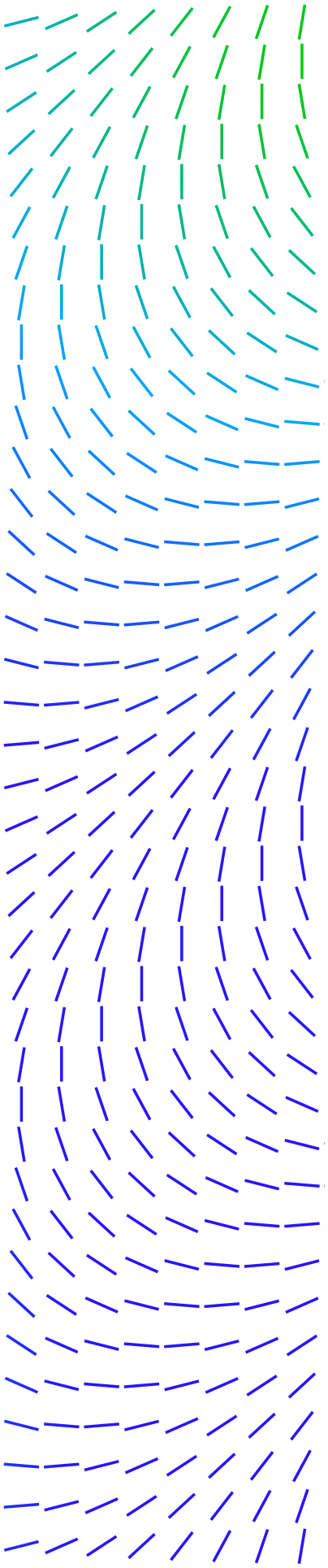

Cross-Generational Security Of Mobile Telephony

D. Kevin McGrath
Threat Labs, Trellix
d.kevin.mcgrath@trellix.com

Trellix

Abstract— With the recent roll-outs of 5G networks and the rise of phones supporting the standard, it's critical to examine the technical underpinnings of 5G system security. The fifth generation of 3GPP (3rd Generation Partnership Project) mobile telephony, the lack of understanding, outright hostility, and general confusion surrounding this roll-out is unmatched in the history of mobility. We aim to alleviate much of the confusion and hostility by providing an overarching description and security document.

Further, there has been minimal recent discussion of 5G security in the literature. With the recent joint publication from the NSA, the Office of the DNI, and CISA[16], this may change. That work was solely a high-level overview of what concerns exist amongst three-letter agencies regarding 5G. This paper also aims to provide a starting point for broader industry research interest of 5G and related technologies.

I. BENEFITS OF 5G FROM A SECURITY PERSPECTIVE

While there are many consumer benefits to 5G, this work focuses on the security benefits 5G brings to the table. These include, but are not limited to, the following:

- Flexibility
- Firmware push security enhancement
- Closure of flaws in earlier protocols

We explore each of these benefits in detail below.

A. Flexibility

Flexibility is one of the most significant aspects of 5G. One of the primary technical underpinnings of 5G is known as the 5G New Radio (NR). Unlike in previous generations, which made use of a fixed-function radio block, 5G NRs make use of software-defined radio (SDR). While we address the technical implications and definitions of SDR in §IV.B, SDR brings significant flexibility to any radio system via its separation of the analog and physical domains of RF communication.

Allowing encoding, modulation, and data processing to happen on a general-purpose CPU[i] (with some time-critical aspects handled via FPGA[ii]), software-defined radios differ significantly from traditional radio blocks, where custom ASICs did all processing. Using custom ASICs meant that previous-generation radios operated with the exact modulation, encoding, and encryption schemes for their entire life-cycle. If a flaw arose, the sole recourse for a given piece of hardware was replacement. 5G NRs solve this problem by providing all the digital aspects of radio transmission (modulation, encoding, encryption, and so forth) via software. Even time-critical operations on the FPGA can be re-written with a firmware update.

The flexibility of 5G NRs provides the option to patch a discovered flaw quickly, without replacing expensive telecoms equipment. This aspect of 5G cannot be overstated. As 5G evolves, be it in response to consumer needs, security needs, or business needs, the entire network can be reconfigured – at the physical layer – to meet these evolutionary requirements.

Of equal importance, this flexibility also provides a potential lifetime enhancement for a given piece of hardware. Historically, as protocols evolved and moved from generation to generation, entirely new equipment was necessary – at both the consumer and telecoms levels. Leveraging new standards required retiring functional hardware, spending money, and filling landfills. With software-defined radios at the heart of 5G, leveraging advances is no more difficult than rebooting the device after installing a software patch. As smartphones get ever more capable and battery technology continues to increase, expected device lifetime will only increase (from approximately 31 months among consumers in 2014 to 38 months in 2020, projected to be over 45 months in 2024 [1]), necessitating this capability – the longer devices last, the more likely they will continue to be used across a service update. This longevity is good for the consumer, the telecoms, and the environment.

B. Enhancing Security with a Firmware Update

While enhancing security with a firmware update is clearly coupled with the flexibility benefit, it is distinct when discussing the security of a standard. Whether user equipment (handsets, IoT devices, called UE in standards) or core infrastructure, should a flaw be discovered in the protocol, new hardware is not required to implement the fix. This capability is directly related to the 5G NR – its software-defined nature allows quick and easy patching.

Flashing an FPGA requires very little hardware, especially in systems designed for field programmability. Encoding schemes can be easily changed. As the security landscape requires, carriers and OEMs can update encryption algorithms and keys in real-time. Whether the OEMs or the carriers would provide such updates is left as an exercise for them to figure out, but the likelihood is high they would come from one or the other. Whether the US requires legislation to mandate this for the benefit of consumers is unclear at this time.

Regardless of mandate or availability from carriers or OEMs, there are no technical limitations to user equipment firmware updates to enhance communications security at the protocol level. So long as user equipment ships with a 5G NR certified modem, it should[1] be capable of such updates.

C. Closing off flaws in earlier protocols

Every generation of mobile protocols has attempted to close any known flaws in previous generations. Every system has flaws, whether weak encryption, government-mandated backdoors, or purely an implementation detail leveraged by a bad actor (Stingray devices come to mind). 5G is no exception to this trend. While many details remain unclear, devices such as the aforementioned Stingray would likely not work as transparently as they do currently.

As recently as 2019, South Korean researchers discovered 36 new bugs in the LTE control plan.[2] They implemented a semi-automated fuzzing tool dubbed LTEFuzz and used only client side logging to discover the vulnerabilities. These vulnerabilities existed in both the standard itself and in the carrier implementations. While 2018 research indicated some still exist in 5G – such as within the AKA (authentication and key agreement) protocol [3], within the intervening four years the 3GPP has updated the protocol to (theoretically) close off this flaw prior to carrier deployment.

Of equal (and in an ongoing sense, greater) importance, 5G brings the capability of closing off flaws without waiting for a new standard, meaning the window of exploitation can be (but may not be, depending on many factors) curtailed. It does this by moving to an entirely software-defined infrastructure.

II. HISTORICAL BACKGROUND INFORMATION

While the name makes it seem obvious, 5G is the fifth generation of GSM mobile networking. While there are marketing names for each generation (which is how this section shall be organized), the names are primarily that: marketing. In any real sense, 5G is truly the fourth (or even the third, depending on how you choose to count) significant technological progression.

More detail appears below, but technologically, the main progressions have been

- from analog fixed-function to digital fixed-function (radio and network): 1G → 2G/3G.
- from digital fixed-function networking to digital software-defined networking: 3G → 4G
- from fixed-function radio and software-defined networking to fully software-defined (radio and network): 4G → 5G.

This last step is simply an extension of what came before rather than a radical shift in approach. Technology was able to catch up in the radio domain to where the providers already were in the networking domain.

[1] While the standard requires it, standards are guidelines and certification requirements. That does not mean all OEMs will follow said requirements. While the major players likely will (Google, Apple, Samsung, etc.), but the majority of devices are manufactured by smaller players.

A. Generation Progression

0) 0G – Radio Telephony

While not considered part of the history of mobile telephony, it is worth highlighting that radio-to-PSTN (public switched telephone network) links have existed since (no later than) 1920, with the first "carphone" demonstrated in 1920! [4] Maritime vessels frequently used such links to connect ship-to-shore radios to the PSTN.

While radiotelephony is quite distinct from mobile phone networks, it provided the foundation for mobile networks as we understand them today.

1) 1G – Mixed analog/digital networks

In the late 1970s and 1980s, first-generation networks used analog encoding of the voice channel. What this means, in practice, is that while the towers connected to the broader world with digital signaling, an analog carrier frequency modulated the connection to the tower (typically 150MHz and up).

This is important to note for multiple reasons:

- While the inter-tower signal was susceptible to the "digital cliff" phenomenon – where a digital signal is either fully detectable or not at all – the analog signal from the phone to the tower was subject to all the pitfalls of analog radio communications: lack of quality, voice encoding leading to artifacts, gradual connection decay (tunnel effect), etc.
- Encoding analog data into a digital transmission was not unique to 1G networks – hams had been using packet radio to send information since the early 1970s, with RTTY going back to World War 2! Using a broad network of towers was also not a new idea, as radio repeaters had been in use since (at least) 1976.
- The breakthrough, in this case, was the nature of the signal: it was full-duplex rather than half-duplex. In practice, this allows a cellular phone to simultaneously transmit and receive, unlike typical radio hardware, which could be used as both a transmitter and a receiver, but not simultaneously.

While it wasn't unknown to have a proper handheld mobile phone (such as the Motorola Dynatac), car installation was also typical during this time.

There were no data services in use on 1G networks. These needed a digital connection between the handset and the tower, which necessitated migrating to 2G (and later) networks in the early 1990s.

Technologies

- GPRS – general packet radio service
- EDGE – Enhanced data rates for GSM evolved
- UMTS – Universal Mobile Telecommunications System
- W-CDMA – Wideband code division multiplex access
- HSPA – High-speed packet access
- LTE – Long Term Evolution
- HAM – Amateur Radio
- RTTY – Radio Teletype

2) 2G – GSM and other digital networks

In 1991, Europe launched the first 2G network. This network distinguished itself from the (retroactively renamed) 1G network primarily through the use of digital connections to the cell phone towers.

2G had multiple variants in use throughout the world, including GSM (TDMA[iii]), D-AMPS[iv] (TMDA), and cdmaNOW (CDMA[v]). D-AMPS had a significant advantage in that it made use of dual-mode handsets – they would use the digital channels if available but would fall back on the analog network (which used AMPS).

Initially, 2G networks did not have data capabilities. Often called 2.5G, GPRS brought data modes to mobile telephony around the turn of the century. Akin to packet radio in amateur radio, it provided IP data communication from the mobile device to the broader internet. While limited to 40 kbps, connecting millions of mobile terminals enabled significant technological advances – remote monitoring, smart meters, etc.

EDGE , also called 2.75G or even 2.9G (naming clearly not the strength of the GSMA[viii]), brought faster data rates to 2G networks – up to roughly quadruple

that of GPRS in a typical situation. Implemented as a super-set of GPRS, EDGE capable devices would work on GPRS-only networks. The ITU (International Telecommunication Union) standard for a 3G network initially required a minimum bandwidth of 144 kbps for mobile use, meaning that EDGE, at a theoretical peak of 236 kpbs, meets this requirement. Labeling EDGE a 2G network is partially a marketing issue, while also a matter of rapidly advancing technology near the beginning of the 21st century blurring the lines between 2G and 3G networks.

3) 3G – Just a faster 2G?

When Cingular, now AT&T, deployed the first spec-compliant 3G network in the United States, there was little distinction in real-world speeds between their EDGE network and their 3G network based on the UMTS standard. However, this situation was short-lived, as the limited channel bandwidth of EDGE dead-ended the technology while UMTS continued to push forward on data rates.

3G was the time period that saw the most considerable proliferation of competing standards. CMDA-2000 was widely deployed in the US by multiple carriers. UMTS/W-CMDA was an evolution of the GSM standard used by much of the rest of the world. Further confounding the issue, OEMs produced phones which offered 2G and 3G radios, with a myriad of air interfaces and frequency bands supported.

While not explicitly a security issue in the traditional sense, this time period also saw the rise of "unlocking" services to allow users to port phones between carriers. This unlocking was a circumvention of "security features" as defined by the Digital Millennium Copyright Act (DMCA) and saw a significant increase in the prevalence of "hacked" phones – well before the smartphone era.

UMTS also defined HSPA and its variants: an asymmetric packet-switched data interface. Offering speeds exceeding typical US home broadband deployments (128 Mbps down, 22 Mbps up), HSPA gave rise to the idea of "fixed-mobile" deployments, where a given location could receive IP services over a fully wireless link, rather than fixed cabling.

3G was the last standard to use disparate technology for voice and data – that transition is one of the most significant of 4G.

4) 4G – The Move to IP Everything

Moving the entire mobile experience (voice and data) to IP made sense: data is data, whether it's encoded voice, video calls (though these first showed up in the 1939 Worlds Fair), or the transfer of any media. Quality of service (QoS) and data management become more straightforward, as network operators can simplify algorithms to consider only a single type or class of data.

4G introduced *software-defined networking* (SDN) in response to the need for a more defined network approach. SDN provides a *logical overlay network* on the underlying physical network. In other words, it offers a *control plane* that operates independently of the *data plane*.

Having a separate control plane allows routing decisions based not on the whims of BGP on the open internet but rather other metrics. These metrics could be some form of "network distance" or based on significantly more data points than exist in standard IP routing.

As in everything, the move to SDN saw some tradeoffs. Max packet throughput at the network layer lessened, though average throughput could increase (various factors involved). SDN introduces additional complexity and hardware to the radio tower. Moving the control plane functions (routing decisions in this situation) to a centralized system offsets the complexity of an additional networking layer by:

- decreasing the time to propagate changes over a geographically diverse network,
- reducing the likelihood of misconfiguration in a subset of network devices,
- allowing a set of network devices to operate as

if they were virtual functions (network as code), and

- allows highly granular network monitoring.

Hardware as code is a concept often synonymous with SDN. Interested readers may find more discussion of SDN in §IV.

5) 5G: Software-defined Telephony

4G was titled Long Term Evolution, with the intent to provide the basis for all future standards. In fact, within the overarching specification known as 4G, there was marked improvement from the technology's debut to the present.

Unfortunately, at least for the namers of the 4G standard, many updates would break backward compatibility. These include the software-defined nature of 5G radios, access and authorization modes, and even the packet layer itself. 5G introduced many of these necessary, compatibility-breaking changes over 4G.

The *Evolved Packet System* (EPS) introduction laid the groundwork for a higher IP load – more throughput was available. Coupled with technologies such as *mmWave*, densely populated urban areas and venues such as sports arenas could overcome past deficiencies, which often manifested as limited capacity, poor or slow network speeds, and frequent dropped calls.

As likely apparent by the section title, 5G also saw the introduction of another software-defined technology. The 5G NR (5G new radio) is software-defined at the tower and user equipment (UE) levels. §IV.B. contains many of the technical details, but moving to SDR-based radios provides the necessary flexibility to see 5G evolve in ways that curtail the potential impact of security or performance flaws. Should the key-exchange protocol for attestation be flawed in a way that allows an attacker to perform a man-in-the-middle attack, OEMs or carriers can provide updates to the protocol itself without either living with the flaw or requiring new hardware on both ends of the conversation. §IV covers the technical details of *infrastructure-as-code*.

In addition to providing rapid update capabilities, 5G allows telecoms to move away from fixed-function hardware and bespoke radio solutions and towards commercial, off-the-shelf (COTS) hardware solutions for both network management and radio interfacing. While still using some "exotic" hardware (at least relative to consumer-level equipment), custom hardware solutions are no longer required. Instead, a mobile telephony stack consists of rack-mounted servers and rack-mounted SDR hardware connected to antenna arrays. While it is undoubtedly still a truth that a radio setup is only as good as the quality of the antennas to which it is connected, antenna usage is a well-understood problem-space.

COTS hardware provides significant savings simply due to volume. Perhaps more importantly, it de-incentivizes the "security through obscurity" mentality while incentivizing a proper security life-cycle across the entire stack. There will be growing pains, as in every move to a new approach. Ultimately, this is likely to result in a much greater security posture, as well as a more mature security life-cycle.

One of the more novel aspects of the 5G standard is that it calls out (at least) one specific use case: vehicle-to-anything (V2x) communication. This includes

- vehicle-to-vehicle (V2V): a mesh network which exists between vehicles to enable beyond-line-of-site decision-making capabilities possible – for both vehicle and driver;
- vehicle-to-infrastructure (V2I): communications between vehicles and traffic lights, speed limit postings, and various other pieces of infrastructure which make up the road network;
- vehicle-to-network (V2N): the vehicle itself acts as a UE node, connected to cellular towers via a 5G NR, providing vehicle tracking and other advanced IoT like services;
- vehicle-to-pedestrian (V2P): provide opportunistic guidance to both pedestrians and drivers in situations where only incomplete visual information is available (phone, wearable device, etc.).

See §III.A.1. for more detail on V2x.

LTE frequencies range from approximately 600 MHz to approximately 3,800MHz. 5G frequencies go much lower - down to 410MHz - and much higher - up to and over 7GHz in FR1, with 24-52GHz in FR2. While FR1 allows for frequencies above 7GHz, nearly all frequencies defined for use in 5G are in the sub-6GHz range. As such, you will often hear FR1 described as sub-6GHz 5G, with FR2 known as the mmWave 5G.

It should be noted that in both cases, the standard divides the allocated frequencies into channels. Channel width ranges in size from 5MHz to 40MHz in LTE and 5MHz to 100MHz in 5G. In most cases, uplink and downlink are separate frequency ranges, though some channels define one large block rather than two smaller blocks.

In context, this means increased range from cell towers, significantly enhancing coverage areas due to lower frequencies, which have more penetration through buildings, the earth, etc. This also considerably increases available bandwidth, even without entering the mmWave bands (FR2). This increase is the result of several aspects. The channels are simply wider in 5G than in previous specifications. Wider channels with increased penetration will see more available bandwidth in a given location with 5G than with earlier specifications. See Tables 1-3 below for frequency details.

Table 1 defines the main frequency ranges: FR1 and FR2. Table 2 shows the currently reserved bands (also known as channels). Notice the gaps in numbering - these missing bands are defined but are not currently in use. mmWave communications use the FR2 bands seen in Table 3.

These frequencies have a very short range and lack of penetration but have significant bandwidth. Take band *n257*: uplink and downlink both have 300MHz of bandwidth.

5G added an approximate 190MHz of usable frequency bands at the lower end of the spectrum. While there are some carve-outs for uses such as amateur radio, this additional spectrum allows for longer-range links in rural environments and increased bandwidth in urban settings (due to the increased building penetration capabilities).

Frequency range designation	Frequency Range (MHz)
FR1	410 - 7,125
FR2	24,250 - 52,600

Table 1: Frequency Ranges, FR1 & FR2 for 5G NR

Frequency Band	Uplink Band (MHz)	Downlink Band (MHz)	Duplex Mode
n1	1,920 - 1,980		FDD
n2	1,850 - 1,910		FDD
n3	1,710 - 1,785		FDD
n5	824 - 849		FDD
n7	2,500 - 2,570		FDD
n8	880 - 915		FDD
n12	699 - 716		FDD
n20	832 - 862		FDD
n25	1,850 - 1,915		FDD
n28	703 - 748		FDD
n34	2,010 - 2,025		TDD
n38	2,570 - 2,620		TDD
n39	1,880 - 1,920		TDD
n40	2,300 - 2,400		TDD
n41	2,496 - 2,690		TDD
n50	1,432 - 1,517		TDD
n51	1,427 - 1,432		TDD
n66	1,710 - 1,780		TDD
n70	1,695 - 1,710		TDD
n71	663 - 698		TDD
n74	1,427 - 1,470		TDD
n75	--	1,432 - 1,517	SDL[a]
n76	--	1,427 - 1,432	SDL
n77	3,300 - 4,200		TDD
n78	3,300 - 3,800		TDD
n79	4,400 - 5,000		TDD
n80	1,710 - 1,785	--	SUL[a]
n81	880 - 915	--	SUL
n82	832 - 862	--	SUL
n83	703 - 748	--	SUL
n84	1,920 - 1,980	--	SUL
n86	1,710 - 1,780	--	SUL

Table 2: 5G FR1 Frequency Bands

a: SDL bands are supplementary downlinks; SUL bands are supplementary uplinks

Frequency Band	Uplink Band (MHz)	Downlink Band (MHz)	Duplex Mode
n257	26,500 - 29,500	26,500 - 29,500	TDD
n258	24,250 - 27,500	24,250 - 27,500	TDD
n260	37,000 - 40,000	37,000 - 40,000	TDD
n261	27,500 - 28,350	27,500 - 28,350	TDD

Table 3: 5G FR2 Frequency Bands[b]

b: FR2 bands are for short-range, high bandwidth communication

III. MODES of OPERATION OF 5G

In order to ease the initial deployment of 5G, the standard allows the use of 4G/LTE networks as backhaul – meaning the transit of data from the tower to an internet gateway. Known as *non-standalone mode* (NSAM), this mode of operation leaves a 5G network vulnerable to what is referred to as a downgrade attack, where the 5G signal is rendered unusable (through whatever means), causing user equipment to connect to the existing 4G/LTE signal.

While NSAM does require a full 5G stack at the base station/tower, it does not require the use of 5G end-to-end. Standard 15 of 3GPP defines the interoperability of 5G and previous networking technology, dealing with topics such as downgrades, security feature transference, and other technical details.

The other mode of operation is known as *Standalone mode* (SAM) and is a complete, end-to-end 5G network, from the user equipment to the public data network.

Distinct from both SAM and NSAM, 5G makes available the option of private networks in a much more accessible fashion than private LTE networks. Private networks are expected to be an area of significant growth within industry – with a commensurate increase in interest among attackers. The more valuable the sector in question, the more likely well-funded adversaries will target such

networks. Understanding the security landscape and threat model of 5G will be crucial to securing these critical networks within high-value industrial targets.

A. 5G Use Cases

5G enables a variety of use cases:

- V2x providing safer roads
- Business routing solutions
- IoT/IIoT access enabling remote deployment
- Rapid evolution to enable higher availability and reliability
- Higher throughput and longer range for mobile devices
- Richer metadata for augmented reality (AR) applications.

1) V2x

Vehicle-to-vehicle networking was initially envisioned as an ad-hoc network utilizing 802.11p networking technology to provide a mesh network of all vehicles on the road [5]. Vehicles could relay information about road conditions, accidents, intent to change lanes (based on the ability of the driver to use a turn signal), locations relative to other vehicles, and myriad other safety data. This data could additionally benefit autonomous vehicles, giving them access to information beyond their line-of-sensing to provide advanced decision-making capabilities.

Unfortunately, to truly leverage this technology required ubiquitous deployment. Critical mass was simply never reached. One potential cause for this was the mesh nature of the network. Densely trafficked areas would not see an issue with this, but sparsely traveled highways, rural routes, and other similar types of roads would simply see no benefit due to a lack of range on the V2V communication signals.

V2I aimed to provide a potential fix for this situation by adding additional nodes to the mesh network within fixed infrastructure – road signs, traffic lights, etc. While it could offer benefits, the lack of ubiquity and range hampered this effort also.

V2P aims to include pedestrians as a mode of transportation equal to a vehicle (within the confines of the mesh network). A pedestrian would act as a first-class node within the network through some form of computing platform (AR, phone, wearable), receiving and sending information to vehicles. This would increase safety, decrease accidents, and improve non-motor-vehicle traffic safety.

V2N is not a new concept. Many vehicles had 3G and 4G radio links, allowing them access to the mobile network. Lack of bandwidth often relegated these links to solely entertainment purposes, with a small quantity of telematics use, particularly outside dense urban areas. By moving to 5G, bandwidth is no longer lacking.

By providing much longer distance links, 5G overcomes one of the critical flaws in a mesh protocol – namely, a lack of over-the-horizon visibility. It does this not by overhauling the mesh protocols defined in 802.11p but rather by moving V2x technologies to be V2N – V2V then becomes a broadcast technology on the local 5G network. Similarly, with V2P and V2I: V2x messages are broadcast messages on the local towers rather than being point-to-point.

As a specific example, consider an out-of-service bridge. This bridge serves as access to a rural community, with a reasonably long access road leading to it (on the order of several km) and no turn-offs along the length of the access road. With traditional V2I technology, the range is limited to roughly 1km (based on 802.11p frequencies), meaning residents would have to drive the majority of the access road before discovering they need to turn around. The lack of turnouts could result in a dangerous situation as vehicles turn around within the confines of the road.

While this is a contrived situation, the implications are clear. Longer range communications due to lower frequencies within 5G FR1 can significantly enhance safety, incentivize OEMs to include V2x capabilities, and potentially save lives. Transmitting all V2x information over the 5G network simplifies the radio

engineering required in a vehicle. No longer needing multiple radios will allow deployment of features such as V2x a purely software concern, rather than hardware.

2) Business Routing Solutions

Business fleets will often use tracking and routing automation systems. Such systems utilize GPS, mobile networks, and central route management tools to track, route, and optimize fleet operations. Last-mile delivery companies will be the specific case study for this section.

Last-mile delivery companies handle logistics for large retailers, typically multiple such retailers, from a central hub to delivery endpoints. In this way, deliveries can be optimized in terms of miles traveled, gas used, delivery throughput, etc. These optimizations require knowledge of the current location of the delivery vehicles.

5G would allow for continuous monitoring of not only location but also driver state, driving patterns, etc. Bandwidth or geography would no longer limit the data collected. 5G's lower frequencies and higher bandwidth would move the limiting factor from network access and availability to a question of "what metrics would increase delivery throughput and minimize costs?"

3) Remote Deployment of IoT/IIoT access

Previous to 5G, many IoT and medical devices required fixed broadband. That is, they simply wouldn't have the capacity to be useful over LTE networks. An example of this is remote surgery: currently only fixed, high-capacity networks could be used to tele-operate surgical robots.

Based on available capacity within the 5G network, tele-operation of a surgical robot is theoretically possible. Bandwidth limitations in the lower range of FR1 would not be usable, as the throughput and latency would be too high. FR2 offers the necessary low latency and high throughput necessary for robotic surgery.

This use-case is a little special, in that technology is not the only limitation in this case. FDA approval would also be required in order to operate a surgical robot over 5G.

4) Rapid Evolution

One significant benefit of moving to a fully software-defined architecture within 5G is the ability to rapidly iterate the standard without requiring new hardware on both sides of the connection.

Any updates to the frequencies in use or the encryption schemes can be deployed in nearly real-time. New features can similarly be deployed rapidly without requiring new hardware.

5) Mobile Device usage improvements

While many of the benefits of 5G are seen on the carrier and device OEM side, consumers are not left out in the cold. Capacity increases and range benefits will allow consumers to have better connections in more places than ever before.

As a specific example, COVID-19 has seen a rise in so-called "digital nomads." A solid connection in their location du jour serves as a limiting factor for these workers. Many of the best places to set up for a week or longer have very limited 4G signal coverage, due primarily to the remoteness of the location. In the absence of new tower deployments, LTE will not be able to cover such areas in the future. On the other hand, 5G makes use of lower frequencies, which have a range advantage over the frequencies in LTE. Combining this range with wider channels, remote areas will have more capacity, allowing digital nomads greater range in their travels.

6) Richer AR Metadata

A perennially "next-gen" technology is wearable AR devices. AR requires significant quantities of metadata to provide relevant information overlays. This is a bi-directional technology, in that the wearable device needs to send location and poise data (orientation in multiple planes) at minimum, and

possibly image data as well. Processing on the server results in overlay information for the images to include the requested metadata.

While many see AR glasses as "creepy" and "weird", the benefits for tourism, expert tasks, and even driving are huge. The limiting factor up to now has been network capacity and display technology. While 5G doesn't solve the display side of the equation, the network capacity factor is readily addressed, especially within FR2 channels.

IV. SOFTWARE-DEFINED EVERYTHING

Software-defined networking (SDN) is a critical portion of 4G/LTE. SDN separated the control plane (routing decisions, etc.) from the data plane. Sometimes referred to as an overlay network, SDNs have significant resilience and the ability to rapidly respond to changing needs in the control plane. SDN typically takes the form of software sitting on top of the physical network, network function virtualization, and network virtualization. Lifting the control plane to a logically centralized, abstract network provides various benefits:

- Increased visibility into data flows
- Increasing traffic management capabilities
- Running on COTS systems rather than bespoke, comms grade hardware

Software-defined radios (SDR), on the other hand, are peripherals that provide an analog signaling interface to COTS systems. SDR hardware is immensely flexible, typically consisting of paired, high-quality ADC/DAC hardware, an FPGA of significant size, and some form of host interface (gigabit ethernet, USB3, PCIe). Rather than using fixed-function radio blocks, as in previous standards, 5G NR (an SDR-based radio) offers the capability of changing everything about the network's physical layer with nothing more than a firmware update.

The ability to run on COTS hardware has additional benefits. By its very nature, off-the-shelf hardware is inherently fungible. If a component suffers a failure, replacement parts are readily available. New system deployments require shortened lead time, leading to more rapid turnaround on network upgrades. Whether there would be some form of certification or required hardening is unclear, but solutions from other spaces may be adaptable in the telecom sector.

A. Why software-defined everything?

The obvious question is, "what does moving to software-defined everything give us?" In other words, why go this route? Answering this question requires some additional discussion on the benefits, as well as the downsides, of moving to software-defined infrastructure. Determining a correct answer also involves an investigation of the stated use-cases of 5G.

1) Benefits

The benefits of software-defined infrastructure can take many forms. One of the most tangible is the idea of infrastructure-as-code – which is nearly synonymous with "software-defined everything." Moving away from a deployment consisting of custom hardware (with trained technicians necessary for installation and maintenance) and towards the idea that the infrastructure itself – radio protocols, networking, modulation, encoding (everything required for a wireless communication base station) – exists in a tracked version control repository, with whole chain of custody on what changes were made by whom lends itself firmly to the notion of secure infrastructure. Maintaining secure infrastructure will become increasingly important with the increased prevalence of critical infrastructure attacks.

Further, this *infrastructure-as-code* concept leverages decades of experience in software engineering, both in terms of the development process as well as in the realm of configuration management – a critical aspect of a mature security posture. From a cost and security perspective, the ability for an infrastructure-wide audit and

update alone is reason enough for moving towards *infrastructure-as-code*.

While a mature security posture is a by-product of *infrastructure-as-code*, it serves as a critical pillar of software-defined infrastructure itself. Prior to 5G (4G for SDN), should an exploit be deployed against a wireless carrier, mitigation and response was an arduous process, involving hardware at nearly every site and a veritable army of technicians. Fixing a flaw in a radio protocol required physical hardware modification or outright replacement. Fixing a flaw in the network stack similarly often necessitated hardware replacement.

With the move to *infrastructure-as-code*, flaws can be corrected within the code itself and pushed to all impacted systems. These flaws need not just be security vulnerabilities either – a switch failing previously required a technician to replace it. Now a simple software reconfiguration can remove the faulty hardware from the SDN and simply route around the fault. A radio malfunction could disrupt service over a large area. As long as physical damage isn't the cause, this can be corrected remotely via a push of updated firmware for the SDR.

2) Costs

While it is clear there are many benefits (a non-exhaustive list can be found in §IV.A.1), there are costs associated with the move to *infrastructure-as-code*. The telecoms industry has decades of experience with fixed-function hardware, with a combined centuries of experience among many talented technicians and engineers accustomed to working with it.

Bringing in an entirely new way of working with critical infrastructure renders much of that experience obsolete. While it is undoubtedly true that the need for experienced engineers and technicians will never be obviated, a new set of skills is required to work within a 5G deployment. Software expertise, FPGA design and synthesis, software project management, and all of the associated tooling and software required are not core competencies of many wireless providers (not to say they don't have these skills, but they were likely within the minority of their front-line infrastructure maintenance employees).

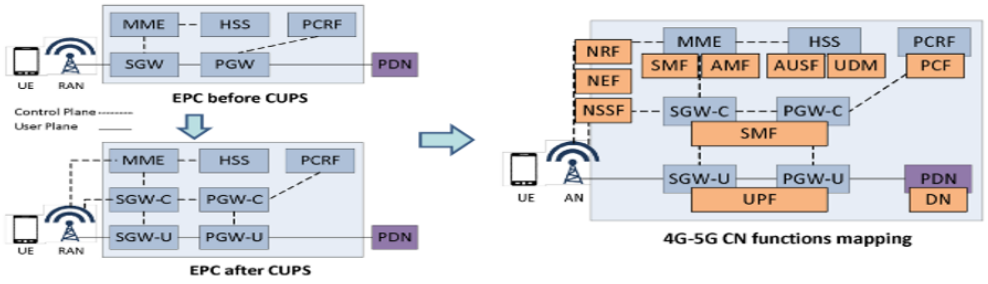

Figure 1: Base station architecture -- upper left is 3G, bottom left is 4G, right figure is 5G

AMF: Access and Mobility Management Function
AUSF: Authentication Server Function
CUPS: Control and User Plane Separation
HSS: Home Subscriber Server
MME: Mobility Management Entity
NEF: Network Exposure Function
NRF: NF Repository Function
NSSF: Network Slice Selection Function
PCF: Policy Control Function
PCRF: Policy and Charging Rules Function
PDN: Public data network
PGW: PDN Gateway
SBI: Service-Based Interfaces (Namf, Nsmf, Nudm, Nnrf, **Nnssf**, Nausf, Nnef, Nsmsf, Nudr, Npcf)
SGW: Serving Gateway
SMF: Session Management Function
UDM: Unified Data Management
UPF: User Plane Function

With new ways of doing things, new risks also rear their head. Previously, to exploit a wireless node, be it a tower, a site, or other, explicit knowledge of the hardware in question was necessary, as well as significant levels of access. With the move to COTS-based infrastructure, operators must now secure an additional layer of the stack: the operating system and network interfaces on the host systems themselves.

It is essential to remember that an SDN is essentially an overlay network. As such, it is a logical construct *on top* of the physical network itself. In other words, rather than having a segregated network at the physical level, SDNs often run on the public internet and provide logical (that is to say, virtual) segregation. The upshot of this layered approach is flexibility. The downside of this layered approach is complexity. With complexity comes potential new security vulnerabilities – the more moving parts a system has, the higher the likelihood that something will fail.

The costs primarily center upon the complexity of securing the infrastructure and a potential skills gap in maintaining and securing that infrastructure.

B. Software-Defined Radio

The following is a technical description of how SDR hardware functions. Please skip to §V below if the technical detail is not of interest

Software-defined radio architecture involves a set of analog-to-digital converters (ADCs) coupled with an FPGA and a CPU interface. Software running the CPU provides radio algorithms and frequency selection.

1) The Hardware

In its simplest form, an SDR consists of an antenna interface coupled with one or more ADCs. These ADCs take the analog RF signal from the tuned antenna and convert them to IQ samples, which define the full signal. The radio front-end splits the incoming signal and multiplies the I portion by the "in-phase" carrier signal – also the real component – while the Q signal is the "quadrature" signal – the carrier signal rotated by -90°.

Once these multiplications occur, the I and Q samples are combined as a single IQ sample. If plotting IQ samples in the time domain, you will see a corkscrew.

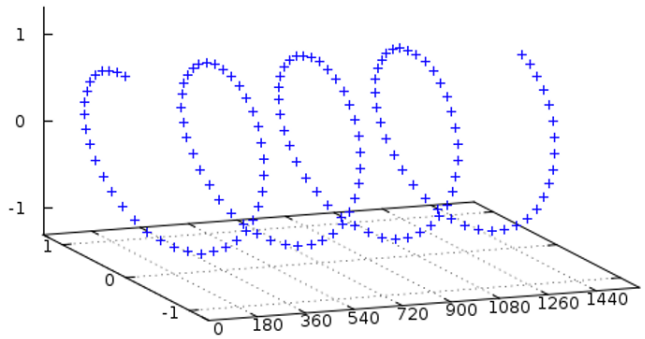

Figure 2: IQ data plotted in the 3D plane as a function of time.[6]

If you look at the cross-section of this in the "in-phase" plan, you will see the typical sine signal you'd expect from a carrier. Likewise with the Q plane, rotated by -90° – which makes it look like a cosine signal. The direction of the corkscrew, whether clockwise or counter-clockwise, allows you to determine if the frequency of the signal is positive or negative.

Once the IQ signals are calculated for each sample, the data is typically handed over to the firmware. This firmware might be running on an FPGA or an ASIC, depending on the design.

2) The Firmware

Depending on the SDR design there will be several levels of firmware. At minimum, the firmware will package the IQ samples for the interface to the CPU. USB, PCIe, and gigabit ethernet are among the most common.

There can also be an intermediate stage between the radio front-end and the interface packaging layer – typically an FPGA. By making use of the FPGA, interpretation logic can be implemented at the hardware level, rather than running on the CPU of the host system. For example, an FPGA core could implement ADS-B decode logic or a WiFi interface.

3) The Software

Once the IQ samples or their interpreted signal are on the host system, additional processing can occur. The host system can control many of the parameters of the SDR, making use of the same *infrastructure-as-code* idea as within software defined networking. The host system will define the frequencies considered by the radio front-end, as well as what firmware runs on the SDR – both FPGA and interface translation layer.

As a specific example, consider the National Instruments USRP B205mini-i. [7] Connecting via the USB 3.0 interface, it also includes an FPGA.

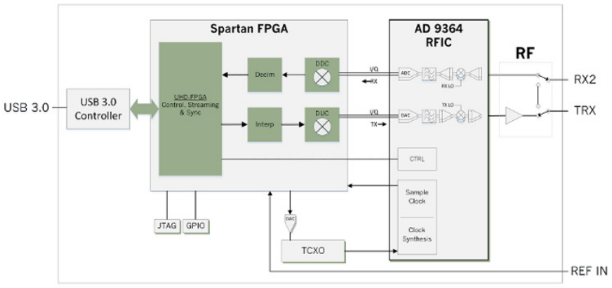

Figure 3: Block diagram for USRP B205mini-i

As seen above, the device uses three main blocks: the RFIC (radio frequency integrated circuit), also called the radio front-end. This then passes data to the Spartan FPGA, which provides control and streaming to the USB 3.0 controller. The USB 3.0 controller packages the data in USB packets and passes them to the host device.

The host device uses the USB interface to also provide control of the FPGA and the RFIC. Adding a tuned antenna prior to the RFIC allows for capturing the signals of interest.

V. SECURITY ARCHITECTURE AND ATTACK SURFACE

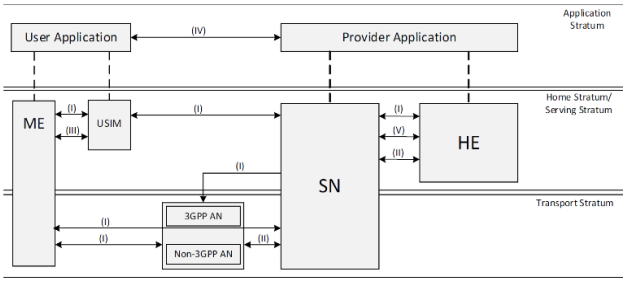

Figure 4: Overview of 5G security architecture[4]

3GPP TS 33.501 [8] defines the security architecture of 5G – in excruciating detail. This section summarizes the particulars deemed relevant to our proposed attack surface. [8] covers much more than just the device-to-network security architecture. While the document covers network-to-network, network-to-device, and even internal communications within the network, we will focus primarily on the device-to-network and network-to-device components. After all, who needs ME if you have the posture to mount an attack from within the network itself?

Of concern to users, a network-to-device attack might take the form of a rogue access point, where the *users* are the targets. While of interest[2], the 5G network itself is our primary target in this work. Rogue access points or so-called "stingray" devices are an avenue of interest for further work.

Much like the OSI model for networking, 5G is a stratified architecture. Figure 2 above demarks the boundaries between strata and the interaction points between elements. Each interaction point consists of at least one security domain.

There are six domains of security within the architecture. They are as follows (taken from [8]):

I. Network access security: the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly *[sic]*, to protect against attacks on the (radio) interfaces. In addition, it includes

the security context delivery from SN to AN for the access *[sic]* security.

II. Network domain security: the set of security features that enable network nodes to securely exchange signaling *[sic]* data and user plane (UP) data.

III. User domain security: the set of security features that secure the user access to mobile equipment.

IV. Application domain security: the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.[3]

V. SBA[ix] domain security: the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. *[sic]* Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces.[4]

VI. Visibility and configurability of security: the set of features that enable the user to be informed whether a security feature is in operation or not.

The secure edge protection proxy (SEPP) handles perimeter security for the 5G core network. The inter-PLMN (public land mobile network - think service provider) UP security (IPUPS) protects user plane data as it transits between PLMNs.[5]

Security domains I-III are the primary thrust of this work, in approximate numerical order of interest. While domain I defines requirements for UE access to the radio access network (RAN), much of what is required also protects the UE from malicious actors within the network.

The standard has strict requirements for user equipment. Some specific highlights:

- Bid-down attacks are explicitly mitigated. Bid-down attacks are attempts by an attacker to use older, less secure connection options by claiming they don't support current modes.
- The specification delegates to the UE much of the responsibility for the integrity and encryption of user data. Due to this responsibility, packet size will increase, as will processing load.
- Secure storage of long-term keys and subscriber privacy also belong to the UE.

Interestingly, the NR node B (gNB[6]), which acts as the physical interface to the radio - an inherent separation in the architecture of an SDR - receives its own specific set of requirements, which mirror those above.

A question that may or may not be evident at this point is, "why are these requirements new to 5G?" In previous specifications (2G through 4G), the radio portion of user equipment was its own hardware domain. A typical phone on a 4G network consists of three distinct hardware domains:

- an *application processor*, which manages user interaction, the user-facing operating system services, and abstract interfaces to communications hardware;
- a *baseband processor*, which arbitrates access to the radio hardware, handles all modulation, encoding, and encryption responsibilities for accessing the network; and
- the *subscriber identity module* (SIM) is its own CPU with its own real-time operating system - and it also has the ability to access the radio interface managed by the baseband processor and communicate independently of the application processor [9].

5G switches this up a bit. The 5G NR is an SDR stack, with firmware handling much of the previous baseband processor. The implication here? The application processor could potentially influence or interact with the radio hardware. The design of the security architecture within the specification explicitly spells out what UE can and cannot do and still maintain certification as a 5G capable device.

[3] Much like the application layer in the OSI model, all network communication is media agnostic, and strictly logical. Examples here would be TLS and similar.
[4] SBA domain security is new to 5G.
[5] Not shown in the diagram.
[6] Yeah, no idea

So what if it lies? While a commercially available device must meet strict anti-tampering requirements within the specification, there is little beyond complexity and lack of experience preventing an adversary from taking a software-defined radio and building a frankenphone. Such a device wouldn't have typical phone capabilities, but at a radio interface level would be an otherwise acceptable 5G device. This theme of malicious hardware plays out in several other aspects of the specification.

A significant portion of the remainder of the security architecture of the specification details the storage, physical tamper-resistance, and provisioning on the network of the gNB. The ME, in this case, attests to meeting these requirements. By creating a full-stack variant of a device, it may be feasible to supply a false attestation that the device meets the requirements, thereby gaining access to the 5G network.

Gaining secure access to the network could allow for various skullduggery – DOS attacks against other users connected to this cell, incorrect signaling to take the cell itself offline, etc. This is one of several avenues of attack we are considering for future research.

The specification requires EAP [10] for UE to 5G network authentication. The RFC defines three roles:

- The UE acts as the peer
- The *pass-through authenticator* is the security anchor function (SEAF)
- Authentication server function (AUSF) acts as the *backend authentication* server

EAP is a well-studied protocol. Used in VPN authentication, RADIUS, and other secure systems, it is unlikely EAP will serve as a protocol vulnerability within 5G. Of course, that does require well-behaved actors within the system. A malicious device could potentially compromise much of the security offered by 5G. The device attests that it meets the requirements to gain network access. A malicious peer could undermine the protection provided by EAP. Future work in this area would be to engage in good faith but use the provided security context to unencrypt traffic – much like how TLS stripping works by not maintaining the confidentiality of the negotiated keys.

There is a complex key hierarchy within a 5G network. Some of these keys reside in the USIM, some in the ME, and some within the serving network (currently connected network). The USIM stores the root key *K* in secure storage and only forwards derived material to the ME. As secure storage for keys is a requirement for 5G, and the network will accept only well-behaved entities, it must logically follow that "there is no way to obtain access to root key *K*."[7]

As the specification explicitly spells out the algorithms and procedures for each subsequent key derived from the root key, *K*, it may be feasible to create a custom firmware for an SDR to allow it to act in the role of ME. With such a hardware/firmware combination, root key *K* should be accessible. Lack of secure storage (or worse, active exposure of confidential information) in a malicious device may be all that is necessary to determine root key *K*.

While much of the above details an attack surface of the access conditions for 5G devices, the other direction merits consideration. In the case of a malicious ME, the network itself serves as the target. But what if we desired something else? Rather than the network itself being the target, what if users of the network were the target?

This gets back to the idea of a rogue access point. If you are familiar with WiFi (Mitre ATT&CK T1465)[11] as well as cellular networks (T1467)[12], these aren't new ideas. But with the advent of accessible SDR platforms, adversaries have more resources than ever before. Inexpensive platforms such as the USRP B210[7] were actively designed for the use case of 5G base station development. While not plug-and-play, there exist multiple open-source projects to enable this functionality.

Currently, such projects only allow self-provisioned devices to access the base station. What exactly

[7] Clearly tongue in cheek.

would be necessary to go from such a research platform to an attack platform is an open question for future work. Such work could allow for MiTM attacks, active IMSI catchers (stingrays), or end-user device compromise if coupled with other vulnerabilities (think watering hole attack for a geographically focused target group).

A. Device Characteristics

Several times, malicious hardware was mentioned as a possible avenue of attack. This would need to take the form of a malicious mobile device. So how might this device look? We can use the device security guidelines to inform the design:

- Secure storage: the standard requires this but leaves it to the device to attest to its existence. A malicious device would lie regarding the security of its storage.
- Key derivation: this dovetails with secure storage, but a malicious device would expose the root key *K*.
- EAP: A malicious device could perform EAP, then strip the security of all communications, mirroring them to some other destination (unencrypted).
- Physical tamper resistance: a malicious actor wouldn't need to worry about this. In fact, after development, the ME could be encased in vibranium or similar unobtainium, and it wouldn't matter – the malicious actor built the hardware to do what they wanted. No need to directly access it.
- 5G-NR makes use of a software-defined radio. So must our malicious hardware.
- By leveraging the FPGA present in many SDRs, a malicious actor could provide all the necessary components of 5G ME:
  - SIM slot
  - storage
  - gNB
  - 5G NR
  - Application processor
- Most suitable SDR FPGAs are of sufficient size to provide the hardware and processing required to implement a certified[8] device.
- All of the above depends upon a base station we control – at no point would we consider attaching such a device to a public network without permission.
- A malicious device would also provide a fuzzing platform of both data and signaling aspects of the 5G network.

As can be seen, building a malicious device which can connect to our own base station will be a significant amount of effort, *on top* of the effort of creating our own base station. While there do exist open source projects that implement portions of a 5G base station, research into device-level work seems to be in its infancy.

This future work would enhance the state of the art in vulnerability research involving 5G. A "turnkey" research platform for 5G would be of immense value

VI. MYTHS AND LEGENDS OF 5G

A. 5G only brings benefit if Line of Sight (LoS)

There is a common misconception that the only benefit 5G offers over LTE is within the mmWave band (FR2). The frequencies in FR2 are all quite high and have very limited penetration. Because of that deficiency, mmWave does operate best within LoS of the base-station.

While mmWave does require LoS to be of use, 5G also uses lower frequencies than LTE, allowing for significant expansion of range, especially in rural areas and dense urban areas. These lower frequencies offer both increased bandwidth and longer range, bringing better coverage relative to LTE.

B. 5G caused COVID-19

Around the internet, there have been many conspiracy theories that the root cause of COVID-19 was the deployment of 5G networks.

There is absolutely no basis for this theory. For one,

[8] Certified in this context means on a self-provisioned network initially.

commercial deployment of 5G was not widespread at the time of origin of COVID-19. For another, the frequencies in use of 5G are the same frequencies in use by LTE and multiple other pervasive technologies.

Further, the power levels in use around the world for 5G do not translate to significant ionizing radiation, which would be the only way the signal could impact the human body.

C. 5G causes planes to fall out of the sky

There has been a lot of news recently regarding 5G interfering with radio altimeters, which would result in planes falling out of the sky, crashing into runways, and generally grounding the entire fleet. Media has reported this as "Band C deployment."

Physics disagrees with this entirely. The FCC required a significant guard-band between 5G signals and the frequencies used by radio altimeters. A radio front-end that accepts spurious signals so far down the spectrum is very poorly implemented if it was even possible to build.

Further, the C-Band entirely overlaps the CSRB band – which Verizon already makes use of for LTE deployments. If the FAA's complaint is that 5G would cause significant interference, why has the Verizon deployment not already done so?

While it is true that absence of evidence is not evidence of absence, at the time of writing, the FAA complaint had yet to be substantiated with any technical evidence. That it was later withdrawn with no explanation or change to the FCC decision corroborates this lack of evidence.

VII. FUTURE WORK AND RESEARCH OVERVIEW

This document is only the first step of longer-term research into 5G security. Further research will consist of multiple stages. Initially, a private deployment of 5G in a lab environment will be necessary.

Once we have a base station, we will need to develop malicious hardware to test our attack surface.

A. 5G network setup

In order to deploy a private 5G base station, the open-source OpenAirInterface[13]. Using a USRP B210 with a band 7 multiplexer[14], the radio interface for 5G can be deployed. The SDN and back-end functions would require multiple network hosts to run the required tooling for access, authorization, and management.

This network base station would offer FR1 frequencies. In order to examine mmWave (FR2) frequencies, we would need some form of frequency converter, such as [15]. While mmWave would be a valuable investigation, the investment in deploying a network serving such frequencies is high, pushing it down the priority queue. As the security protocols are the same between FR1 and FR2, any flaws discovered in FR1 should be equally applicable to FR2 channels.

B. Rogue Access point

Given that a private deployment of 5G will be necessary for investigating user-side security, studying network-side security should also be an avenue of research.

Such a base station, combined with a commercially available device, could be used to study the feasibility of a 5G rogue access point.

C. Analysis of underlying software

As more functionality moves from bespoke ASICs and single-purpose hardware to more general functional blocks running against a typical COTS server stack, the attack surface of 5G could potentially be significantly increased. This hardware/software typically lives below the level of the SDN. It is (to my understanding) internet-facing – could we leverage flaws in the underlying system to compromise the control plane of 5G? Rather than coming in through the front gate, this is more akin to using sappers to tunnel under the fortification's walls.

System binary fuzzing, reverse engineering, and other approaches could be of value here.

D. 5G Fuzzing – signal, logical, control

This could be immensely valuable, both as a general-purpose RF fuzzer and as a custom 5G solution for fuzzing. Much more research is necessary to determine how this could work and what would be required.

---

[1] "Smartphones replacement cycle in the US 2014-2024," Statista. https://www.statista.com/statistics/619788/average-smartphone-life/ (accessed Jun. 23, 2021).

[2] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," in 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2019, pp. 1153–1168. doi: 10.1109/SP.2019.00038.

[3] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols," 1175, 2018. Accessed: Jan. 31, 2022. [Online]. Available: http://eprint.iacr.org/2018/1175

[4] S. Magazine and M. Novak, "The World's First 'Carphone,'" Smithsonian Magazine. https://www.smithsonianmag.com/history/the-worlds-first-carphone-24664499/ (accessed Dec. 06, 2021).

[5] A. Demba and D. P. F. Möller, "Vehicle-to-Vehicle Communication Technology," in 2018 IEEE International Conference on Electro/Information Technology (EIT), May 2018, pp. 0459–0464. doi: 10.1109/EIT.2018.8500189.

[6] "I/Q Data for Dummies." http://whiteboard.ping.se/SDR/IQ (accessed Jan. 31, 2022).

[7] E. R. Brand a National Instruments, "USRP B210 USB Software Defined Radio (SDR)," Ettus Research. https://www.ettus.com/all-products/ub210-kit/ (accessed Jan. 12, 2022).

[8] 3GPP, "Security architecture and procedures for 5G system."

[9] D. A. Burgess, "What is AT&T doing at 1111340002?," Telecom Expert, Dec. 02, 2021. https://medium.com/telecom-expert/what-is-at-t-doing-at-1111340002-c418876c212c (accessed Jan. 12, 2022).

[10] "rfc3748." https://datatracker.ietf.org/doc/html/rfc3748 (accessed Jan. 11, 2022).

[11] "Rogue Wi-Fi Access Points, Technique T1465 - Mobile | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1465/ (accessed Jan. 12, 2022).

[12] "Rogue Cellular Base Station, Technique T1467 - Mobile | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1467/ (accessed Jan. 12, 2022).

[13] "OpenAirInterface – 5G software alliance for democratising wireless innovation." https://openairinterface.org/ (accessed May 21, 2021).

[14] "Band 7 cavity duplexer – 4G and 5G reference software." https://open-cells.com/index.php/opencellsband7duplexer/ (accessed May 21, 2021).

[15] "mmWave Test Beamforming Solutions," Solubit, Apr. 08, 2021. https://solubit.com/mmwave-test-beamforming-solutions/ (accessed May 21, 2021).

[16] "Potential Threat Vectors to 5G Infrastructure," NSA, CISA, ODNI, 2021

---

[i] CPU: Central Processing Unit – the brain of a computer

[ii] FPGA: Field Programmable Gate Array – a configurable array of logic gates which can be combined in different ways to provide hardware processing with a simple firmware flash.

[iii] TDMA: Time division multipex access – access chunked in time

[iv] D-AMPS: Digital AMPS (advanced mobile phone system)

[v] CDMA: carrier division multiple access – access chunked in space (specific width pieces of spectrum)

[vi] GPRS: general packet radio service

[vii] EDGE: Enhanced Data-rates for GSM Evolution

[viii] GSMA: GSM Alliance – standards body for GSM through 3G.

[ix] SBA: Service-based architecture.