SS7 Vulnerabilities

A solution to address SS7 security exposures

Signaling System #7 (SS7) networks form one of the pillars of today's successful telecommunications industry. And yet, for all its importance to enable telecommunications services, SS7 incorporates only minimal security features. Unfortunately, in the past 35 years since SS7 was introduced, the telecommunications marketplace has dramatically changed and SS7 vulnerabilities have become more exposed. Ribbon Communications and its partner Cellusys have joined together to provide a solution to address SS7's security flaws.

Deployed for the past 35 years, SS7 provides signaling that enables mobile and fixed network operators to set up/tear down calls, to route text (SMS) messages, support inter-network connectivity and transparent roaming, and provide per-session information such as Caller ID. As such, SS7 is a critical part of the global telecommunications infrastructure. However, because SS7 networks were originally designed to work within an operator's trusted domain or to interwork between trusted operators, security was not a top design consideration, nor has it adequately been addressed in the intervening years. Cellusys, the signaling network security experts, have stated that a hacker's access to SS7 technical product information, SS7 protocol message generation, and to the SS7 network itself is easy and inexpensive.

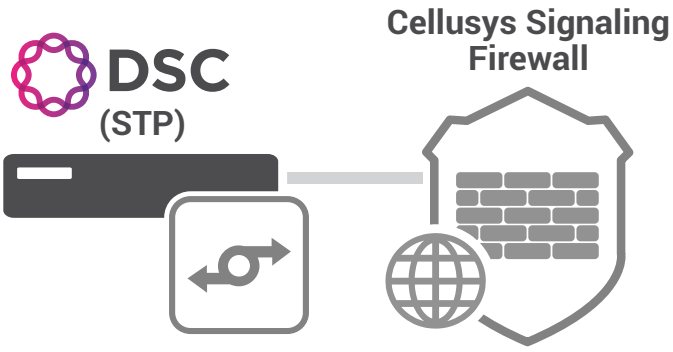
Examples of SS7 Vulnerabilities

When discussing SS7 vulnerabilities, it is easiest to group them into the following categories:

- Obtaining subscriber information
- Eavesdropping on subscriber traffic
- Financial theft
- Disruption of subscriber service

Obtaining Subscriber Information

It is possible to use legitimate functions associated with Short Message Service (SMS) to illegally gain access to a subscriber's unique identifier (International Mobile Subscriber Identity—IMSI) or to a subscriber's location (Cell ID, Mobile Country Code, Mobile Network Code, and Location Area Code). Both of these open the door to all other security threats. In addition, this information can be sold on the open market as a source of revenue.



Eavesdropping on Subscriber Traffic

There are several vulnerabilities that would allow an intruder to listen to or record a subscriber's conversation on incoming/outgoing calls, or to intercept and or modify incoming text messages to a target subscriber. In each of these attacks the intruder uses legitimate call set-up processes to establish themselves as a "man-in-the-middle" without the target subscriber having any knowledge this has occurred.

Financial Theft

The basis for these vulnerabilities is to falsely represent the target subscriber's Mobile Switching Center (MSC) in order to illegally receive SMS messages, or to request the target subscriber's current account information based on Unstructured Supplementary Service Data (USSD). Acting as the MSC, an intruder can obtain or reset subscriber account information or even request account funds transfers. For example, by redirecting SMS text messages an attacker can retrieve username and password information from a bank that uses SMS messages to reset passwords.

Disruption of Subscriber Service

This category is about vulnerabilities used to interrupt service to any subscriber or to activate / change billing, thus enabling fraudulent calls to be made from the mobile device. Both of these scenarios can cause a significant financial impact to the mobile network operator. If experienced often enough, service interruption can cause subscriber churn due to a perceived lack of service, thus reducing service revenue. Fraudulent calls which do not get paid cause network resources to be used without compensation, eventually leading to higher cost of conducting business.

What About Migration or Replacement of SS7 by Diameter Signaling?

Many people wonder why SS7 networks should even be fixed, because 4G/LTE and Diameter technologies are the fastest deployed network in telecommunication history and therefore SS7 will be displaced. Unfortunately, this is just not true. The fact remains that the vast majority of mobile customers worldwide are still served by SS7. Currently, there are 4.1+ billion mobile subscribers worldwide served by SS7 networks, which is 87% of the total mobile population. With this large population of SS7-based subscribers, it seems that the SS7 network will be with us for some time; therefore the security of the SS7 network should not be delayed.

What is the Cost of Doing Nothing?

So SS7 vulnerabilities exist, and Diameter is not yet the solution, but this has been a potential issue that has gone largely unaddressed for years, so what is the cost of doing nothing? There are both hard and soft costs. As mentioned above, service disruptions, such as theft of service and Distributed Denial of Service (DDOS) attacks, are direct revenue hits to a mobile operator. Regulatory fines, such as those levied when theft of subscriber personal information occurs, can also be quantified as hard costs. But no less important are the soft business costs that come in the form of negative media, unwanted regulatory investigations/ oversight, and loss of confidence by subscribers.

What is Needed to Stop SS7 Attacks?

While it might seem that the industry should simply define modifications to the SS7 protocol to prevent these attacks, that is not really a practical path forward. Even if standardization bodies developed new specifications for call setup, completion, and roaming, network equipment vendors would have to implement the new standards and network operators would have to upgrade all of their switches to use the new versions of software. This task would be monumental, with very high implementation costs and a deployment timeline that would surely take multiple years.

Instead, GSMA is working to identify, categorize, and propose remedies in their specification IR.82 and in updates to specifications from the GSMA Fraud and Security Group (FS.11, FS.07, IR.70, and IR.71).

One possible path forward is to add comprehensive security features to the SS7 Signaling Transfer Point (STP), which already sees every incoming/outgoing SS7 message. While this may be technically possible, it is not aligned with STP design, which is to be as efficient as possible at SS7 message routing. Even though processing power keeps increasing, by adding more comprehensive security within the STP, it may become too message-processing intensive, introducing negative effects on signaling network traffic.

A better approach would be to implement a multi-layer solution that leverage the existing security capabilities of STPs and incrementally adds Signaling Firewall capabilities to address the need for context-sensitive assessment of SS7 messages. The first step in protecting the network is to use gateway screening and statistics features on the STP to filter out many common threats and provide the data (statistics) needed for initial analysis. STP provides gateway screening, which is the definition of rules per linkset to specify which SS7 messages are allowed or disallowed to enter an operator's network. For messages where there might be some concern regarding legitimacy, the STP will forward SS7 messages to the Signaling Firewall for further assessment and analysis. The Signaling Firewall will provide context and stateful message assessment and, where necessary, return error messages to prevent information from being exposed. Figure 1 on the next page shows this multi-layer approach.

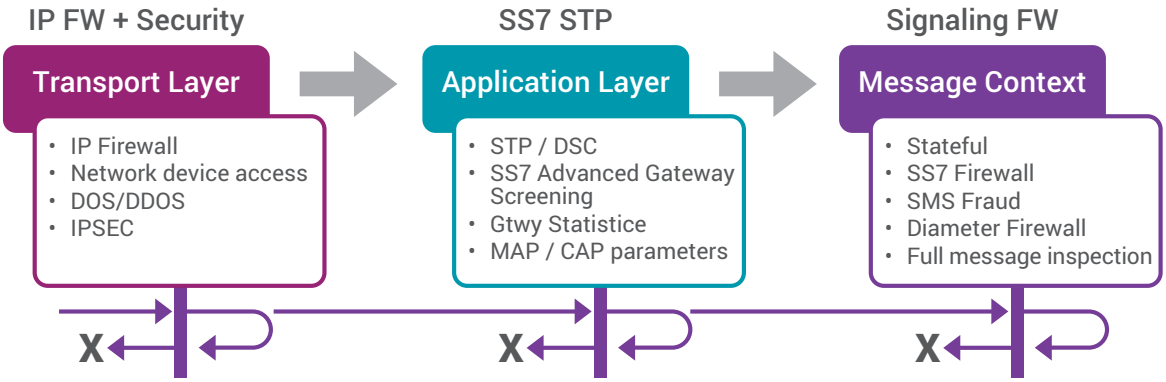


Figure 1 – Multi-layer SS7 Defense

SS7 Security Solution from Sonus and Cellusys

A multi-layer security solution as described above is available from Ribbon and its partner Cellusys. With this combination (Ribbon STP and Cellusys Signaling Firewall), a network operator gets a complete system that is context and state aware and is even capable of launching queries to the HLR to verify the context of messages. A deployment model of this joint Ribbon/Cellusys solution is shown below in Figure 2.

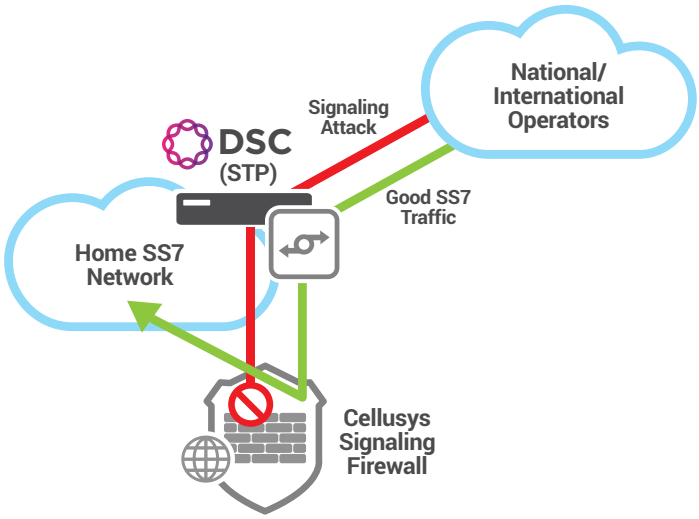


Figure 2 – Deployment of joint Ribbon/Cellusys solution

Microsoft Partner
Gold Communications

Voice
Unified Communications
Business Productivity Solutions
Midmarket Solution Provider

With communication between the two functions, the Signaling Firewall can also supply instructions to the STP so the STP can prevent certain messages from even being forwarded into the signaling network. This joint solution provides a comprehensive counter to multiple SS7 threats, supporting all related protocols—SCCP, TCAP, MAP, and CAP.

This solution is also ideal when a network operator begins their migration or transition to Diameter signaling. This is because the Ribbon STP is simply software options on the Diameter Signaling Controller (DSC), and the Cellusys Signaling Firewall supports Diameter as well as SS7 protocols. Therefore, the same security threats that would be seen in SS7 networks will already be addressable for Diameter signaling without another round of investment.

About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.

Contact Us Contact us to learn more about Ribbon solutions.