GPS has its own 19-year cicada problem

April 3 2019, by Gopal Ratnam, Cq-Roll Call

Credit: CC0 Public Domain

Most people of a certain age remember the Y2K problem that worried digitalists worldwide when we transitioned from 1999 to 2000 on the night of Dec. 31, 1999. What would happen to computers and systems when the last two digits on the date went from 99 to 00?

In the end, not much. The transition went smoothly for digital networks worldwide.

But a similar transition is happening on April 6, and this time the change is at the heart of the U.S. global positioning system satellites that send out not only precise geographic coordinates, but also vital time signals to billions of computer users around the world. The satellites will reset their onboard week counters to zero this Saturday, and that could leave some older GPS receivers unprepared for the change and potentially out of sync with other systems.

The 24 satellites operated by the U.S. Air Force that make up the GPS system provide longitude, latitude and altitude measurements to users on Earth. They also offer very precise time, thanks to multiple atomic clocks onboard. GPS receivers embedded in everyday devices such as smartphones, as well in industrial and banking applications, decode these signals to determine time to within 100 billionths of a second accuracy.

As part of its timekeeping function, GPS signals track the number of weeks lapsed since the satellite constellation began keeping time on Jan. 6, 1980. Because the onboard computers use a 10-bit system to track the number of weeks, the counter needs to reset to zero every 1,024 weeks or every 19 years—computers use a binary system to represent values, so a bit can be either a 1 or a 0, and with 10 bits, the maximum value is 2 to the 10th power, or 1,024.

Since the GPS system went into use in 1980, the first reset of the week counters happened on Aug. 21, 1999, so the next one is set to take place on April 6. Officials at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency have warned critical infrastructure operators in communications, transportation, power grid, finance and other fields to ensure that their GPS receivers can handle the resetting of the counters this week.

When GPS time is used for navigation, "a nanosecond error in GPS time can equate to one foot of position error," DHS said in a notice issued to critical infrastructure operators. "Critical infrastructure and other owners and operators are strongly encouraged to investigate and understand their possible dependencies on GPS" for obtaining Coordinated Universal Time (abbreviated as UTC), the notice said.

UTC is the gold standard of time—and has replaced the pre-digital era's Greenwich Mean Time, which was based in England. UTC is used to synchronize clocks across 24 time zones around the globe. Devices that provide UTC do so by converting GPS time using several parameters, including the week counters inside the satellites, the DHS notice said.

With GPS time becoming the de facto time standard for the world, the number of devices that depend on the satellite network's navigation and time measurements is set to reach 8 billion by 2020—or a little more than one device per person on the planet—DHS said in a statement.

Unlike the Y2K event, which was marked by uncertainty and was one that manufacturers hadn't planned for, the rollover of GPS week counters poses fewer risks, Bob Kolasky, director of the National Risk Management Center, which is part of DHS, said at an event last week.

"The risk was sort of designed in that this was going to happen after 1,024 weeks," Kolasky said. "It was planned for and judged a reasonable

risk," and GPS receivers that were made and sold in the past 15 years were designed with the changeover in mind, he said.

The precision time stamps provided by GPS are used in a wide range of applications, from soil sampling and data collection in farming to positioning and navigation of aircraft and time-stamping of stock trades to help detect fraud. As autonomous cars and internet connected devices proliferate, precise timing will become vital to those applications as well.

"Financial services companies are very aware of the need for precision time," said Charles Palmer, a distinguished research member at IBM, where he focuses on security and privacy. "They have extraordinarily stringent time guidelines" to follow, he said.

In Europe, for example, the European Security and Markets Authority stipulates that to validate stock trades, the maximum divergence from UTC cannot exceed 100 microseconds, Palmer said.

Kolasky said that banking and financial services companies have "enough resources to invest in resilience" and have invested adequately to understand and plan for the change.

Time for cybersecurity

Precise time is also critical to cybersecurity, experts said.

The Department of Defense and the National Security Agency are working on programs to explore the linkages between time and cybersecurity, Cheri Caddy, who leads a public-private program at the National Security Agency, said at an event last week.

"We are looking at how time is critical to everything you do in cyber, from forensic logs to cryptography," said Caddy, who's also a senior

fellow at Auburn University's Center for Cyber and Homeland Security. "If you lose access to precision time, you can unlock everything, from a cryptography standpoint, or lock things forever."

Increasingly, time is a determinant in computer system administrators having access to networks, Caddy said. "If things are reset to zero you may not have access to some systems," she said.

If a computer network security system in a globalized company detects and blocks malware and puts a time stamp on the event, then security researchers use that information to conduct a forensic examination. But if different computers located in different offices around the world are off by a few seconds from one another, conducting such an examination could become difficult, Palmer said.

Just as wireless signals can be spoofed and mobile devices tricked into connecting with fake transmitters that then collect private information, GPS devices can be tricked into connecting to fake devices that can then manipulate location and time signals.

Last week, C4ADS, a nonprofit group that focuses on security, released a report showing that it found 9,883 cases of GPS spoofing across 10 locations in and around Europe, which affected 1,311 civilian navigation systems since February 2016.

A majority of those false GPS signals were generated by Russian-made equipment and were likely used by Moscow's security services to protect Russian President Vladimir Putin from possible attacks, as well as for strategic reasons in Syria, Crimea and in the Black Sea region to defend Russian interests, C4ADS said.

"By attacking positioning, navigational, and timing data through electronic warfare capabilities, state and non-state actors can cause

significant damage to modern militaries, first-world economies, and everyday consumers alike," the report said.