International Journal of Communication Networks and Security

Volume 1 | Issue 4 Article 14

April 2012

CYBER SECURITY SOLUTIONS FOR DLMS METERS USING GSM/ GPRS TECHNOLOGY

ANJU P RAJAN MATHEW
Department of CSE, The Oxford College of Engineering, Bangalore, anjuplamthottam@gmail.com

A. AJILAYLWIN
Department of CSE, The Oxford College of Engineering, Bangalore, aajilnila@gmail.com

SHAILESHWARI M U
Engineering Officer Grade 2, Central Power Research Institute, Bangalore, India,, shaileshwari@cpri.in

CYBER SECURITY SOLUTIONS FOR DLMS METERS USING GSM/GPRS TECHNOLOGY

ANJU P RAJAN MATHEW[1], A. AJILAYLWIN[2] & SHAILESHWARI M U[3]

[1&2] Department of CSE, The Oxford College of Engineering, Bangalore
[3]Engineering Officer Grade 2, Central Power Research Institute, Bangalore, India,
E-mail : anjuplamthottam@gmail.com, aajilnila@gmail.com & shaileshwari@cpri.in

Abstract - The Smart meters are used in the areas of generation, transmission, distribution and consumption. The capabilities of smart meter systems and grid networks, such as distributed intelligence and broadband capabilities can greatly enhance efficiency and reliability, but they may also create much new vulnerability if not deployed with the appropriate security controls. Much of the technology currently in use by the meters are outdated and in many cases unreliable. A system architecture implementing should recognize security threats and capture events that result not from external threats but from internal mistakes, with human error being a more common occurrence. An effective security approach enhances reliability because some security failures might be people failures, while others might be equipment failures, might be due to natural causes or might be deliberate. A simple perimeter defense is not sufficient; monitoring, both for events and physical actions, is required to bring the benefits of smart meters with minimal risk to this vital part of the infrastructure of modern life.

Keywords-*DLMS/COSEM, SmartMeters, Application Association (AA),GPRS, GEA, Signaling System 7 (SS7), TMSI, IMSI.*

I. INTRODUCTION

DLMS/COSEM specification specifies a data model and communication protocols for data exchange with metering equipment. It follows a three-step approach:

- Step 1. Modelling: This covers the data model of metering equipment as well as rules for data identification. The data model provides a view of the functionality of the meter, as it is available at its interface(s). It uses generic building blocks to model this functionality. The model does not cover internal, implementation-specific issues.
- Step 2, Messaging: This covers the communication services and protocols for mapping the elements of the data model to application protocol data units (APDU).
- Step 3, Transporting: This covers the services and protocols for the transportation of the messages through the communication channel.

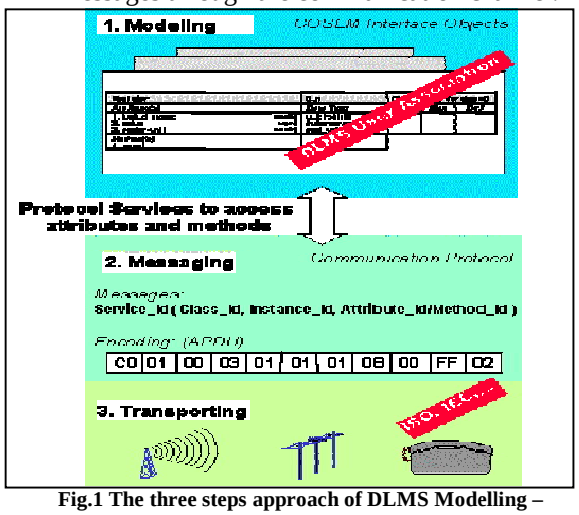

Fig.1 The three steps approach of DLMS Modelling – Messaging – Transporting

A. DLMS Based Smart Meter Overview

The liberalized energy market requirements given by DLMS meters are;

- Unbundling of monopolistic utilities.
- Introduction of competition in all activities: – generation – transport – supply – customer management -meter operation –meter reading – meter data management.
- Geographical dispersion, volatile customer base.
- Multi-energy - multi-user - multi-vendor environment.
- Need selective and secure access to data and interoperability.

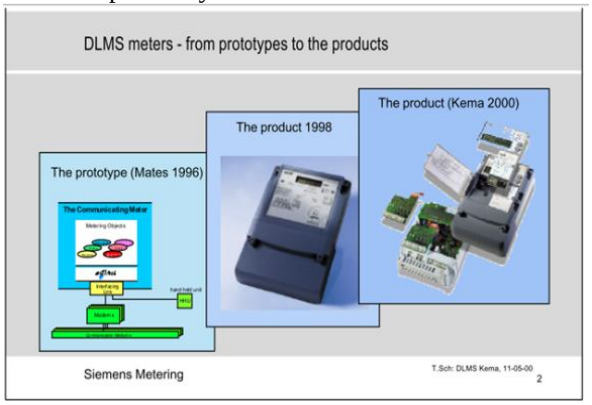

Fig.2 DLMS meter

B. Why DLMS

DLMS is comparable to a set of rules or a common language, on which the various operators have agreed. The DLMS-protocol enables the integration of energy meters with data management systems from other manufacturers. This secures that the energy supplier gets the full advantage of the meter functions. The utility that has invested in a smart metering solution pulls an enormous amount of

information out of the meters ie;information that can be used for a lot more than billing purposes such as:

- Load control
- Development of tariff models for special customer segments

DLMS-protocol enables Energy trade and has Low communication overhead. When using it only necessary data reaches utility software.

II. DATA ACCESS SECURITY IN DLMS METER

Data access security concerns role based access to data in a DLMS/COSEM device. It is managed by the Association LN / Association SN objects. Each COSEM server i.e., a logical device may support AAs with various clients, each having a different role, and with this, different access rights. Each AA is identified with a pair of lower layer addresses. Each Association object provides a list of objects visible in that particular AA and the access rights to their attributes and methods. To be able to access data, the client must be properly authenticated. Upon AA establishment, an authentication context is negotiated between the client and the server. This specifies the required authentication of the peers, and, where needed, the security algorithm to verify the authentication.

A. Authentication In Data Exchange

The security of exchanges includes authentication of the Client and the Server, confidentiality of exchanged datacontrol of access to the variable objects of the Server. Authentication enables the Server to control the identity of the Client in order to provide with proper access rights. When this authentication is mutual, the Client can also control the Server. The data confidentiality is taken care for authorized readings only and data exchange is protected. Masking options of the message and time provides additional and adequate security.

The standard supports two security schemes that are defined in ICS:

- Basic security
- Advanced security.

B. Basic security (Authentication)

Basic security is an access control which provides authentication as addressed in COSEM specification. In order to provide different levels of security for authentication support, COSEM specifies three levels of authentication securities:

- No authentication (lowest level) security.
- Low level, password based authentication security (LLS) identifying only the client.
- High-level, four-pass authentication security (HLS) identifying both the client and the server.

The meter supports three associations in the Management Logical Device:

- Public Client association (PC)
- Meter Reader association (MR)
- Utility Settings association (US)

C. No authentication security

This level provides access to the server without any authentication during sign on the access to the server is read only for PC association.

D. Low-Level Security

Low level authentication security offers adequate security to avoid eavesdropping and message (password) replay during data transfer. This level of security is mandatory in MR association which will have a password for data download. The association objects provide an attribute called 'LLS_secret' to change the secret (low level security password) only by the authorized client.

Verification of Low-Level Security: Client transmits a 'secret' to the server, by using the 'Calling Authentication Value' parameter of the COSEM-OPEN. Request service primitive of the client application layer.The server verifies the received 'secret' with the corresponding client identification and the association is established, if the received 'secret' is valid.

E. High Level Security

High-level authentication security is typically used when the communication channel offers extrinsic security and suitable measures to be taken to avoid eavesdroppers and message (password) replay. This level of security is mandatory for the US mode of association. HLS mechanism defines a 4-pass sign-on scheme where the client and server exchange challenges and then reply to the challenges with a processed response. The processing performed on the challenges is an encryption using a secret key.

Pass1: The client transmits 'challenge' to the server (CtoS).

Pass2: The server transmits 'challenge (as acknowledgement)' to the client (StoC).

Once the Pass 2 is also valid, the association is formally established between the client and the server but the access of the client is restricted to the method "reply to HLS authentication" of the current "association" object.

Pass3: The client processes StoCin a secret way. The result of (StoC) is sent back to the server. The server checks the result of correct processing and if correct the server accepts the authentication of the client.

Pass4: If the client is authenticated, the server processes (CtoS) in a secret way. The result of (CtoS) is sent back to the client. The client checks the result of the correct processing and if correct, the client accepts the authentication of the server.

Pass3 and Pass4 are supported by the method"reply_toHLS_authentication"of the association object(s). If both passes are successfully executed, then full access is granted according to the current association. Otherwise, either the client or the server aborts the association. Inaddition; the association object provides the method to change the HLS 'secret' (e.g. the encryption key):

change_HLS_secret.

F. Advanced Security (Data Security)

Transport of data is done in secret way e.g. the encryption key. Encryption is the conversion of data into a form, called a cipher text. Chipper text cannot be easily understood by unauthorized client. It is mostly used for data security purpose. The proposed standard for encryption is AES GCM for ICS.

III.GRID NETWORK VULNERABILITIES

The listed vulnerabilities are not necessarily ordered according to severity, which is affected by the particular utility type, infrastructure, potential attacker profile and many other factors that need to be determined in the general risk assessment process.

A. Network Management from Remote Nodes

Each meter is a node in the Smart Grid network. Although the processesbeing executed on the network require only data to be read and commands tobe sent to the meter, the management applications and services remainexposed and available for all the nodes.The practical implications of this scenario is that without explicit constraints,an attacker who uses the communication module of the smart meter cancause network-wide changes, ranging from disrupting the communication flowto rerouting all the traffic to his node for later manipulation.

B. Lack of Authentication

Security [6] has encountered numerous meters that didn't have anyauthentication or encryption support. This design flaw makes it possible for anattacker to impersonate the control center and send unauthorized commandsto meters or read metering data. The consequence of a successful attack onmeters with disconnection capabilities is particularly destructive. It should be noted that although some of the metering protocols supportencryption, which can be viewed as a network access password, most of thedeployments we've encountered so far did not enable these features. Sinceevery metering standard includes support for "no encryption" or "noauthentication", it usually poses too great a temptation for the integrationteams which prefer to choose these settings in order to avoid additionaldeployment problems.

C. Authentication Bypass

Several metering protocols (DLMS, IEC 60870-5-102) implementation havefunctions to read metering data which do not require a password, andconfiguration/disconnect functions that require the operator password. Twometers that we audited retrieved the password for the restricted functionsusing the unprotected read function. This implementation makes theauthentication/password protection completely useless.

D. Slave Meter Data Tampering

The protocol used for communication between the master (smart) meter andthe slave meter is usually considered of lesser importance as its impact isrestricted to the single customer household. Although this is generally correct,from a risk management point of view it is important to identify and address asituation where a cheap "man in the middle" device is inserted between themaster and slave meters which lowers the usage reading by a constantdivision.

This manipulation is both very hard for the utility to identify and canhappen in a large scale if a criminal party decides to mass produce andmarket these devices – much like pirate cable set-top boxes / satellitedecoders.

E. Slave Meter Unauthorized Disconnection

Some slave meters support disconnection of the customer upon receiving arequest from the master meter. Normally the associated risk is minimal as ifan attacker was to disconnect the slave meter, as these meters are commonlyconnected by wire to the master meter the physical presence is required andtherefore disconnection could be achieved by bringing a hammer. Thisassumption causes to set low security settings to this communication channel,as it is perceived as non-critical. Unfortunately, some of the meteringprotocols used between meters are wireless (e.g. WMBUS, Z-Wave) making itpossible for an attacker with a potent transmitter to send a disconnect signalto multiple customers, especially in crowded urban areas. The attacker will notneed receive the data back from the meters to issue this command.

F. Insecure Protocol Implementation

Meters from a variety of vendors that were audited by Security [6] were foundto improperly handle malformed requests. When a meter firmware makescertain assumptions regarding the data it receives, and in particular themaximum size of each message type, it may be vulnerable to a very well-known attack condition named Buffer Overrun/Overflow Vulnerability. Thisvulnerability may allow the attacker to cause system instability or freeze,change values of parameters which are saved in the memory stack or evenexecute arbitrary code. In most of the meters and RTUs that were audited byour "red team", such a condition was identified and exploited.

G. Firmware Upgrade Vulnerabilities

Firmware upgrades are a double edged sword. The existence of the capabilityto remotely upgrade the meter firmware is of crucial importance – as securityexperts like to repeat a well-known, and true, mantra that "what is consideredsecure today may be proven otherwise tomorrow". There's no assurance thata new unforeseen attack will successfully compromise a meter model and soin order to be able to respond the operator must have the ability to securelyupdate the meter firmware to upgrade as many meters as it can before theyare compromised.The other side of firmware upgrades is

that they serve as a powerful tool forattackers, if they can be abused. For example, an attacker who can push hisown firmware to other meters can execute a disconnect action and then makethe meter completely unresponsive till it is returned to the manufacturer, thusmaking it impossible for the network operator to reverse his actions.To conclude, it is crucial to have a remote firmware upgrade capability, butone that was designed with security in mind and audited thoroughly byexperts.

H. Input Validation

The all-too-familiar security problem of input validation, which is unfortunatelyquite common in control systems, was found to exist in Smart Grid meters andservers as well. Should an attacker be able to broadcast malformedmessages to a node on the Smart Grid (which we elaborated on why that cannormally easily be done) it will have a relatively high success probability tocause the node to fail. The failure is a result of assuming that the datareceived is in the expected message format, whereas when a malformedpacket is parsed it causes an exception that may even lead to arbitrary codeexecution.

IV.GPRS SECURITY ARCHITECTURE

In order to meet security objectives, GPRS employs a setof security mechanisms that constitutes the GPRS security architecture. Most of these mechanisms have beenoriginally designed for GSM, but they have been modified to adapt to the packet-oriented traffic nature and theGPRS network components. The GPRS security architecture, mainly, aims at two goals: a) to protect the networkagainst unauthorized access, and b) to protect the privacyof users. It includes the following components:

- Subscriber Identity Module (SIM)
- Subscriber identity confidentiality
- Subscriber identity authentication
- User data and signaling confidentiality between the MS and the SGSN
- GPRS backbone security

A. Subscriber Identity Module – SIM

The subscription of a mobile user to a network is personalized through the use of a smart card named SubscriberIdentity Module (SIM). Each SIM-card is unique andrelated to a user. It has a microcomputer with a processor, ROM, persistent EPROM memory, volatile RAM and an I/O interface. Its software consists of an operatingsystem, file system, and application programs (e.g., SIMApplication Toolkit). The SIM card is responsible for the authentication of the user by prompting for a code (Personal Identity Number PIN).

A serious weakness of the GPRS security architecture isrelated to the compromise of the confidentiality of subscriber identity. Specifically, whenever the serving network (VLR or SGSN) cannot associate the TMSI withthe IMSI, because of TMSI corruption or database failure, the SGSN should request the MS to identify itself bymeans of IMSI on the radio path. Furthermore, when theuser roams and the new serving network cannot contactthe previous (the old serving network) or cannot retrievethe user identity, then, the new serving network shouldalso request the MS to identify itself by means of IMSIon the radio path. This fact may lead an active attackerto pretend to be a new serving network, to which theuser has to reveal his permanent identity. In addition, inboth cases the IMSI that represents the permanent useridentity isconveyed in clear-text over the radio interfaceviolating user identity confidentiality.

B. Subscriber Identity Authentication

A mobile user that attempts to access the network mustfirst prove his identity to it. User authentication protects against fraudulent use and ensures correct billing.GPRS uses the authentication procedure already definedin GSM with the same algorithms for authentication andgeneration of encryption key, and the same secret key, Ki. However, from the network side, the wholeprocedure is executed by the SGSN (instead of the basestation) and employs a different random number (GPRS-RAND), and, thus, it produces a different signed response(GPRS-SRES) and encryption key (GPRS-Kc) than theGSM voice counterpart.

The authentication mechanism used in GPRS also exhibits some weak points regarding security. More specifically, the authentication procedure is one-way, and, thus, it does not assure that a mobile user is connected to anauthentic serving network. This fact enables active attacks using a false base station identity. An adversary, who has the required equipment, may masquerade as alegitimate network element mediating in the communication between the MS and the authentic base station. Thisis also facilitated by the absence of a data integrity mechanism on the radio access network of GPRS, which defeats certain network impersonation attacks. The resultsof this mediation may be the alternation or the interception of signaling information and communication dataexchanged.

C. Data and Signaling Protection

User data and signaling protection over the GPRS radioaccess network is based on the GPRS ciphering algorithm (GPRS-A5), which is also referred to as GPRS Encryption Algorithm (GEA) and is similar to the GSMA5. Currently, there are three versions of this algorithm: GEA1, GEA2 and GEA3 (that is actually A5/3), whichare not publicly known, and, thus, it is difficult to performattacks on them. The MS device (not the SIM-card) performs GEA using the encryption key (GPRS-Kc), since itis a strong algorithm that requires relatively high processing capabilities. From the network side, the serving SGSNperforms the ciphering/deciphering functionality protecting signaling and user data over the Um, Abis, and Gbinterfaces.

An important weakness of the GPRS security architectureis related to the fact that the encryption of signaling anduser data over the highly exposed radio interface is notmandatory. Some GPRS operators, in certain countries,are never switch on encryption in their networks, sincethe legal frameworks in these countries do not permit that. Hence, in these cases signaling and data traffic are conveyed in clear-text over the radio path. This situation isbecoming even more risky from the fact that the involvedend-users (humans) are not informed whether their sessions are encrypted or not.

D. GPRS Backbone Security

The GPRS backbone network includes the fixed networkelements and their physical connections that convey userdata and signaling information. Signaling exchange inGPRS is mainly based on the Signaling System 7 (SS7)technology, which does not support any security measure for the GPRS deployment. Similarly, the GTP protocol that is employed for communication between GSNsdoes not support security. Thus, user data and signalinginformation in the GPRS backbone network are conveyedin clear-text exposing them to various security threats.In addition, inter-network communications (between different operators) are based on the public Internet, whichenables IP spoofing to any malicious third party who getsaccess to it. In the sequel, the security measures appliedto the GPRS backbone network are presented.

Based on the analysis of the GPRS security architectureit can be perceived that the GPRS securitydoes not aim at the GPRS backbone and the wire-lineconnections, but merely at the radio access network andthe wireless path. Thus, user data and signaling information, conveyed over the GPRS backbone, may experience security threats, which degrade the level of securitysupported by GPRS. In the following, the security weaknesses of the GPRS security architecture that are relatedto the GPRS backbone network for both signaling anddata plane are presented and analyzed.

V.CONCLUSION

System security and Data security is a critical issue today. A comprehensive architecture with security built in from the beginning is necessary. Grid security involves an architecture that includes security from the beginning, consists of more than just protective devices such as firewall, and engages processes as well as products. A simple perimeter defence is not sufficient; monitoring, both for events and physical actions, is required to bring the benefits of grid with minimal risk to this vital part of the infrastructure of modern life. GPRS promises to benefit network users greatly by providing always on higher bandwidth connections than are widely available today. In order to be successful, data connections must be secure and be available all the time from anywhere. The maturity of security in the air interface and the low bandwidth available limits the effectiveness of the Network Station as the source of attacks. With the increase in the use of wireless media, security problems of confidentiality, integrity, and authentication are also increasing. The weak points of the GPRS security architecturemay lead to compromises of end-users and network security of the GPRS system. The proposed enhancements can be easily integrated in the existing GPRS infrastructure, minimizing the required changes.

ACKNOWLEDGMENT

Authors gratefully acknowledge the officers of Utility Automation Research Center in Central Power Research Institute, Bangalore for the technical support provided by them. We would like to thank all the lectures in the Dept.of CSE from The Oxford College of Engineering whose support made a difference in research. We also thank the HOD of CSE Dr. R. J. Anandhi for her encouragement and support in our endeavors.

REFERENCES

[1] BLUE, GREEN & YELLOW BOOK FROM DLMS UA.

[2] SOMOGYI Tibor, "DLMS-the Application Protocol for communicating meters", *Essen*, April, 1997.

[3] *Report of High Level Committee on Standardization of Meter Protocol*,Central Electricity Authority New Delhi, December 2008.

[4] Rupok, M.S.A,"Design and implementation of a novel remote metering system using USB GPRS/EDGE modem",Electronics Computer Technology (ICECT), 2011 3rd International Conference on,July 2011

[5] GPRS Security Threats and Solutions,March 2002[Online], Available:http:// www. netscreen.com /us/ en/training/ GPRS Security.pdf.

[6] The Dark Side of the Smart Grid -Smart Meters (in) Security, 2011[Online], Available:http:// www.c4security.com/c4/TheDarkSideofheSmartGridSmartMeters (in) Security.pdf.

[7] Wilayat Khan and HabibUllah," Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography",*IJCSI International Journal of Computer Science Issues*, Vol. 7, Issue 3, No 9, May 2010.

[8] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun.17,2009 [Online]. Available:http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf.

◈◈◈