HANDLING CYBER SECURITY UPDATES FOR PROTECTION AND CONTROL IEDS IN SUBSTATION DURING PRODUCT'S LIFE CYCLE

Sukumara T
ABB GISL – India
sukumara.t@in.abb.com

Eashwar Kumar R
ABB GISL – India
eashwar.r.kumar@in.abb.com

Niko LEHTONEN
ABB Oy - Finland
niko.lehtonen@fi.abb.com

Janne STARCK
ABB Oy – Finland
janne.starck@fi.abb.com

Fabrizio COMUZZI
ABB AG – Switzerland
fabrizio.comuzzi@ch.abb.com

ABSTRACT

Intelligent Electronic Devices (IEDs) used for protection and control of distribution networks are gaining increasing importance on the way towards Smart Grids. With the increasing communication capability, IEDs are imminently inheriting the cyber security related vulnerabilities. The challenge here is not just to develop secure communication architecture for IEDs but also create a robust firmware update process to resolve cyber security vulnerabilities being reported frequently these days. This paper presents an approach taken to handle these cyber security vulnerabilities by way of careful assessment of vulnerability reports and its applicability to IEDs/devices. Also described are careful analysis of cyber security updates, integration of these updates into the IED software architecture and making the IED’s cyber security architecture remain relevant and able to handle the cyber security vulnerabilities effectively.

INTRODUCTION

Smart grid deployments require data to flow seamlessly from various devices like protection relays, smart meters, controllers, gateways in a substation to enterprise level control centers over private and public communication networks.

Protection and control IEDs (Intelligent Electronic Devices), which are the first level intelligent devices in substations, play a critical role in substation protection, control and monitoring functionalities. They aid in the optimized management of substation primary devices, as well as the overall transmission and distribution power network, which is integral to the smart grid vision and framework. By adopting Ethernet based communication technology in its architecture, IEDs are able to exchange huge amount of data with local SCADA systems or remote control and maintenance centers. But this technology also introduces cyber security concerns previously associated only with office or enterprise IT systems.

Cyber security risks are inherited once an IED is connected on to the communication network. Securing IED communication is part of the *Defense-In-Depth* strategy which is a layered security approach that uses multiple layers of network security to protect the power system/substation automation network against intrusion from physical and cyber-borne attacks.

Concepts such as remote configuration/parameterization, monitoring, remote SCADA communication, remote diagnostics and firmware updates are becoming important requirements for IEDs. This leads to inherent requirements for Confidentiality, Integrity and Availability (CIA triad part of Information Security concept [2]) of information and data in Substation automation systems network. Secure communication, strong user authentication, authorization, logging and reporting have to be considered in the design and development of protection and control IEDs.

Development of security architecture design for IEDs should be able to adopt both current and upcoming cyber security standards like NERC CIP regulations, IEEE 1686, IEC 62351 etc. as parts of these standards define the cyber security capabilities to be adopted by IEDs in the substation and distribution systems.

With cyber security features becoming more dynamic, today’s ciphers and security protocols become vulnerable within years if not in months. As a consequence of this we have corresponding updates being released to overcome these vulnerabilities. IED software architecture teams need to analyze and validate these updates before integrating them into the software and releasing the firmware updates. This poses a challenge for device vendors in assigning resources to assess the impact of these cyber security updates and adopt these updates in the architecture of the IED. Moreover vendors must provide firmware updates to customers as a part of deployment process with minimal/no impact to existing customer configurations and minimal down-time.

FIRMWARE UPDATE CHALLENGES

IED firmware patch management is usually a cumbersome effort for the IED manufacturers as well as customers or power utilities. IED firmware upgrade process in field is challenging due to several reasons. Unlike desktop machines, banking software and any other commercial systems and applications, IEDs are pure embedded devices with a life cycle of 15 to 20 years. Also once the IED is in service on critical feeder or primary equipment, it's very difficult to obtain shutdown in order to update firmware at customer site/field. Also it's very important to retain or restore the customer's own customized configuration and protection settings after the completion of firmware update process.

Though some operating system vendors claim that we should be able to download cyber security libraries without updating the whole firmware, it requires having some supporting agents running in the device. In Substation automation context, the IEDs are being totally self-contained devices and should be able to perform their core operation without any external dependency, and therefore demand for a complete update of working binary or firmware.

Firmware update process usually requires secondary injection for Protection & Control application testing to validate the performance of the IED and also assess that the update does not have any impact on the existing functionalities. This can mean the update handling process is time and resource consuming especially if not planned properly.

CYBER SECURITY VULNERABILITY INCIDENTS

Consider a recent example of "Heartbleed" security bug in the OpenSSL cryptography library which had an impact on certain versions of OpenSSL library [4]. When this kind of issue comes up, there is an immediate OpenSSL patch released by open source organizations or community. But the IEDs at the substation automation level cannot be patched immediately and so frequently. This kind of knee jerk reaction is very risky. Careful evaluation is required to take decision on whether the released version of IED firmware has the affected version of OpenSSL library. If the OpenSSL version used in the IED does not have the Heartbleed bug, IEDs need not be updated at all! The update can wait or can be clubbed with some other significant updates. There are other factors that need to be considered, as well. For example, new cryptographic algorithms in future can be too complex and resource extensive that are not possible to handle in the existing hardware. Software update only may therefore not be enough.

Another vulnerability called SSLv3 POODLE cyber security was reported sometime during October 2014 [5], which forced manufacturers to disable support for SSLv3 version in the SSL/TLS stack and release the new firmware update for the IED. The issue was applicable for both SSL 3.0 server and client but server had highest impact. As IEDs mostly act as server device or information provider, the fix was more critical from the IED architecture perspective.

The frequency of these kinds of vulnerability reports will most probably increase further in coming days. The IED device manufacturers need to follow published alerts and advisories and analyze how these can impact the devices used on power system protection and automation devices.

CYBER SECURITY ARCHITECTURE IN IED

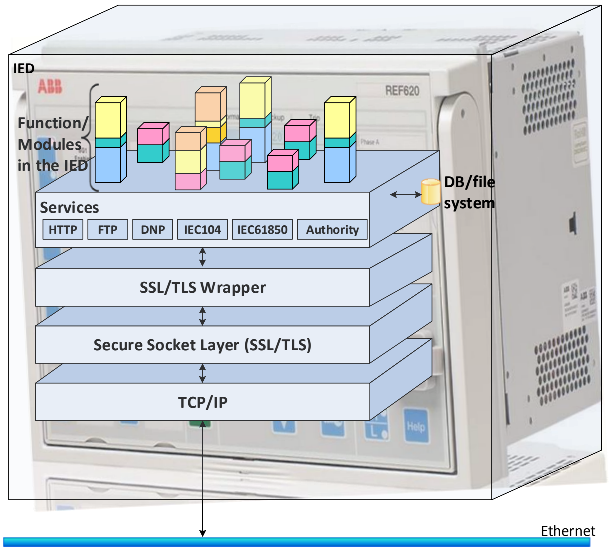

Figure 1 Cyber Security based Communication architecture overview in the IED

TLS based secured communication architecture suits IED for Ethernet network based communication design. Apart from secured communication, remote authentication, authorization, security log data transfer also go through the same SSL/TLS layer in the IED. Combining strong user access credentials verification along with TLS based communication mechanism provides better security architecture for IED.

Keeping the continual evolving and enhancements in cyber security features and its dynamics in mind, there is a need for maintaining the architecture design in-line with current and upcoming cyber security standards like NERC CIP regulations, IEEE 1686, IEC 62351 etc. as parts of these standards define the cyber security capabilities to be adopted by IEDs in the substation and distribution systems quickly without affecting its core architecture and functionalities.

Traditionally Ethernet based application protocols use TCP sockets to access the network layer and in-turn Ethernet network. With secured connectivity option, these socket objects are in-turn taken over by TLS module in order to establish secured channels with proper handshaking process like mutual authentication, key exchange and encryption of data packets. TLS protocol and crypto algorithms are part of the TLS module. Usually application protocol modules are independent of these crypto and TLS protocols with-in the IED architecture.

In the real implementation, as shown in *figure 1*, there will be a common wrapper for TLS stack with a set of common interfaces to provide transparent access to TLS layer. The intermediate TLS wrapper layer provides the abstraction. This wrapper can be extended to enable security for other protocols. This approach makes it easier to adapt the solution in the future depending on IEC 62351 standard.. Moreover, TLS stack upgrades do not affect the application protocols implemented in the IED.

The TLS handshake and session set-up in an IED is a CPU intensive operation with activities such as client authentication, certification handling and session key exchange. For SCADA protocol modules like DNP and IEC 61850, the handshake process takes place only at the beginning of the connection, as the session is expected to be continuous. On the other hand, in the configuration/engineering of protocol modules like FTPS and HTTPS, the handshake process could take place more often as the data transfer is not continuous and is only based on user request/operation. The TLS handshaking process is an independent activity and each application module/session will have a separate handshake process within the IED.

HANDLING CYBER SECURITY UPDATES

There are many cyber security vulnerabilities being reported these days in security protocols like TLS and cryptography libraries. Corresponding updates with fixes for these vulnerabilities/bugs are released frequently.

There has to be a systematic approach on how manufacturer needs to analyze and validate these updates thoroughly before adopting these updates within the IED product architecture.

The cyber security update process broadly involves the following steps:

1. Incident
2. Analysis
3. Change Management
4. Product decision
5. Product notification for Customer support Organization

This is explained in detail as shown in *figure 2*.

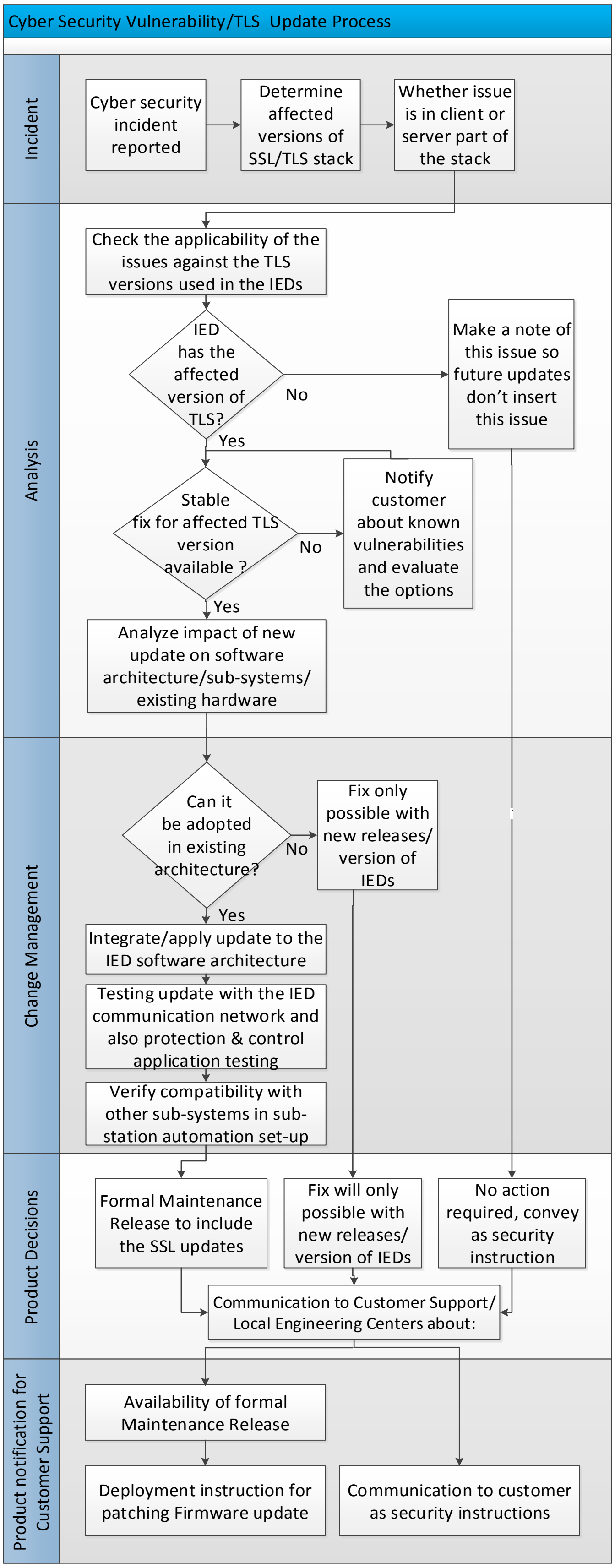
Cyber Security Vulnerability/TLS Update Process
Incident
Cyber security incident reported
Determine affected versions of SSL/TLS stack
Whether issue is in client or server part of the stack
Analysis
Check the applicability of the issues against the TLS versions used in the IEDs
IED has the affected version of TLS?
No
Make a note of this issue so future updates don't insert this issue
Yes
Stable fix for affected TLS version available ?
No
Notify customer about known vulnerabilities and evaluate the options
Yes
Analyze impact of new update on software architecture/sub-systems/ existing hardware
Change Management
Can it be adopted in existing architecture?
No
Fix only possible with new releases/ version of IEDs
Yes
Integrate/apply update to the IED software architecture
Testing update with the IED communication network and also protection & control application testing
Verify compatibility with other sub-systems in sub-station automation set-up
Product Decisions
Formal Maintenance Release to include the SSL updates
Fix will only possible with new releases/ version of IEDs
No action required, convey as security instruction
Communication to Customer Support/ Local Engineering Centers about:
Product notification for Customer Support
Availability of formal Maintenance Release
Deployment instruction for patching Firmware update
Communication to customer as security instructions

Figure 2 A typical Vulnerability handling process for IED

Firmware update usually requires secondary injection for testing all Protection & Control functions as well as extensive communication testing in substation automation set-up/communication network to validate the performance before formal maintenance release.

FIRMWARE UPGRADATION PROCESS

A typical substation automation communication set-up has been shown in *figure 3*. The various scenarios are covered in the figure about how the firmware upgradation can be done for the IEDs.

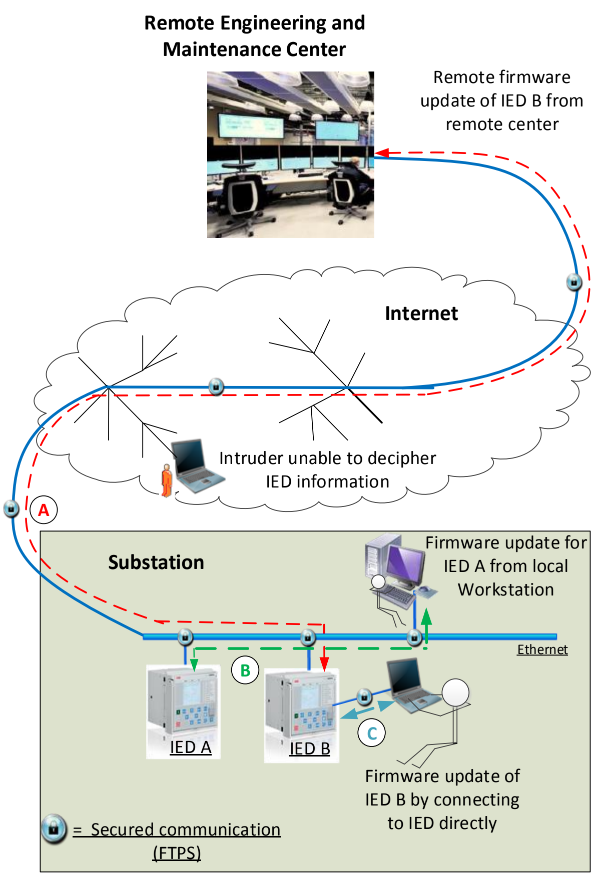
Remote Engineering and Maintenance Center
Remote firmware update of IED B from remote center
Internet
Intruder unable to decipher IED information
A
Substation
Firmware update for IED A from local Workstation
Ethernet
B
IED A
IED B
C
Firmware update of IED B by connecting to IED directly
= Secured communication (FTPS)

Figure 3 A typical Substation Communication network set-up with multiple firmware upgradation scenarios.

The firmware update can be done from remote Maintenance / engineering center (A). Firmware upgradation can be done within the substation by connecting to IED on the local Ethernet communication network (B). Firmware upgradation can also be done directly by connecting to front side maintenance Ethernet port of an IED (C).

For remote firmware update, prerequisite is that communication link must be secured. It's also very important to have rollback functionality supported in the IED so that in case of failure of firmware upgradation process, IED can still rollback to the previous stable version of the firmware and IED is still active and performing its core operation.

Once user has the formal compatible version of the Maintenance Release firmware for the IED, user has to check the deployment instructions/guidelines for the upgradation process. The generic flow chart for firmware upgradation process is shown in *figure 4.*

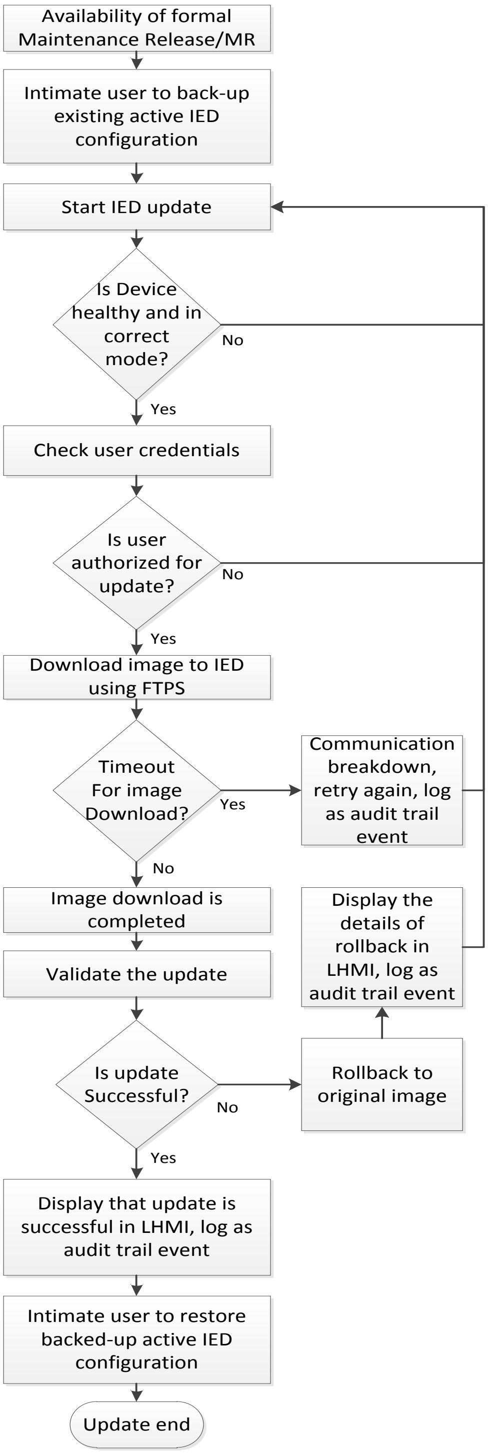
Availability of formal Maintenance Release/MR
Intimate user to back-up existing active IED configuration
Start IED update
Is Device healthy and in correct mode?
No
Yes
Check user credentials
Is user authorized for update?
No
Yes
Download image to IED using FTPS
Timeout For image Download?
Yes
Communication breakdown, retry again, log as audit trail event
No
Image download is completed
Validate the update
Display the details of rollback in LHMI, log as audit trail event
Is update Successful?
No
Rollback to original image
Yes
Display that update is successful in LHMI, log as audit trail event
Intimate user to restore backed-up active IED configuration
Update end

Figure 4 Overview of firmware upgradation flow chart

The firmware validation is also a part of the update process. This step is to ensure that the new firmware is compatible with existing hardware and software set-up of IED and when the active customer configuration is restored back, performance of the IED remains unaffected.

CONCLUSIONS

Cyber security environment is very dynamic and development efforts should be constantly vigilant and check regularly for new technology trends, vulnerability reports and related updates. The impact of these updates on the architecture of the IED and its adoptability needs to be assessed thoroughly before updating the IED firmware.

IED’s cyber security architecture should remain relevant, flexible and be able to adopt new cyber security updates with minimal impact on its core functionalities. This minimizes the possible IED protection and control testing time and also enables timely release of firmware upgrades.

Once we have the latest firmware maintenance release, deployment instructions, firmware upgradation process of IEDs must be clearly defined and passed on to customers. The firmware can then be upgraded properly in such a way that the active configuration is maintained and IED’s core operation and performance remain unaffected.

REFERENCES

[1] Sukumara T, Janne Starck,, Kishan SG, Harish G, Eashwar Kumar, 2013, *“Cyber Security – Secure Communication design for protection and control IEDs in sub-station”,* CIGRE D2 Colloquium, Mysore.

[2] Jacques Benoit, 2008, *“Meeting IED Integration Cyber Security Challenges”* Eskom Southern Africa Power System Protection Conference.

[3] Markus Braendle, Steven A. Kunsman, *“White paper Balancing the Demands of Reliability and Security Cyber Security for substation Automation, Protection and Control Systems”*, Cyber Security ABB White Paper.

[4] Alert (TA14-098A), 2014, *“OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)”*, https://www.us-cert.gov/ncas/alerts/TA14-098A

[5]Alert(TA14-290A), 2014,*“SSL 3.0 Protocol Vulnerability and POODLE Attack”*, https://www.us-cert.gov/ncas/alerts/TA14-290A