SecurityGen

Telecom Security. Transcending Generations.

SS7: Protection Bypass Using Variable Length XUDT on SCCP Layer

Introduction

The SS7 (Signaling System No. 7) stack, which is a set of telecommunication protocols used for call setup, routing, and other functions in the global public switched telephone network (PSTN), has been widely adopted for decades. However, with the rise of digital communication and the increased reliance on interconnected networks, it has become evident that the SS7 stack architecture has certain flaws that can be exploited by hackers and other malefactors. Threats from malicious actors using the SS7 network for attacks are critical for both businesses and individuals. We frequently encounter reports in the media about real-life incidents such as location tracking of private individuals and officials, phishing SMS delivery, theft of one-time authentication passwords, call redirection, and other genuinely dangerous attacks. One key advantage for intruders in these types of attacks is the absence of a broad list of hardware and software requirements - merely connecting to the SS7 signaling network and having a set of scripts is sufficient for most attacks. Therefore, it is crucial for subscribers to understand that in this case, only the mobile network operator can ensure security.

In order to combat these threats, mobile operators use a wide range of auxiliary tools, such as home routers, firewalls, and "smart" STPs. However, these protective technologies often do not cover all possible signaling messages and deviations from the 3GPP/GSMA standards and recommendations.

Security Bypass Techniques

As mentioned above, a communication operator's network is usually protected by one or more security measures (home router, SS7 firewall, or "smart" STP). However, even when all these components are in place, the network can still be vulnerable to attacks if one or a combination of previously unknown techniques are exploited to bypass the security measures.

As part of our SS7 operator network security audits, we regularly test all known security bypass techniques, typically installed at the network's border with roaming networks.

Here is a list of the main techniques for bypassing security measures that are most often exploited in operator networks:

- **Parameter manipulation of the Called Address**
  With this technique, a malicious actor tries to find errors in routing tables by directing signal traffic directly to the target node, bypassing the firewall.
- **Parameter manipulation of the Calling Address**
  In this technique, the attacker also tries to find a weak spot in the routing table by substituting an unexpected role for the traffic source.

- **Message segmentation via SCCP XUDT**
  In this case, the attacker tries to make the request unreadable so that the firewall considers it an unrecognized message and hands over the decision to the destination node.
- **Abnormal Application Context Name**
  The attacker intentionally distorts the values of “insignificant” fields so that security tools stop inspecting the signaling message and push it into the network.
- **Global OpCode**
  The attacker exploits an addition to the standard that is not used in practice but must be supported by equipment vendors.
- **Abnormal handshake**
  The attacker uses an SMS anti-spam technique to deliver an illegitimate request to the target node and exploits bugs in the software of that node to execute the sent request.
- **Double MAP**
  In this case, the attacker forms the request in such a way that the first component looks like a completely legitimate message, while all the malicious payload is contained in the second component. The first component “distracts” security measures while the second one executes the illegitimate request.

One way or another, a technique for bypassing security measures often involves a slight modification of the basic (according to the specification) signaling message. For instance, it can be a change of one or several bytes in the message that does not affect the useful payload at the application level, but makes the equipment process the traffic in a slightly non-standard way for security systems. Thus, the delivery of an illegitimate signaling message to the destination node is achieved, and the message will be processed as legitimate traffic.

In the course of our research, we constantly try new ideas that will help us discover certain ways to bypass security systems. If successful, we begin to apply such a method on a permanent basis, testing the networks of mobile operators.

Description of the Discovered Vulnerability

During one of the security audits of the SS7 network, we tested a communication operator’s network using already known techniques for bypassing security measures. Among them, there was one of the most common - packet segmentation at the SCCP level using XUDT.

In general, segmentation is used when transmitting large volumes of data, with a maximum number of segments up to 16. Segmentation is only possible using the XUDT type, and the algorithm for selecting the segment length is left to the choice of equipment vendors and is not strictly standardized.

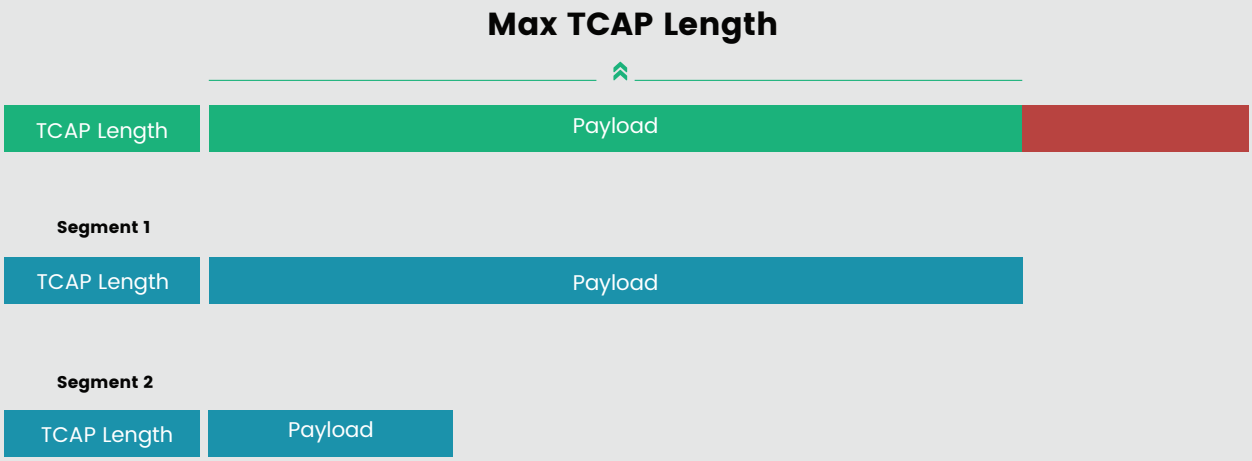

Figure 1. Message Segmentation using SCCP XUDT

If the payload size exceeds the maximum allowable size of the upper layer (TCAP), the payload is divided into multiple segments, each of which is delivered in a separate signaling message. The message segmentation and reassembly mechanism is implemented by the SCCP layer in XUDT messages. In some operators' networks, the use of message segmentation at the SCCP XUDT level allows bypassing security measures.

The XUDT packet length indicator is optional, which is probably why the equipment (protection) does not always correctly process multiple received packets. However, the destination node usually correctly matches the sequence and forwards the response to the roaming SS7 network.

Recently, more and more telecom operators are installing security measures that can effectively handle segmented messages and successfully filter them in case of an attack. However, during our testing, we were able to discover additional opportunities for using this bypass method. We encountered the following equipment algorithm (which allows us to consider the bypass method effective):

- For various MAP operation codes specified in the message body, the bypass method works when the message is divided into segments of different lengths. Below are schematic images and an example of anonymized traffic.

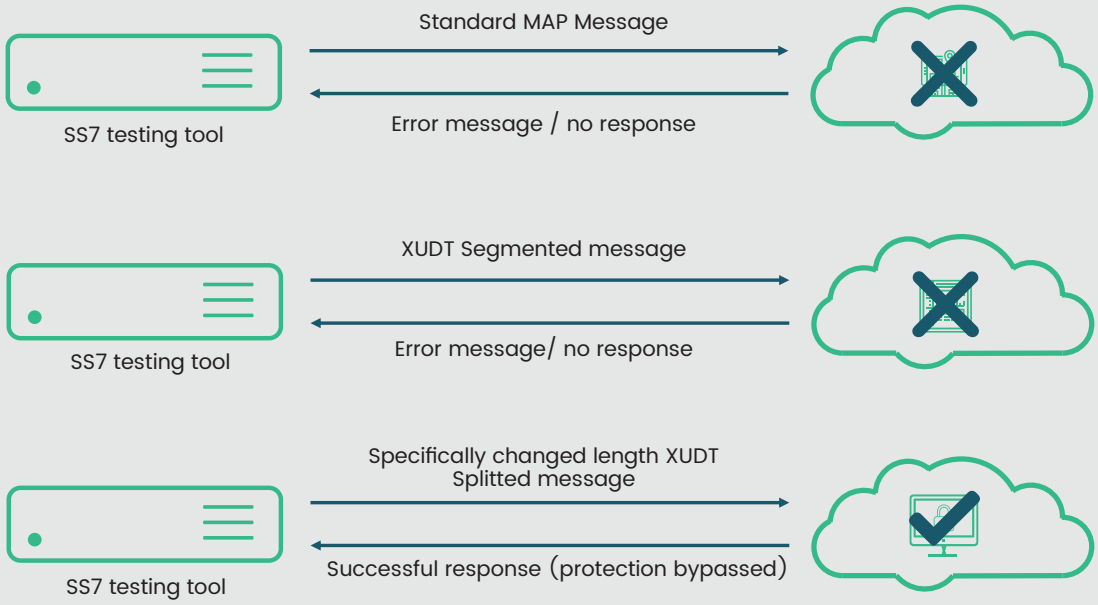

Figure 2. Protection means bypass via XUDT split message length change

As can be seen from the schematic images, attempting an attack without using XUDT segmentation or with basic segmentation resulted in the network responding with an error or ignoring the messages altogether. However, when a specific length of XUDT segment was found, the destination node received all the message segments, processed them correctly, and sent a response.

Let's take a closer look at an example on live traffic:

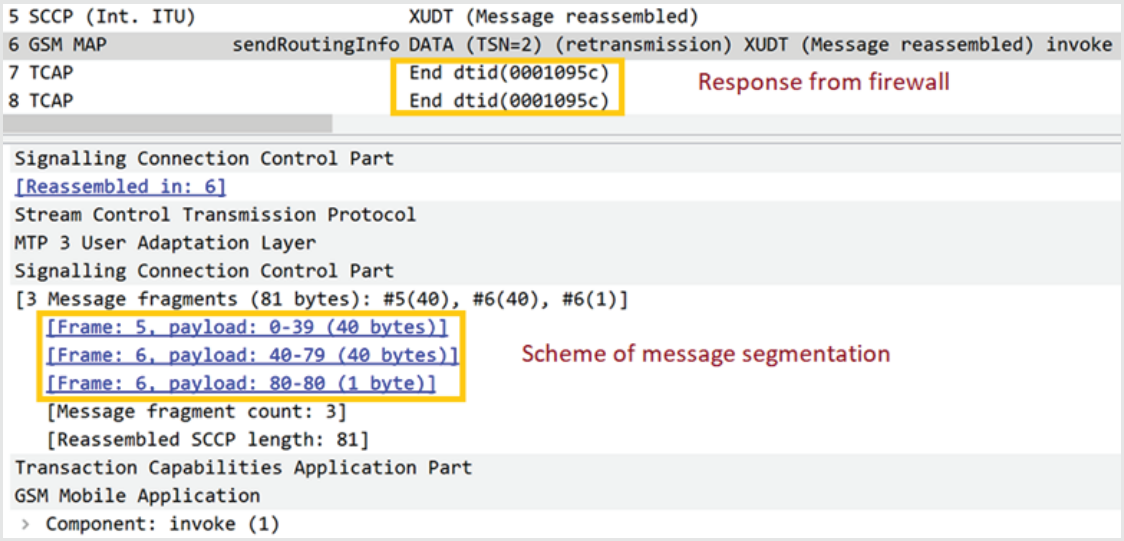

Figure 3. Attack with XUDT segmentation blocked by firewall

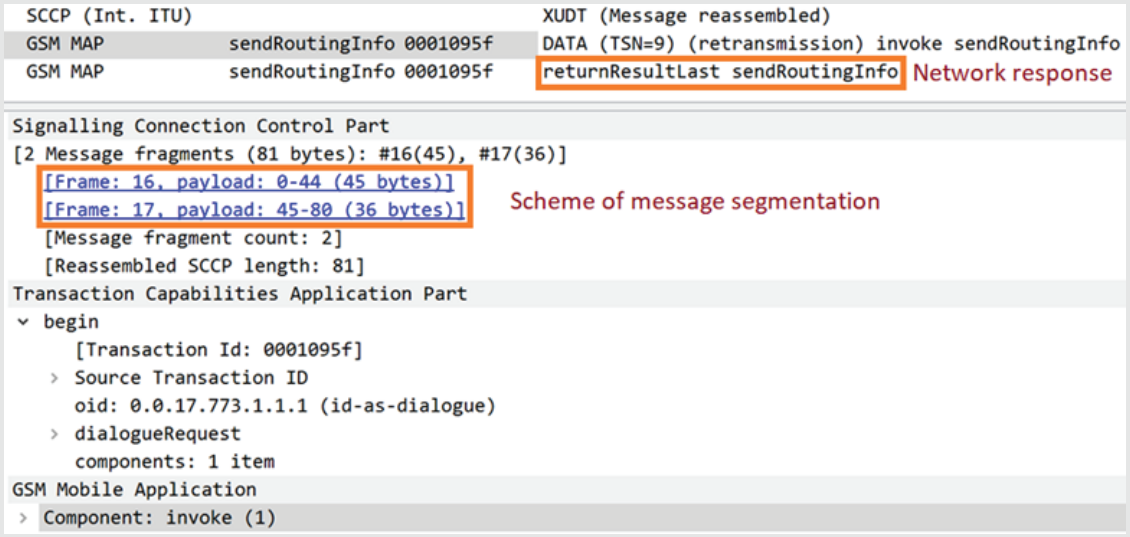

Figure 4. Attack with XUDT segmentation successfully executed

As can be seen from the two examples above (Figures 3 and 4), the segment lengths differ, and by changing this parameter, the network returns a valid response to the request. In the current instance (Figure 4), for the SendRoutingInfo operation, the network correctly processes the request with a first segment length of 45 bytes. In our work, we observed a similar pattern for other operation codes, where different segment lengths were applied.

In summary, our testing has revealed a new extension to the XUDT segmentation attack method that can bypass protection measures in some SS7 networks. By adjusting the length of XUDT segments, an attacker can exploit vulnerabilities in STP/FW and successfully execute attacks. This information should be included in standard recommendations for protecting against SS7-related attacks.

In cases where we encounter such equipment on an operator's network, we notify both the operator and the manufacturer of the signaling security tools about the vulnerability found. We do believe that every step the community takes towards ensuring signaling security and responsible implementation of the latest protection tools makes this world a little better.

Conclusion

Even though the SS7 network has been in use for several decades, vulnerabilities in it are already widely known and security measures are at a fairly mature level - nevertheless, even in 2023, new attack methods and bypassing of security measures for these networks are being discovered. Many operators, in pursuit of the latest technologies (5G), often forget about the need for close attention to legacy infrastructure, which also requires investment. Otherwise, one can build a huge and expensive new 5G network, while attacks on subscribers will still occur through such old and well-studied technologies as SS7.

Abbreviation list

Abbreviation	Description
3GPP	Third Generation Partnership Project
5G	Fifth generation of mobile networks
FW	Firewall
GSM	Global System for Mobile communication
GSMA	GSM Association
MAP	Mobile Application Part
OpCode	Operation Code
SCCP	Signaling Connection Control Part)
SMS	Short Message Service
SS7	Signaling System #7
STP	Signaling Transfer Point
TCAP	Transaction Capabilities Application Part
XUDT	Extended Unidata