Agent-based Transactions for Home Energy Services

Song, Ronggong; Korba, Larry; Yee, George

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Agent-based Transactions for Home Energy Services *

Song, R., Korba, L., and Yee, G.
September 2005

* published in the Proceedings of the 2005 International Workshop on Mobile Systems, E-commerce and Agent Technology (MSEAT'2005) Joint with the 11th International Conference on Distributed Multimedia Systems (DMS'2005). Banff, Alberta, Canada. September 5-7, 2005. NRC 48257.

Canada

Agent-based Transactions for Home Energy Services

Ronggong Song, Larry Korba, and George Yee

Institute for Information Technology
National Research Council of Canada
Ottawa, Ontario K1A 0R6, Canada
{Ronggong.Song, Larry.Korba, George.Yee}@nrc.ca

***Abstract*—Current home energy management systems (HEMS), which use the existing home networks and Internet as the communication infrastructure, are both inexpensive and offer definite consumer advantages. However, most of them don't support e-services such as reporting and dealing with monthly expenses for services like power, gas, and water. A key deterrent for the handling of the e-services in this environment is that the data may be subject to a variety of active and passive attacks if the system is not designed properly. This paper describes a lightweight security architecture for e-services related to home energy services. The system is intended to protect against both inside and outside attacks by using the existing HEMS and combining the tamper-resistant devices with Internet security techniques.**

1 Introduction

Home energy management systems (HEMS) [1, 2, 3] are designed to control home appliances automatically for the purpose of both convenience and saving energy. However, most of them do not support e-services such as reporting the monthly expenses for services and dealing with the billing statements of customers. Not having automatic e-reporting built into HEMS is also unfortunate due to the inefficiency and inconvenience of having to use a separate billing procedure (often involving manual processing). Furthermore, security technologies such as SSL [4] or VPN used in the current HEMS such as [3] are insufficient for providing secure communications required for e-reporting between energy devices and the service providers. This is because VPN and SSL services are both controlled by the customers leading to the possibility that customers may easily make a number of possible active attacks on the e-reporting data (e.g. changing the amount of the energy consumption).

An additional challenge is that providing a secure architecture to handle e-services for home energy services must deal with the fact that the devices embedded within the meter normally have limitations computationally in order to keep costs down.

In order to solve the above problems, we propose a lightweight security architecture for the e-reporting and billing of home energy services based on tamper-resistant technology and SSL (or TLS [5]) technology. The security architecture consists of three parts: a meter reading device (MRD), a middleware agent, and a service provider's server. The middleware agent is located on the customer's computer or home network gateway. It registers the customer to the service provider's server and forwards the e-reporting protocol messages between the MRD and the server. The e-reporting protocol could be initiated by the middleware agent or the service provider's server depending on different implementation. Communications between the MRD, the agent, and the server are protected with a combination of security mechanisms (See Section 3.3). The meter reading device is a tamper-resistant device. It uses a keyed hash function with a secret key shared between the MRD and server. The data transferred from the MRD to the provider must be accompanied with a hash result for the data integrity and authentication protection against some inside and outside active attacks (e.g. replay and modification). The data is then forwarded to the provider by the middleware agent through an SSL secure channel in order to provide data confidentiality, authentication, and integrity protection against outside attacks. In addition, since the security architecture is based on the existing home network, Internet, and SSL security technology, the new system only needs new hardware in the form of the MRD, new software – the middleware agent, and some new security protocols.

The rest of the paper is organized as follows. A home energy management system [3] is briefly reviewed, and the security requirements for the e-reporting are analyzed in the next section. In Section 3, the security architecture is proposed for the e-reporting. In Section 4, the new security protocols are described for the security architecture. In Section 5, some characteristics of the new secure architecture are summarized. In Section 6, the security of the new protocols is analyzed. Finally, concluding remarks are given in Section 7.

2 Review of Home Energy Management System

2.1 Home Energy Management System

Based on [3], a home energy management system comprises an in-house system connected to service control servers via the Internet. The in-house system

includes a home network and network adapters for the energy service appliances. The service control servers include the service provider's server, the information provider's server, and the energy control server. The home network and Internet provide the network communication infrastructure for the communications between the energy appliances and service control servers. Figure 1 depicts a home energy management system. In this paper, we only talk about the security architecture for the e-reporting and billing among the energy appliances, the customers, and the service providers. The service providers include a gas service provider, a water service provider, and a power service provider.

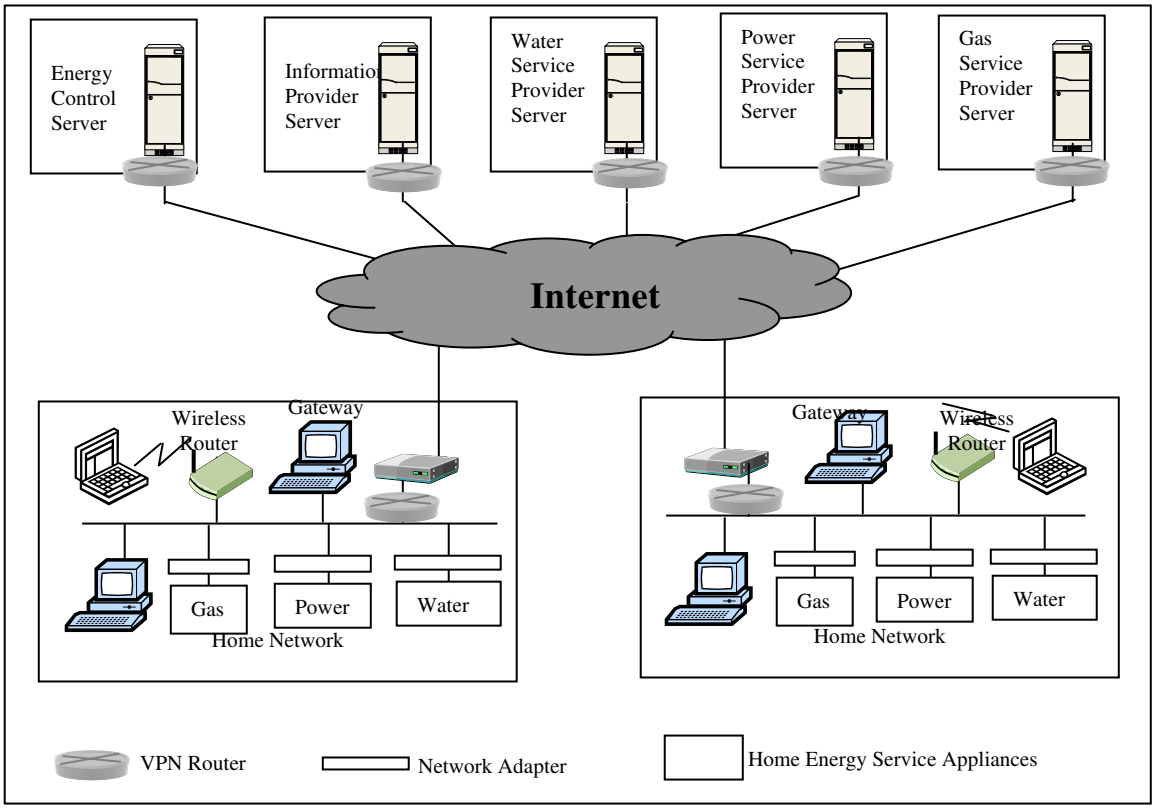

Fig. 1. A home energy management system

2.2 Security Analysis of HEMS

The current home energy management systems use VPN or SSL as their security architecture. VPN provides the security communication protection between the home network domain and the server domain (for instance, the above energy control server domain). SSL provides the security communication protection between the customer's application and the remote server. However, these two security technologies are not enough to protect the security communications between the energy appliance and the service provider since the customers usually have full control over their home network domain, i.e., the customers can easily make some inside attacks on the communications if the communications are not protected properly including some attacks made by outside hackers. In addition, the conflictive benefits between the customers and service providers may encourage the customers to make these attacks, for instance, changing the amount of energy consumption for the e-reporting. Thus we need other security technologies to protect the communications.

In addition, since SSL has provided the security communications between the application and the service provider server against the outside attacks, a confidentiality protection is not very important on the home network for the reporting data transferred from MRD to the provider's server but the integrity and authentication protection may become very important against some inside and outside active attacks like replay and modification. This special situation gives an opportunity to make a lightweight security architecture for it.

3 Security Architecture

The security architecture for the e-reporting of HEMS consists of three parts: a meter reading device, a middleware agent, and a service provider's server.

3.1 Meter Reading Device

The meter reading device is a tamper-resistant device which is embedded with the meter together. The device directly connects with a network adapter to communicate with outsider through the home network. Figure 2 depicts the functionality of MRD.

In MRD, h is a keyed hash function and P is a control processing part for verifying whether or not the input data is correct. The secret key is stored in the hiding area of MRD. It is a shared key with the service provider, i.e. except the provider, other people including the customer knows nothing about the key. The output data from MRD to the provider is hashed by the hash function with the secret key for the data integrity and authentication protection. The provider verifies the data received from the MRD using the hash function and the shared secret key. Likewise, the data transferred from the provider to the MRD should be verified in the control processing part. In order to make the system stronger each MRD should choose a different secret key.

The functionality of the tamper-resistant device embedded in MRD is similar to a simple smart card. We could use a simple smart card technology for it. The expensive strong tamper-resistant devices are not necessary for this system since the main purpose of the tamper-resistant device is to protect the shared secret key. In addition, the providers could physically check the randomly selective meters and devices, especially if they find some suspicious cases.

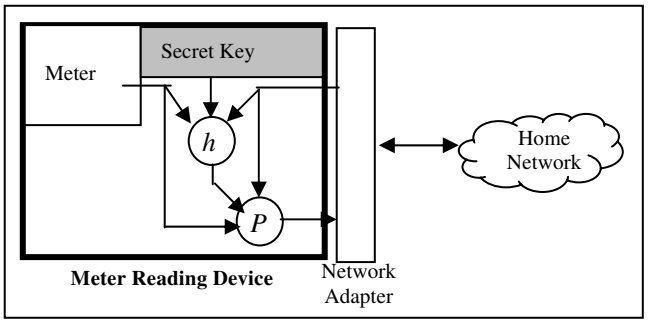

Fig. 2. The Functionality of MRD

3.2 Middleware Agent

The middleware agent could be located on the customer's computer or home network gateway. After installing the middleware agent, the customer then uses it to register his service account in the service provider's server and set up a schedule for reporting the mount of energy consumption and billing the statement for payment. The e-reporting and billing protocol could be initiated with the middleware agent or the service provider's server. For the former, the customer should set up the time and period to wake up the protocol implemented in the middleware agent. For the latter, the customer should set up the initiating (waking up the protocol) condition as getting the initiating message from the service provider's server. The middleware agent forwards the messages between MRD and the server during the e-reporting and billing. Figure 3 depicts the state of the middleware agent.

The communications among MRD, the middleware agent, and the service provider's server are protected by a combination of secure mechanisms. Figure 4 depicts the security channels where the SSL (or TLS) secure channel protects all communications between the agent and server in the transport layer against outside attacks for the data confidentiality and integrity. The message authentication code (MAC) channel protects the communications between MRD and the service provider's server in the application layer against the inside and outside active attacks. The SSL secure channel will wrap the integrity secure channel between the agent and server. The SSL secure channel is an option depending on the requirements.

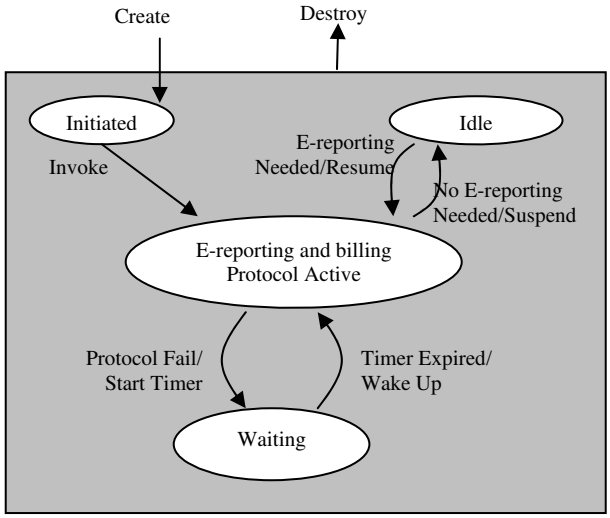

Fig. 3. The State of Middleware Agent

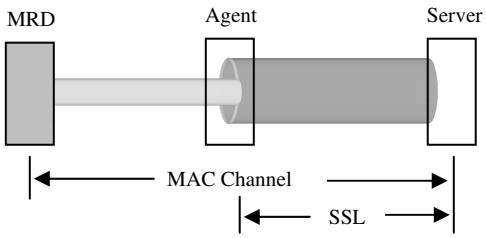

Fig. 4. The Security Channels

3.3 Service Provider's Server

The service provider's server is a normal application server but it is implemented with the SSL secure technology in the transport layer and the MAC authentication functionality in the application layer. The integrity and authentication processing will be described in the following security protocols.

4 Security Protocols

In order to implement the security functions, the security architecture has two protocols: registration protocol and e-reporting and billing protocol.

4.1 Terminology and Notations

Terminology and notations used in the protocols are defined as follows.

- *C*: a customer
- *A*: a middleware agent
- *P*: an energy service provider
- *MRD*: a meter reading device
- ID_C: customer *C*'s identity
- ID_{MRD}: an identity number of MRD
- $Account_C$: customer *C*'s account number
- N_P: a nonce made by energy service provider *P*
- $Time_P$: a time stamp made by provider *P*
- *SK*: a secret key embedded in MRD
- *H*(): one-way hash function

4.2 Registration Protocol

All customers are required to register with the energy service provider's server and set up their service accounts in the server when they first install the middleware agent in their computer. Figure 5 depicts the message flow of the registration protocol. In the protocol, the communications between the middleware agent and the server is protected with the SSL secure channel in the transport layer.

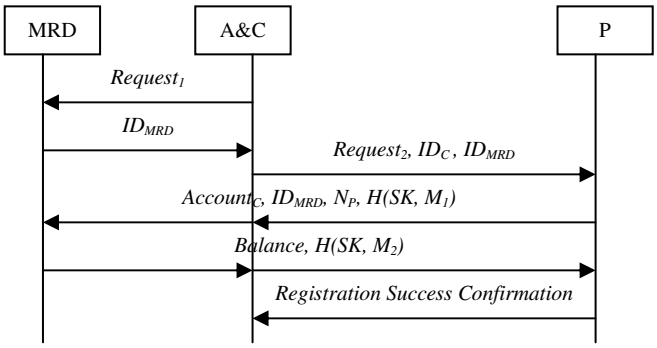

Fig. 5. The Registration Protocol

The registration protocol is described as follows.

Step 1: The agent *A* sends a request message ($Request_1$) to MRD for its identity number.

Step 2: MRD responds to the request message giving its identity number (ID_{MRD}).

Step 3: The agent *A* then sends another request message ($Request_2$) to the energy service provider's server with the customer's personal information (ID_C, e.g., Name) and MRD's identity number (ID_{MRD}) together. In this step, all messages are protected with the SSL secure channel.

Step 4: After receiving the above messages, the server first verifies if the customer's personal data and MRD's identity are correct through its database or social network. If they are correct, the server then sets up an account for the customer and sends the message [$Account_C$, ID_{MRD} , N_P , $H(SK, M_1)$] to the agent *A* where *SK* is a shared secret key between the service provider and MRD, and M_1 = [$Account_C$, ID_{MRD}, N_P].

The agent *A* then verifies and forwards the message to MRD.

Step 5: MRD verifies if the message [ID_{MRD}, $H(SK, M_1)$] is correct. If it is correct, MRD then sends the energy consumption balance (*Balance*) and keyed hashing result [$H(SK, M_2)$] to the agent *A* where M_2 = [$Account_C$, ID_{MRD}, N_P, *Balance*].

The customer then checks if the balance is correct. If it is correct, the customer could let the agent *A* forwards the message to the server.

Step 6: The server then verifies if the message is correct. If it is correct, the server then sends a registration success confirmation message to the agent *A*.

4.3 E-reporting and billing Protocol

After registration, the customer and provider could set up the time and period for initiating the e-reporting and billing protocol. The e-reporting and billing protocol could be initiated with either the middleware agent or the service provider's server depending on the different implementation. We design two different e-reporting and billing protocols for them. Their features are shown in Section 5.

The first e-reporting and billing protocol is initiated with the middleware agent. For this implementation, the middleware agent is like client-side software which makes the implementation more simple and low cost. Figure 6 depicts the message flow of the e-reporting and billing protocol.

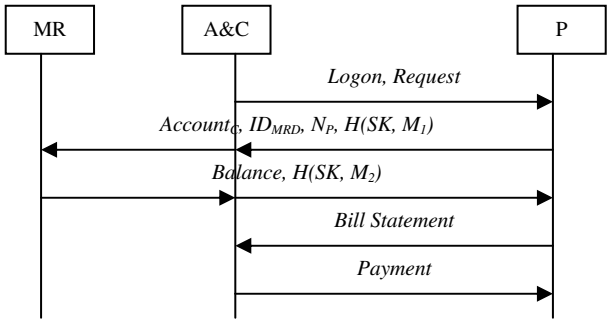

Fig. 6. The E-reporting and billing Protocol

The protocol is described as follows.

Step 1: The agent *A* first logs on the server and requests the bill statement.

Step 2: After verifying the user's name and password, the server sends the message [$Account_C$, ID_{MRD}, N_P, $H(SK, M_1)$] to the agent *A* where $M_1 = [Account_C, ID_{MRD}, N_P]$.

After receiving the messages, the agent *A* first verifies if the message [$Account_C$, ID_{MRD}, N_P] is correct. If it is correct, the agent *A* then forwards the message to MRD.

Step 3: MRD verifies if the message [ID_{MRD}, $H(SK, M_1)$] are correct. If it is correct, MRD then sends the current energy consumption balance (*Balance*) and hashing result [$H(SK, M_2)$] to the agent *A* where $M_2 = [Account_C, ID_{MRD}, N_P, Balance]$.

The customer then checks if the balance is correct. If it is correct, the customer could let the agent *A* forwards the message to the server.

Step 4: The server first verifies if the message is correct and then calculates the balance of the energy consumption in the last period. Finally, the server makes a bill statement and sends it to the agent *A* and customer *C*.

Step 5: The customer *C* could directly pay the bill through the agent *A* using his/her credit card, or make the payment through other Online Banking.

The second e-reporting and billing protocol is initiated with the service provider's server. For this implementation, the middleware agent works like server-side software or client-side software with push technologies which requires the customer to install it to an application server. Figure 7 depicts the message flow of the protocol.

In the protocol, the service provider's server first logs on the customer's middleware agent and sends the message [$Account_C$, ID_{MRD}, N_P, $H(SK, M_1)$] to the agent *A*. Other steps are same as the Step 3, 4, 5 of the first e-reporting and billing protocol.

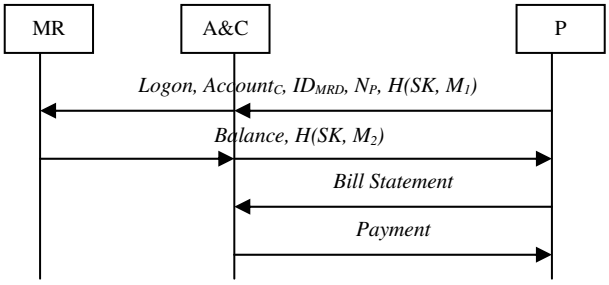

Fig. 7. The Second E-transaction Protocol

5 Architecture Characteristics

5.1 Lightweight Secure Architecture

In order to make the MRD implementation simple and low cost, we only use a keyed hash algorithm in MRD. However, this could provide enough security protection for the system since active attacks (e.g., replay and modify), especially inside active attacks in the home network, are the most important attacks for the reporting and billing system. Furthermore, in order to protect the communications between the agent and server against outside attacks, we employ the existing SSL secure technology. Except for the simple secure algorithm - hash function, we don't use any other complex secure functions like signature in the system server-side application layer. All these make the system implementation simple and low cost.

5.2 Highly Efficient Processing

The secure architecture can automatically report the customers' energy consumption data, generate an e-bill statement and process an e-payment. This would make the system more efficient, and overcome some labor-intensive activities (e.g. physically checking the meters). In addition, the lightweight secure architecture also improves the system scalability.

5.3 Flexible Alternative Implementations

As we mentioned, we have two different implementations for the system which depend on which part (the middleware agent and the service provider's server) initiating the e-reporting and billing protocol. For the former, the advantages include easy implementation, low cost, and convenient customer-side control. The main limitation is the scalability since all customers may initiate their e-reporting protocol in the same time. In order to solve this problem, the server could set up the different initiating time period for the different customers when the customers register their service accounts. For the latter, the advantages include more scalability and convenient server-side control. The main limitation is that the middleware agent needs to be installed in a computer or implemented with a special hardware in the customer side but this would increase the cost. In addition, the extra security protection may need to be considered for the computer and hardware.

6 Security Analysis

In this section, we briefly demonstrate that the secure architecture does provide sufficient protection for the system against active and passive attacks.

6.1 Active Attacks

The new secure architecture provides protection against inside and outside active attacks, for instance, replay and modification. First, the MRD and the server can easily discover the modified or impersonated message by verifying the keyed hashing result since all messages between the MRD and the server have been hashed with a keyed hash function (e.g. *H(SK,M)*), and only the MRD and the server know the secret key (*SK*). Even the customers themselves cannot change the message since they don't have the secret key. Secondly, the server can easily find the replayed message by comparing the Nonce

since all messages are sent to MRD from the server with the Nonce (N_P). This is very important since SSL already provides anti-reply protection but the protection cannot reach to MRD, i.e., the anti-reply protection only protects the homeowner not MRD. Finally, for the communications between the agent and the server, they are protected with the SSL technology which includes confidentiality, authentication, and integrity protection.

6.2 Passive Attacks

In the new architecture, as we mentioned in the above, all communications between the agent and the server are protected with the SSL Technology. Outside attackers cannot understand the content of the messages since they are encrypted for the confidentiality protection. It is unnecessary to provide the confidentiality protection between MRD and the agent since the customer has the whole control for his/her home network and the content of messages in the protocols shouldn't be confidential for the customer. Furthermore, the server could very easily verify the attacks even if the hackers successfully attack the home network and change the reporting data.

7 Conclusions

We have presented a secure architecture for the e-reporting and billing of home energy services. Our secure architecture combines lightweight secure technology with SSL technology and provides good secure protection for the system. Our low cost architecture can improve the transaction processing of home energy services substituting electronic processing for labor-intensive manual paper-based work. In addition, we proposed two e-reporting and billing protocols with different implementations and briefly discussed their advantages and limitations.

The secure architecture is based on the existing home energy management system [3], i.e. the local net interface, adapters, and network connections are already existed for the home energy appliances. Of course, it may cost lots if the homeowners don't have this kind of systems in their home.

Acknowledgements

We would like to thank all members of IIT at the NRC of Canada for their support towards our R&D projects in Information Security and Privacy Protection. We are also grateful to the anonymous referees for helpful comments.

References

[1] M. Inoue, K. Uemura, Y. Minagawa, M. Esaki, and Y. Honda, "A Home Automation System", *IEEE Trans. On Consumer Electronics*, CE-31, No. 3, 1985.

[2] D. S. Kim, G. Y. Cho, W. H. Kwon, Y. I. Kwan, and Y. H. Kim, "Home Network Message Specificaiton for White Goods and Its Applications", *IEEE Trans. On Consumer Electronics*, Vol. 48, No. 1, pp. 1-9, Feb. 2002.

[3] M. Inoue, T. Higuma, Y. Ito, N. Kushiro, and H. Kubota, "Network Architecture for Home Energy Management System", *IEEE Trans. On Consumer Electronics*, Vol. 49, No. 3, pp.606-613, Aug. 2003.

[4] SSL 3.0 Specification. http://wp.netscape.com/eng/ssl3/. 1996.

[5] The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard). ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt. 1999.