Chemicals, Controls and Cyber

Mr. Munish Sharma

The author is an Associate Fellow with the Cyber Security Project at IDSA, New Delhi.

Summary

Process automation across industries depends heavily on Industrial Control Systems for monitoring, controlling and supervision. Computer viruses and worms specifically designed to target these control systems deployed in the chemicals processing facilities could be a potent threat if Toxic Industrial Materials are released into the atmosphere, following an engineered accident(cyber attack).

Introduction

In October 2008, a series of explosions at the aniline plant of Jilin Petrochemicals in Northeast China killed five workers and injured about seventy. Aniline, a toxic organic compound leaked into the Songhua River and polluted the drinking water for millions of people. The investigation concluded that a valve was left open, and as a result temperature rose rapidly and the stocked nitrobenzene, benzene and nitric acid also caught fire and exploded.[1] Accidents taking the shape of disasters are rare in the chemical industry, but these rare instances have severe consequences for public safety, public health and environment. These accidents could arise out of an equipment failure, a human error, a physical attack or an advanced cyber-attack having dire physical consequences.

The rise in the number of cyber-attacks on the control systems of the Critical Infrastructure installations function is a precursor to the upcoming change in security perception of the enterprises engaged in deployment and operations of such installations. Computer viruses and worms specifically target Industrial Control Systems (ICS), which are the building blocks of industrial automation deployed in electricity grids, power generation, and chemical processing plants and so on. Chemicals throughout their life cycle, formulation, usage, storage, and distribution or transportation need security from threats including terrorism and accidents. The threats could be significant, as some of the facilities possess highly toxic materials, which may be transformed into weapons, while an attack on a high-risk facility could cause a significant number of deaths and injuries.[2] There are very few reported instances of

cyber incidents at chemical plants only four of such incidents were reported to the U.S. ICS-CERT[3] in 2014. Although, the number could be high, but small incidents are generally not reported as companies do not publish such information.[4]

Chemistry of Cyber Threats

Cyber attacks on a Chemical facility could manifest in two ways. It could either be an espionage operation to gain access to the intellectual property such as formulation or process flow diagrams, or an attack on the ICS, which control critical functions of the plant and a malfunction arising due to a well mounted attack may have physical consequences. The Nitro Attacks of 2011 stole intellectual property such as design documents, formulae, and manufacturing processes, targeting private companies involved in the research, development, and manufacture of chemicals, using a Remote Access Tool (RAT) called Poison-Ivy.[5] Therefore, along with ICS networks, it is equally important to secure the process flow documentation. A generic cyber attack on the control systems network may at the most gain access to the sensor sending real-time information back to the control room, or manipulate measurements to alter the instructions sent by the controllers, which may set the safety mechanism to trigger alarms or at the most, shutdown the process. But process flow documents have ample information for the attacker to strike at the point where consequences are catastrophic.

The malware unveiled in 2010, Stuxnet, targeted the Programmable Logic Controllers installed at various nuclear facilities in Iran. Consequently, it exposed the vulnerabilities hidden in the process control systems, which are an integral part of plant automation across the industries. Perhaps, enterprise software vendors such as Windows and Apple have become security-oriented, but the ICS, with a higher lifespan, still run on legacy systems which were not designed from security point of view. Hence, ICS is an easy and obvious target for attack. In terms of security management, ICS and their networks are fundamentally different from the enterprise networks and assets. The foremost priority for enterprise networks is confidentiality, but ICS are built on availability and integrity. ICS are designed to last for decades, and they need to be operational round the clock, ensuring availability. It is operationally not feasible to shut them down for regular software updates or patch installation even in the case of an attack. The development and deployment of ICS solutions is highly customized, according to the requirements of the specific industry and the specific plant. Despite the difference, both enterprise networks and ICS are under constant threat from attackers gaining access to the networks for espionage and possibly for sabotage as well. The risk increases manifold for the chemical facilities dealing with materials which are toxic and have proven health hazards if released in the environment.

Vulnerable Toxic Industrial Materials

The Chemical Industries store and process various materials or chemicals, but some of them are classified as Toxic Industrial Materials[6] (TIMs), including Chlorine, Hydrogen chloride, Nitric acid, Ammonia, Vinyl Chloride and Methyl Isocyanate. Toxic Industrial Materials are widely used by the fertilizers, textiles, plastics, pesticides and petrochemical industries.[7] TIMs have well-known hazards for biotic life, specifically humans. Chlorine, Phosgene and Hydrogen Cyanide were used to kill thousands of soldiers during the First and Second World War.[8]

Given the fact that a lot of TIMs are stored, processed and transported throughout the globe, acquired TIMs or a sabotage amounting from a cyber attack on the control systems pose a potent threat. TIMs are likely to be used by terrorists to launch a chemical attack. The stringent controls on Chemical Warfare agents coupled with ease of availability and production in large volumes of TIMs make them a lucrative option. Due to the ease of availability and known hazards, these chemicals would be easier for terrorists to use than chemical warfare agents to cause mass casualties and destruction. The rise in the number and sophistication of attacks on enterprise networks of chemical industries and industrial control systems of their faculties have already raised alarms with the security professionals and senior management.

Conclusion

One of the worst accidents in the history of chemical industry, the Bhopal Gas Tragedy of 1984 claimed lives of 3800 people and injured 11,000, when methyl isocyanate from the Union Carbide facility was released. The chemical industry certainly cannot afford an incident of the scale of Bhopal gas tragedy, either accidently or triggered by a cyber attack on the Industrial control systems. Large international firms do recognize the imperatives of cyber security in chemical industry, but for small enterprises it is an expensive affair.[9] Since many cyber incidents do not get reported to the government, coordination and exchange of information within the industry will form the first line of defence against the common cyber threats. Voluntary participation is not sufficient in the face of the sophisticated threats and the risks involved; a comprehensive regulatory framework is warranted to secure the enterprise networks and most importantly, the industrial control systems of the chemical industry to ensure that Toxic Industrial Materials do not take the form of chemical warfare agents.

Endnotes:

1. "A guide to major chemical disasters worldwide", available at http://www.icis.com/resources/news/2008/10/06/9160653/a-guide-to-major-chemical-disasters-worldwide/

2. "Chemical Security and Resilience", available at http://www.dhs.gov/topic/chemical-security

3. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). ICS-CERT provides focused operational capabilities for defense of control system environments against emerging cyber threats.

4. "Security experts warn chemical plants are vulnerable to cyber-attacks", Chemistry World, available at http://www.rsc.org/chemistryworld/2015/06/chemical-plants-vulnerable-cyber-attacks

5. "The Nitro Attacks Stealing Secrets from the Chemical Industry", Symantec Security Response, available at https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

6. Toxic industrial chemicals are industrial chemicals that are manufactured, stored, transported, and used throughout the world. Toxic industrial chemicals can be in the gas, liquid, or solid state. They can be chemical hazards (e.g., carcinogens, reproductive hazards, corrosives, or agents that affect the lungs or blood) or physical hazards (e.g., flammable, combustible, explosive, or reactive), see "Toxic Industrial Chemicals (TICs) Guide", United States Department of Labor, available at https://www.osha.gov/SLTC/emergencypreparedness/guides/chemical.html.

7. Ammonia is essential to fertilizer production, and used widely in pharmaceuticals. Phosgene is used in plastics and the pesticides industry.

Chlorine has its applications in making plastics, solvents, textiles, agrochemicals and insecticides.

8. “Cyanide”, available at http://fas.org/nuke/guide/usa/doctrine/army/mmcch/Cyanide.htm and “Facts About Phosgene”, Center for Disease Control and Prevention, available at http://emergency.cdc.gov/agent/phosgene/basics/facts.asp

9. ibid. 3.