Hello, and greetings from the Central Office! Spring means that everything is blooming and the Pacific Northwest is even more green. Of course, I'm allergic to all of it. My nose turns into a faucet and I blow my nose with paper towels, not even bothering with Kleenex. Worse than all of that, though, are the cottonwood trees next door. While the trees are on the neighbor's side, the roots are on our side and they're absolutely relentless at breaking into our sewer line. Our toilets are backed up, the sinks are full, and there is a Porta Potty out in front of the building while the company decides whether indoor plumbing is actually required by our union contract. These days, nothing is done or fixed unless it's either required by law, contractually obligated, or will drive revenue. And whatever is fixed is done as cheaply as possible, after a long, slow, and deliberative process. I'm hoping by the time I write the fall column, we'll have running water again.

The problem of SS7 fraud is similar. It's an issue that, like the cottonwood trees, is well known. It's one that could have been prevented with some investment in maintenance. However, it's now a problem that is responsible for the seven calls (all of which were spoofed) that I have received so far today tutoring timeshares in exotic El Salvador. I wrote about the spoofed call problem in detail in the Winter 2017-2018 issue of 2000: The Hacker Quarterly. If you didn't see it, the problem in a nutshell is that SS7 is (more or less) completely unauthenticated, so it's possible for anyone who has access to the network to claim that they're calling from any phone number they'd like to impersonate. What's more, even if I know that a call is totally bogus (for example, a call coming from an international gateway that claims to be a number assigned to my Central Office), I'm not allowed to block it because both policy and tariffs require me to deliver all calls. And this, after all, makes sense. Delivering calls usually means revenue to the company. Rejecting them means we'd only have to spend money on recognizing and rejecting bogus calls, but we'd also lose out on the revenue.

When I wrote my last column, I didn't think the FCC would take any action that would stop robocalls. However, there has been a big change in the landscape: some debt collectors and IRS scammers started calling with spoofed numbers that pointed to Public Safety Answering Points (PSAPs). This, while possibly effective, was a major strategic miscalculation on the scammers' part. PSAP phone numbers are essentially a "back door" to 911. While the National Emergency Number Association (NENA) has been making efforts to lock down access to PSAP phone numbers (to the point where they charge $5,000 per year for access to a comprehensive database), a lot of these are publicly available. For example, one state publishes the addresses, phone numbers, and points of contact for every PSAP in the state.

Predictably, 911 operators are now being flooded with people returning missed IRS scam and other junk calls, which is now impairing the ability of public safety agencies to answer legitimate calls. There aren't many things that drive a hopelessly divided government to action, but failure of 911 services is one of them. The FCC issued a proposed order in November, and will vote in March. This order will allow phone companies to do the following:

- Block calls claiming to be from numbers that are not configured to place outgoing calls (such as PSAPs).
- Block calls claiming to be from phone numbers that are obviously bogus, such as disconnected numbers.

Naturally, this is tougher to implement than you might expect because, although they could be adapted, SS7 call flows weren't really designed for this use case. In fact, the whole telephone system is designed to deliver calls, not block them. It's possible to send calls through with missing or incorrect CN and CPN and, in fact, carriers are required to deliver all calls as long as the SS7 mandatory fields are valid. Not all fields are mandatory, though, and many fields are missing and invalid.

A few years ago, we actually got pretty close to fixing this before it all fell apart. Starting in the mid-2000s but reaching a fever pitch around 2010, rural wireline carriers got very interested in fixing one part of the problem: "phantom traffic." This is traffic that was intentionally obfuscated to avoid paying access charges. It got to the point where around 20 percent of calls delivered to rural, high-cost areas lacked the appropriate billing information.

This was done by providers using VoIP switches
that allowed SS7 fields to be modified en route. Obviously, this was an activity that was never contemplated by the original design of SS7. When a long distance call is placed, it is handed off from your local phone company to an interchange carrier (typically your long distance company). If you're using a VoIP calling service, the process is essentially the same. However, interchange carriers don't always route calls over their own network. Now that traffic is carried by VoIP on the back end, it can easily be routed using a "least cost routing" table.

What is the least cost routing for any call? When you're delivering the traffic as a local call and not paying access charges, of course! Unsavory carriers began modifying the CN (Charge Number) field at the time calls were delivered to the tandem closest to the destination, substituting a local number for the originating number. Like magic, there were no access charges!

Well, if you want to get the attention of phone companies, mess with billing. By 2008, lobbying by rural phone companies was intense. There was even a Congressional hearing. The issue reached a fever pitch in 2010, with loud protests from rural carriers who were being shorted. In the middle of all of this, Congress passed the Truth in Caller ID Act, which addressed spoofed and bogus calls (a different part of the SS7 problem).

With this much momentum, the FCC had a real opportunity to (mostly) phase out SS7, limit who could access the network, and transition the phone system to 21st century technology. Instead, they decided to muddle through. The existing networks remained in place and nothing got fixed, but the FCC issued an order requiring carriers to accurately report CN information and maintain it throughout the entire call path. And while there were high initial hopes, the Truth in Caller ID Act was impossible to build any real implementation rules around because of technical problems and loopholes in the law.

If you have been a longtime reader of this column, you probably remember that rural carriers could once profit handsomely by generating large volumes of incoming calls, which gave rise to free conference calling services, free voicemail, and other services operating - improbably - from small towns in rural states. This had been a thorn in the side of long distance companies for a long time, and although a two decades-long game of cat and mouse ensued (spanning complaints from rural carriers ranging from long distance carriers throttling and failing to complete calls to delivering phantom traffic), it became clear that revenue based on voice minutes was declining and no longer reliable. The FCC, in one sweeping order, rendered the whole issue moot. Access charges, a scheme in use since 1984, were to be phased out for large carriers by the middle of 2018, and for small carriers by the middle of 2020. The Universal Service Fund would be maintained, but funded in other ways and prioritized around the build-out of broadband services.

Unfortunately, the phase-out of access charges meant that there wasn't any real long-term incentive to improve the architecture of SS7; billing was only temporarily threatened, so it wasn't worth the investment. Carriers all over the country began applying for (and receiving) waivers from new CN delivery rules. In all fairness, older telephone switches don't support this; some parts of rural Alaska still don't even use SS7! However, the FCC also signed a consent order with Level 3, which was the largest offender in delivering phantom traffic.

Once again, the FCC is revisiting an issue for which the design and implementation of SS7 is the root cause, and once again there is a chance to make real improvements to the phone system. We'll see what the new rules look like, and how carriers agree to implement it. Most are lobbying for a watered-down ruling that allows them to block bogus calls in the two specific categories referenced above, but doesn't require them to do so. If there is no requirement, then expect the phone companies to show up with a begging bowl and stories about hardship and difficulty in implementing the feature.

And with that, it's time to bring another column to a close. Have a wonderful spring, and I'll see you again in the summer!

References
- [https://www.cs.rutgers.edu/~rmartin/teaching/fa1104/c552/readings/ss7.pdf](https://www.cs.rutgers.edu/~rmartin/teaching/fa1104/c552/readings/ss7.pdf) - Very readable and understandable introduction to SS7