authenticated by UEs before they are used which has led to several SIB attacks such as the presidential alert spoofing attack [6, 22]. As we noted in Section 6.1, prior work authenticated SIBs by attaching signatures onto existing SIBs and using certificate chains or pre-shared keys to verify them [19, 36]. Cramming signatures into the extremely limited spare room meant that several design tradeoffs had to be made, including limited protection for other SIBs, vulnerability to replay attacks, cipher suite inflexibility, and/or an expensive signature verification algorithm.

Prior attacks on the physical layer have shown that it's possible to fabricate, modify, or even jam traffic at the symbol level [12, 37]. Other work on the PHY ranged from tampering with control plane traffic to carrying out denial of service attacks [12, 14, 24].

Extensive research has been conducted on cell-site simulators that adversaries use to intercept, modify, fabricate, or drop phone calls, text messages, or data services. IMSI catchers are a class of cell-site simulators that trick UEs into divulging the IMSI [8, 9, 26, 27, 32]. Cell-site simulators often employ bidding down attacks to force UEs to connect over 2G which uses insecure authentication [19, 30]. Prior work has examined whether cell-site simulators can be fingerprinted by detecting unusual protocol requests, such as insecure cipher suite requests [9, 27].

Cellular protocols have also been studied extensively to identify flaws that enable attackers to impact the security, privacy, availability, and/or trustworthiness of cellular and telephony networks [33, 35]. Research aimed at verifying protocol correctness has uncovered numerous potential vulnerabilities in several procedures. [17, 18, 21, 30, 31, 34]. Several tools were developed to examine the LTE and 5G network protocols for vulnerabilities [7, 17, 18]. Some research studies have also examined the impact of misconfigured security and privacy protections in commercial networks [8].

8 CONCLUSION

Although modern cellular networks contain numerous security features, current cellular network standards do not feature integrity protection or authentication for SIB messages, thereby leaving UEs vulnerable to SIB tampering and spoofing. With the creation of Broadcast But Verify, we introduce a new security mechanism that permits UEs to verify SIBs before attempting to connect to the network while remaining backwards compatible with existing UEs. Broadcast But Verify eliminates several major classes of SIB tampering and spoofing attacks. It also eliminates virtually all fake base station attacks as adversaries cannot fabricate, replay, modify, or drop a SIB without detection, nor can they forge a valid signing SIB. While this does not completely solve the problem of pre-authentication attacks, it is an important step forward to securing future cellular generations. The time has come to fix insecure cellular system information broadcasts for good.

ACKNOWLEDGMENTS

We thank our anonymous shepherd and reviewers for their support of the paper. This material is based upon work supported by the National Science Foundation under Award No. CNS-2142930.

REFERENCES

[1] 2020. Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools. https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

[2] 3rd Generation Partnership Project (3GPP). 2022. 5G; NR; Radio Resource Control (RRC); Protocol specification (Release 17). *3GPP TS 38.331, V17.0.0* (May 2022).

[3] 3rd Generation Partnership Project (3GPP). 2022. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 17). *3GPP TS 36.300, V17.0.0* (May 2022).

[4] 3rd Generation Partnership Project (3GPP). 2023. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 17). *3GPP TS 36.331, V17.5.0* (July 2023).

[5] 3rd Generation Partnership Project (3GPP). 2024. Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (Release 17). *3GPP TS 33.310, V17.8.0* (Jan. 2024).

[6] Evangelos Bitsikas and Christina Pöpper. 2022. You have been warned: Abusing 5G's Warning and Emergency Systems. In *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC '22)*. Association for Computing Machinery, New York, NY, USA, 561–575. https://doi.org/10.1145/3564625.3568000

[7] Yi Chen, Yepeng Yao, XiaoFeng Wang, Dandan Xu, Chang Yue, Xiaozhong Liu, Kai Chen, Haixu Tang, and Baoxu Liu. 2021. Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1197–1214. https://doi.org/10.1109/SP40001.2021.00104

[8] Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE security disabled: misconfiguration in commercial networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Miami Florida, 261–266. https://doi.org/10.1145/3317549.3324927

[9] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14*. ACM Press, New Orleans, Louisiana, 246–255. https://doi.org/10.1145/2664243.2664272

[10] Kieran Devine. 2023. Ukraine war: Mobile networks being weaponised to target troops on both sides of conflict. https://news.sky.com/story/ukraine-war-mobile-networks-being-weaponised-to-target-troops-on-both-sides-of-conflict-12577595

[11] D. Dolev and A. Yao. 1983. On the security of public key protocols. *IEEE Transactions on Information Theory* 29, 2 (March 1983), 198–208. https://doi.org/10.1109/TIT.1983.1056650 Conference Name: IEEE Transactions on Information Theory.

[12] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. 2022. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking (MobiCom '22)*. Association for Computing Machinery, New York, NY, USA, 743–755. https://doi.org/10.1145/3495243.3560525 event-place: Sydney, NSW, Australia.

[13] Ettus Research. [n. d.]. Ettus Research USRP.

[14] Felix Girke, Fabian Kurtz, Nils Dorsch, and Christian Wietfeld. 2019. Towards Resilient 5G: Lessons Learned from Experimental Evaluations of LTE Uplink Jamming. In *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, Shanghai, China, 1–6. https://doi.org/10.1109/ICCW.2019.8756977

[15] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano, and Doug J. Leith. 2016. srsLTE: an open-source platform for LTE evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*. ACM, New York City New York, 25–32. https://doi.org/10.1145/2980159.2980163

[16] Jeff Hodges, Collin Jackson, and Adam Barth. 2012. HTTP Strict Transport Security (HSTS). RFC 6797. https://doi.org/10.17487/RFC6797

[17] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2018.23313

[18] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 2019. 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, London United Kingdom, 669–684. https://doi.org/10.1145/3319535.3354263

[19] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. Insecure connection bootstrapping in cellular networks: the root of all evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Miami Florida, 1–11. https://doi.org/10.1145/3317549.3323402

[20] Roger Piqueras Jover. 2016. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *arXiv:1607.05171 [cs]* (July 2016). http://arxiv.org/abs/1607.05171 arXiv: 1607.05171.

[21] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1153–1168. https://doi.org/10.1109/SP.2019.00038

[22] Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. 2019. This is Your President Speaking: Spoofing Alerts in 4G LTE Networks. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, Seoul Republic of Korea, 404–416. https://doi.org/10.1145/3307334.3326082

[23] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. 2017. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2017.23098

[24] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed. 2016. LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine* 54, 4 (April 2016), 54–61. https://doi.org/10.1109/MCOM.2016.7452266

[25] Alessandro Lotto, Vaibhav Singh, Bhaskar Ramasubramanian, Alessandro Brighente, Mauro Conti, and Radha Poovendran. 2023. BARON: Base-Station Authentication Through Core Network for Mobility Management in 5G Networks. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Guildford United Kingdom, 133–144. https://doi.org/10.1145/3558482.3590187

[26] Stig F. Mjølsnes and Ruxandra F. Olimid. 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. In *Computer Network Security*, Jacek Rak, John Bay, Igor Kotenko, Leonard Popyack, Victor Skormin, and Krzysztof Szczypiorski (Eds.). Springer International Publishing, Cham, 235–246.

[27] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, Andrew Martin, and Jean-Pierre Seifert. 2017. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. USENIX Association, Vancouver, BC. https://www.usenix.org/conference/woot17/workshop-program/presentation/park

[28] Eric Priezkalns. 2023. Paris IMSI-Catcher Mistaken for Bomb Was Actually Used for Health Insurance SMS Phishing Scam.

[29] Eric Priezkalns. 2023. Thousands Tricked Into Revealing Banking Details by Smishing IMSI-Catcher Driven around Norway. https://commsrisk.com/thousands-tricked-into-revealing-banking-details-by-smishing-imsi-catcher-driven-around-norway/

[30] Muhammad Taqi Raza, Fatima Muhammad Anwar, and Songwu Lu. 2018. Exposing LTE Security Weaknesses at Protocol Inter-layer, and Inter-radio Interactions. In *Security and Privacy in Communication Networks*, Xiaodong Lin, Ali Ghorbani, Kui Ren, Sencun Zhu, and Aiqing Zhang (Eds.). Vol. 238. Springer International Publishing, Cham, 312–338. https://doi.org/10.1007/978-3-319-78813-5_16 Series Title: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.

[31] Muhammad Taqi Raza, Yunqi Guo, Songwu Lu, and Fatima Muhammad Anwar. 2021. On Key Reinstallation Attacks over 4G LTE Control-Plane: Feasibility and Negative Impact. In *Annual Computer Security Applications Conference*. ACM, Virtual Event USA, 877–886. https://doi.org/10.1145/3485832.3485833

[32] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Pöpper. 2018. On Security Research Towards Future Mobile Network Generations. *IEEE Communications Surveys & Tutorials* 20, 3 (2018), 2518–2542. https://doi.org/10.1109/COMST.2018.2820728

[33] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Popper. 2019. Breaking LTE on Layer Two. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1121–1136. https://doi.org/10.1109/SP.2019.00006

[34] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 73–88. https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht

[35] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *Proceedings 2016 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2016.23236

[36] Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, Attila Yavuz, and Elisa Bertino. 2021. Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (ASIA CCS '21)*. Association for Computing Machinery, New York, NY, USA, 501–515. https://doi.org/10.1145/3433210.3453082

[37] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, S. Kim, and Yongdae Kim. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 55–72. https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[38] Kim Zetter. 2020. How Cops Can Secretly Track Your Phone. https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

A BBV CELL SELECTION AND HANDOVER PROCEDURES

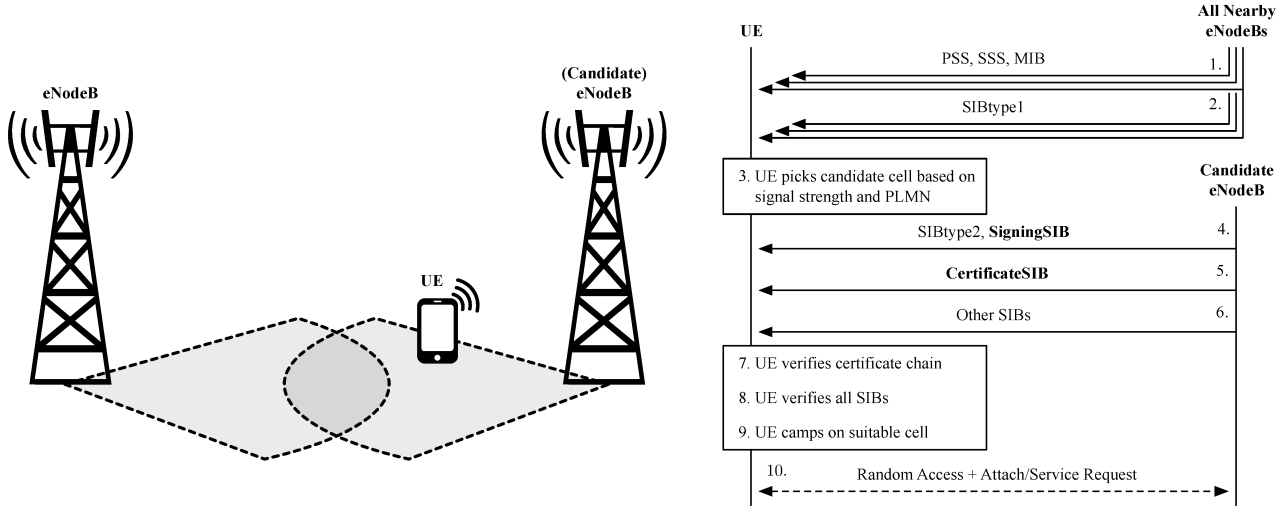

Figure 5: BBV UEs verify all SIBs before camping on the cell.

BBV UEs begin cell selection by searching for and synchronizing with all nearby eNodeBs as shown in step 1 in Figure 5. The UE then obtains SIBtype1 in step 2 and picks a candidate cell in step 3. After picking the candidate cell, the UE will then receive SIBtype2 and the signing SIB from this cell in step 4. If the UE does not have all certificates required to validate the signing SIB, it will receive the certificate SIB in step 5. The UE will then receive all other SIBs in step 6. After receiving all SIBs, the UE will verify the certificate chain in step 7 and verify all SIBs, including the signing SIB itself, in step 8. Assuming the signing SIB validates and the current cell meets all other suitability criteria, the UE will camp on the cell in step 9 and initiate the random access procedure to connect in step 10.

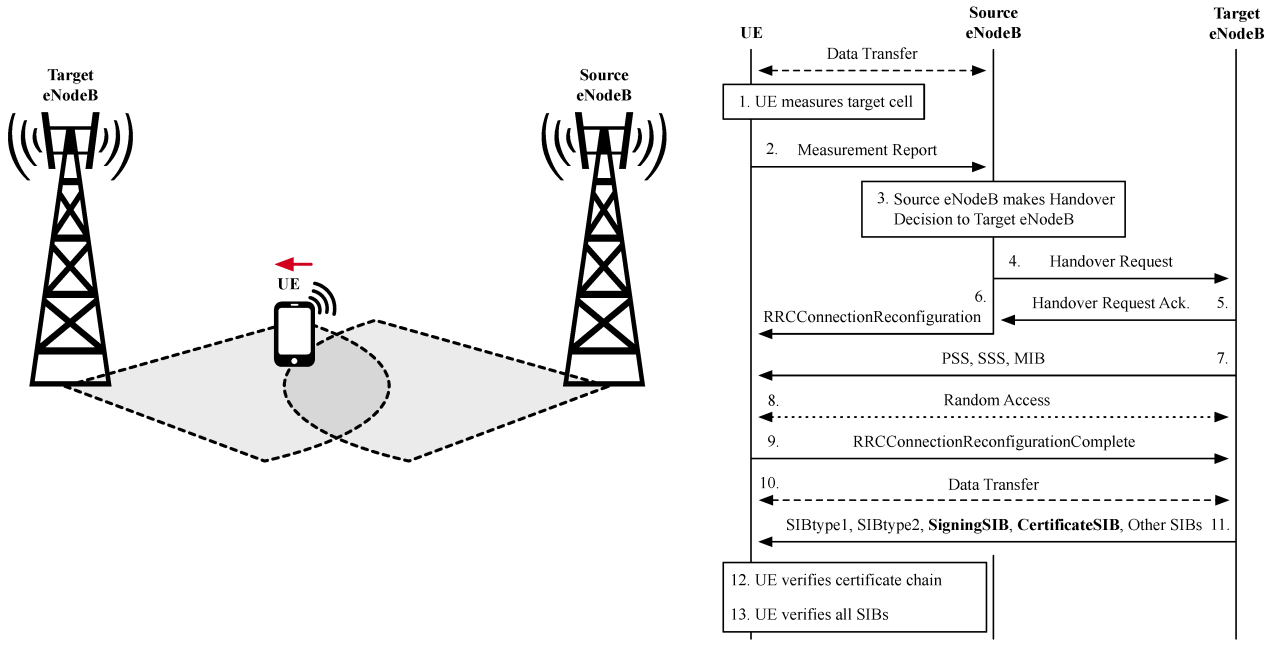

Figure 6: BBV UEs wait to validate SIBs until after the handover has completed.

For BBV UEs, a "UE assisted" handover begins with the UE measuring the surrounding radio environment as shown in step 1 in Figure 6. The UE then sends a measurement report back to the eNodeB in step 2. The source eNodeB makes a handover decision to send the UE over to a new target cell in step 3. If the network was performing a "blind" handover, the process would start here. The source eNodeB then sends a Handover Request to the target eNodeB in step 4. If the target eNodeB can accept the handover, it responds with a Handover Request

Acknowledgement in step 5. Upon receiving this acknowledgment, the source eNodeB sends an `RRCConnectionReconfiguration` message to the UE to instruct it to move to the target eNodeB in step 6. At the same time, the source eNodeB begins forwarding traffic for the UE to the target eNodeB. The UE then synchronizes with the target eNodeB in step 7 and then performs the random access procedure in step 8. Upon successful completion of this procedure, the UE then sends an `RRCConnectionReconfigurationComplete` message to the target eNodeB to complete the process in step 9. At this point, the ongoing data transmission resumes and the target eNodeB issues a path switch request to the core network in step 10. In the background, the UE receives all SIBs, including the signing SIB and the certificate SIB in step 11. Upon receiving these SIBs, the UE will verify the certificate chain in step 12 and verify all SIBs, including the signing SIB itself, in step 13.

B ACRONYMS

ASN.1 Abstract Syntax Notation 1
CA Certificate Authority
CMAS Commercial Mobile Alerting System
COTS Common Off The Shelf
CRL Certificate Revocation List
DCI Downlink Control Information
eNodeB Evolved Node B
EPC Evolved Packet Core
eSIM Embedded Subscriber Identity Module
HN Home Network
HSS Home Subscriber Server
IMSI International Mobile Subscriber Identity
LTE Long Term Evolution
MAC Message Authentication Code
MBMS Multimedia Broadcast Multicast Service
MIB Master Information Block
MME Mobility Management Entity
MNO Mobile Network Operator
MVNO Mobile Virtual Network Operator
NR New Radio
OCSP Online Certificate Status Protocol
PKI Public Key Infrastructure
PLMN Public Land Mobile Network
PSTN Public Switched Telephone Network
RLF Radio Link Failure
SDR Software Defined Radio
SI System Information
SIB System Information Block
SIM Subscriber Identity Module
SMS Short Message Service
SN Serving Network
UE User Equipment
USRP Universal Software Radio Peripheral
WEA Wireless Emergency Alert
3GPP 3rd Generation Partnership Project