Micro Secure Socket Layer (MSSL) for micro server

Conference Paper · January 2009

DOI: 10.1145/1882486.1882506 · Source: DBLP

3 authors, including:

Kensuke Naoe
Keio University
16 PUBLICATIONS **18** CITATIONS
SEE PROFILE

Yoshiyasu Takefuji
Keio University
427 PUBLICATIONS **2,798** CITATIONS
SEE PROFILE

Micro Secure Socket Layer (MSSL) for Micro Server

Nguyen Thanh Hoa
Graduate School of
Media and Governance
Keio University, Endo 5322
Fujisawa, Kanagawa, JAPAN
hoant@sfc.keio.ac.jp

Kensuke Naoe
Graduate School of
Media and Governance
Keio University, Endo 5322
Fujisawa, Kanagawa, JAPAN
naoe@sfc.keio.ac.jp

Yoshiyasu Takefuji
Faculty of Environment
and Information Studies
Keio University, Endo 5322
Fujisawa, Kanagawa, JAPAN
takefuji@sfc.keio.ac.jp

ABSTRACT
In this paper, we propose Micro Secure Socket Layer (MSSL) for 8-bit flash micro controller that is about 1.3 Kbytes in code size. We have analyzed and compared various cryptographic protocols in TCP/IP stack for Micro Server to propose a simple secure layer based on simple handshake processing and encryption. Security implementation for Micro Server, which has very limited size of memory with a small processor, is very difficult and challenging task. However, security on the applications of ubiquitous sensors has become very important issues recently. Crackers can easily access to the sensor nodes or Micro Servers without security. Because the proposed MSSL is very small in code size, it can be implemented and is suitable for small sensors and Micro Server systems.

Keywords
MSSL, SSL, Micro Server, 8-bit microcontroller, sensor.

1. INTRODUCTION
Nowadays, with the devel**o**pment of technology and science, we can make small sensors and Micro Servers very easily with low cost. Security is important when these devices are used in health care applications, home appliances, etc. It is a challenging task because of very small processor and limited memory [6]. This paper analyzes normal security methods using cryptographic protocols and then proposes a Micro Secure Socket Layer – MSSL that has very small code size and can protect very small sensors and Micro Server.

2. BACKGROUND

2.1 Micro Server

Figure 1: Micro Server

We made a Micro Server gadget that followed the design of Takefuji [7] as Figure 1. Micro Server uses 8bit microcontroller Atmega168 with 16 Kbytes flash memory. Adam Dunkels, the author of the simple TCP/IP stack embedded inside this Micro Server with size of flash memory is about 8466 bytes [4].

ANCS'09, October 19-20, 2009, Princeton, New Jersey, USA.

2.2 The security methods for TCP/IP protocol

2.2.1 IPSec protocol
IPSec is a complex protocol [2]. This protocol includes: processing key exchange; processing Security Policy, Security. Association, two protocols AH (Authentication Header), ESP (Encapsulating Security Payload).

2.2.2 SSL – Secure Socket Layer
SSL (Secure Socket Layer) [3] consists of two phases: handshake and data transfer. Of these tasks, handshake processing takes the most computing power, followed by encryption, decryption [1].

Although SSL is not complex as IPSec but more the computing power of handshake processing makes SSL difficult to implement. Therefore, we propose a Micro Security Socket Layer – MSSL as explained in the following section.

3. THE PROPOSED MICRO SECURE SOCKET LAYER FOR MICRO SERVER
We propose micro secure socket layer – MSSL with the diagram as Figure 2 shows. MSSL has 2 phases: Simple Handshake processing and Encryption.

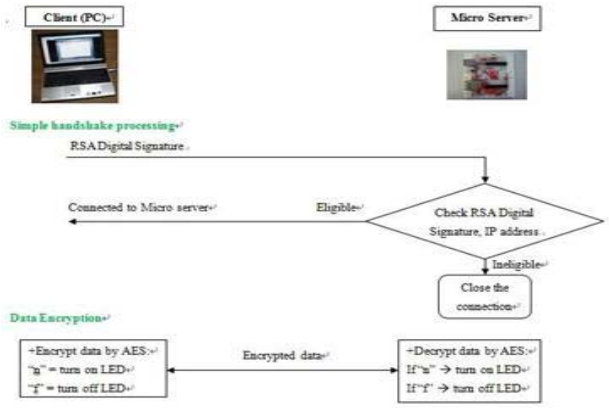

Figure 2: The diagram of MSSL.

3.1 Simple Handshake Processing
SSL has complex handshake processing with high computing power because of public-key computations and random-number generation for public-key encryption [1]. 8-bit microcontroller

with 16 Kbytes flash memory has many limitations so processing public-key cryptography in this microcontroller is not possible.

As a third party, we establish a program to create RSA digital signature to have agreement between hosts and Micro Server. If a host want to access to Micro Server, this host has to agree the RSA digital signature with Micro Server about: the host identity, what tasks host can do with Micro Server.

Besides, to avoid the attack of hackers who want to capture the packets and send the same command to the Micro Server, we will recognize eligible client by IP address or MAC address. The simple handshake processing will allow which host can access and what tasks these host can do by only Digital Signature. This authentication method make Micro Server can authenticate the connection easily and fast.

3.2 Encryption by AES

After finishing handshake processing, both host and Micro Server use the secret key to encrypt and decrypt data by AES – Advanced Encryption Standard Algorithm.

4. IMPLEMENTATION & EXPERIMENT RESULTS

We have implemented MSSL in Micro Server, Client side and have finished testing the securable connection between client and Micro Server.

4.1 RSA Digital Signature

We used Matlab to establish a program that creates RSA Digital Signature. We have results of RSA Digital Signature as the following Figure 3.

Figure 3: RSA Digital Signature for MSSL

4.2 Encryption Implementation

Figure 4: AES testing environment for Micro Server

We followed the standard of AES (Advanced Encryption Standard) to implement this algorithm [5]. We tested this algorithm implementation by turn on or turn off LED in the Micro Server gadget as Figure 4 shows.

4.3 MSSL Implementation

We established MSSL in Micro Server with code size about 1.322 Kbytes. We have implemented simple MSSL in the client by Java. This program established telnet client to support client can connect with Micro Server and has result as the Figure 5

Figure 5: MSSL implementation results in the client

5. PROOF OF SECURITY

When we try to use another PC with different IP address to imitate the hacker, this PC cannot access to the Micro Server. Therefore, we avoided the attack from hackers who want to capture the packets between PC and Micro Server and use the same commands to destroy Micro Server. This method protected Micro Server from same command attacking. We use Wireshark to capture packets in the connection between host and Micro Server. These captured packets are RSA digital signature and encrypted data. Hence, data in packets is hidden and the connection is secured.

6. DISCUSSION & FUTURE WORK

MSSL has 2 phases as SSL: handshake processing and data encryption but MSSL is very simple and much faster than SSL. MSSL has memory size is about 1.3 Kbytes not much as Mbytes as SSL. We will study and propose other ways for authentication to connect Micro Server and client more flexibly.

7. CONCLUSION

In this paper, we have analyzed security methods for Micro Server which has limited memory and small processor. We proposed Micro Secure Socket Layer for establishing secure layer in a simple TCP/IP stack. This MSSL has simple handshake processing by using RSA digital signature and data encryption by only AES algorithm with code size of only about 1.322 Kbytes.

8. REFERENCES

[1] Wesley Chou, *Inside SSL: The Secure Sockets Layer Protocol,* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1046644

[2] AbdelNasir Alshamsi, Takamichi Saito, Tokyo University of Technology, *A technical Comparison of IPSec and SSL.* http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1423719

[3] Eric Rescorla, *SSL and TLS, Designing and Building Secure Systems*, Addison-Wesley, 3rd Printing, Aug. 2001.

[4] *The open-source uIP TCP/IP stack*. Available from www.dunkels.com/adam/uip

[5] Federal Information Processing Standards Publication 197, *Announcing the Advanced Encryption Standard (AES)*.

[6] Konrad Lorincz, Harvard University, *Sensor Networks for Emergency Response: Challenges and Opportunities*.

[7] Yoshiyasu Takefuji, http://www.neuro.sfc.keio.ac.jp/