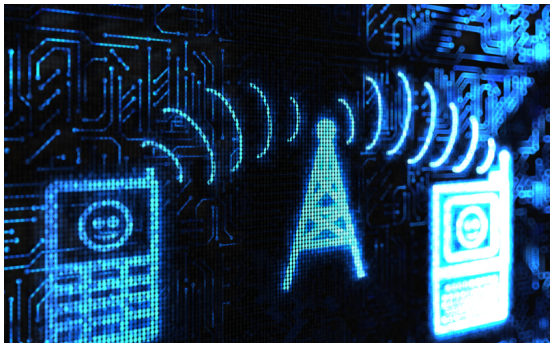
Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 8

Wireless Security Standards

By Alan Zeichick



Security standards for cellular communications are pretty much invisible. The security standards, created by groups like the 3GPP, play out behind the scenes, embedded into broader cellular protocols like 3G, 4G, LTE and the oft-discussed forthcoming 5G. Due to the nature of the security and other cellular specs, they evolve very slowly and deliberately; it's a snail-like pace compared to, say, WiFi or Bluetooth.

Why the glacial pace? One reason is that cellular standards of all sorts must be carefully designed and tested in order to work in a transparent global marketplace. There are also a huge number of participants in the value chain, from handset makers to handset firmware makers to radio manufacturers to tower equipment to carriers… the list goes on and on.

Another reason why cellular software, including security protocols and algorithms goes slowly is that it's all bound up in large platform versions. It's clear that 3G is quite different from 4G, and that 5G is something else entirely. The current cellular security system is unlikely to change significantly before the roll-out of 5G… and even then, older devices will continue to use the security protocols embedded in their platform, unless a bug forces a software patch. Those security protocols cover everything from authentication of the cellular device to the tower, to the authentication of the tower to the device, to encryption of voice and data traffic. When 5G rolls out (the best estimates are 2020, but who knows?), we'll see new standards.

We can only hope that end users will move swiftly to 5G, because 4G and older platforms aren't incredibly secure. Sure, they are good enough today, but that's only "good enough." The downside is that everything is pretty fuzzy when it comes to what 5G will actually offer… or even how many 5G standards there will be.

What's Wrong with LTE?

Has your phone ever wanted to update its "carrier settings?" That may be a reaction to a flaw in cellular security, either in the design of a standard, or in the implementation of the standard through firmware. One example of a recent flaw was published in October 2015. Called "Voice over LTE implementations contain multiple vulnerabilities," the report from CERT said,

"Current LTE networks rely on packet switching, rather than the circuit switching of previous generations of the mobile network. The use of packet switching and the IP protocol (particularly the SIP protocol) may allow for new types of attacks not possible on previous generation networks. Such types of attacks are well-known in the security community; for example, see previous attacks against Voice over IP (VoIP)."

The report went on to talk about problems with incorrect permission assignments for critical resources, improper access control, improper authentication, and session fixation (which might lead to denial-of-service attacks on the network).

The CERT report is only one demonstration of less-than-Fort-Knox security model in today's cellular network. Daksha Bhasker of Bell Canada served up a very detailed paper, "4G LTE Security for Mobile Network Operators," in which she writes,

"…in reviewing the 4G LTE architecture, the 3GPP, next generation mobile network (NGMN) alliance and international telecommunications union (ITU) have identified security vulnerabilities and recommended mitigation strategies. Consideration and implementation of these security enhancing measures are discretionary to the many LTE stakeholders including MNOs. As a result, the security of LTE networks and services will vary widely between MNOs, subject to the MNOs knowledge of security risks and impacts, the MNOs risk appetite and wallet size among other factors. Speed to market, tight budgets, profit targets, concerns with network performance, business models, network interoperability, regional regulations and business priorities lead to further inconsistencies in security implementation amongst MNOs."

We could go on and on… but let me point to one more source, a presentation at the RSA Conference in April, 2015, entitled, **"LTE Security — How Good Is It,"** by Jeffrey Cichonski and Joshua Franklin, both of NIST. The paper presentation identifies several weak spots (and possible attack vectors) in the end-user device, the tower, the network core, and the IP network (i.e., the Internet).

While our focus here is on the OTA security aspects of the device and tower, vulnerabilities anywhere along the chain can compromise the whole system. That includes radios, mesh networks, packet gateways, signaling systems (i.e., the control plane), crypto, subscriber identity, and more. See slides 25-32, which go into a wide range of possible attacks that would defeat LTE security. Scary stuff.

Cellular Network Security Protocols

There are so many standards, it's hard to know where to begin. The standards are also embedded within other standards. Let's take one simple set of protocols: UEA2 and UIA2, which have been around since the early 2000s. UEA2 is an algorithm that defines the confidentiality of communications. Its partner UIA2 specifies algorithms for protecting the integrity of communications. UEA2 and UIA2 are functions used by SNOW 3G, a stream cipher that generates and uses crypto keys – and is used heavily in OTA cellular security.

UEA2, UIA2 and SNOW 3G come from the **3GPP** (3rd Generation Partnership Project), a vast international consortium that defined GSM (i.e., 2G cellular), UMTS (i.e., 3G) and LTE (i.e., 4G) and which is spearheading 5G. 3GPP is truly global, and has driven the cellular industry since 1992. Every quarter, 3GPP releases new specifications. Every couple of years 3GPP releases new protocol sets; sometimes they are major, like 4G

There are so many standards, it's hard to know where to begin

LTE, and sometimes they are minor, like the new **"LTE-Advanced Pro"** spec that came out in October, 2015, and which might find its way into the global cellular networks and consumer devices in late 2016 or early 2017. Glacial, remember?

Slow and steady wins the race, but threats evolve quickly. There are threats for service delivery, handling privacy, man-in-the-middle. It's a complex landscape, and all it takes is one exploit to succeed to allow bad actors into the network. In some cases, as mentioned in the papers mentioned above, the weaknesses are in the security architecture and protocols in 4G and older cellular OTA networks.

I suspect that the biggest threat to cellular security is bugs: flaws in the firmware and operating systems embedded into smartphones and other cellular devices, as well as in towers and other carrier equipment. Given that carriers have direct control over their towers, and can do testing and other QA, my sense is that handset vulnerabilities are the biggest problem facing the industry…. well, other than directed attacks against the physical infrastructure.

The Work of the 3GPP on 5G

The 3GPP specifications are numbered according to their general purpose. Modern cellular radios, for example, are in the **25 Series** of specifications. The security work within the 3GPP is broken up into two different series: **33 Series** is for general security, and **35 Series** is for security algorithms. UAE2 and UAE2 are defined in **35.215**, and SNOW 3G is in **35.216**. Browse through the 33 Series and 35 Series specifications, and see links to protocols, reports, studies and more. It's a goldmine of technical information about LTE, much of which, unfortunately, requires a lot of contextual knowledge. Note that some of those links are to industry proposals, some of which were later withdrawn.

The work on 5G is collected in another area called, "**Release 14.**" Unfortunately, it's very sketchy, which

reflects that 5G is still four years away, perhaps more. The 3GPP says that it is committed to release an initial technology submission by June, 2019, and a more detailed specification by October, 2020. We'll see; it's a big job, and a lot of information is not available.

That doesn't mean that we know nothing. One of the major participants in the 5G security work is Ericsson, which put out a **paper on the subject** in June, 2015. Ericsson says that that 5G's security will evolve from 4G to focus on four main areas:

1. **New trust models:** 5G services are expected to serve safety-critical systems, such as in public safety. Devices will explode beyond phones to the Internet of Things (IoT), including shipping containers, industrial controls, and connected vehicles. The report brings up an unpleasant thought: "Devices have so far been assumed to comply with standards and not to deliberately attempt to attack networks. But how well protected are very low-cost devices? Can a single connected device be used as a stepping stone for cyber-attacks deep into the system? And what is the attack surface of a 5G system with billions of inexpensive, connected devices?"

2. **Security for new service delivery models:** In the 4G and older cellular era, everyone assumed that a cellular end node (like a handset or tower) was a dedicated, proprietary piece of hardware. In 5G, much more will be virtualized through NFV (Network Functions Virtualization) and SDN (Software Defined Networks). New security protocols are needed to isolate virtualized services from each other.

3. **Evolved thread landscape:** 5G devices will be part of critical infrastructure which will attract new attackers who will go beyond simply disrupting services (like destroying a cell tower). Instead, attackers may attempt to co-opt those 5G devices and networks. This will require stronger protocols for device authentication, user authentication (often clear-text usernames and passwords), and strong cryptography.

4. **Increased privacy concerns:** Users are concerned about mass surveillance, and there have been reports of rogue base stations conducting man-in-the-middle attacks. The Ericsson report also mentions the user identifiers for cellular devices, which haven't been updated in a very long time. While there are proposals for replacing new protocols, the study says, "the benefits of full International Mobile Subscriber Identity (IMSI) protection have so far not seemed to outweigh the complexity of implementing it."

The scalability of billions of embedded devices ... is a major challenge within the field of IoT security

More Unknowns than Knowns

While 4G LTE has good enough security for today's smartphones, it's not enough for the future especially when you factor in IoT. We will have new devices and new ways of using those devices. Oh, and scalability will be a challenge as well. To quote from **"Security and impact of the IoT on LTE mobile networks,"** a pre-publication book chapter by Roger Piqueras Jover of the AT&T Security Research Center:

"As mobile networks evolve and transition towards 5G, the capacity and throughput of the wireless interface is scaled up to tackle the goals of massive device connectivity and 1000 times more capacity. To do so, researchers are already prototyping advanced systems at high millimeter wave frequencies and implementing massive MIMO [multiple input multiple output] systems. However, a common topic of discussion at a major 5G industry forum was how it is not all about speed, but also about scalability. The scalability of billions of embedded devices joining existing LTE and future 5G networks is one of the major availability challenges within the field of IoT security."

There's a lot riding on 5G. We need it, and we need its security. We'll continue to keep an eye on it.