Is Penetration Testing recommended for Industrial Control Systems?
By Ngai Chee Ban, CISSP, Honeywell Process Solutions, Asia Pacific

Cyber Security Assessment for Industrial Automation

Conducting a cyber-security assessment is an important step in an industrial IT lifecycle because it can pro-actively address any shortcomings and vulnerabilities. The intent and purpose is to identify security weaknesses and to follow up with actionable recommendations that will promptly plug the gaps before any security breach can occurs. One of the techniques involved, known as system vulnerability assessment, is to find out if the systems contain any vulnerabilities that is susceptible to viruses or Trojan horses or in a worst case scenario - a malicious cyber hack.

The question is whether a cyber security assessment for industrial automation should include penetration testing as an extension of the system vulnerability assessment.

Before we go further, it is important to make a clear distinction between system vulnerability assessment and penetration testing.

What is System Vulnerability Assessment?

In a vulnerability assessment, data is collected from the system and compared with documented issues to deduce if the system is vulnerable to any known exploits. When we say “documented issues”, we are referring to vulnerabilities or systems weaknesses that have been discovered and therefore known and, hence, they have been documented and most probably made available to the public for awareness. Most of the time, these publishing of vulnerabilities would also have included remedial measures to address the weakness.

In an attempt to categorize and to rank the severity of vulnerabilities in information systems, a few computer security communities have developed standards for this. Among the well known standards are the Common Vulnerabilities and Exposures (CVE) dictionary and the Common Vulnerability Scoring System (CVSS). The CVE system provides a reference-method for publicly known information-security vulnerabilities and exposures, and is maintained by MITRE Corporation with funding from the National Cyber Security Division of the United States Department of Homeland Security. The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities, and is under the custodianship of the Forum of Incident Response and Security Teams (FIRST). There are a few others as well such as the Common Vulnerability Reporting Framework (CVRF) by the Industry Consortium for Advancement of Security on the Internet (ICASI) and the OWASP Vulnerability Classification Mappings by the Open Web Application Security Project (OWASP) which focus more on web systems’ vulnerabilities.

Figure 1: Many consortiums and computer security organizations have sought to categorize and to rank the severity of vulnerabilities in information systems, and have developed standards for this.
Figure 2: US-CERT Cyber Security Bulletin (SB13-038) - These days, most known systems vulnerabilities are published together with information on fixes and patches to address them so as to prevent exploitation (in exception, are the zero-day exploits). An example of a published system vulnerabilities is shown here. CVE references are used in the Common Vulnerabilities and Exposures system to identify publicly known information about security vulnerabilities.

CVE and CVSS are among the most widely used standards including by the US National Vulnerability Database. Many vulnerability scanning tools like the Tenable Network Security utilizes the CVE or CVSS program to reference each of the vulnerabilities detected by its Nessus scanner.

Figure 3: In certain mine sweeping operations, the soldiers just detect and mark the land mine when it is discovered. The defusing work or disposal of the explosive devices by blowing them up may be left to the experts Explosive Ordinance Disposal unit later.

Similarly, during a system vulnerable assessment the testing involves only discovering any systems vulnerabilities and reporting them.

This is where in a vulnerability assessment, the system’s configuration and settings data are collected by the scanner and compared with the scanner’s dictionary-list of CVE or CVSS-referenced vulnerability information to deduce if the system is susceptible to any known weakness. In the event of a match, the finding is reported as vulnerability discovered. The testing stops here and does not go further, like for example, seeking ‘to prove’ if the found vulnerability is indeed exploitable.
Figure 4: A sample screenshot in a vulnerability assessment. The system was discovered with Windows shares that provides unauthorized access. In this case, the vulnerability has to do with Windows Server Message Block potentially sharing password and unprivileged access via an online game download. And the vulnerability has previously been classified under CVE-1999-0519 and CVE-1999-0520.

What is Penetration Testing?

Penetration testing, however, takes a further step into simulating the exploitation on the found system vulnerability to confirm if a security breach or a catastrophic damage can really be inflicted on the system if it would have been a real cyber attack. Exploitation may involve automated techniques using software programmes or scripts that were developed, possibly available on the Internet openly and ready for running on the vulnerable system to effect an outcome, and this is often malicious in nature. Other exploitation may involve keying in invalid inputs into the requesting field of a flawed application that has been discovered with security weakness that leads on to the application’s breakdown (an example of such vulnerabilities is the widely known SQL-injection weakness). Yet other exploitative venture may involve devising own scripting and techniques to make use of the vulnerability to break into the system further.
Figure 5: Explosive Ordinance Disposal unit is a team of experts tasked to defuse bombs. In a bomb disposal operation, one does not know for certain if the suspicious package really carries an explosive device, and even if it does, whether the device is ‘live’ or inactive. The technique is invasive and it potentially destabilizes the device. The risk of accidentally setting off an explosion is high. Similarly, penetration testing on industrial control systems carries substantially high risk.

Such techniques are often invasive and potentially result changes to the system’s settings which in a real malicious attempt may have an end-goal of rendering the system’s functionality unable to perform to its original intend or reducing its capability or even in some cases totally disabling it, like in a total system-shutdown. Other more sophisticated exploitative technique may be to extract critical data such as confidential information but leaving the system intact and still operating as if nothing untoward has happened.

Why some prefer penetration testing?

As we can see now, penetration testing has a conclusiveness to the investigation. Hence, it holds strong appeal to many security practitioners. They see it as an added benefit to exhaustively find out the reality of cyber security threat to their systems.

Many, however, may not be aware that a penetration test can have the potential of destabilizing the system. In certain instances, the impact on the system is irreversible such that it can no longer be restored back to its original state. In some other situation, the impact of the destabilizing can even propagate the effect upstream or downstream affecting other inter-connected systems. In industrial control systems – such impact has a very high risk of destabilizing the manufacturing processes and potentially resulting a volatile chemical reaction that poses danger to human safety and also to the environment.

So we ask: Is penetration testing recommended for a cyber security assessment on industrial control systems? If it is for the purpose of confirming a found vulnerability – which if, for example already has a CVE registered to it, and hence, the fixes and patch are likely also available – why the need to prove its exploitability anymore?

Figure 6: Penetration Testing for Industrial Automation Control Systems: The impact of destabilizing the manufacturing processes and potentially resulting a volatile reaction poses very high risk to human safety and also to the environment.
What should we do?

In today’s ICS landscape, many plants are yet to be assessed to ascertain the security health of their systems, processes and operations since their DCS migration to open-systems architecture.

For them, the urgency may be to conduct an immediate security assessment that is broad-based because the results of first-time assessments are usually both sporadic and wide-ranging. Often too, security gaps tend to be inter-related in a way that a primary system vulnerability can derive many secondary weaknesses. Hence, a collective few inherent weaknesses may actually be dealt with when a single system patch is applied. This is how single service packs work in comparison to individual hotfixes.

Figure 7: For first-time audit review, a broad-based assessment may be more suited especially when the plant’s security weakness are expected to be distributed and wide-ranging, and perhaps, mostly rudimentary.

The security gaps tend to be inter-related in a way that a primary system vulnerability can derive many secondary weaknesses.

Hence, it is usually more practical to start with a broad-based assessment. The real value of pin-point testing such the surgical penetration test may find its merits when a more exacting security assessment is necessary later. This is because most common issues would have been cleared after the initial assessment.

How can Honeywell help?

Honeywell has the largest number of experienced industrial cyber security consultants in the industry. In addition, it draws on its experience in more than 70 control system versions and hundreds of key industrial cyber security projects around the globe. Armed with this knowledge, Honeywell is well equipped to help users develop or refine and execute their Cyber Security Vulnerability Assessment Program. Click here to know more about Honeywell’s comprehensive Cyber Security Assessment Program.

To determine the most effective way to test your Industrial Control Systems against cyber threats, please write to us at hpsmarketing@honeywell.com or cheeban.ngai@honeywell.com

About the Author:

Ngai Chee Ban leads Honeywell’s Industrial IT Solutions in Asia Pacific. He is accredited with CISSP (Certified Information Systems Security Professional) and CISA (Certified Information Systems Auditor). For over 18 years he has provided consulting expertise in the Oil and Gas and in Corporate IT sectors focusing on cyber security, remote services and information risk management.