



APPLICATION NOTE 4015

Secure User Authentication with Network Microcontrollers

Abstract: This application note describes the Windows® NT LAN Manager (NTLM) protocol and explains its use in secure user-authentication applications. It introduces the NTLM library available for use with the Maxim® network microcontrollers, and demonstrates the library's use with POP3.

Introduction

Everyday, computer users are required to log into web services and verify themselves. This authentication allows the service provider to grant access to protected information. Password authentication is the most common method currently in use, but plaintext passwords are only as secure as the network on which they are transmitted. Anyone "listening" on the network can see the username and password as it is transmitted, in the clear, to the server. Clearly, plaintext password authentication provides insufficient protection for any application requiring secure access.

The Windows NT LAN Manager (NTLM) authentication protocol used by Microsoft in protocols such as HTTP, SMTP, POP3, and Telnet provides a far more secure authentication solution. Maxim provides libraries for simple integration of NTLM authentication in client applications using the [DS80C400](#) and [DS80C410/DS80C411](#) microcontrollers. This application note describes NTLM authentication and its usage in network applications. A demonstration with the POP3 protocol is provided.

NTLM Overview

NTLM utilizes a challenge-response mechanism for authentication, thereby protecting the user's password with a cryptographic hash. A typical NTLM exchange consists of three messages, referred to as Type1 (negotiation), Type2 (challenge), and Type3 (authentication).

1. The client sends the server a Type 1 message containing the user name and a list of supported features.
2. The server responds with a Type 2 message containing agreed protocols and a random challenge generated by the server.
3. The client replies with a Type 3 message containing domain and username, and the cryptographic hash of the password. The actual password is never exchanged.

The DS80C400/DS80C410/DS80C411 NTLM library provides the following routines for NTLM authentication.

```
void generate_type1_msg(type1msg *t1_msg, char *user);  
void generate_type3_msg(type2msg *t2_msg, type3msg *t3_msg, char *user, char *pass);
```

These routines allow NTLM authentication to be added easily to any client application by abstracting the NTLM internals from the user. Refer to the *Additional Information* section below for detailed descriptions of the NTLM protocol.

Usage with POP3

The POP3 NTLM authentication handshake occurs in the POP3 "authorization" state. The client requests a list of supported authentication mechanisms by using the AUTH command with no arguments:

```
AUTH
```

The server responds with a "success" message, followed by the list of supported mechanisms. This list should include "NTLM," and is terminated by a line containing a single period ("."):

```
+OK The operation completed successfully.  
NTLM
```

```
.
```

The client initiates NTLM authentication by sending an AUTH command that specifies NTLM as the authentication mechanism:

```
AUTH NTLM
```

The server responds with a success message:

```
+ OK
```

The client sends the Type 1 message (Base-64 encoded):

```
TlRMTVNTUAABAAAAB7IAAAUABQAgAAAABQAFACUAAABzZWVuaXNlZW5p
```

The server replies with the Type 2 challenge message (Base-64 encoded). The challenge format is specified by RFC 1734 ("+", followed by a space, followed by the challenge message), as shown below:

```
+TlRMTVNTUAACAAAADwAPADAAAAHAgiAbYIeZCZESTMAAAAAAAAAAAAAAAAAAAAAAbWFpbC5kb21haW4uY29t
```

The client calculates and sends the Base-64 encoded Type 3 message:

```
TlRMTVNTUAADAAAAGAAYAEAAAAAYABgAWAAAAA8ADwBwAAAAACgAKAH8AAAAKAAoAiQAAAAUABQCTAAAABwICA  
FadILoghkFeli66HycIYmjpnmm6XToht7yZrLzrNb8CV7gLSwRScY1FQQ86d+hWnmlhaWwuzG9tYwluLmNvbX  
MAZQBlAG4AaQBzAGUAZQBuaGkAZHVtbXJ
```

Finally, the server validates the response and indicates the result of authentication process:

```
+OK User successfully logged on
```

After successful authentication, the POP3 session enters the "transaction" state, allowing messages to be retrieved by the client.

Authentication Demonstration

By default, the DS80C400 POP3 library uses plain text authentication. It also provides a callback interface that

allows users to implement additional authentication methods. The callback function shown below performs NTLM authentication. The complete NTLM demo is available from the Maxim website (see *Additional Information*, item 1 below). This authentication function can also be used with the SMTP library.

```
int ntlm_authentication(pop3_session *pop3_handle)
{
    char buf[MAX_LINE_SIZE];
    char *mimebuf;
    int size;

    sprintf(buf, "AUTH NTLM\r\n");

    //request NTLM authentication mechanism to choose for authentication with server
    if(send(pop3_handle->handle, buf, strlen(buf),0)!=0)
    {
        return POP3_SOCKET_ERROR;
    }

    if((size=recv(pop3_handle->handle,buf,MAX_LINE_SIZE,0))==0xFFFF)
    {
        return POP3_SOCKET_ERROR;
    }

    buf[size]='\0';

    //if server doesn't support NTLM, return with error
    if(strncmp(buf,"+",1)!=0)
    {
        return POP3_RECEIVEMAIL_ERROR;
    }

    //generate type1 ntlm message, give user name as input
    generate_type1_msg(&t1_msg, pop3_handle->user);
    //encode type1 message in base64 format
    mimebuf=mime_encode((unsigned char
    *)&t1_msg,(sizeof(typlmsghdr)+t1_msg.buf_index), BASE64);

    strcpy(buf,mimebuf);
    strcat(buf,"\r\n");

    //send type1 message to server
    if(send(pop3_handle->handle, buf, strlen(buf),0)!=0)
        return POP3_SOCKET_ERROR;

    //receive server response
    if((size=recv(pop3_handle->handle,buf,MAX_LINE_SIZE,0))==0xFFFF)
        return POP3_SOCKET_ERROR;

    //ignore server response status mark and extract server type2 message response
    if(buf[0]=='+' && buf[1] == ' ')
        mimebuf=mime_decode((char far*)(buf+2), BASE64);
    else
        mimebuf=mime_decode((char far*)buf, BASE64);

    memcpy((char *)&t2_msg,mimebuf,mem_sizeof(mimebuf));

    //generate type3 ntlm message
    generate_type3_msg(&t2_msg, &t3_msg, pop3_handle->user,pop3_handle->pass);
}
```

```

//encode type3 message in base64 format
mimebuf=mime_encode((unsigned char
*)&t3_msg,(sizeof(type3msghdr)+t3_msg.buf_index), BASE64);

    strcpy(buf,mimebuf);
    strcat(buf,"\r\n");

    //send type3 message to server
if(send(pop3_handle->handle, buf, strlen(buf),0)!=0)
    return POP3_SOCKET_ERROR;

    if((size=recv(pop3_handle->handle,buf,MAX_LINE_SIZE,0))==0x0FFFF)
        return POP3_SOCKET_ERROR;

    buf[size]='\0';

    //check server response to see whether authentication is successful or not.
    //if authentication is not successful, send error code to POP3 library
    if(strncmp(buf,"+",1)!=0)
    {
        return POP3_INVALID_USER_PASSWORD;
    }
    //we have gone through authentication successfully, return success status code
return POP3_STATUS_SUCCESS;
}

```

Conclusion

Network applications require secure user authentication to protect personal data, and NTLM is one of the most widely used authentication methods in the world. The NTLM library provided by Maxim enables simple integration of secure NTLM authentication into any application.

Additional Information

1. [DS80C400/DS80C410/DS80C411 C Libraries Project Home Page](#)
2. [The NTLM Authentication Protocol Specification](#)
3. [Using the Keil compiler for the DS80C400](#)

Windows is a registered trademark of Microsoft Corp.

Dallas Semiconductor is a registered trademark of Dallas Semiconductor Corp.

Maxim is a registered trademark of Maxim Integrated Products, Inc.

Dallas Semiconductor is a wholly owned subsidiary of Maxim Integrated Products, Inc.

Application Note 4015: www.maxim-ic.com/an4015

More Information

For technical support: www.maxim-ic.com/support

For samples: www.maxim-ic.com/samples

Other questions and comments: www.maxim-ic.com/contact

Keep Me Informed

Preview new application notes in your areas of interest as soon as they are published. Subscribe to [EE-Mail -](#)

[Application Notes](#) for weekly updates.

Related Parts

DS80C400: [QuickView](#) -- [Full \(PDF\) Data Sheet](#) -- [Free Samples](#)

DS80C410: [QuickView](#) -- [Full \(PDF\) Data Sheet](#) -- [Free Samples](#)

DS80C411: [QuickView](#) -- [Full \(PDF\) Data Sheet](#) -- [Free Samples](#)

AN4015, AN 4015, APP4015, Appnote4015, Appnote 4015

Copyright © by Maxim Integrated Products

Additional legal notices: www.maxim-ic.com/legal