Security/Integrity/Availability Leftovers

By *Roy Schestowitz*
Created *21/01/2020 - 10:29am*
Submitted by Roy Schestowitz on Tuesday 21st of January 2020 10:29:12 AM Filed under Security [1]

- **DDoS Mitigation Firm Founder Admits to DDoS [2]**

  A Georgia man who co-founded a service designed to protect companies from crippling distributed denial-of-service (DDoS) attacks has pleaded to paying a DDoS-for-hire service to launch attacks against others.

- **Siemens Warns of Security Risks Associated With Use of ActiveX [3]**

  Some of Siemens? industrial products ? the list includes SIMATIC WinCC, SIMATIC STEP 7, SIMATIC PCS 7, TIA Portal, and S7-PLCSIM Advanced ? rely on ActiveX components and customers need to use Internet Explorer to execute these components.

  However, the German industrial giant has warned that using Internet Explorer to access untrusted websites can pose serious security risks. Siemens recommends using a web browser that does not support ActiveX if accessing web pages other than the ones associated with the company?s products.

- **Y2038: It's a Threat [4]**

  On Unix-derived systems, including Linux and MacOS, time is stored internally as the number of seconds since midnight GMT, January 1, 1970, a time known as "the Epoch." Back when Unix was created, timestamps were stored in a 32-bit number. Well, like any fixed-size value, only a limited range of numbers can be stored in 32 bits: numbers from -2,147,483,648 to 2,147,483,647. (Without going into technical details, the first of those 32 bits is used to denote

a negative number. The asymmetry in range is to allow for zero.)

I immediately got pushback: did I really think that 18 years hence, people would still be using 32-bit systems? Modern computers use 64-bit integers, which can allow for times up to 9,223,372,036,854,775,807 seconds since the Epoch. (What date is that? I didn't bother to calculate it, but it's about 292,271,023,045 years, a date that's well beyond when it is projected that the Sun will run out of fuel. I don't propose to worry about computer timestamps after that.)

It turns out, though, that just as with Y2K, the problems don't start when the magic date hits; rather, they start when a computer first encounters dates after the rollover point, and that can be a lot earlier. In fact, I just had such an experience.

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://krebsonsecurity.com/2020/01/ddos-mitigation-firm-founder-admits-to-ddos/
[3] https://www.securityweek.com/siemens-warns-security-risks-associated-use-activex
[4] http://www.circleid.com/posts/20200120_y2038_its_a_threat/