SS7 routing-protocol breach of US cellular carrier exposed customer data

40-year-old SS7 is being actively used to track user locations and communications.

DAN GOODIN - 5/30/2018, 3:05 PM | PUBLISHED ON ARSTECHNICA.COM

https://arstechnica.com/information-technology/2018/05/nefarious-actors-may-have-abused-routing-protocol-to-spy-on-us-phone-users

The US Department of Homeland Security recently warned that malicious hackers may have targeted US phone users by exploiting a four-decades-old networking protocol used by cell phone providers around the world, according to a spokesman for US Senator Ron Wyden (D-Ore.). Meanwhile, the spokesman said, one of the nation's major cellular carriers recently experienced a breach of that same protocol that exposed customer data.

Short for Signaling System No. 7, SS7 is the routing protocol that allows cell phone users to connect seamlessly from network to network as they travel throughout the world. With little built-in security and no way for carriers to verify one another, SS7 has always posed a potential hole that people with access could exploit to track the real-time location of individual users. In recent years, the threat has expanded almost exponentially, in part because the number of companies with access to SS7 has grown from a handful to thousands. Another key reason: hackers can now abuse the routing protocol not just to geolocate people but, in many cases, to intercept text messages and voice calls.

SS7 already being exploited

In a letter Sen. Wyden received last week, DHS officials warned that "nefarious actors may have exploited" SS7 to "target the communications of American citizens," Wyden spokesman Keith Chu told Ars, confirming an article published Wednesday by *The Washington Post*. On Tuesday, Wyden sent a letter to Federal Communications Commission Chairman Ajit Pai that heightened concerns of SS7 hacks on US infrastructure.

"This threat is not merely hypothetical—malicious attackers are already exploiting SS7 vulnerabilities," Wyden wrote. "One of the major wireless carriers informed my office that it reported an SS7 breach, in which customer data was accessed, to law enforcement through the government's Customer Proprietary Network Information (CPNI) Reporting Portal."

Such reports are legally required when carriers believe customer data has been illegally accessed. Chu declined to say who the US carrier is.

It's not clear if the DHS warning involving nefarious actors is related to the SS7 breach involving the unnamed US carrier. It's also unknown how many customers are affected by the SS7 breach or whether the nefarious actors the DHS warned of work on behalf of a nation-sponsored espionage operation or as part of a profit-motivated crime operation. Chu said that neither the DHS nor US carriers have provided those details to Wyden's office.

In 2016, US Representative Ted Lieu (D-Calif.) got a vivid demonstration of the threat posed by SS7. He gave reporters from CBS News magazine *60 Minutes* permission to abuse their access to the routing protocol to record his calls and monitor his movements using nothing more than the public 10-digit phone number associated with the handset he used.

A year later, thieves used SS7 to bypass two-factor authentication that banks used to prevent unauthorized withdrawals from online accounts. The hack allowed the attackers to intercept one-time passwords before they could be received by the intended bank customers. Exploit brokers have offered $100,000 payouts for hackers who develop reliable SS7 exploits.

The renewed focus on SS7 as a backchannel for spying on cellphone users comes almost three weeks after The New York Times reported that a little-known company called Securus allowed law enforcement officers to locate most American cell phones within seconds. The privacy concerns such services raise mushroomed in the coming days when hackers and researchers discovered vulnerabilities that exposed usernames and password data for Securus customers and leaked the real-time locations of US cell phones from LocationSmart, the company that provided the data to Securus.

"Market failure"

Sen. Wyden's letter this week to the FCC chairman is a reminder that loopholes that allow all the carriers to share customer location data aren't the only threat facing cellphone users. In responses sent late last year to Wyden's questions about SS7 security, both Verizon and T-Mobile confirmed that they were still in the process of implementing firewalls that would filter malicious requests. AT&T, meanwhile, said it implemented such firewalls but didn't say when.

The senator accused the FCC of failing to adequately answer the threat posed by SS7, noting among other things that a working group the FCC convened in 2016 to address SS7 vulnerabilities was dominated by carrier insiders and comprised no academic experts. He called on Pai to compile a list of SS7 breaches that have occurred in the past five years.

"The FCC must now take swift action, using its regulatory authority over the wireless carriers, to address the market failure that has enabled the industry to ignore this and other serious cybersecurity issues for decades," Wyden wrote. He asked for Pai to respond by July 9.