GSM CRACKING

Partner I, Partner II, Partner III, legacv, Partner IV, Partner V

Abstract—A5/1 is an algorithm used to encrypt GSM traffic, especially in phones, to ensure communication such as calls and texts between end users is secure. The A5/1 cryptographic algorithm was developed in 1987 and then accepted for use as the algorithm for GSM communications in Europe and the United States of America, with A5/2 (a significantly weaker version of A5/1) being exported for use in other countries. A5/1 was found to be vulnerable and was attacked by various hackers. The creation of rainbow tables allowed the public to easily crack GSM, which was explored in this experiment. The tools needed to accomplish this process are Airprobe, which is used to decode the GSM data frames for usage and analysis; Wireshark, which is used to visualize the GSM frames and extract necessary information from the frames; and Kraken, the open-source software tool and its utilities. Together with the necessary rainbow tables, these tools can process the data needed to crack the GSM data frames and derive the KC needed to decrypt the frames. This paper aims to discover the ease of cracking such sensitive data and determine how at risk these systems are. Bringing these types of issues to light will help increase user security over time. There needs to be more study done into ensuring these systems are updated.

Index Terms— Global System for Mobile Communications (GSM), Cryptography, Mobile Forensics, International Mobile Equipment Identity (IMEI), SIM Card

1 Introduction

THE demand for modern mobile communication and de- With the standardization of the Global System for Mobile Communications (GSM) technology, mobile devices and networks have become the medium for everyday communication and exchange. Nonetheless, concerns about the vulnerability of the GSM encryption techniques have raised the mission-critical awareness of fundamental security efforts. As the market for mobile communication for communities, governments, and organizations grows, the need to address GSM issues and vulnerabilities becomes a requirement to meet the goal. This paper provides an in-depth investigation into GSM cell phone security, covering both its inception and its destruction. Existing research is analyzed, the project's design and methodology are outlined, evaluation findings are shared, the implications for future research directions are explored.

Entering the domain of telecommunication technology, GSM pivoted the first milestone for mobile communications however the initial design originated in the 80s. GSM arose as the first standard for mobile communication beginning in the European Union to centralize communication across borders. The standard's popularity skyrocketed, as it was robust and scalable compared to other telecommunication mediums during the era.

In this paper, the Broadcast Control Channel (BCCH) is exploited within a controlled environment called a sandbox to simulate the interception of GSM signals and messages. Once intercepted, the hashes correlating to the signal or message sent are loaded into the Unix-based tool Kraken. Kraken utilizes rainbow tables, powerful cryptography tools which enable threat actors to decode keys from the signal source. Finally, the decrypted keys are used to decrypt and access the data being sent.

2 Related Work

In order to effectively discuss GSM technology and the A5/1 cryptographic algorithm it depends upon, as well as methods of cracking it, previous work in the field must be studied. The A5/1 cryptographic algorithm was developed in 1987 and then accepted for use as the algorithm for GSM communications in Europe and the United States of America, with A5/2 (a significantly weaker version of A5/1) being exported for use in other countries [1]. It was originally kept secret by its developers, but in 1999, Marc Briceno, Ian Goldberg, and David Wagner published “A pedagogical implementation of A5/1” [2] which essentially reverse-engineered the algorithm and provided a block of code that made the A5/1 algorithm free-to-use by all. Though A5/1 was strong, it was not strong enough; in 2000, Eli Biham and Orr Dunkelman of the Israel Institute of Technology published a paper entitled “Cryptanalysis of the A5/1 GSM Stream Cipher,” which effectively cracked the cipher “with total work complexity 239.91 of A5/1 clockings, given 220.8 known plaintext” [3]. Their diagram explaining the structure of A5/1 can be seen in Figure 1. Other methods of cracking the cipher (and, by extension, GSM communications) ensued; these can be seen in the form of online articles, blogs, and videos from students and independent researchers making the effort to capture GSM traffic and crack it using rainbow tables. The concept of a “rainbow table” originated in 2003 after a researcher, Philippe Oechslin, wanted to improve upon the original time-memory trade-off used to efficiently crack keystreams developed by Martin Hellman of the Diffie-Hellman key exchange [4]. It is a table of hashes that have been pre-computed and are used to compare a certain key against, so that an attacker can save both time and computing power by simply looking up a hash rather than creating and computing one in real time. A paper published

in 2012 by Maria Kalenderi, Dionisios Pnevmatikatos, Ioannis Papaefstathiou, and Charalampos Manifavas titled “Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-End FPGAS,” though possibly not the first of its kind, serves to propose a method by which Oechslin’s rainbow tables can be used to crack A5/1 encryption [4]. Their depiction of a rainbow table can be seen in Figure 2. This project relies on the work done by these researchers and independent bloggers and students that published their methods on the wider Internet [8-10].

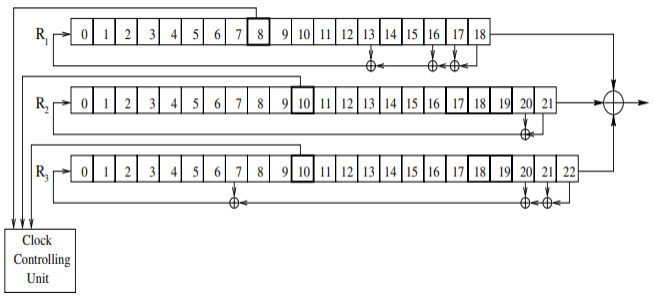

Figure 1: A5/1, as drawn by Biham and Dunkelman [3]

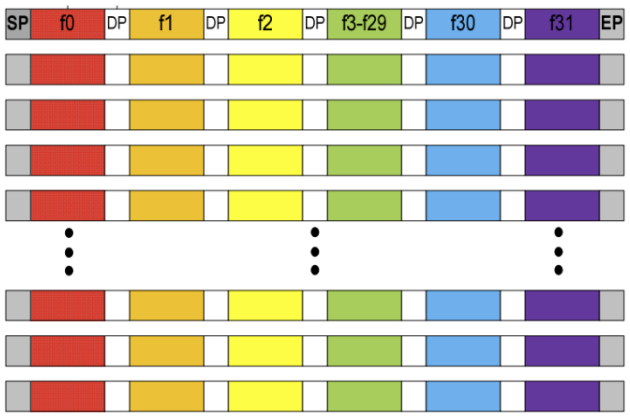

Figure 2: The structure of a rainbow table [4]

3 Project Design

The below figure is a brief overview of the GSM network. It begins with the mobile system, or phone that communicates with the cell tower. This is done on two separate uplink and downlink bands 45 megahertz apart. This requires separate receivers to capture both uplink and downlink traffic. This project, however, is limited to sniffing a single frequency. Therefore, the cellular receiver is to be put on the downlink band to record the traffic coming from the tower to the phone. Once a connection with the tower is established, the data gets forwarded to a Mobile Switching Center (MSC) that then authenticates the phone through a Home Location Record. This project will take the data recorded and crack the encryption.

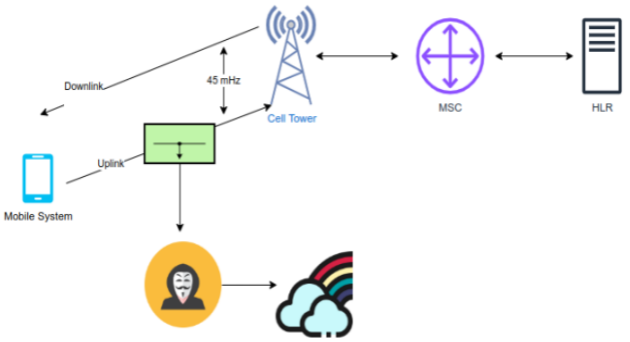

Figure 3: GSM network diagram

The project design was constructed so that the environment would be sandboxed. The GSM capture data file used was acquired with permission from the owner and did not contain any sensitive data. The set up and tools utilized to derive the KC (Key Cipher) used to decrypt the GSM data will be described below. The tools needed to accomplish this process are airprobe, which is used to decode the GSM data frames for usage and analysis. Wireshark, which is used to visualize the GSM frames and extract necessary information from the frames and finally Kraken the open-source software tool and its utilities together with the necessary rainbow table to process the data needed to crack the GSM data frames and derive the KC needed to decrypt the frames. The first step in cracking the GSM data is to use airprobe to decode the BCCH (broadcast control channel) these frames will reveal the different transmissions currently present in the capture file. From this one can find the appropriate allocation on time slot of the transmission in which the KC is attempting to be found for. The next step is to use Airprobe to decode the GSM SDDCH (Standalone Dedicated Control Channel) data on the specified time slot. The SDDCH is responsible for call establishment and other critical functions for the transmission between the mobile device and network infrastructure. With the decoded output of the transmission the KC is being found for, Wireshark can be used to confirm that the Data Frames are using A5/1 encryption. This is the version of the A5 encryption capable of being cracked by Kraken. A5/0 indicates no encryption and A5/3 cannot be cracked using the method detailed in this paper. Confirming A5/1 encryption algorithm is being used, one can proceed to output the bursts of frames with Airprobe to a text file for further processing. 2 frames will need to be used. The first is an unencrypted LAPdm frame, the second an encrypted LAPdm frame. A guess is able to me made to what the encrypted LAPdm frame is given the reasoning that these are sent every 100 frames. This leads us to conclude that upon finding an unencrypted LAPdm frame the next frame at offset 100 is likely to be the encrypted LAPdm frame. Having acquired the LAPdm frame bursts in their binary format, the encrypted frame bursts can be XORed with the unencrypted frame bursts. After having derived the XORed bursts these can then be inputted into Kraken which will attempt to crack the bursts as one of them will

be the crackable key stream needed to derive the KC that will be used to decrypt the GSM frames. With the found key provided by Kraken it is now possible to regenerate the KC by using the Kraken utility find_kc binary included in the utilities folder of the tool. Providing find_kc with the key found by kraken, its bit position in the burst, the previous unencrypted LAPdm unencrypted burst, the previous LAPdm encrypted burst and the previous XORed burst find_kc can regenerate KC. With the KC now found Wireshark or other tools can be used to easily decrypt and visualize the GSM data being captured.

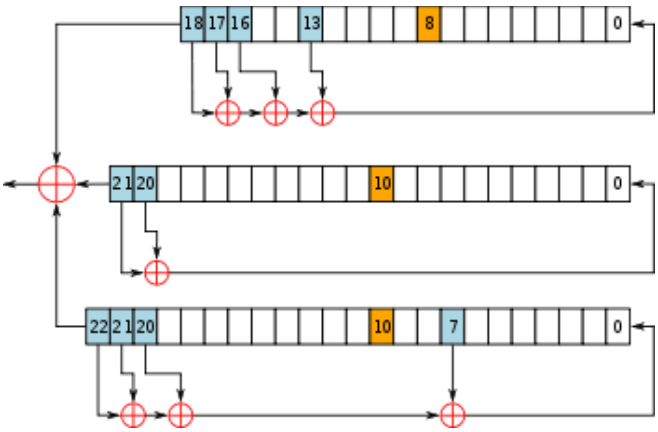

Figure 4: A5/1 Stream Cipher Algorithm

4 Evaluation

The figure below shows the resulting captured data. Given the scope of cracking non-hopping, single-band traffic, the project was a success. The complete plaintext data has been exposed and viewed in a common network analysis tool Wireshark. Overall, once the data has been captured the amount of time to crack the capture is around thirty minutes. The tools used here are also free and open source which adds to the availability of this exploit. Additionally, the cheap cost of the sniffing devices allows for easy exploitation of this vulnerability.

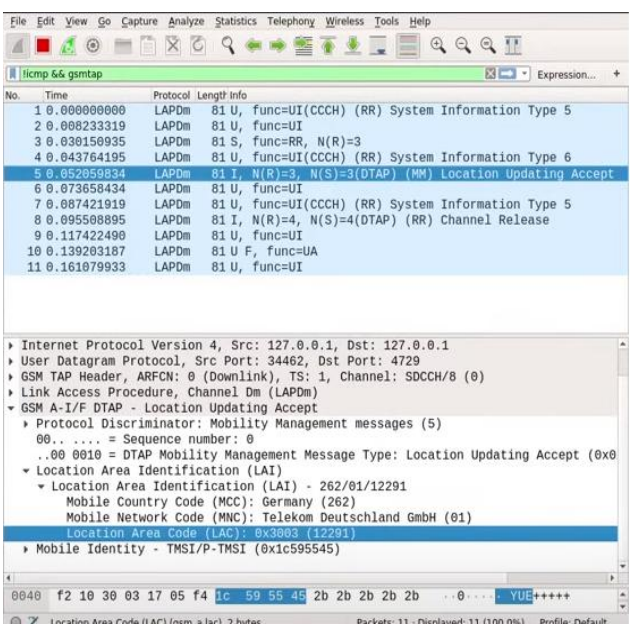

Figure 5: Decrypted Network Traffic

This is of critical importance for both the telecommunications sector and the end user. For the communication provider, they can no longer assume secure communications on legacy GSM connections, which results in the requirement of new networking protocols. This, largely, is not the protocol used on most phones of the past ten years, but now legacy mobile systems need to be reevaluated and new security controls applied. This highlights the security issues that arise in encryption with a known plaintext attack and the lack of forward secrecy. Furthermore, this project highlights the necessity of modern encryption algorithms to implement forward secrecy due to the triviality of cracking old encryption systems. The more robust A5/3 algorithm is constructed similarly and may be vulnerable to a similar style of attack. This demonstrates the importance and effect of one cracked encryption system. Other systems use the same style of algorithm, and the vulnerability may be applied to other crypto systems.

5 Discussion

Several challenges exist that further confound the confidentiality of GSM communications. The nature of this study exploited a man-in-the-middle attack. This vulnerability arose in GSM networks as the user does not authenticate the network, but the network authenticates the user. Authenticating both parties was considered unnecessary due to the preconceived notion that acquiring the hardware to mimic a BTS (Base Transceiver Station) would be costly, so improbable. It should also be noted that encryption only exists between the mobile device and the BTS station, and not between other parts of the network such as between the BTS and the Base Station Controller (BSC). This further facilitates the ease of man-in-the-middle attacks. This flaw in GSM security can be described as short-range encryption. Another flaw corresponds directly to the nature of the cryptographic algorithms used. The GSM network typically uses the A5/2 and A5/1 algorithms. Both ciphers use a form of Linear Feedback Shift Registers (LFSR). The source code for the former was leaked and proved to be the downfall of the A5/2 cipher. The A5/1 cipher proved easily crackable by powerful computers due to the shortness of the key used.

In order to ameliorate the GSM service, end-to-end encryption using a secure cryptographic algorithm is most important. This requires no change in hardware, but only that the right ciphers be used. The A5/3 cipher is the successor to the A5/1 cipher and is significantly more secure. Finally, to prevent the attacker from spoofing the identity of a BTS tower and disabling encryption, both the device and the tower should program each other.

6 Future Works

Even though GSM has been supplanted by many new technologies in general, there remains some less important services that use GSM. GSM is still relied on services in less developed regions, particularly where upgrading for small and remote communities is not cost effective. GSM is also used as a fallback network in areas where network congestion renders more modern networks unavailable temporarily. Additionally, it supports a small number of Internet of Things (IoT) devices such as electrical and water meters at remote wind, and solar farms. Following that, dedicated or nation-state actors could turn to electrical infrastructure as an attack vector in the future, which could cripple industrial-scale electric systems across a country. As such, understanding this research can further be broadened to include exploring the use and vulnerabilities these GSM networks. Specifically, future research could explore vulnerabilities relating to manipulating data between the sender and the BTS. This can be preceded by attempting to observe and assess the impact of replay attacks.

7 Conclusion

A sandbox was used for implementing rainbow tables aimed at cracking the A5/1 algorithm. Airprobe was used to decode the captured file to extract the frame bursts. These frame bursts were then cracked through Kraken and the downloaded rainbow tables. Each GSM frame is a collection of 8 bursts in a binary format. Once the frames were cracked, a key was extracted which allowed one to see the decoded frames on Wireshark. The frames were successfully decoded and understood. At the time, GSM was revolutionary as it was a major advancement in technology. Though, these findings have shown how easy it is to decode sensitive information such as SMS (Short Message Service), which are used very heavily. Anyone's private messages can be looked at by anyone, making them public. Voice calls which also use GSM are made public as well. GSM is not secure and poses a major security threat. GSM is still heavily used especially for SMS, more research and policies need to be put in place to secure the data of users. GSM should not be used for private information and users should not be told their information is secure when this is very far from the case.

Acknowledgment

The authors wish to thank the professor and TA.

References

[1] M. Briceno, I. Goldberg, and D. Wagner, “A pedagogical implementation of the GSM A5/1 and A5/2 ‘voice privacy’ encryption algorithms.,” 1999. http://www.mirrors.wiretapped.net/security/cryptography/algorithms/gsm/a5-1-2.c (accessed Apr. 19, 2024).

[2] M. Briceno, D. Wagner, and I. Goldberg, “A pedagogical implementation of A5/1.,” 1999. https://mtlin.org/article/a51.html (accessed Apr. 19, 2024).

[3] E. Biham and O. Dunkelman. “Cryptanalysis of the A5/1 GSM Stream Cipher.” 2000. In: Roy, B., Okamoto, E. (eds) Progress in Cryptology —INDOCRYPT 2000. INDOCRYPT 2000. Lecture Notes in Computer Science, vol 1977. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44495-5_5

[4] M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou and C. Manifavas, "Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAS," 22nd International Conference on Field Programmable Logic and Applications (FPL), Oslo, Norway, 2012, pp. 747-753, doi: 10.1109/FPL.2012.6339146.

[5] S. Gold, “Cracking GSM,” Network Security, vol. 2011, no. 4. Mark Allen Group, pp. 12–15, Apr. 2011. doi: 10.1016/s1353-4858(11)70039-3.

[6] B. Rose, “Is GSM still in use today, or has it been replaced by newer technologies?,” *Medium*, Sep. 22, 2023. https://medium.com/@Breadarose/is-gsm-still-in-use-today-or-has-it-been-replaced-by-newer-technologies-5c8fe3f201b3 (accessed Apr. 20, 2024).

[7] M. Toorani and A. Beheshti, “Solutions to the GSM Security Weaknesses †,” pp. 576–581, 2008, doi: https://doi.org/10.1109/NGMAST.2008.88]

[8] “Cracking GSM With RTL-SDR For Thirty Dollars,” Hackaday, Oct. 22, 2013. https://hackaday.com/2013/10/22/cracking-gsm-with-rtl-sdr-for-thirty-dollars/ (accessed Apr. 20, 2024).

[9] “The big GSM write-up - how to capture, analyze and crack GSM?,” Romanian Security Team, Oct. 24, 2013. https://rstforums.com/forum/topic/71485-the-big-gsm-write-up-how-to-capture-analyze-and-crack-gsm/ (accessed Apr. 20, 2024).

[10] P. Krysik, “ptrkrysik/gr-gsm,” GitHub, Apr. 17, 2024. https://github.com/ptrkrysik/gr-gsm (accessed Apr. 20, 2024).