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

How Telecom Got Security Wrong

By: Travis Russell

The telecommunications industry needs to rethink security. The concept of trust among roaming partners has proven to be inaccurate, and the industry is now seeing evidence that trust is no longer a reasonable assumption. As service providers struggle with this breach of trust, the industry is rapidly moving to an IT-based model, with its own set of vulnerabilities.

When the industry began work on a new signaling technology a few decades ago, the intent was to eliminate the fraud and security concerns of the time. Long distance and international calling was being compromised through clever techniques such as the Captain Crunch whistle that produced a perfect 2600 Hz. Black boxes were being used to create the tones used by pay phones to signal switching systems and fool them into connecting long distance and even international calls at no charge. The answer to the problem was the elimination of in-band MF signaling, and the implementation of signaling system #7.

The new signaling technology was designed to be used in closed network architectures, and therefore today does not possess authentication mechanisms. If someone is connected to the network, that person becomes part of the closed community — a trusted partner in the telecom ecosystem.

When the industry began implementing IP as a transport in 2000, many industry experts began sounding warnings that the industry was introducing new vulnerabilities found on the Internet into the United States' critical infrastructure. These warnings were not fully heeded, mostly because connections to other networks still utilized time division multiplex (TDM) circuits, inherently secure due to the technology itself. Plus, the industry was still operating with a concept of trusted partners.

Introduction of Untrusted Partners

With wireless networks, many new types of partners, including content providers, were added. As more and more partners were added into the ecosystem, the industry lost control of any “trust” and was now allowing anyone access to critical infrastructure via an insecure technology (IP) without

extensive vetting, on a global basis.

What has come to light of late is the truth about the industry's "trusted" partners. Many have been found to be complicit in offering connections to the signaling network for a small fee, treating it as a revenue stream. This provides an easy avenue for any hacker or nation-state to gain access through the roaming ecosystem to access the control plane of any connected telecommunications network in the world.

This notion that a trusted partner would grant access to any entity for a small fee is what the industry failed to recognize. No one (this author included) believed that it would be possible to purchase network connectivity using an IP connection, and purchase the necessary network credentials along with it. This combination allows for any entity to masquerade as a legitimate roaming partner, and extract sensitive subscriber information from any network in the world.

We have seen this demonstrated many times already, but we have moved from purely theoretical and academic conjecture to reality. After more than a decade, we can now see evidence of breaches in wireless networks, utilizing exploits made possible through IP connections (such as SIGTRAN in SS7). Subscribers have had their bank accounts drained after hackers accessed their bank accounts, and intercepted two-factor authentication sent via SMS. Hackers have demonstrated the ability to track anyone's location using the control plane of the wireless roaming ecosystem. SIP spoofing continues to support a multitude of crimes, including impersonation of law enforcement agencies and the IRS. These vulnerabilities are not limited to any one technology; they are possible using any technology used to connect two networks.

Evolution to Mature Hacking Model

We have evolved from theoretical, to full-blown service offerings for location tracking and SMS/voice interception. New products utilizing the toolkits created by the hacking community have become available. Companies on the Dark Web openly advertise their capabilities as a service, providing the technical know-how to anyone wanting to exploit the telecommunications network.

One does not have to access the Dark Web to find these offerings. A simple search on Google for HLR look-ups produces a list of companies in the main stream offering the ability to search for any MSISDN, and provide their current location and status (inactive, idle, registered, etc.). We have clearly moved to a much more mature hacking model as exploits have been productized and made available to the mainstream public.

Despite all of this, the industry as a whole has not yet implemented proper network fortification in response to the varied techniques used in hacking today. Many do not take into account the motivations of a hacker, and therefore discount the purpose of many of the exploits we currently see. This is dangerous, and should be addressed by companies of all sizes.

For example, in one conversation I recently had, a network engineer was disputing the value of location tracking because the network only produced the cell ID currently serving a subscriber. This could mean the subscriber would be anywhere within a mile of the tower, which is true, but if that subscriber were a law enforcement official, or the CEO of a major corporation in the middle of an acquisition, the general vicinity could be all that is needed.

That location information also discloses the VLR currently serving the subscriber, which then becomes the target of more dangerous exploits such as redirecting text messages and voice calls, or a denial of service. This proves that as network engineers, many of us were not trained on motivations of the hacking community, or nation state activity. And many are not part of the security circles where these discussions are being had, and therefore are out of the loop.

There is a tremendous amount of work being done to identify best practices focusing on all three of the signaling technologies currently being used. SS7, Diameter, and SIP all have a number of best practices created through various standards bodies addressing the known vulnerabilities.

The GSMA Fraud and Security Group (FASG) have created a number of best practices for SS7, Diameter, and VoLTE just in the last few years. These best practices provide details on how to

identify a breach, and how to mitigate the breach. Every major wireless provider in the world is citing these best practices as they begin to look at security measures in their own networks. The hacking community has joined the GSMA sharing their most recent research, further validating these best practices.

The IETF has begun addressing the issue of SIP spoofing through the SIP Telephone Identity Revisited (STIR) working group, and has issued new protocol requirements to enable authentication of SIP identities. ATIS has produced implementation guidelines for these standards through the Signature-based Handling of Asserted information using toKENs (SHAKEN) working group. Hopefully through the work of both of these standards organizations, SIP spoofing will at least become more difficult.

NIST has provided excellent framework for implementing security in any network, used as the baseline by most organizations engaged in security discussions. This framework provides a good foundation to begin addressing security as a whole, without focusing on specific technologies or vulnerabilities.

A Distributed Approach Is Best

We should begin seeing advancements in security implementations, but sadly, this is still not the case across the board. Many have been quick to introduce a simple firewall appliance at the network edge to address SS7 or Diameter known vulnerabilities, but as some have recently discovered, this is not the answer. Simply throwing a box at the network edge is a temporary and risky proposition. Some networks have already seen outages when using this approach.

The proper approach is defense in depth. I know this may be cliché, but ask any security professional about the best security architecture, and you will find a distributed approach to be the best. This means not relying on a box at the edge, but relying on security implemented in your gateways (such as SBCs, STPs, and DEAs). This means security implemented in the HLR and HSS, the SGSN/GGSN and SGW/PGW. This means implementing security throughout the network and at every layer to make it as difficult as possible for hackers to get through.

There are many network providers who have already taken this approach with great success. We have a ways to go though, and we need more network providers taking these threats seriously. We are moving our critical infrastructure into the data center, using technologies that have been around for many years, and exploited for as many years. Even simple things like monitoring should be an essential part of any network security plan.

Security is not easy. It is a complex problem that requires careful planning and implementation. Instead, defense in depth is the only implementation plan that has a record of accomplishment, and better positions your network to remain protected for many decades to come.