Control Systems Cybersecurity growing problems

Joe Weiss on Sun, 04/07/2019 on the Unfettered Blog

https://www.controlglobal.com/blogs/unfettered/control-system-cyber-attacks-have-become-more-stealthy-and-dangerous-and-less-detectable

Control Systems Cybersecurity Expert, Joseph M. Weiss, is an international authority on cybersecurity, control systems and system security. Weiss weighs in on cybersecurity, science and technology, security emerging threats and more.

Control system cyber attacks have become more stealthy and dangerous - and less detectable. The reason for control system cyber security is to protect equipment, people, and the environment not just networks. I have seen a number of timelines that identify key cyber attacks in ICS cyber history. Most of the timeline attacks I have seen include some combination of Slammer, Stuxnet, Shamoon, the German steel mill attack, Havex, Sandworm, BlackEnergy, CrashOverride/Industroyer, and Triton. However, with more than 1,100 actual control system cyber incidents in my database, it is not clear it is possible to identify specific cases nor provide appropriate context. Rather, I think a more interesting approach is to identify key changes in control system cyber attacks. This approach can help demonstrate what is missing in control system cyber security.

Following the 9/11 attacks in 2001, cyber security became a national security issue and cyber security was moved from the engineering organizations to the IT organizations. Additionally, it was at this time that process sensors, actuators, and drives were left out of the cyber security process. This move has plagued control system cyber security to this day as the control system and safety engineers and process control/safety system devices were effectively removed from the cyber security process.

Until about 2003, control system cyber incidents were either unintentional such as the Olympic Pipeline rupture or insider attacks such as the Maroochyshire wastewater hack. There were exceptions such as the Chinese government attempting to hack the California Independent System Operators (CAL ISO) **SCADA** systems in 2001 (they were not able to reach the SCADA system). In 2003, as the level of connectivity increased and control systems were moving to Windows-based HMIs, Microsoft-based attacks such as Slammer, Blaster, and Conficker affected control systems. That is, control systems became the unintended "recipients" of Windows-based Denial-of-Service (DOS) attacks. Until 2007, control system cyber "attacks" and demonstrations were almost all DOS events not equipment damage. As a result, many in industry simply **didn'**t take control system cyber security seriously (which unfortunately is still the case).

Because of industry's lack of taking control system cyber threats seriously, the Idaho National Laboratory (**INL**) conducted the **Aurora** vulnerability demonstration in March 2007 to demonstrate physical damage from a cyber event. Aurora was a physics-based attack that caused physical damage – **destroyed the generator**. It was a game-changer as it demonstrated that cyber attacks were no longer just DOS attacks like in IT systems, but could be an existential threat to a modern country. At this time, cyber attacks like Aurora, were still perceived to be so sophisticated they had to be performed by a nation-state.

It has been stated that the 2016 Crashoverride/Industroyer **malwar**e marked the first time that engineering expertise was used in developing cyber attack methodologies because of the use of SCADA-specific protocols. In reality, it was Aurora and **Stuxnet** in the 2007-08 time frame that marked the **sea change** in control system cyber security threats. In Aurora and Stuxnet, the attacks were designed to physically damage equipment based on engineering "weaknesses". The cyber methodologies were utilized based on what was needed to accomplish the engineering goals. Consequently, the cyber tools necessary could range from trivial to zero days depending on the functional need.

This is different than the IT/OT approach of assessing network vulnerabilities. However, this engineering approach is still not well appreciated and this is deadly dangerous. In August 2008, the Siemens International User Group meeting had an INL presentation on hacking Siemens PLCs. It was essentially Stuxnet but the attendees didn't recognize the implications of the presentation. In the 2009-10 time frame, Stuxnet was damaging centrifuges in Iran. For a year, the damage was thought to be centrifuge malfunctions, not cyber attacks. Following Stuxnet becoming public, control system cyber security changed dramatically as many in the attacker community which previously paid little attention to control systems (they were focused on money and fame), pivoted to control systems. Metasploits (hacking tools) were developed for the major control system platforms and made available over the Internet. It longer took the sophistication of a nation-state to attack control systems.

In the 2012-14 time frame, control system supply chain attacks were attacked to use as "back doors" into the end-users' control systems. Vendors compromised by the supply chain attacks included Telvent, Siemens, GE, and others. How deep into the supply chain the hacks were occurring has not been documented. It doesn't appear the NERC Supply Chain initiative will adequately address these concerns.

In the 2015-16 time frame, the Russians attacked the Ukrainian power grid. This should not have been a surprise as DHS provided an almost step-by-step procedure in the May-June 2015 time frame if control systems were connected to the Internet. Fortunately, the 2015-16 Ukrainian cyber attacks were only DOS attacks as the attackers remotely opened the breakers to cause the outages but chose not to reclose the breakers to cause physical damage (Aurora). However, the June 2017 the Triton attack on the Triconex safety systems in a Saudi Arabian plant was a game changer in a number of ways. It was an attack against safety systems meaning the intent was to blow up the plant and kill people not cause a DOS. The plant tripped because of malware yet it was not detected as a cyber attack but as a malfunction.

The Triton attack also demonstrated that sophisticated cyber attacks could be carried out against any control or safety system supplier. The Triton attack demonstrated that neither control system cyber security nor process safety policies, procedures, or standards were adequate. Additionally, it raised the question as to how many "successful" control system cyber attacks are occurring if cyber attacks can be misidentified as malfunctions. Facility operators are trained to trust their sensors/displays. As both Stuxnet and Triton compromised Windows-based networks and associated operator displays, the need for out-of-band sensor monitoring systems becomes critical to have an independent, uncompromised view of the process. The Triton attack was only against the safety system and needed a separate attack against the plant Distributed Control System (DCS) to be effective. This certainly raises the question as to whether integrated control and safety systems can be demonstrated to be cyber secure and safe when it only takes one attack to cause a catastrophic safety situation. The Triton attack also demonstrates the culture gap between IT/OT and Engineering/Safety is wide and growing.

Where is the future in control system cyber security threats/mitigation? Artificial Intelligence (AI), Machine Learning (ML), and 5G networks all have capabilities for providing significant productivity advancements and control system cyber security improvements. Unfortunately, these technologies in the wrong hands can cause devastating problems. The Internet of Things (IOT) and its variations including the Industrial Internet of Things, the Battlefield Internet of Things, etc., and Industry 4.0 are dependent on "lots of sensors" and big data analytics. However, if you can't trust your sensors as they have no cyber security or authentication, what does that mean for big data analytics and thus for IOT and Industry4.0? Moreover, what is the "I" in IOT? If it is the Internet, it goes against DHS and industry recommendations about not connecting control systems directly to the Internet which was used in the Ukrainian cyber attacks. We need to rethink how we secure control systems in a holistic manner. This includes appropriate control system cyber security policies, procedures, training, and technologies, some that don't yet exist.

https://www.controlglobal.com/blogs/unfettered/control-system-cyber-attacks-have-become-more-stealthy-and-dangerous-and-less-detectable, --- Joe Weiss