Alex Kukura and Thomas Waggoner

Professor Xing

CSCI-B 433/INFO-I 433

May 2, 2024

Cell Phone communication is Insecure and outdated

With the rise of smartphones in the early early 21st century, wireless communication has become virtually ubiquitous. Beyond liberating phone calls from wall-attached wires, the wireless revolution has led to the widespread use of text messaging for everyday communications. Indeed, by 2020, 2.1 trillion text messages were sent each year, equaling more than 250 for every person on Earth.[1] It is evident, therefore, that wireless communications, and especially text messages, play an important role in modern life. This raises several important questions about the security of these now heavily relied-upon systems.

Section 1: Approach

This paper will analyze security flaws in existing wireless communication systems, focusing specifically on lack of encryption and insecurity of physical infrastructure. Drawing on a variety of sources, it will identify several real-world examples of the vulnerabilities created by the lack of encryption and lack of physical security measures in Section 2. In Section 3, it will then examine existing solutions to these problems, including both the theoretical and the practical. Finally, the paper conclude by providing recommendations in Section 4 for which solutions should be focused on for widespread adoption, being a valuable resource for policymakers and other interested parties.

Section 2: Existing Lapses in Wireless Communication Security

[1] Jowi Morales, “How SMS and MMS Gave Birth to Instant Mobile Messaging.” MakeUseOf, 2022, https://www.makeuseof.com/sms-mms-instant-mobile-messaging-history/.

Phone calls and text messages are still using protocols developed in the early 90s when cyber security was not as robust as today's standards. The universal standard for all phone manufactures is Short Message Service (SMS) which was developed in 1992 and later Multimedia Messaging Service (MMS) in 2004 for larger files like images. These standards were developed when transmission rates were much slower and consumer cellphone computing was a fraction of what it is today. Cell Phone infrastructure has been mostly additive with each new generation of cell phone transmission building upon previous generations still utilizing SMS and MMS as a common communication service between cellphones as a base while adding on more features on top to allow for the widest amount of compatibility with all devices.

This has left huge gaps in security in recent years due to having an unencrypted standard with relatively low amounts of data being transferred over that protocol. SMS is still used as the main form of transmission for authentication codes using two factor authentication, this is due to companies like Apple that currently only support iMessage and SMS/MMS and Android only supporting RCS and SMS/MMS. Since SMS/MMS are the only communication protocols the two major platforms have in common it has become the default for some sites that promote 2FA since it is such a universally adopted standard that anyone would have access to. While SMS 2FA does provide more security than just having a password it opens opportunities for targeted attacks if a target is valuable enough.

SMS has also led to massive leaks for privacy. In 2003 AT&T allowed the NSA to collect information on its customer and other companies traffic that was being routed through AT&T infrastructure. The NSA was able to wiretap and data-mine customers since both text and calls were using unencrypted standards. While the NSA claims this was done to protect the American people from terrorist plots they were still able to listen into any customer communication that went through AT&T infrastructure casting a wide net over millions of customers. This a huge violation of confidentiality for all customers as their data can be collected without their knowledge. If government agencies are able to easily collect this information through a back door it should be assumed that hackers could potentially get access to this data as well, which can compromise more than just the current phone call. Important business, medical, and legal information is often discussed over these unencrypted forms of communication potentially putting millions of people at risk of losing their accounts and identities.

Spam and spoof calls have also been able to take advantage of this infrastructure as well. Spam callers are able to send out hundreds of thousands of calls and messages for cheap, causing customers to ignore calls from phone numbers that they are not familiar with. This can be annoying for regular customers but businesses especially suffer when they have to have dedicated employees answer calls, this wastes valuable time and resources for businesses especially local businesses that have limited employees. Since spam callers realized that people stop picking up for phone numbers that they don’t know they have started utilizing spoof calls. This is when the caller is able to hide their real number with a fake phone number, the number will often mimic your area code so you are more likely to pick up the phone.[2]

Spoof callers are able to utilize Voice over IP (VoiP) and then use an unsuspecting person’s phone number for a brief time. This can be extremely dangerous if used in conjunction with a spear phishing attack as family and friends can receive phone calls from a spoofed family member's phone. Then with some clever social engineering the attackers can trick victims into sending thousands of dollars to overseas accounts where legal recourse is extremely unlikely. Attackers can also try and pose as government officials, IRS agents, or any other person to try

[2] TransNexus, “Understanding STIR/SHAKEN,” TransNexus, accessed April 25, 2024. https://transnexus.com/whitepapers/understanding-stir-shaken/.

and make you divulge private information or money. This makes it difficult to defend against because caller ID that is supposed to help mitigate calls like this are easily fooled by the masking phone calls. Also it is difficult to shutdown the places operating overseas as even though the United States has put laws and regulations in place to fight against spoof calls they do not apply to overseas countries with lower standards.

While encryption and other digital security considerations are no doubt imperative to the security of wireless communications, the security of physical infrastructure is also of paramount importance. Indeed, recent events have demonstrated that wireless communications infrastructure is subject to unsophisticated yet impactful attacks. In the early months of 2020, as the world was reeling from the onset of the COVID-19 pandemic, another pandemic swept the nation: fear of Fifth Generation (5G) telecommunications technology. The new technology, which began to see widespread deployment and use at the end of 2019 and the beginning of 2020, is merely an update to existing and widespread wireless communications standards, capable of moving digital information at higher speeds with lower latency.[3]

What was intended to be a relatively routine technology upgrade turned into an international phenomenon as conspiracy theories began circulating about the potential effects of 5G technology on humans. These conspiracies became swept up in the broader conversation of COVID-19, and soon conspiracies discussing the virus and the technology became irreversibly linked.[4] As a result, a non-insignificant number of people began to fear the adoption of 5G technology, believing that it would have harmful effects on their health, safety, and even

[3] Qualcomm, “What is 5g?,” Qualcomm, accessed April 25, 2024, https://www.qualcomm.com/5g/what-is-5g.

[4] Ken Klippenstein, “White Supremacists, Conspiracy Theorists Are Targeting Cell Towers, Police Warn,” *The Intercept,* March 17, 2021, https://theintercept.com/2021/03/17/5g-white-supremacists-conspiracy-theorists-critical-infrastructure/.

freedoms. As a result of this fear, believers in the conspiracies began carrying out attacks against 5G infrastructure. These attacks included setting fire to towers, shooting at 5G antennae, verbally and physically abusing workers installing new infrastructure, and destroying cables and other communications equipment installed at the base of cell towers.[5]

While this example is far from the typical archetype of traditional cyber attacks, it demonstrates that physical wireless communications infrastructure, which is responsible for maintaining critical communications channels that are necessary for 21st century living, are subject to critical security risks. As these attacks show, it does not require a nation-state or organized criminal hacking organization to threaten wireless infrastructure. Instead, individual actors can cause significant damage and temporarily disable cell towers and other wireless communications equipment, causing outages or slowdowns in service. It is evident, therefore, in addition to addressing the problem of encryption in wireless communications, the physical security of the infrastructure responsible for maintaining and serving those wireless communications must also be improved.

Section 3: Existing Solutions

In recent years there have been some alternatives to SMS/MMS, one of the most notable introductions was Apple's iMessage which utilizes end-to-end encryption with AES encryption which is still used and is still considered a very secure standard. Unfortunately this communication standard is locked behind Apple's walled garden only allowing other apple products to communicate over iMessage. This is an issue as if there is communication between Apple and another platform like Android the text messages will default to using SMS/MMS. This is and issue especially in countries like the United States where Apple phones have a

[5] Klippenstein, "White Supremacists."

majority market share with 55% of people owning an iOS device.[6] This makes it difficult as both iOS and Android would have to agree on a unified communication service.

There have also been other apps that boast end-to-end encryption and are available to download on any device like Telegram, Signal, or WeChat. These apps help bridge the gap between Apple and Android devices as they can be used by anyone with an account and can offer more features than texting and phone calls. However there are some notable downsides many of these apps require the user to have a phone number so it is more of an addition to the pre-existing system rather than a complete alternative. There is also the issue that there are multiple different messaging apps with some being very popular in one country but not supported at all in another like WeChat is widely popular in China but has very limited reach in the US. In order for a solution to fix the issues discussed in the previous section it would have to be an universal standard accepted by all phones by default rather than an app that people can choose to use.

Rich Communication Service (RCS) is Android's preferred text messaging service. It was developed in 2007 because there was a “need for a more sophisticated universal messaging standard, the GSM Association (GSMA), a trade body made up of cellular carriers around the world, came up with the next generation of SMS/MMS: a new technology known as Rich Communication Services (RCS)” (Hollington 2024) It allows for features like read receipts, better image quality that MMS, and most importantly encryption. While encryption isn’t a part of the base RCS Google has added it to their implementation of RCS for their phones. RCS is a standard that allows different carriers and manufacturers to add on new features that they prefer. This allows flexibility and also compatibility, while certain carriers might promote features that

[6] Lance Whitney, “iOS vs Android Market Share: Do More People have iPhones or Android Phones?” *TechRepublic,* June 29, 2023, https://www.techrepublic.com/article/ios-vs-android-market-share/.

can benefit users they will still be able to use the widely adopted base standard across all platforms.

On the other side of cellphone communication services the voice call has also been left woefully behind many standards that we have implemented today. Landlines while still present are largely falling out of fashion. This is good because landlanes are susceptible to wiretapping since the conversation is traveling unencrypted through a physical wire.[7] Most calls are made on mobile devices that send out encrypted signals This will help prevent cases like the NSA AT&T wiretapping in 2003 from repeating. The spoof phone calls will be a more difficult issue, attackers are taking advantage of VoIP to make it look like they are coming from a number in your area code. To ensure that phone numbers belong to the actual customers that pay for them there needs to be a way to authenticate the caller. A method called STIR/SHAKEN is a system that uses public key cryptography and digital certificates. This system is very similar to what https does and would eliminate spoof calling.[8] While this will require telephone service providers to put in more effort for each phone call to authenticate the user it also will reduce the amount of spoof phone calls reducing the overall amount of traffic on the cellphone infrastructure. Each time a phone call is made it is routed through the sender's phone company verifying that this is your phone attached with the phone number and then passes on your certificate to the receiver's phone company. The receiver's phone company can then check this certificate with a certificate repository and verify this call is coming from the verified phone number. If the certificate doesn't match then the phone call can be dropped or have a warning.

[7] DigitalInformationWorld, "Here's What you Need to Know About Call Encryption and Security in 2020," *DigitalInformationWorld,* September 30, 2020, https://www.digitalinformationworld.com/2020/09/call-encryption-and-security-in-2020-the-fundamentals.html.

[8] TransNexus, "Understanding STIR/SHAKEN."

Turning to the physical security of wireless communications infrastructure, there are several improvements that stand to be made. While wireless communications infrastructure encompasses many different installations, this analysis will focus specifically on cell towers, given that, in order to function effectively, they must be installed outdoors in prominently visible locations, making them more susceptible to physical attacks than infrastructure located inside of buildings or other closed-off infrastructure.

With this caveat in mind, it is possible to turn to improving the physical security of cell towers. The most effective way to improve physical security is through the introduction of additional access control measures. Such measures would make it more difficult for would-be attackers to get near enough to crucial infrastructure to carry out attacks by ensuring that only authorized personnel are able to gain access to cell towers' footprint area. The most effective way of achieving this is, of course, an increase in the use of fences and gates.[9] While most cell towers already have these in place, they are located very close to the base of the tower, allowing attackers to still carry out attacks by shooting or throwing explosive objects at the tower's infrastructure, even if they cannot get inside. Thus, increasing the security perimeter of cell towers, wherever possible, could help in lowering the risk of a successful physical attack.

While increasing physical barriers around cell towers could diminish the occurrence of attacks, they would not prevent all attacks. Given this, improved mechanisms to monitor and identify potential threats and attacks before, during, and after they occur, as well as identify the perpetrator, are also necessary for the cell towers' security. In short, cell towers need improved active intrusion detection and monitoring systems. Such systems would include cameras and

[9] Asentria, "Telecom Sites Physical Security: How Telecom Network Operators and Tower Companies Can Improve Physical Security at Base Stations and Protect their Networks," *Asentria,* August 2019, https://www.asentria.com/wordpress/wp-content/uploads/2019/08/telecom-sites-physical-security-whitepaper.pdf. Accessed April 15, 2024.

sensors capable of picking up on irregular movement or activities around the tower and reporting them to a central location for human review and action.[10] Through such automated surveillance, cell tower operators can better understand what is happening at their towers and respond quickly to any attacks, potentially cutting down on the success of attacks and allowing the operators to report perpetrators to law enforcement, leading to more arrests and, by extension, a reduction in attack frequency.

Finally, in addition to increased access control and intrusion-detection systems, wireless infrastructure should be improved by increasing redundancy. While the aforementioned solutions may reduce the quantity of attacks, they cannot prevent attacks altogether. Therefore, networks and operators must be prepared to continue to provide service in the event of a successful attack. The most efficient way of doing this is through increasing redundancy by increasing the number of towers and improving mechanisms that transfer tower coverage in the event of a tower outage.[11] Such efforts would ensure that if a successful attack takes out one tower, it does not lead to a major disruption in service or availability in that cell tower's covered area, minimizing the overall impact of any successful attack.

Section 4: Recommendations

In order to transition away from the old standards there needs to be a transfer to a newer more secure system. The first step of that should be making RCS the standard for all text message communication. While RCS is being used encryption needs to be a part of the standard not just an optional addition. This will ensure that all users are as protected as possible by default

[10] Asentria, "Telecom Sites Physical Security."

[11] Chris Bihary, "Why Cybersecurity Relies on Redundancy to Ensure Network Availability," *Garland Technology,* August 20, 2020, https://www.garlandtechnology.com/blog/why-cybersecurity-relies-on-redundancy-to-ensure-network-availability.

rather than an opt in feature that would leave many users unprotected. RCS also needs to be accepted by all manufacturers. Currently Apple is the major outlier using iMessage instead. RCS needs to be mandated as an option for all service providers and phone manufactures so there is not a segmentation in the consumer base. While companies can choose to use their own standard there needs to be an option for using end to end encrypted RCS. Also SMS/MMS shouldn't disappear; it is still valuable as a lightweight alternative that can be used in emergency situations. When cell reception is limited SMS/MMS can still be sent so it is still a valuable standard. There should be warnings whenever a user is using SMS/MMS though letting both sender and receiver know that it is unencrypted and try and steer them to using RCS. This would be similar to the transition from http to https, both are still usable but users are steered to use the safer https. Using a similar method to transition cell phone texting could be effective and non-intrusive.

To reduce the number of spoof calls a certificate authority and public key encryption system is needed to verify a user's phone numbers. The STIR/SHAKEN method seems to be an easy to implement system that could heavily reduce the number of spoof calls. While this would only be effective on cell phones and not landlines the majority of phone calls are trending towards cell phone calls currently so that can help the majority of users.

In addition to improvements to encryption, we also have recommendations for the improvement of physical security. First and foremost, cell tower operates should ensure that they have adequate access control mechanisms in place, including fences and gates around cell towers preventing intrusion and protecting ground-level infrastructure. If possible, these fences should be pushed back further away from the base of the tower, making it more difficult to reach the tower with attacks from outside of the fencing. In addition to physical barriers, operators should also ensure that they have adequate intrusion detection and surveillance systems, allowing them to be notified of any unusual or unauthorized activities at their towers and report perpetrators to the authorities. Finally, redundancy should be improved through the installation of more towers and the improvement of event-response systems that reallocate surrounding towers to fill in gaps caused by outages at individual towers. The adoption of each of these methods should decrease the frequency and severity of attacks on cell towers, improving the overall availability of wireless communications systems.

Section 4: Conclusion

Cell phone infrastructure is one of vital parts of many people's lives that allows them to communicate with anyone around the world at the press of a button but it can be greatly improved. It has been taken advantage of by government agencies, spam callers, and corporate negligence to severely compromise users' trust in phone calls and text messages. In order to address the glaring issues with the current systems cellphone infrastructure needs to adopt some of the modern advancements in public key cryptography, encryption, certificate authorities, data privacy, and universally accepted standards users can be more protected and not see any difference in the quality of their experience. Furthermore, in order to prevent widespread outages and the loss of availability of now-necessary wireless communications systems, the physical security of cell towers must be improved. By combining these two solutions, wireless communications can be well-protected and guaranteed well into the future, ensuring that everyone is entitled to safe, secure, and consistent interpersonal communications.

References

Asentria. “Telecom Sites Physical Security: How Telecom Network Operators and Tower Companies Can Improve Physical Security at Base Stations and Protect their Networks.” *Asentria,* August 2019. https://www.asentria.com/wordpress/wp-content/uploads/2019/08/telecom-sites-physical-security-whitepaper.pdf. Accessed April 15, 2024.

Bihary, Chris. “Why Cybersecurity Relies on Redundancy to Ensure Network Availability.” *Garland Technology,* August 20, 2020. https://www.garlandtechnology.com/blog/why-cybersecurity-relies-on-redundancy-to-ensure-network-availability.

Business Insider. 2018. “AT&T Buildings Around US Reportedly Used As Part of NSA Spying.” Business Insider. https://www.businessinsider.com/att-buildings-around-us-reportedly-used-as-part-of-nsa-spying-2018-6.

DigitalInformationWorld. “Here’s What you Need to Know About Call Encryption and Security in 2020.” *DigitalInformationWorld,* September 30, 2020. https://www.digitalinformationworld.com/2020/09/call-encryption-and-security-in-2020-the-fundamentals.html.

Hollington, Jesse. 2024. “What is RCS messaging? A briefing on the SMS successor.” Digital Trends. https://www.digitaltrends.com/mobile/what-is-rcs-messaging/.

Klippenstein, Ken. “White Supremacists, Conspiracy Theorists Are Targeting Cell Towers, Police Warn.” *The Intercept,* March 17, 2021.

https://theintercept.com/2021/03/17/5g-white-supremacists-conspiracy-theorists-critical-infrastructure/.

Morales, Jowi. 2022. "How SMS and MMS Gave Birth to Instant Mobile Messaging." MakeUseOf. https://www.makeuseof.com/sms-mms-instant-mobile-messaging-history/.

Privacy Tools. n.d. "Apple's iMessage Service and Privacy - Privacy Guides." PrivacyTools.io. Accessed April 25, 2024. https://www.privacytools.io/guides/apple-s-imessage-service-and-privacy.

Qualcomm. "What is 5g?" Qualcomm. Accessed April 25, 2024. https://www.qualcomm.com/5g/what-is-5g.

TransNexus. n.d. "Understanding STIR/SHAKEN." TransNexus. Accessed April 25, 2024. https://transnexus.com/whitepapers/understanding-stir-shaken/.

Whitney, Lance. "iOS vs Android Market Share: Do More People have iPhones or Android Phones?" *TechRepublic,* June 29, 2023. https://www.techrepublic.com/article/ios-vs-android-market-share/.

YouMail. 2017. "PR Newswire." Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index. https://www.prnewswire.com/news-releases/americans-hit-by-just-under-46-billion-robocalls-in-2020-says-youmail-robocall-index-301215139.html.