الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونيرسيتي إسلام انتارابغسا ملسيا

SECURING A LOW LEVEL READER PROTOCOL (LLRP) CONNECTION AND AN EVALUATION OF ITS PERFORMANCE

BY

SANA QADIR

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Science (Computer and Information Engineering)

Kulliyyah of Engineering
International Islamic University Malaysia

JANUARY 2010

ABSTRACT

EPCglobal Inc is the body in charge of supervising the development of RFID standards for supply chain management. One of the latest EPCglobal Standards to be in the limelight is the Low Level Reader Protocol (LLRP). This protocol standardizes the interaction between a Client and a Reader. A major hurdle to the widespread adoption of standards like LLRP is the concern over security, e.g. threats posed by malicious Readers and eavesdropping. The LLRP standard permits the use of Transport Layer Security (TLS) to secure an LLRP connection but until today no secure implementation of LLRP has been developed. This project aims to be the first to setup a TLS-LLRP connection. A virtual LLRP Reader is extended to function as a TLS-LLRP Reader while a basic LLRP Client program is extended to perform the function of a TLS-LLRP Client. To investigate if the TLS-LLRP Reader developed is practical, its resource requirements are determined and compared with the resources of Readers currently available in the market. It was found that the resources required by the TLS-LLRP Reader are beyond the resources of current Readers but not beyond the resources of Java-based Readers expected in the near future. The performance of TLS-LLRP endpoints and connection is evaluated using four metrics. These metrics are recorded during each of the ten runs made using the different cipher suites, key sizes and certificate combinations supported by TLS. Since no performance studies have been done for LLRP, the results are compared to an LLRP connection that does not use TLS. Because of TLS, the minimal overhead on the four metrics occurs when cipher suite TLS_RSA_WITH_AES_128_CBC_SHA is used. Specifically, this cipher suite causes an overhead of 419.8 ms on the mean Duration of Handshake. It also slows the performance of the TLS-LLRP Client by 895.6 ms and the TLS-LLRP Reader by about 385 ms. Its effect on the mean propagation time of an LLRP message, for example, SetReaderConfig is to increase it by about 4.4 ms. Further statistical analysis of the data shows that, for the next level of security, the cipher suite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (with 224 bit ECC keys and certificates signed using SHA1withECDSA) should be used. This research, however, has a few limitations. An emulator, instead of a real Reader, was used to create a virtual TLS-LLRP Reader. This was unavoidable because no open source implementation of the LLRP Reader is available. As the emulator used is written in Java, the TLS-LLRP endpoints developed are also in Java. This is despite the fact that C/C++ is the more common language used by Readers.

ملخص البحث

EPCglobal Inc هي الهيئة المسؤولة عن تطوير مقاييس RFID لإدارة سلاسل التوريد. واحدة من أحدث المعايير والتي ستكون مركز الاهتمام هي بروتوكول Low Level Reader Protocol (LLRP). هذا البروتوكول يضع مقاييس للتفاعل بين العميل والقارئ.من أهم العقبات التي تواجه تطبيق هذا المقياس هي مشكلة الأمن، مثلا: القارئ الخبيث و التنصت .هذا البروتوكول يسمح باستخدام Transport Layer Security (TLS) حتى يؤمن اتصال LLRP لكن و حتى اليوم لا يوجد أي تطبيق آمن ل LLRP قيد التنفيذ.هذا المشروع يهدف إلى أن يكون الأول من نوعه لتنصيب اتصال TLS-LLRP. قارئ LLRP ظاهري سوف يطور حتى يقوم بدور قارئ TLS-LLRP. بينما برنامج عميل LLRP أساسي سوف يطور حتى يقوم بدور عميل TLS-LLRP. حتى نبحث عما إذا كان القارئ المطور عمليا أم لا، قمنا بتحديد موارده و مقارنتها بالأنظمة المتوفرة حاليا في الأسواق. بعد هذه الدراسة، وجدنا أن الموارد اللازمة ل TLS-LLRP أكبر من الموارد اللازمة للأنظمة المتوفرة حاليا و لكنها ليست أكبر من الموارد اللازمة للأنظمة التي تعتمد على الجافا و المتوقعة في المسقبل القريب. أداء نقاط النهاية و نظام الاتصال ل TLS-LLRP حلل باسخدام أربعة مقاييس. هذه المقاييس سجلت في خلال كل عشرة محاولات باستخدام شفرات مختلفة، رموز حماية بأطوال مختلفة، و أنظمة تصديق مختلفة مدعومة من قبل TLS . حيث أنه لا توجد أي دراسات أقيمت على LLRP لذلك قمنا بمقارنة النتائج ب LLRP والذي لا يستخدم TLS. بسبب TLS ، فإن أقل overhead في المقاييس الأربعة يحصل عند استخدام مجموعة التشفير TLS_RSA_WITH_AES_128_CBC_SHA . هذه الشيفرة سببت overhead لحوالي 419.8 مللي ثانية في متوسط فترة الاتصال .هذه الشيفرة أيضا قللت من سرعة أداء عميل TLS-LLRP بحوالي 895.6 مللي ثانية و كذلك قللت من سرعة قارئ TLS-LLRP بحوالي 385 مللي ثانية . استخدام هذه الشيفرة يؤثر أيضا على متوسط فترة البث لرسالة LLRP ، على سبيل المثال زيادة فترة البث بحوالي 4.4 مللي ثاني . المزيد من التحليل الإحصائي للبيانات يبين أنه ينبغيا ستخد اممجموعة التشفي TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA مع 224 بت من رموز ECC و أنظمة تصديق معتمدة باستخدام SHA1 مع ECDSA من أجل مستويات الحماية المستقبلية .
هذا البحث يحتوي على بعض القيود . بدلا من استخدام قارئ حقيقي، قمنا باستخدام قارئ محاكي حتى ننشئ قارئ TLS-LLRP ظاهري. لم نستطع تفادي ذلك لعدم توفر تطبيق من أي من المصادر المفتوحة ل LLRP . حيث أن المحاكي المستخدم يعتمد على الجافا، فإن نقاط النهاية ل TLS-LLRP أيضا طورت باستخدام الجافا . هذا بغض النظر عن أن أنظمة القراءة غالبا تستخدم لغة C/C++.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science (Computer and Information Engineering).

…….....
Mohammad Umar Siddiqi
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science (Computer and Information Engineering).

…….....
Akhmad Unggul Prinatoro
Internal Examiner

…….
Barun Jeoti
External Examiner

This dissertation was submitted to the Department of Electrical and Computer Engineering and is accepted as a partial fulfilment of the requirements for the degree of Master of Science (Computer and Information Engineering).

…….....
Othman O. Khalifa
Head, Department of Electrical and
Computer Engineering

This dissertation was submitted to the Kulliyyah of Engineering and is accepted as a partial fulfilment of the requirements for the degree of Master of Science (Computer and Information Engineering).

…….....
Amir Akramin Shafie
Dean, Kulliyyah of Engineering

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Sana Qadir

Signature …… Date ……..

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

SECURING A LOW LEVEL READER PROTOCOL (LLRP) CONNECTION AND AN EVALUATION OF ITS PERFORMANCE

Affirmed by Sana Qadir

…… ……...……..

Signature Date

ACKNOWLEDGEMENTS

IN THE NAME OF ALLAH, MOST GRACIOUS, MOST MERCIFUL

First and foremost I would like to thank Allah for His most generous blessings because of which I was able to complete this thesis. My deepest gratitude to my supervisor Prof. Dr. Mohammad Umar Siddiqi for his continuous guidance and support. Many thanks also to Br. Nor Ashid bin Jamil for his technical advice and to all online correspondents for their help. Finally, my heart-felt appreciation to my family for their love and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIDC	Automatic Identification and Data Collection
RFID	Radio Frequency Identification
EPC	Electronic Product Code
LLRP	Low Level Reader Protocol
TLS	Transport Layer Security
SSL	Secure Socket Layer
WTLS	Wireless Transport Layer Security
WAP	Wireless Application Protocol
HTTP	Hypertext Transfer Protocol
RSA	Rivest-Shamir-Adleman
ECC	Elliptic Curve Cryptography
IMAP	Internet Message Access Protocol
SMTP	Simple Mail Transfer Protocol
LDAP	Lightweight Directory Access Protocol
JNI	Java Native Interface
NTP	Network Time Protocol
UHF	Ultra-High Frequency
TCP	Transmission Control Protocol
IP	Internet Protocol
RFC	Request For Comments
IETF	Internet Engineering Task Force
MAC	Message Authentication Code
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
SHA	Secure Hash Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature
AES	Advanced Encryption Standard
DES	Data Encryption Standard
CBC	Cipher Block Chaining
SECG	Standards for Efficient Cryptography Group
PKIX	Public-Key Infrastructure X.509
SDK	Software Development Kit
JDK	Java Development Kit
JRE	Java Run-time Environment
JSSE	Java Secure Socket Extension
JCA	Java Cryptographic Architecture
JCE	Java Cryptographic Extension
API	Application Programming Interface
NSS	Network Security Services
JKS	Java Keystore

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

The largest deployment of RFID technology is projected to be for supply chain management. The underlying mechanism is the intelligent identification and tracking of goods throughout their lifecycle using a unique code called the Electronic Product Code or EPC. The EPC is stored on an RFID Tag that is attached to a good. The EPC can be read using an RFID Reader whenever the good needs to be identified. The EPC will indicate the owner, type, as well as the serial number of the good.

RFID is reputed to have two distinct advantages: unique identification and automation (Juels, 2006). Automation is realized by eliminating the need for line-of-sight reading and the precise positioning of tags that is generally done by humans. It also obviates individual scanning of items. In the supply chain, this improves the accuracy and timeliness of information about the movement of goods and thus enables better management of out-of-stock problems, inventory inaccuracies, etc. (Das, 2007). Companies like Wal-mart, Metro Group, Boeing and Airbus have invested heavily in the technology and the return on investment is obvious for *closed loop applications*. Closed loop applications (e.g. assembly lines or asset management) are those applications that function within a single plant and do not involve open transmission of data and other information to business partners (Stroh & Ringbeck, 2004). Stroh and Ringbeck also explain that the benefits of RFID translate into the following tactical advantage (2004: 1):

> *As companies pursue more sophisticated mass customization, they need to track and analyze supply chain data at an increasingly granular level. To give customers what they want when they want it — customized, quickly, inexpensively, and efficiently — companies must know the status of supplies, inventory, manufacturing, and shipments almost to the moment. RFID could become the spy on the supply chain that every company wishes it had.*

Benefits are expected to multiply when *open loop applications* (i.e. those applications that involve businesses and their suppliers) are deployed.

Any significant adoption of RFID infrastructure necessitates the standardization of RFID hardware, software and data management. EPCglobal is the body in charge of supervising the development of RFID standards for supply chain management. Users that adopt their standards i.e. Subscribers of EPCglobal Standards, are assured interoperability. This has induced many RFID hardware and software companies to develop and market components that comply with EPCglobal standards.

Components that implement cross-enterprise EPCglobal standards, however, are not yet available. This is because some of these standards were ratified very recently while the rest of them are still being determined. Thus, currently, only the *intra-enterprise* section of a supply chain can be set up with components that comply with EPCglobal standards. An example of a simple intra-enterprise section of an RFID-enabled supply chain is illustrated in Figure 1.1. In-coming goods have tags attached to them. The enterprise's Readers identify the goods by reading the EPC stored on the attached Tag. The Reader forwards this data to the Client machine where it is accumulated and filtered to generate business events. The business events are then utilized by other nodes in the enterprise's network.

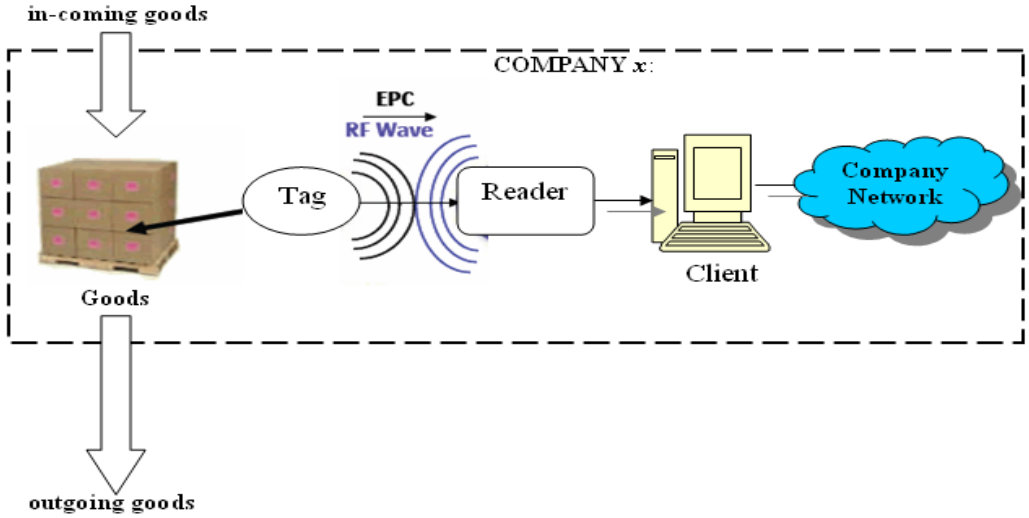

Figure 1.1 Intra-enterprise RFID-enabled Supply Chain

One of the latest EPCglobal standards belonging to the intra-enterprise section of the supply chain is the **Low Level Reader Protocol** (**LLRP**). This protocol defines the communication between the Client and Reader (see Figure 1.2) and is the focus of this thesis (Dobkin, 2007).

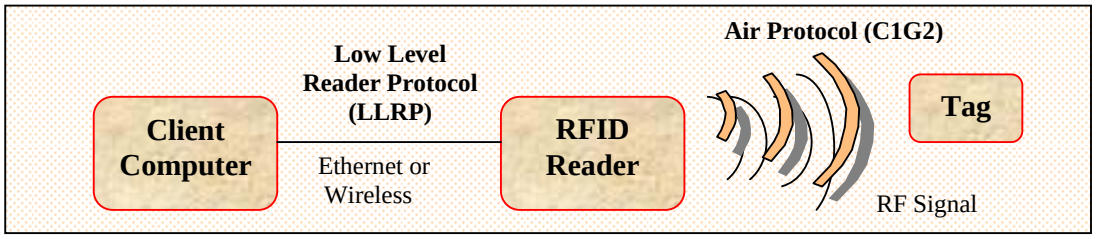

Figure 1.2 Client – Reader – Tag Interaction

1.2 SIGNIFICANCE

The full benefits of automatic identification and data collection technology (AIDC) are reaped only when information and the generated business events are shared. A key enabler for this is the security of the communication channels over which this

information is sent. In particular, this includes the channel through which data enters a company's network from RFID Readers.

Konidala et al., undertook to analyze the security threats to a supply chain management system that comprised of components that comply with EPCglobal Standards (2006). They found that one of the most significant threats in an intra-enterprise scenario is posed by malicious Readers. The security risks multiply when Readers are networked and the RFID data is to be sent to more than one application (e.g. in supply chain management and logistics). Authentication of Readers is, therefore, vital. Additionally, some Readers nowadays (e.g. the handheld models), include a wireless interface (802.11b/g) to communicate with the Client. To protect against eavesdropping on this channel, confidentiality becomes another important security requirement. Demonstrating that secure implementation of EPCglobal standards is both possible and practical is important for their wide-scale adoption.

Security comes at a cost and the impact of using 'secure' components on performance has to be examined. In this thesis, the performance of an LLRP connection secured in the manner permitted by the LLRP standard is studied. In other words, the performance of a connection established between an LLRP Client and an LLRP Reader that include an implementation of Transport Layer Security (TLS) is evaluated.

Despite being fine-tuned for wireless or mobile environments, Wireless Transport Layer Security (WTLS) was not recommended by EPCglobal for use with LLRP. This was because EPCglobal considered it important to remain interoperable with wired systems that use the ubiquitous TCP/IP stack and public key infrastructure. Moreover, WTLS is part of the Wireless Application Protocol (WAP) suite. This

means that its use requires the application protocol to be Hypertext Transfer Protocol (HTTP) and not LLRP as is the case in this thesis.

The widespread adoption of TLS for securing HTTP connections was preceded not only by performance studies but also by identification of reasons for delay in performance and the eventual modification and refinement of both HTTP and TLS (Apostolopoulos et al., 1999). It is hoped that the security solution implemented in this thesis will provide much-needed feedback to the EPCglobal community.

1.3 PROBLEM STATEMENT

One of the major hurdles to the widespread adoption of EPCglobal standards is the concern over privacy and security. Any supply chain management system built using current RFID components is vulnerable to several security threats. This is because commercial RFID applications do not emphasize security and RFID Tags and Readers communicate with each other using open, unencrypted messages. The most common reasons for not including security mechanisms in RFID components are to reduce cost and the lack of resources such as computing power and memory especially on RFID Tags.

With advances in technology, resource limitation is becoming less of a constraint and security mechanisms and solutions for RFID systems are now being actively researched. Security solutions generally take the form of defining or recommending the inclusion of a security protocol. This is to ensure that cryptographic algorithms are used in a way that provides the required security service (Burnett, 2002: 83). It is for this reason that EPCglobal's Low Level Reader Protocol (LLRP) standard permits the use of TLS to secure an LLRP connection. There are however, no secure implementations of LLRP endpoints available. This project aims

to be the first to secure an LLRP connection using TLS. In other words, it is the first to develop TLS-LLRP endpoints that will communicate via a TLS-LLRP connection.

To the author's knowledge very little work has been done on LLRP. In fact, no extensive study of this protocol has been undertaken. In a business context, performance is paramount, and so an evaluation of the performance of TLS-LLRP endpoints and connection is considered important. It will help identify the TLS options and cipher suites that cause minimum delay. It will also help identify the TLS options and cipher suites that should be adopted in the coming years when a move to a higher level of security becomes imperative.

Lastly, an important consideration that has to be kept in mind is the resource requirement of the developed TLS-LLRP Reader. A feasible implementation should be able to run using the resources available on current LLRP Readers or on LLRP Readers that are expected to be available in the near future.

1.4 OBJECTIVES

The objectives of this research are:

i. To study and explore the protocols LLRP and TLS.

ii. To design and implement TLS-LLRP endpoints.

iii. To investigate if the TLS-LLRP Reader developed in this thesis is feasible, in terms of the resources available to current Readers in the market.

iv. To evaluate the performance of the TLS-LLRP connection and TLS-LLRP endpoints under different TLS cipher suites and options.

1.5 METHODOLOGY

The steps involved in this research are:

i. The first step is to explore LLRP and TLS protocols. This is followed by a review of performance studies carried out on Web servers secured using TLS.

ii. Design and implement TLS-LLRP endpoints. The starting point is the `Rifidi Emulator` (the only open source LLRP Reader implementation available). It is used to create a virtual LLRP Reader. This is possible because `Rifidi` functions like a real reader down to the packet level and can emulate TCP communication (Pramari, 2007). `Rifidi Emulator v1.5` is extended to include TLS and so operate as a TLS-LLRP Reader. Similarly, an LLRP Client, that sends typical LLRP messages, is extended to function as a TLS-LLRP Client. The Eclipse Software Development Kit (SDK) is employed for development activity.

iii. Experiments are carried out with the TLS-LLRP Reader running on one machine and the TLS-LLRP Client running on the other machine. The machines are networked using a wireless connection. The performance of the TLS-LLRP endpoints and the TLS-LLRP connection is measured using four metrics. Ten runs are carried out for each different combination of cipher suites, key sizes and certificate provided by TLS. Recording the metrics required generating high resolution timestamps and the synchronization of the clocks on the two machines.

iv. The resource requirements of the TLS-LLRP Reader developed is compared to the capabilities of current Readers to determine if the

proposed technique of securing an LLRP connection is feasible using present day technology.

1.6 SCOPE

This research fits into the area of performance evaluation of an application layer protocol. The protocol in question is the LLRP and this thesis emphasizes the need for evaluating the performance of LLRP endpoints and connection secured using TLS. In line with this the follow areas are covered:

i. The LLRP standard, the TLS protocol and their existing implementations
ii. The design and implementation of a virtual TLS-LLRP Reader and a TLS-LLRP Client.
iii. The selection of appropriate performance metrics and the issues faced in generating accurate timestamps to record the chosen performance metrics
iv. Experimentation using the TLS-LLRP endpoints
v. Data analysis on the results of the experiment. We concentrate only on those TLS combinations that provide a level of security that is considered reasonable by today's standards. In other words, we focus on Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC) public-key cryptosystems and Advanced Encryption Standard (AES) symmetric-key cryptosystem.
vi. The practicality of any security solution has to be evaluated and, as such, the resource requirements of the developed TLS-LLRP Reader implementation is determined as well as the resources provided by existing Readers in the market.

1.7 THESIS OUTLINE

The thesis is organized in six chapters. This chapter consists of the background, significance, problem statement, scope, objectives and research methodology. Chapter 2 introduces EPCglobal's LLRP standard as well as the TLS standard. Lastly, it reviews performance studies of HTTP over TLS.

The high-level design of a TLS-LLRP connection is given in Chapter 3. This Chapter also introduces the LLRP Client and the LLRP Reader that are extended in this thesis. Chapter 4 begins by discussing the TLS implementation selected and then describes how the LLRP Reader and LLRP Client are extended to function like TLS-LLRP endpoints. A description of how the performance metrics are recorded is also presented together with the experimental setup and procedure. Some of the difficulties encountered are also discussed together with the solutions employed.

Chapter 5 presents the data analysis and discusses the results of this analysis. Conclusion and recommendations are given in Chapter 6.

There are nine appendices in this thesis. The first appendix shows the LLRP messages exchanged between the TLS-LLRP endpoints. The next five appendices (Appendix II to Appendix VI) contain the code for the classes modified for extending LLRP endpoints into TLS-LLRP endpoints. The remaining three appendices (Appendix VII to Appendix IX) contain the data recorded for the performance metrics and statistics calculated using this data.