Modelling Approach for Crypto based Security Service in Embedded Environment

S.N.Sivanandam[1] G.R.Karpagam[2]
[1]Professor and Head [2]Assistant Professor
Department of Computer Science and Engineering, PSG College of technology, Coimbatore-641004
Email: rm_grk@yahoo.com

Abstract

The aim of the paper is to investigate how to take advantage of Object Management Group's (OMG) Model Driven Architecture (MDA) for Security service design in Embedded systems. The requirements for security services do not remain constant, during its lifetime. Therefore, solutions have to evolve in order to fulfill the new requirements. This work tackles the problems related to evolution of crypto based security services. MDA concepts like Platform Independent Models (PIMs), Platform Specific Models (PSMs) and Transformation models between PIM and PSM are used in security service modeling, design and evolution. The intensive use of models helps the embedded system developer in achieving round trip engineering and subsequently preserves the efforts involved in security service development.

Key Words: Model Driven Architecture - Platform Independent Model - Platform Specific Model- Embedded system - Security Services

1 Introduction

An Embedded environment captures, stores, manipulates, and accesses sensitive data. Therefore, it poses several security challenges. Security has been the subject of intensive research in the areas of Embedded environment and networking. Researches in security services are two fold Design of reusable security service components and implementation of new findings, refinements in security algorithms and protocols. Scope of this paper is towards the first fold.

2 Related Work

Embedded systems are constrained by the environments they operate in, and by the resources, they possess. For such systems, there exist several factors like security against software, side-channel attacks, computational demands, tradeoffs between factors such as security, cost and performance, operations under stringent resource constraints, rapid evolution of security mechanisms, standards etc. This requires moving security considerations from a function centric perspective into system architecture [6].

Cryptography in Embedded Systems

The work of Thomas Wollinger introduces the basic concepts, characteristics, and goals of various cryptographic algorithms. It is shown that embedded systems are essential parts of most communications systems and how this makes them especially attractive as a potential platform to implement cryptographic algorithms. Furthermore, although a challenging task, previous implementations of arithmetic intensive cryptographic algorithms seem to indicate that they can achieve acceptable performance on embedded processors and constrained platforms. Thus, designing and implementing efficient cryptographic algorithms on embedded systems will continue to be an active research area.

Security requirements for Embedded systems

In the paper by Paul Kocher, in an Embedded environment, when two entities send or receive sensitive information using public networks or communications channels accessible to potential attackers, they should ideally provide security functions such as *data confidentiality*, *data integrity*, and *authentication* [12]. Data confidentiality protects sensitive information from undesired eavesdroppers. Data integrity ensures that the information has not been changed illegitimately. Authentication verifies that the information is sent and received by appropriate parties rather than masqueraders. Access to the embedded system should be restricted to a selected set of authorized users (*user identification*), while access to a network or a service has to be provided only if the device is authorized (*secure network access*). Another essential security function is the *availability* of the embedded system. *Secure storage* involves securing information in the embedded system's storage devices, external or internal to the system. *Content security* protects the rights of the digital content used in the system and T*amper resistance* refers to the desire to maintain these security requirements even when the device falls into the hands of malicious parties. The evolution of cryptography based security services for embedded environment stared from user password to Identity-Based Encryption. Embedded systems are responsible for the availability and functionality of many critical systems, from factory automation to networking equipment. One appealing solution to the key size disparity problem is the promising family of asymmetric algorithms known as Elliptic Curve Cryptography, or ECC.ECC uses much smaller key sizes than other asymmetric techniques, while providing equally strong security. Due to the difficulty in breaking its encryption, Elliptic Curve Cryptography can provide the same level of RSA encryption at a greatly reduced bit size. This is very important to embedded developers and vendors for whom power drain, memory, processor requirements and bandwidth requirements are limited and of concern. There is an obvious cost savings to the use of ECC algorithm [8].

Model Driven Architecture

Model Driven Architecture is an approach to IT system specification that separates the specification of system functionality from the specification of the implementation of the functionality on a specific technology platform. Models in MDA are of two types – **Platform Independent Model** (PIM) and **Platform Specific Model** (PSM). PIM describes a platform independent specification of the functionality of the application. PSM defines a platform specific model of the system incorporating technology-specific details. It is derived from PIM by applying platform specific translation rules.

Key standards in MDA are UML, XMI, MOF and CWM. **UML** (Unified Modeling Language) has become the language of choice for representing software designs and architectures [9,14]. **XMI** (XML Metadata Interchange) is an XML-based representation of the UML models. Saving in XMI provides for vendor interoperability of the models. **CWM** (Common Warehouse Meta-model) is a data warehouse standard that address entire lifecycle of design, build and management of data warehousing applications. All the above standards are built on **MOF** (Meta-Object Facility). MOF provides constructs for representing meta-models [2,3,4,5].

Modeling Methodology for Integrated Simulation of Embedded Systems

The framework described in this paper attempts to fulfill an important void in the area of embedded systems design. The research demonstrates the potential of Model-

Integrated Computing in providing a unified environment for multi-granular simulation of embedded systems. Driving different simulators using automated model interpreters from the same set of models representing a system design helps to maintain consistency and improves design flexibility. Deriving simulations at multiple-levels of granularity helps the system designer in performing rapid trade-off decisions and helps elevate time-to-market pressures. Further, there is a potential of automatically synthesizing systems from the models. This paper illustrates many issues in computer automated Multilanguage modeling, using the Model-based Integrated Simulation Framework (MILAN) project as a vehicle [1,15]

SCADA (Supervisory Control and Data Acquisition)

SCADA is a control system, and a supervisory level software package that is positioned on top of hardware to which it is interfaced, through Programmable Logic controllers. In SCADA system, client layer interacts with user and data server layer handles process data control activities. The data servers communicate with devices through process controllers. Data servers are connected to each other and to client stations through network.

SCADA makes use of multi-tasking and real-time database located in one or more servers. Servers are responsible for acquisition, alarm checking, calculations, logging and archiving.[16]

Attacks over SCADA System

The possible methods of attacks on SCADA systems include Eavesdropping, Masquerading, Tampering and replaying. Eavesdropping is obtaining copies of messages without authority like learning the information from the data server like substation ids, login information of SCADA or near by terminals. Masquerading is Sending/ receiving messages using identity of another without their authority. Tampering is Intercepting messages and altering their contents before passing them to intended recipient, trying to modify corporate data, process set points in SCADA server for malicious purposes. Replaying is Storing messages and sending them later. Impersonation is passing information to a person who poses as intended recipient. Spoofing is pretending as a user, or a computer identifying itself as a site when it isn't.

Cryptographic algorithms that are in existence for SCADA security are 3DES, AES; bit length of 128 minimum for encryption, RSA (1024 bit minimum), ECDSA (160 bit minimum) for Digital Signing and SHA-1, Key exchange for Integrity hashing

3 MDA based security service development for SCADA

SCADA is taken as a case study to prove the applicability of MDA in Cryptographic security evolution. The attacks and possible solutions for attack were analyzed as shown in **Table 1**. MDA tool Generic Modelling Environment (GME) is used for development of the models [7]. SCADA environment and its security services are represented in the Metamodel (Meta PIM, Meta PSM). Transformation is achieved by developing an interpreter. **Figure 1** depicts the phases of the proposed scheme [11,17,18].

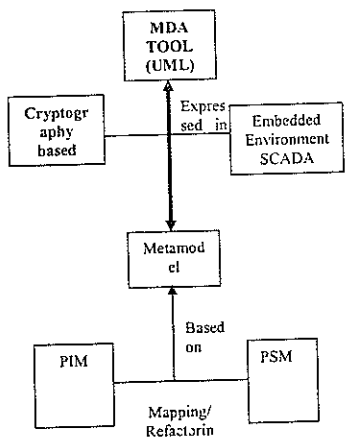


Figure 1 MDA based security Software Development for SCADA

The Sequence of steps involved in the transformation of PIM-PSM (Forward Engineering) are Design of MetaPIM, Mapping of PIM from metaPIM and Transformation of PIM to PSM. The sequences of steps involved in the transformation of PSM-PIM (Reverse Engineering) are Design of MetaPSM from the legacy code, Mapping of metaPSM to met PIM and Transformation of PSM to PIM.

Attack	Impact of Attack
Denial of service	Hanging of the server or shutdown
Username and Password attacks	Information mining
System set point attacks	Information mining
Mine Corporate data for personal gain or to sell to competitor	Information mining
Change of Data Points, Set point(s) System or in Data server	Information Tampering/Replaying
Modify Data points on graphics to deceive Operators that system is out of control and must Shut Down	System shutdown
Capture, Modify, or Delete Data Logged in Operational Database ,Locate Maintenance Database, modify or delete information regarding reliability tests , Calibration for equipment	Information Tampering

Table 1Attacks on SCADA

Forward Engineering Process: (PIM – PSM)

Meta PIM is designed to provide ECC based cryptographic services to the SCADA applications. It simulates the working environment of the SCADA thereby considering and applying the security concerns wherever needed. The process of MetaPIM development involves Identification of the entities., Defining the attributes, Designing the constraints and functions **[19]**. The metaPIM templates of SCADA ECC using GME are shown in **Figure 2 and Figure 3** respectively. **Figure 4** shows the Platform Independent models generated from metaPIM

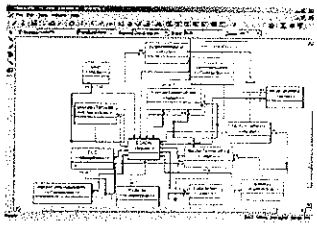


Figure 2 MetaPIM Template of SCADA security

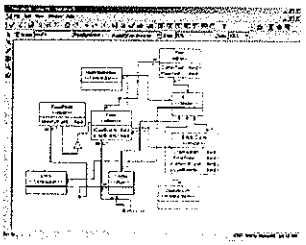


Figure 3 MetaPIM Template of ECC

MetaPIM to MetaPSM Transformation: Models in the Meta PIM are mapped onto the Packages and the atoms they contain are mapped onto classes.. In addition, the different functions and their prototypes are modified so that they are specific to the java platform. The transformation will *map* the platform independent model into a more detailed platform specific model using mapping rules. These rules are specified at a metamodel level so that they are applicable to all sets of source models **[10,20,21]**.

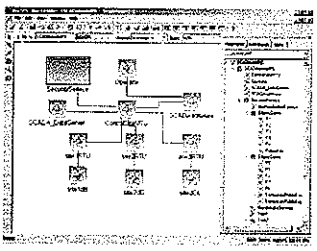


Figure 4 Platform Independent Model Template

Logic of PIM to PSM Transformation:

The three tasks involved in the transformation are: First, it takes an input PIM model as a XML document. Second, it verifies the correctness of the marked PIM. Third, it performs a transformation by activating a matching mapper corresponding to the marked stereotypes in the input model. The mapper takes the marked model and its corresponding annotation to generate the target PSM as shown in **Figure 5 [20,21]**. The output result can directly be generated into an executable code. PSM is based on Java Platform. However, a given PIM can be transformed to any PSM. The PSM can be transformed to code using code generators. The screen shot of skeleton code is shown in **Figure 6**.

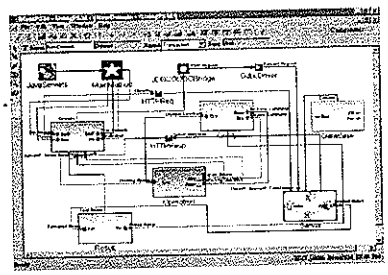


Figure 5 Platform Specific Model Template

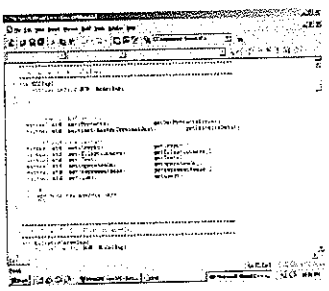
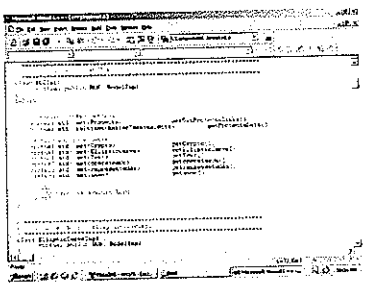


Figure 6 Skeleton Code



4 Discussions and Conclusion

The security service in embedded environment is evolving every day. So, it is required to protect the design and development efforts. This is realized using MDA that envisions software development as a translation of models from stage to stage. It will enable usage of models across technology platforms. This paper demonstrated the MDA approach for security in SCADA application. Models for crypto based security service was designed with Generic Modeling Environment tool and is forward engineered to code. Changes in the code can be reverse engineered to get the updated model. Models are easier to read and understand than source code. The conceptual model of SCADA security software stays the same, when technology changes. The same model may be implemented into multiple platforms and programming languages. The future goal is to extend the work to support for a family of embedded systems, which will help in formalization of ESML (Embedded security Markup Language). The models generated are limited to certain modeling tools. So MDA components can be developed which can be Platform independent, Language independent and Middleware neutral, so that the components are adoptable in any cluster of tools **[13]**.

References

1. Agrawal. A et al . MILAN: A Model Based Integrated Simulation Framework for Design of Embedded Systems, Workshop on Languages, Compilers, and Tools for Embedded Systems (LCTES 2001), Snowbird, Utah, June 2001
2. Alhir. S, Understanding the Model Driven Architecture, Methods & Tools: An international software engineering digital newsletter, Martinig ssociates,2003 www.home.earthlink.net/~salhir / UnderstandingThe MDA.PDF
3. Anneke Kleppe, Jos Warmer, Wim Bast, MDA Explained: The Model Driven Architecture—Practice and Promise Addison-Wesley, First edition 2003.
4. Atif Mashkoor, Investigating Model Driven Architecture,Master Thesis,Department of Computing Science Umea University Umea, Sweden,2004
5. Daniel Exertier, Benoit Langlois Xavier Le Roux, PIM Definition and Description, Thales Research and technology, 2003 www.modeldrivenarchitecture.esi.es/pdf/paper2-1.pdf,

6. Gartner, The evolution of security architecture, (Strategic Planning Series-3.0), 2004 www.regionals4.gartner.com/regionalization/img/gpress/pdf/ 2004_chapter_security.pdf
7. Institute software Integrated Systems, GME user Manual, Vanderbilt University, 2004 www.isis.Vanderbilt.edu
8. Jerry Krasner, Using Elliptic Curve Cryptography for Enhanced Embedded Security(Embedded Market Forecasters), American Technology International, Inc., 2004 www.certicom.com/catchthecurve/emf
9. Miller.J & Mukerj J, Model Driven Architecture, Object Management Group, 2001
10. Nagaraj N.S & Srinivas Thonse, MDA – Enabling seamless application development,(set labs whitepaper) Comfactory, SETLabs, 2001 www.infy.com/Technology/mdaanalysis.pdf
11. Parastoo Mohagheghi, Jan Pettersen Nytun, Selo and Warsun Njib, MDA and Integration of Legacy Systems: An Industrial Case Study, 2003 www.idi.ntnu.no/grupper/su/publ/pdf/mda-paper-19jun2003.pdf
12. Paul Kocher , Ruby Lee, Gary, Anand & Srivaths, Security as a new dimension in embedded system design, DAC 2004, San Diego, California, USA, 2004, 46(1),753.
13. Philippe Desfray MDA – When a major software industry trend meets our toolset, implemented since 1994,– (Softteam R&D-version 1.2), 2003 www.omg.org/mda/mda_files/MDA-Softeam-WhitePaper.pdf
14. Poole J Model-Driven Architecture: Vision, Standards and Emerging Technologies, Position Paper ECOOP 2001: Workshop on Metamodeling and Adaptive Object Models, 2001www.cwmforum.org/Model-Driven%20 Architecture.pdf
15. Selo, MDA and Integration of Legacy Systems, Masters Thesis in Information and Communication Technology, Agder University College, Grimstad, 2003 www.idi.ntnu.no/grupper/su/publ/pdf/mda-paper-19jun 2003.pdf
16. Sivanandam S.N & Karpagam G.R, A Novel approach for practical comparison of crypto techniques using object oriented framework in SCADA system, 2003, pp 53-68
17. Sivanandam S.N & Karpagam G.R, An Emphasis on the need of IDE/ITE , A step ahead into modeling Technology ,Proceedings of 4th National Conference on advanced Computing, 2004 ,Vol 4, 101-107.
18. Sivanandam S.N & Karpagam G.R(2004), Certain Investigations on applying model driven architecture for security services, Proceedings of 4th National Conference on advanced Computing, 2004, Vol 4, pp 95-101
19. Sivanandam S.N & Karpagam G.R, Applying Model driven Architecture for embedded systems,Technology,2003 Journal,13-20.
20. Sivanandam S.N & Karpagam G.R.Design of reusable models for security service in Distributed environment, Technology Journal, P S G College of Technology, Coimbatore College of Technology, 2003 pp 20-24
21. Sivanandam S.N & Karpagam G.R, Novel approach for Implementing Security services,2004,pp13-18, www.acadjournal.com /2004/V13/Part6/p6/ .