Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Texting Turns 25 but Security Concerns are Spoiling the Celebration

By: Travis Russell

One of the world's most popular forms of mobile communications, **SMS**, the technical underpinning of "text messaging," has reached a major milestone: its 25th birthday.

But don't celebrate too loudly. For all it has brought to our personal and professional lives, and despite its ubiquitous role in managing dialog between Internet of Things devices, SMS isn't entirely safe.

Security researchers have known this for years, and the telecommunications industry is now waking up to this undeniable fact. Hackers have demonstrated they can use known vulnerabilities in the SS7 and Diameter signaling system that connects mobile phone networks to re-route two-factor authentication codes wherever they like. They can also divert calls, track callers and eavesdrop on any conversation. They can read and respond to SMS (text) messages sent between phones, passing themselves off as legitimate parties to steal confidential information and money.

Until recently, these vulnerabilities were considered more of a theoretical threat. But last year, 02 Telefonica execs felt the potential for destruction when hackers intercepted SMS messages to steal access codes and drain an untold number of bank accounts across Germany.

The 02 Telefonica incident should serve as yet another wakeup call to the industry that it's time to take action to head off similar disasters related to text messaging. The well-known SS7 vulnerabilities these hackers prey on still exist in many networks, waiting to be exploited again. It's only a matter of time before that happens, which is why the National Institute of Standards and Technology (NIST) last year stopped recommending the use of SMS messages in two-factor authentication.

The top wireless providers in the world have been taking aggressive measures to protect their consumers against these attacks. Here are three places other operators should start in order to get ahead of the problem:

1. Reexamine How Text Messages are Routed Across Networks

Text messaging badly needs a security overhaul. Currently, we have clients on our phones that communicate with network servers using SS7, Diameter, or SIP, and those servers then deliver text messages on our behalf. But this system has too many holes built into it, making it too easy for hackers to spoof and too easy to compromise.

Operators, working through the 3GPP, defined Home Routing as the means for preventing SMS spoofing as well as hijacking. Yet many international networks have yet to support Home Routing (all North American operators use Home Routing).

Encryption offers another protection that the industry should be educating customers about. There are a number of encryption applications, such as Signal, Wickr, and Surespot, that provide consumers with secure voice and text messaging.

Since these messages use signaling protocols to deliver the text, and the messages have to travel through signaling routers to reach their destination, it only makes sense that security policies be implemented in the signaling routers. This means provisioning the signal transfer point (STP), the Diameter edge agent (DEA), or the session border controller (SBC) depending on the network technology. These policies can help prevent unauthorized access to home network HLRs/HSS, which are used to retrieve information about a subscriber that is later used for formulating a hijack attack. By forcing all the text messaging to route back to the home network (home routing) and then applying security policies at the gateways, operators can make life much more difficult for the hacking community.

Mobile operator trade groups, such as the GSMA, have published several guidelines for securing networks against these attacks. And governments are starting to force change through legislation, such as GDPR in Europe, which addresses not only text messaging but also communications in general.

But there are still some operators who treat this threat as more theoretical than actual and view efforts to address it as much ado about nothing. They are the weak link in the chain, and as long as there are operators out there with little to no safeguards in their networks, the vulnerabilities will persist. This mindset must change if we hope to head off more serious and widespread catastrophes in the future.

2. Think Beyond Firewalls (They’re Not That Great)

Some operators believe they can solve the rising security problem by installing standalone firewall appliances. Experts agree that this minimalistic approach is neither realistic nor effective. Traffic travels between networks through the signaling routers. As such, security is best implemented where the networks intersect, rather than in an appliance that becomes a target.

There is no such thing as a Magic Box that you can plug in to make security worries disappear. Every network is different, and each network requires custom provisioning (there is no one-size-fits-all). That’s why you really need a layered approach to security, or what security professionals refer to as “defense-in-depth.”

Operators should take a serious look at their security posture and implement countermeasures throughout the network. Not just in a box or a piece of software, but in the STP, SBC, DRA/DEA, HLR/HSS, SGSN/PGW and across every protocol stack. No network will ever be 100 percent secure, but operators can certainly make it harder for bad guys to penetrate operations by embracing a more comprehensive security approach.

3. Help Consumers Protect Themselves

There’s nothing like a good awareness campaign to address a widespread security problem and help subscribers help themselves.

Operators should start by educating their customers on the risks inherent in using SMS for two-factor authentication and recommending three-factor authentication, or other alternatives. This will be a tall order, of course, given the increasing ubiquity of SMS. So, operators should also spend considerable time and effort advising subscribers to be extremely careful about what information they choose to share via SMS. Subscribers should never, for example, provide sensitive or personally identifiable information (PII) that hackers might use to gain access to financial accounts or steal their identity. Examples of PII might include social security and driver's license numbers, passports, alien registration, or financial account numbers.

Mobile operators should also advise subscribers on the importance of being discerning about which mobile messaging apps they choose for communications. Whether subscribers choose Signal, WhatsApp, G Data Secure Chat or something else, each app has its pros and cons. This is especially true for VIPs who rely on secure communications.

No matter what operators and subscribers do, it's critical that everyone providing service or using a mobile device do his or her part to solve this security crisis. With SMS reaching its 25th year and security becoming more of a concern, the time for action is now. The industry must continue to be aggressive in addressing these concerns, or hackers everywhere will be crashing many more text messaging celebrations to come.