Alex Banning
November 16, 2024
University of Washington, Bothell
CSS 545 – Mobile Computing
HW4 – Advanced Topics

Signaling System Number 7 Vulnerabilities: The Impacts to Mobile Device Users and Potential Solutions to Safeguard Mobile Networks and Users

I. Introduction and Background Information

Signaling System Number 7 (hereafter referred to as SS7) is a signaling and communication management protocol developed in the 1970s to handle telephone traffic. During its initial design, SS7 was built upon a foundation of trust between telecommunications providers that, at the time, were all national and multi-national corporations and governments with regulations and agreements; this trust-based closed system was known as the "walled garden" paradigm because all the access points to the network were innately considered safe due to the trust of the operators involved [1] [3]. As the number of phones and services required increase, however, growth of the signaling protocols and network service providers have led to some issues, namely: rapid increase of actors in the telecommunications sector to accommodate mobile calls has created numerous new entry points into the SS7 network, dismantling the safety of the "walled garden" paradigm; extensions to SS7 like SIGTRAN (SS7 over IP) have created a connection from IP networks to the signaling network, further increasing the attack surface area of the SS7 network [2].

In a recent video by Veritasium (Derek Muller) on YouTube, the vulnerabilities of this protocol were demonstrated by intercepting phone calls and text messages of his target Linus Sebastian of LinusTechTips (video link can be found in References section for more information). Muller reveals to Sebastian that all that is required to perform this hack is a victim's phone number and access to an SS7 network, which can be bought for a couple thousand dollars on the black market or stolen from one of the numerous bad or lax actors in the telecom sector that have popped up out of increased service and network demand [2] [3] [4]. In addition to phone tapping and SMS interception, SS7 hackers can also trace a victim's geolocation and send Unstructured Supplementary Service Data (USSD) commands to billable numbers, among other attacks [1].

These vulnerabilities are extremely dangerous to the privacy and security of mobile cellular users. Any mobile phone still running on 3G and earlier networks are at risk of being entirely exposed by this threat, and even though phones on 4G LTE and 5G networks have updated to newer, more security-focused protocols like Diameter, they still utilize SS7 indirectly and are at risk [3]. The vulnerabilities of the outdated and insecure SS7 protocol and by extension the entire global cellular network require immediate attention and regulation, and until then, software developers need to adjust their practices to mitigate the risk to their users. In this paper, I will outline the current industry trends and needs surrounding the security of SS7 networks, solutions that are currently implemented to detect, prevent, and respond to SS7 attacks, and propose solutions both for long-term restructuring of cellular networks as well as development practices that mitigate the risk of SS7 attacks in the interim.

II. Industry Trends and Needs Regarding SS7 and Possible Solutions

i. Messaging Protocols

The introduction and adoption of Rich Communication Services (RCS) in modern cell phones is a step in the right direction regarding SS7 vulnerabilities; it is projected that by 2026, half of operational mobile devices will be using the new messaging protocol to replace SMS [5]; however, because SMS is still the default fallback option – when no mobile data networks are available to a user – an SS7 attack in conjunction with a DoS attack or using SS7 to block signal pathways for RCS could force a victim's device into the fallback SMS option. To address this issue, the industry needs to develop extensions to the SMS protocols – potentially encrypted services or other security techniques to at least make the retrieval of raw SMS data (which is currently unencrypted) more difficult and time-consuming — or, preferably, overhaul the SMS protocol completely. Alternatively, moving entirely to RCS with no fallback or some quasi-RCS/SMS hybrid that can be transmitted over existing telephone infrastructure without the serious security concerns of transporting unencrypted data provide possible paths forward while the infrastructure is updated to support a secure global communications network.

One significant downside of the destruction of the SMS protocol is that SMS works for every device connected to a cellular network. The universality of this protocol is what made it great, but I believe that the security concerns of transporting sensitive information via an unencrypted channel now outweigh the need for that functionality, and paired with the large increase in internet-capable mobile devices (smartphones and cellular tablets) and the ubiquity of mobile data networks in the modern world, more secure solutions over IP can be implemented. One could argue that this change negatively impacts rural cellular users, where data networks are sparse, and disproportionately benefits urban and suburban users, but I believe solutions like Starlink could help tackle this problem by providing data network accessibility to remote users that currently rely on 2G and 3G towers.

ii. Network Growth and Convergence

The massive growth in availability and popularity of mobile devices on a global scale has hastened the process of expanding cellular networks and extending the functionality of SS7 protocols, but this has occurred with little concern to user security. Because of this rapid growth of cellular networks and technological advancements with internet-connected mobile devices, there has been a convergence between cellular service networks (circuit-switched telephone networks) and data networks (packet-switched IP networks) [3]. This process of slow addition of features and functionality being built on top of legacy SS7 networks is why this problem is so large to tackle now. A complete overhaul of the global cellular network with new infrastructure, protocols, and regulations is required to completely fix the problem, and to accomplish this on a global scale translates to billions or trillions of dollars to fix [6]. Some telecom companies like AT&T and Verizon have started phasing out their 2G and 3G networks in favor of modern 4G LTE and 5G networks [7], but it's slow, and there's little incentive to upgrade on a global scale as a telecom provider because of the immense cost and lack of government regulation requiring such a change. Additionally, some mobile operators are not obligated to follow US law regarding telecom services, and the pushback from users on older mobile devices overseas could be contributing to the problem. Furthermore, some people, like Edward Snowden, claim US government agencies are actively using these exploits to conduct surveillance and investigations, and that is another driving force for the lack of regulation in this matter [2]. Finally, public SOS services like severe weather alerts and other public notification systems rely on SMS protocols, and overhauling the entire public alert system is a massive undertaking as well and contributes to de-incentivizing change.

Ultimately, the potential benefits of updating the global cellular network system to rely more on IP data networks – which are more scalable and secure, and planning to scale for the future far outweigh the cost. The current strategy of simply adding more of the existing infrastructure is purely to meet the growing demand, but it is not good engineering practice, nor is it safe for customers to use, and as the number of entry points into the SS7 network continues to grow with more devices, the ability to prevent hackers from gaining access becomes exponentially more difficult.

iii. 2FA Considerations

The most glaringly obvious trend in mobile computing that is affected by the SS7 vulnerabilities is the use of SMS to deliver One-Time Password (OTP) codes as a method of 2FA. Many banking, personal finance, email, and other apps that contain sensitive information may still allow SMS or Phone Call verification as a valid authenticator. Due to the insecurity of the SS7 network, this is a massive problem. If a phone has been compromised due to this SS7 exploit, hackers can instantly gain access to text or call 2FA forms, and they can even intercept the message then pass it on, so the victim is none-the-wiser [2]. Gaining access to a victim's personal banking information is one of the most desirable outcomes of SS7 attacks, so these 2FA methods should be considered insecure and utterly useless as a form of security in those cases, and for people in positions of power or of significant financial means that are at higher risk of being targeted, these verification methods should be considered unsafe in *all* cases.

Although SMS or call 2FA methods are super fast and user-friendly, if they are insecure channels prone to simple attacks, then they are not serving the purpose of an authentication tool, and even though the process of using 2FA would be made slightly more difficult for the user – like setting up an authenticator app – the benefit of securing an account makes it worthwhile.

III. Current Network Solutions and Recommendations for Developers

Mobile network operators have attempted to implement safeguards against SS7 vulnerabilities by reconfiguring network devices with more security in mind like SMS Home Routing solutions and SS7 perimeter firewalls. This can protect against more basic SS7 attacks but fails against sneakier approaches (I recommend reading about this from the source, as it is quite complex and beyond the scope of this paper to discuss here) [2]. Ultimately, if the hacker is skilled enough and knowledgeable enough in the makeup of data in transmitted signaling messages over SS7 and has access to the network, it takes exceedingly more skill to configure a firewall that can detect the presence of a malefactor in the network in time to make a difference, especially in the case of spoofing a legitimate message from a bank, getting the user to login, receiving a 2FA code, and intercepting it without requiring a victim to click a link like in traditional phishing attempts. Constant monitoring of network resources, infrastructure, and smart algorithms to determine where users are attempting to connect from while spoofing legitimate mobile subscribers are all necessary components in securing the perimeter of the SS7 network [2], but these methods and constant need for oversight require time, resources, and money. Some network operators have begun implementing AI solutions for the monitoring portion of this, but AI models still need constant re-training, fine tuning, review processes, and other time-consuming efforts to be considered truly secure with sensitive information and constantly evolving attacks.

If mobile operators are doing everything correctly in securing their networks and hackers are still getting in, then what is the next best thing to do while patiently waiting for government intervention and regulation? As software developers, we have a responsibility to reasonably protect our users from harm. Therefore, I am recommending that in the case of creating authentication functionality in any apps or software to never use SMS or phone calls as a 2FA method. If possible, use authenticator apps, physical tokens, generated keys that expire on a timer, or other more secure methods to verify a user's identity. In terms of moving forward with the overhaul of the global communications network, I am confident in saying we are headed in that direction due to the scalability of IP networks and the introduction of modern 5G networks, but there are still so many dependencies on the legacy SS7 networks that need to be abandoned to fully adopt a secure global telecom infrastructure.

Although it is slightly annoying for users to setup an authenticator app or use other forms of 2FA compared to the fast and easy SMS or phone call, it is a far more secure option that will benefit the user in the long run.

IV. Conclusion

SS7 is an outdated protocol that has overstayed its welcome. In the modern world, where globalization and worldwide access to the internet has made internet-connected mobile devices ubiquitous, security is now of the utmost importance, and the legacy infrastructure from the 1970s simply did not account for the global scale of telecoms today. Because of the lack of security safeguards in SS7 networks and continued reliance on the legacy networks and protocols for public services and fallback communications options on modern devices, every mobile device user on the planet is at risk. To mitigate SS7 attack surface area, all mobile network operators need to configure and continuously monitor firewalls on the perimeter of SS7 networks, and if abnormalities occur, they need to be dealt with swiftly and prevented in the future. Furthermore, if bad actors are discovered selling access to SS7 they must be dealt with seriously, as the potential risk of government-backed hacking groups exploiting these vulnerabilities and causing irreparable damage is significant. Until the global communications networks that currently rely on SS7 are overhauled, this will always be a potential threat.

In the interim, developers need to be wary of how their user's information can be used and exploited. 2FA verification must not include SMS or Phone Call options and ideally should be an authentication services that is tracked, monitored, and regulated (Microsoft or Google Authenticator). Ultimately, it is imperative that world governments and mobile network providers abandon the old systems and create something new, scalable, and secure and the best way to accomplish that goal is to highlight the glaring security concerns of the old and advocate for positive change in security practices in the telecoms industry. In a globalized modern world with billions of mobile devices and hundreds of thousands of network entry points, security must scale with service. If not, it's only a matter of time before it all comes crashing down.

V. References

[1] G. Redmill, "An Introduction to SS7," Internal Report, Brooktrout Technology, Needham, MA, July 2001. [Online]. Available: http://mirror.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/physical/ss7/brooktrout_into_to_ss7.pdf

[2] S. Puzankov, "Stealthy SS7 Attacks," in Journal of ICT Standardization, vol. 5, no. 1, pp. 39-52, 2017, doi: 10.13052/jicts2245-800X.512. [Online] https://ieeexplore.ieee.org/abstract/document/10255424

[3] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash and H. Abbas, "SS7 Vulnerabilities—A Survey and Implementation of Machine Learning vs Rule Based Filtering for Detection of SS7 Network Attacks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1337-1371, Secondquarter 2020, doi: 10.1109/COMST.2020.2971757. [Online] https://ieeexplore.ieee.org/abstract/document/8984216

[4] Veritasium, "Exposing The Flaw In Our Phone System," *YouTube*, Sep. 21, 2024. [Online] https://www.youtube.com/watch?v=wVyu7NB7W6Y

[5] S. McCaskill, "Nearly half of phones will use RCS by 2026," *TechRadar*, Feb. 02, 2022. [Online] https://www.techradar.com/news/nearly-half-of-phones-will-use-rcs-by-2026 (accessed Nov. 17, 2024).

[6] "Here's how much a 5G wireless network really costs," *Lightreading.com*, 2021. [Online] https://www.lightreading.com/open-ran/here-s-how-much-a-5g-wireless-network-really-costs (accessed Nov. 17, 2024).

[7] "I think there's a growing acceptance that SS7 is a protocol from the past. It's ... | Hacker News," *Ycombinator.com*, 2021. [Online] https://news.ycombinator.com/item?id=25903786 (accessed Nov. 17, 2024).