Cyber Security Maintenance for SCADA Systems

Johannes Schneider, Sebastian Obermeier, Roman Schlegel

ABB Corporate Research
Segelhofstr. 1K, Baden, Switzerland
firstname.lastname@ch.abb.com

***Abstract*—To ensure a high security level in industrial systems over a period of time, maintenance is required. In this paper, we give an overview of security-related maintenance tasks incorporating new technologies employed in industrial control systems such as cloud computing but also new attack technologies such as GPS spoofing. We also provide a threat model that focuses on threats that materialize during the lifetime of an industrial system and that are typically not present during the commissioning phase. Furthermore, we show how the identified maintenance tasks can mitigate these threats.**

I. Introduction

Industrial applications are typically controlled and supervised by SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) systems, which are complex distributed systems used to control diverse industrial assets.

Because of their nature of controlling important critical industry systems, SCADA systems are quickly becoming a more interesting target for cyber attacks. Security for SCADA systems differs from traditional IT system security in several aspects, cf. [1], [2]. For instance, the long lifespan of a SCADA system, including legacy infrastructure parts that are often largely unprotected, increase a potential hacker's interest. Furthermore, SCADA systems are mainly designed to guarantee availability and come with a variety of attackable interfaces, eg. sensors. These aspects often result in different measures for ensuring security as in conventional IT systems.

Security professionals generally agree that cyber security needs processes to be able to cope with changes over time. For example, patch management and virus definition updates are processes that have been well established on personal computers. However, when dealing with large scale industrial systems, the complexity of such processes grows significantly, i.e., due to the variety of interfaces, e.g., sensors, number and diversity of users.

The long lifetime of industrial systems increases the importance of continuous security maintenance, and the security in industrial systems is often directly related to safety of workers at the plant and even society at large, e.g., in the case of nuclear power plants.

A. Contributions

In this paper we provide a comprehensive list of maintenance tasks in the context of industrial systems, including new technologies such as cloud computing and mobile device access. We also explain security risks of new, not yet widely employed technologies such as smart metering for industrial systems as well as new attack technologies like GPS spoofing. Although there is an overlap with conventional enterprise IT systems, there are differences and a significant portion of tasks has not been addressed prior to this work.

II. Security Maintenance Tasks

We differentiate between SCADA security maintenance tasks related to individual components, to the overall system security, and related to personnel.

A. Maintenance of (Security) Components

1) Maintenance of Virus and Malware Definitions: Antivirus software must be updated regularly to include new definitions of threats and updated scanning components. In critical infrastructures, updates should be checked for false positives before the installation. In the past there have been incidents where virus scanners have misclassified operating system files as viruses. Whereas in a conventional IT system this might be a minor concern, since no data is lost, in a high availability industrial system such an error could be critical. If a test reveals that non-malicious files or non-infected files are wrongly classified, the software has to be configured and an exception has to be added.

2) Maintenance of Black-/Whitelists: Application whitelisting allows the execution of a predefined set of software applications, but rejects the execution of any other application. Blacklists allows the execution of all but the predefined set. In a rather static industrial setting whitelists are often preferable, since operators typically do not have to install new applications frequently and urgently. It has been evaluated in [3] and provides an additional layer of defense, especially for industrial systems. However, application whitelisting needs maintenance as whitelists need to be reviewed and adjusted. The application whitelisting application itself needs to be updated, especially if security vulnerabilities are discovered.

3) Maintenance of Security Log System: Examples for security-related events that are stored in a log are user logins (including failed attempts), access to resources. Logs can be stored in a database or just as raw data in files. Log systems are sometimes coupled with analysis components, e.g., security incident management systems for intrusion detection or detection of security policy violations.

Since timestamps of events stem from a variety of devices with different clocks, they must be synchronized with a reference clock to reconstruct the correct sequence of events. If the order of events is not correct, intrusion detection or log analysis software might not be able to detect attacks. Furthermore, the logs might become useless for forensic investigations. It must also be ensured that the logging system offers enough space for storage. Typically, this is done through either deleting or

archiving of logs with digital signatures for a limited amount of time. Signing logs is recommended to detect forging of logs once they have been archived. In particular, logs should be stored separately from the system that generates the logs to prevent manipulation or the loss of log files.

A change in security policies or a change in system components might require to log previously unlogged events or require adjustments of existing logging software. It might also require updating intrusion detection mechanisms to cope with changes in system uses. If the volume or frequency of logging increases, the infrastructure of the log system might have to be updated.

4) Maintenance of Mobile Device Management System (and Mobile Devices): A mobile device management (MDM) system requires constant changes, e.g., if new software needs to be used on mobile devices or new types of mobile devices are used. Thus, these maintenance tasks require not only changes to the MDM, but also constant reviews of the current settings, and whether they correspond with the agreed-upon security policy. The health of mobile devices should be monitored, in particular, devices breaking (security) policies such as rooted Android or jailbroken Apple devices should be detected. Checks for older makes of devices that are no longer supported should be made, and matching devices should be removed.

5) Maintenance of Reference Clock: If a reference clock or integrated time-servers are used to detect GPS jamming or spoofing, they potentially also require maintenance. E.g., time servers from external suppliers run specific firmware that needs to be updated periodically when bugs or vulnerabilities are discovered.

6) Maintenance of Public Key Infrastructure and Certificates: Certificates might be revoked because of security incidents, making it necessary to update devices with new certificates. Certificates also must be renewed from time to time, and the renewal should be done without interrupting the process or otherwise disrupting the system.

The frequency of updates, e.g., download of revoked certificates, is typically done at least daily. Archiving of old (i.e., revoked or expired) certificates for forensic purposes is recommended. In contrast to an enterprise system, in an industrial setting with real-time requirements, these tasks must be performed on time, since an expired certificate might render the system non-available.

7) Maintenance of Cloud Security: When using cloud services of external providers, one might trust the provider to ensure security to some extent, e.g., patching of servers, managing anti-virus software, etc. However, some vulnerabilities and patches can impact software interacting with the cloud but not running on the cloud itself. Also, software running on the cloud might be affected by changes in the software landscape of the cloud provider. Therefore, it is important to monitor security announcements of cloud providers closely. Furthermore, cloud providers provide built-in firewalls that require maintenance. The software used to access the cloud provider should also be monitored for vulnerabilities and a patching process should be in place.

There are additional considerations when using an external provider: Ensuring confidentiality of (customer) data does not only include maintenance related to technology but also monitoring the legal landscape for changes in data privacy regulations and to conduct regular audits of the cloud service provider, e.g., with respect to which countries have a data center hosted by the provider. It is also important to check that the security mechanisms of the provider are up to date.

8) Maintenance of Security Policies: Security policies evolve over time. For example, password policies have evolved drastically over the last 20 years, constantly pushing the user to choose more secure passwords or dealing with breaches of accounts. Regular reviews and changes of security policies, e.g., related to individual components, can be seen as a maintenance task. Changes in security policies can be triggered by changes in legislation or a re-assessment of entry points, e.g., adding of wireless/mobile devices to the IT infrastructure.

9) Maintenance of (Central) Login Services: The central login services and the corresponding servers require patches and maintenance, e.g., making sure that user accounts and access rights are up to date. This might be more challenging in a (distributed) industrial system, where user accounts are often replicated to ensure availability despite (Internet) connection problems to a central service.

10) Maintenance of Vulnerability and Patch Management: Patches fix bugs that pose a security threat for installed software. This applies to software components that perform security operations (e.g., cryptographic functions) as well as software that performs non-security-related operations (e.g., control operations). The vulnerability and patch management systems require constant review of whether all patches have been correctly applied to all devices that need to be updated, and whether new patches have been published or new vulnerabilities have been discovered.

11)Maintenance of VPN Server, Firewall (and Hubs, Switches, Printers): All hardware should be inspected from time to time, e.g., hubs and switches might have warning lights or might emit noises that indicate problems with the fan. Inspections should not only include checking whether hardware components have already failed (e.g., RAM, disk sectors), but also whether resources are being used up, e.g., is there still enough disk space available? Are there applications with memory leaks that potentially exhaust the system in the near future? How is system performance, i.e., has it decreased over time? Memory leakage, for example, can be a problem that eventually leads to a system crash. Is the network topology still robust to fluctuating loads - in particular, does it allow for the addition of new devices? Firewalls should be reviewed with respect to their filter rules, e.g., do anti-spoofing filters block all private and internal addresses? Logs should be reviewed, e.g., denied URLs for web-filtering as well as IP-based firewall logs, to make sure filtering rules are still appropriate. State tables for stateful inspection by firewalls should be reviewed in terms of source IPs, destination IPs, ports and timeouts to ensure that filtering rules are appropriate. Reviews should in particular occur before and after changes to the system. They can also be partially automated [4].

12) Maintenance due to Newly Developed or Changed Non-Security Components: A component can be replaced either by a model of the same type or a newer model. A component can be updated, added or removed from the SCADA system. These activities are frequently not considered as maintenance but rather as part of commissioning. Therefore, we only list security components that are impacted by these actions: Secu-

rity log system, robustness testing procedures, device integrity scanning and authentication, firewall/routers at the SCADA system and remote control center, LDAP server, public key infrastructure server.

B. Maintenance Procedures Related to Personnel

1) Security Awareness of Personnel: Regular refresher courses with respect to security policies and behavior are required to maintain compliance. This might involve disaster (or incident) response training, i.e., how to act efficiently in case the system is compromised by cyber attackers. For a detailed study for factors influencing compliance we refer to [5].

2) Maintenance of User Accounts: Maintaining user accounts, e.g. adjusting rights, adding / removing users in accordance with day-to-day business, e.g., due to employees leaving or joining or changing roles.

C. Maintenance Related to Overall System Security

1) Security Audits: Audits should be conducted to ensure that security policies are maintained, enforced and spot potential weaknesses of current security policies. For example, workplaces of employees should be checked for left-behind, unsecured confidential material. In organizations with frequent visitors, tailgating is often tolerated by employees. This should be checked. Procedures dealing with configuration management should be reviewed and updated periodically.

2) Backups: System information such as component configurations, sensor data, etc. should be backed up on a regular basis. This is not only helpful to minimize outage time in case of hardware failures, e.g., hard drive malfunction or IED failures, but it can also simplify dealing with infected systems, since cleaning a system might be more difficult than restoring an old state of the system. Restoring a system from a backup might also be faster. The backup procedure not only includes regularly backing up the complete system, but also checking whether existing backups are still intact, e.g., by performing system restore tests.

3) Security Fingerprint: An overview of the overall cyber security status should be obtained, including information on the execution of all of the security maintenance tasks described above.

4) Technology Monitoring: New technology emerges and technology constantly evolves. This enables new attacks or makes attacks easier for a wide range of potential attackers.

It is crucial to monitor technologies that might enable adversaries to attack the system as a whole or to attack individual components. For example, cryptographic algorithms might be broken more easily due to the constant increase in computing power or due to the development of new technologies such as quantum computers. GPS spoofing [6] kits to attack GPS-based clocks in automation system might become more readily available. Spear phishing techniques become more sophisticated, making it more likely that sensitive information like account data is leaked or viruses are deployed directly inside the company network. Spear phishing or social engineering techniques in general benefit from social network technology such as Facebook and LinkedIn, by allowing to gather information about targets more easily and more extensively, though this has been debated in the context of smart grids [7].
Even seemingly harmless information like electricity bills can result in financial losses. Knowledge about electricity consumption could allow an adversary to estimate the utilization of a particular plant. This information can be valuable during price negotiations, since it can give an indication of how desperately a company needs a contract. Such information might get more easily exposed for example due to smart metering technology.

III. Threat Model

In this section we define certain threats and the corresponding maintenance activities that mitigate them. Thus, we focus on threats that are frequently triggered by the passing of time, i.e., maintenance frequently deals with renewal and inspection of aged components, or particular events in the life of a SCADA system such as discovery of a new vulnerability. We then match these threats with mitigations in the form of maintenance tasks. Prior work, eg. [8], looked typically at a specific point in time, ignoring the evaluation of the system.

A. Threats

Typically, threats that exist at the time of system commissioning require attention throughout the life cycle of an automation system. However, some threats have a higher likelihood after system commissioning due to causes that can be mitigated by maintenance activities:

1) Security Component Malfunctioning: Almost any component can fail at any time. However, the chances of a failure can increase due to factors such as changes in system structure that put more demanding requirements on a security component. Another factor is the depletion of resources needed by security components. The consequences of a failure of a public key infrastructure or the login service are equal to a successful denial of service attack. On the other hand, a malfunctioning of the security logging system might be less critical in the short term. For instance, a steep rise of the amount of information a security event logger must process due to an increase of the number of controllers can render the event logging system unusable. Exhaustion of disk space or hardware failures can also contribute to malfunctioning or even to an outage of a security component. Missing updates of security components might leave them outdated and ineffective against new forms of viruses or malware.

2) Insider Attacks: Although insider attacks can happen even right after a system has been put into operation, gaining knowledge about the system, in particular about security procedures, makes it easier to conduct such an attack.

3) Unauthorized Access: Employees changing positions internally and externally require corresponding updates of their access rights. In particular, old accounts must be removed. Adjustments of internal policies, e.g., for network administration access, or legal regulations, e.g., for data privacy, might also impact access rights.

4) (Attack) Technology Improvement: Improvements in technology might make previously infeasible attacks feasible or might allow for completely new forms of attacks. For example, an increase in computing power might allow to recover data encrypted with 3DES in “reasonable” time. Further advances in quantum computers might break some protocols completely, e.g., protocols based on prime factorizations (RSA) or the discrete logarithm problem (Diffie-Hellman key exchange).

Improvements in radio technology might allow to pick up signals at greater distance, e.g., short-distance RFID/Bluetooth communication could be received outside of a production facility. Jamming using arrays of directional antennas or antenna arrays might selectively jam certain machines or devices. Low energy radiation from cables could become interceptable, allowing for easier eavesdropping. Therefore, trust boundaries could be altered in unexpected ways due to improvements in technology.

5) Shifting of Trust Boundaries: Even though automation systems are typically systems with a long overall lifetime, individual components are regularly replaced by components having potentially more features and interfaces. This can significantly alter the trust boundaries of a system. For example, a component might become completely configurable remotely (e.g., via wireless access or via remote commands over the network) without physical interaction. Thus, this component is subject to a variety of new threats, e.g., due to wireless access. Business processes might also change, resulting for instance in outsourcing of certain services or replacing components from one vendor by another, or by replacing self-manufactured components by components from third parties. This might also alter the trust boundaries, since third parties are generally less trusted than one's own employees.

B. Threats and Mitigations

The following matrix shows a possible set of threat - mitigation (maintenance) activities:

	Threat											
	Malware, Adware	Security component malfunctioning	Buffer overflow exploit	Insider Attack	Social Engineering	Advanced Persistent Threat	Denial of Service	Configuration Error	0-Day Attack	Unauthorized Access	(Attack) Technology Improvement	Trust Boundary Shifts
Mitigations: Security Maintenance Modules												
Virus and Malware Definitions Update	x				x		x				x	
Vulnerability and Patch Management	x		x			x	x		x		x	
Security Awareness of Personnel	x			x	x			x	x	x	x	x
User Account Maintenance										x		
Security Audits		x		x	x	x		x				x
Backups									x			
Security Log System, Public Key Infrastructure, Login Service Maintenance		x					x			x		
Technology monitoring	x			x	x				x		x	x

Fig. 1. Threat Model Extension

IV. Evaluation

As a case study for a general automation system we are considering a real-world industrial application: a substation automation system (SAS). The SAS monitors, controls and protects power equipment in a switchyard facility. Details can be found in the IEC 61850 standard [9]. The assessment is still ongoing.

V. Related Work

In the work of Igure et al. [10] the relevance of security maintenance for SCADA systems was stressed, mentioning the importance of security policies, 3rd party audits and configuration management. However, individual security tasks were not described.

The textbook on information security by Whitman et al. [11] devotes an entire chapter on information security maintenance. It provides general process models but it neither provides an explicit threat model nor does it discuss industrial automation systems.

VI. Summary and Conclusion

In a long-living industrial automation system, new threats occur due to the changing security landscape. In this paper, these threats have been identified and maintenance tasks that mitigate the risks were discussed and grouped into technology, system security, and personnel tasks. An evaluation on a real-world system is currently in progress. We consider our work as an important step towards a holistic security concept for industrial automation and control systems.

References

[1] M. Naedele, "Addressing IT security for critical control systems," in *HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 2007.

[2] M. Naedele, "IT Security for Automation Systems," in *The Industrial Information Technology Handbook*, R. Zurawski, Ed. CRC Press, 2005, pp. 1–14.

[3] S. Obermeier, R. Schierholz, and A. Hristova, "Securing industrial automation and control systems using application whitelisting," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation, ETFA 2014, Barcelona, Spain, September 16-19, 2014*, A. Grau and H. Martínez, Eds. IEEE, 2014, pp. 1–4. [Online]. Available: http://dx.doi.org/10.1109/ETFA.2014.7005242

[4] S. Obermeier, M. Wahler, T. Sivanthi, R. Schlegel, and A. Monot, "Automatic Attack Surface Reduction in Next-Generation Industrial Control Systems," in *Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Orlando FL, USA*, 2014.

[5] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: a systematic review of quantitative studies," *Information Management & Computer Security*, vol. 22, no. 1, pp. 42–75, 2014.

[6] D.-Y. Yu, A. Ranganathan, T. Locher, S. Capkun, and D. Basin, "Short paper: detection of GPS spoofing attacks in power grids," in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*. ACM, 2014, pp. 99–104.

[7] H. Holm, W. R. Flores, and G. Ericsson, "Cyber security for a smart grid-what about phishing?" in *Innovative Smart Grid Technologies Europe (ISGT Europe), 2013 4th IEEE/PES*. IEEE, 2013, pp. 1–5.

[8] D.-J. Kang, J.-J. Lee, S.-J. Kim, and J.-H. Park, "Analysis on cyber threats to scada systems," in *Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009*. IEEE, 2009, pp. 1–4.

[9] International Electrotechnical Commission, IEC TC57, "IEC 61850."

[10] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.

[11] M. Whitman and H. Mattord, *Principles of information security, 4th edition*. Cengage Learning, 2011.