Security Negotiation in CIFS in Active Directory

Jim McDonough
Samba Team
IBM

April 14, 2003

Security Negotiation in CIFS

- Negotiation Imbedded inside core SMB calls
  - Enables backward compatibility
- Negotiated mechanism may be implemented inside of SMB calls, or externally, or a mixture of both.

GSSAPI

- Generic Security Service Application Program Interface
- RFC 2743
- Not much is seen on the wire for CIFS
- Used to encapsulate SPNEGO and Kerberos as required

SPNEGO

- Simple Protected GSS-API Negotiation
- RFC 2478
- Allows selection of security mechanism, including mechanism-specific options

SPNEGO steps

- negTokenInit
  - List of security mechanisms, preferred first
  - Optional data for first mechanism (mechToken)
  - Optional integrity check (mechListMIC)
  - More than one may be issued while deciding on the mechanism
- negTokenTarg
  - Result (accept, reject, imcomplete)
  - Mechanism chosen
  - Negotiation data blobs (responseToken)
  - Optional integrity check (mechListMIC)

CIFS encapsulation of SPNEGO

- Triggered by bit 11 of Flags2 in SMB header during Negotiate Protocol (NegProt) Request
- Directory Service Agent's GUID added at the end of the NegProt Response, followed by a blob containing the start of the SPNEGO converstation
- Session Setup contains a blob near the end (before OS and LAN Manager strings), in both request and response, containing the continuing conversation.

Negprot request

```
SMB (Server Message Block Protocol)
    SMB Header
        Server Component: SMB
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags: 0x18
        Flags2: 0xc853
            1... .... .... .... = Unicode Strings: Strings are Unicode
            .1.. .... .... .... = Error Code Type: Error codes are NT error codes
            ..0. .... .... .... = Execute-only Reads: Don't permit reads if execute-only
            ...0 .... .... .... = Dfs: Don't resolve pathnames with Dfs
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
            .... .... .1.. .... = Long Names Used: Path names in request are long file names
            .... .... .... .0.. = Security Signatures: Security signatures are not supported
            .... .... .... ..1. = Extended Attributes: Extended attributes are supported
            .... .... .... ...1 = Long Names Allowed: Long file names are allowed in the response
        Reserved: 000000000000000000000000
        Tree ID: 0
        Process ID: 65279
        User ID: 0
        Multiplex ID: 0
    Negotiate Protocol Request (0x72)
        Word Count (WCT): 0
        Byte Count (BCC): 98
        Requested Dialects
            Dialect: PC NETWORK PROGRAM 1.0
            Dialect: LANMAN1.0
            Dialect: Windows for Workgroups 3.1a
            Dialect: LM1.2X002
            Dialect: LANMAN2.1
            Dialect: NT LM 0.12
```

Negprot Response

```
SMB (Server Message Block Protocol)
    SMB Header
        SMB Command: Negotiate Protocol (0x72)
        NT Status: STATUS_SUCCESS (0x00000000)
        Flags2: 0xc853
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
    Negotiate Protocol Response (0x72)
        Dialect Index: 5, greater than LANMAN2.1
        Security Mode: 0x07
            .... ...1 = Mode: USER security mode
            .... ..1. = Password: ENCRYPTED password. Use challenge/response
            .... .1.. = Signatures: Security signatures ENABLED
            .... 0... = Sig Req: Security signatures NOT required
        Capabilities: 0x8000f3fd
            1... .... .... .... .... .... .... .... = Extended Security: Extended security exchanges are supported
        System Time: Jul 26, 2002 13:56:21.971273026
        Server Time Zone: 240 min from UTC
        Key Length: 0
        Byte Count (BCC): 116
        Server GUID: 9094DD81F008DB4084FC3CB48F9859AE
        Security Blob: 606206062B0601050502A0583056A030...
            GSS-API
                OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                SPNEGO
                    negTokenInit
                        mechType
                            OID: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                            OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                            OID: 1.2.840.113554.1.2.2.3
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        mechListMIC: psflinux2k$@MCD.MAINE.RR.COM
```

Negotiated Mechanisms

- Kerberos 5
  - MS erroneous variant of the Kerberos 5 OID
    - 1.2.840.48018.1.2.2
  - Kerberos 5
    - 1.2.840.113554.1.2.2
- User<->User Kerberos 5
    - 1.2.840.113554.1.2.2.3
- NTLMSSP
    - 1.3.6.1.4.1.311.2.2.10

Kerberos 5 in CIFS

- Usually the preferred mechanism
- Triggered by SPNEGO
- AS_REx, and TGS_REx are done natively
- AP_REx are encapsulated within CIFS
  - SessSetup
  - GSSAPI
  - SPNEGO negTokenInit and negTokenTarg

Sample KRB5 Negotiation

```
>SMB (Server Message Block Protocol)
    +SMB Header
        SMB Command: Negotiate Protocol (0x72)
        +Flags2: 0xc853
            .... 1... .... .... = Extended Security Negotiation: Extended security negotiation is supported
    +Negotiate Protocol Request (0x72)

>SMB (Server Message Block Protocol)
    +Negotiate Protocol Response (0x72)
        Server GUID: 9094DD81F008DB4084FC3CB48F9859AE
        +Security Blob: 606206062B0601050502A0583056A030...
            +GSS-API
                OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                +SPNEGO
                    +negTokenInit
                        +mechType
                            OID: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                            OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                            OID: 1.2.840.113554.1.2.2.3
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        mechListMIC: psflinux2k$@MCD.MAINE.RR.COM

>Kerberos (udp 88)
    Version: 5
    MSG Type: AS-REQ
    +Request
        Client Name: jmcd
        Realm: MCD
        Server Name: krbtgt
    +Addresses
```

Sample KRB5 Negotiation (continued)

```
>Kerberos (udp 88)
    MSG Type: AS-REP
    Realm: MCD.MAINE.RR.COM
    Client Name: jmcd
    +Ticket
        Realm: MCD.MAINE.RR.COM
        Service Name: krbtgt

>Kerberos (udp 88)
    MSG Type: TGS-REQ
    +Request
        Realm: MCD.MAINE.RR.COM
        Server Name: HOST/psflinux2k.mcd.maine.rr.com

>Kerberos (udp 88)
    MSG Type: TGS-REP
    Realm: MCD.MAINE.RR.COM
    Client Name: jmcd
    +Ticket
        Realm: MCD.MAINE.RR.COM
        Service Name: PSFLINUX2K$

>Kerberos (udp 88)
    MSG Type: TGS-REQ
    Request
        Realm: MCD.MAINE.RR.COM
        Server Name: krbtgt

>Kerberos (udp 88)
    MSG Type: TGS-REP
    Realm: MCD.MAINE.RR.COM
    Client Name: jmcd
    Ticket
        Realm: MCD.MAINE.RR.COM
        Service Name: krbtgt
```

Sample KRB5 Negotiation (continued)

```
+SMB (Server Message Block Protocol)
    +Session Setup AndX Request (0x73)
        +Security Blob: 60820A2706062B0601050502A0820A1B...
            +GSS-API
                +OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                +SPNEGO
                    +negTokenInit
                        +mechType
                            OID: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                            OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                            OID: 1.2.840.113554.1.2.2.3
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        +mechToken
                            +krb5_blob: 608209D906092A864886F71201020201...
                                OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                                krb5_tok_id: KRB5_AP_REQ (0x0001)
                                +Kerberos
                                    Version: 5
                                    MSG Type: AP-REQ
                                    +Ticket
                                        Realm: MCD.MAINE.RR.COM
                                        Service Name: PSFLINUX2K$

+SMB (Server Message Block Protocol)
    +Session Setup AndX Response (0x73)
        +Security Blob: A182012E3082012AA0030A0100A10B06...
            +GSS-API
                +SPNEGO
                    +negTokenTarg
                        negResult: Accept Completed (0x0000)
                        supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                        +responseToken
                            +krb5_blob: 60818306092A864886F7120102020200...
                                OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                                krb5_tok_id: KRB5_AP_REP (0x0002)
                                +Kerberos
                                    MSG Type: AP-REP
                        +mechListMIC - the responseToken duplicated !
```

MS SPNEGO/Kerberos Quirks

- Incorrect OID
- mechListMIC never contains integrity check
  - Service Principcal for server
    - reduces number of round trips
  - duplication of mechToken or responseToken
    - no known reason

User2User Kerberos

- Enables user to host short-lived service without exposing long-term keys
  - Server's TGT (but not session key) sent to client
  - User gets ticket encrypted with both session keys
    - both can decrypt and verify each other
- Requires one extra round trip
- Note: I have not seen this on the wire

NTLMSSP

- NTLM Security Support Provider
- Negotiate many options for NTLM
- May be contained within SPNEGO
  - Usually when the server is in a domain
- May be sent "raw" - in place of SPNEGO
  - Usually for a standalone server

NTLMSSP steps

- Negotiate
  - Client offers options (flags), e.g.
    - Unicode vs. ASCII
    - Sign, Seal
    - LanMan, NTLM, NTLMv2
- Challenge
  - Server presents flags selected
  - Server offers challenge
- Authenticate
  - Client offers challenge response(s), depending on flags
  - User, domain, workstation
  - Optionally session key and flags
    - Opengroup doc specifies during Datagram (flag) authentication
    - MS sends anyway
- Accept/Reject
  - Not specified within NTLMSSP
  - Wrapping protocol carries the return code

Sample NTLMSSP Negotiation

```
>SMB (Server Message Block Protocol)
    +SMB Header
    +Session Setup AndX Request (0x73)
        +Security Blob: 604006062B0601050502A0363034A00E...
            +GSS-API
                OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                +SPNEGO
                    +negTokenInit
                        +mechType
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        +mechToken
                            +NTLMSSP
                                NTLMSSP identifier: NTLMSSP
                                NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
                                +Flags: 0xe0008297
                                    .1.. .... .... .... .... .... .... .... = Negotiate Key Exchange: Set
                                    ..1. .... .... .... .... .... .... .... = Negotiate 128: Set
                                    .... .... 0... .... .... .... .... .... = Negotiate Target Info: Not set
                                    .... .... .... 0... .... .... .... .... = Negotiate NTLM2 key: Not set
                                    .... .... .... .0.. .... .... .... .... = Negotiate Challenge Non NT Session Key: Not set
                                    .... .... .... ..0. .... .... .... .... = Negotiate Challenge Accept Response: Not set
                                    .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set
                                    .... .... .... .... 1... .... .... .... = Negotiate Always Sign: Set
                                    .... .... .... .... .0.. .... .... .... = Negotiate This is Local Call: Not set
                                    .... .... .... .... ..0. .... .... .... = Negotiate Workstation Supplied: Not set
                                    .... .... .... .... ...0 .... .... .... = Negotiate Domain Supplied: Not set
                                    .... .... .... .... .... ..1. .... .... = Negotiate NTLM key: Set
                                    .... .... .... .... .... ...0 .... .... = Negotiate Netware: Not set
                                    .... .... .... .... .... .... 1... .... = Negotiate Lan Manager Key: Set
                                    .... .... .... .... .... .... .0.. .... = Negotiate Datagram Style: Not set
                                    .... .... .... .... .... .... ..0. .... = Negotiate Seal: Not set
                                    .... .... .... .... .... .... ...1 .... = Negotiate Sign: Set
                                    .... .... .... .... .... .... .... .1.. = Request Target: Set
                                    .... .... .... .... .... .... .... ..1. = Negotiate OEM: Set
                                    .... .... .... .... .... .... .... ...1 = Negotiate UNICODE: Set
                                Calling workstation domain: NULL
                                Calling workstation name: NULL
```

Sample NTLMSSP Negotiation (continued)

```
>SMB (Server Message Block Protocol)
    +SMB Header
        NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
    +Session Setup AndX Response (0x73)
        +Security Blob: A182019730820193A0030A0101A10C06...
            +GSS-API
                +SPNEGO
                    +negTokenTarg
                        negResult: Accept Incomplete (0x0001)
                        +responseToken
                            +NTLMSSP
                                NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
                                +Flags: 0xe0818295
                                    .... .... 1... .... .... .... .... .... = Negotiate Target Info: Set
                                    .... .... .... ...1 .... .... .... .... = Negotiate Challenge Init Response: Set
                                    .... .... .... .... .... .... .... ..0. = Negotiate OEM: Not set
                                NTLM Challenge: 8F466EACBC058F8D
                                Reserved: 0000000000000000
                                +Address List
                                    Domain NetBIOS Name: MCD
                                    Server NetBIOS Name: PSFLINUX2K
                                    Domain DNS Name: mcd.maine.rr.com
                                    Server DNS Name: psflinux2k.mcd.maine.rr.com
                        +mechListMIC - a duplicate of responseToken !
```

Sample NTLMSSP Negotiation (continued)

```
>SMB (Server Message Block Protocol)
    +Session Setup AndX Request (0x73)
        +Security Blob: A181A53081A2A2819F04819C4E544C4D...
            +GSS-API
                +SPNEGO
                    +negTokenTarg
                        +responseToken
                            +NTLMSSP
                                NTLM Message Type: NTLMSSP_AUTH (0x00000003)
                                Lan Manager Response: 4F3E273838DC9C6FC57A10DDAB52B5E6...
                                NTLM Response: E145562018DD2894E91A0283A462EA02...
                                Domain name: MCD
                                User name: jmcd
                                Host name: DANCE2K
                                Session Key: 54BFABFD12ACDE88F93B7FBB06A3D0F7
                                +Flags: 0xe0808295
                                    .... .... .... ...0 .... .... .... .... = Negotiate Challenge Init Response: Not set

>SMB (Server Message Block Protocol)
    +Session Setup AndX Response (0x73)
        +Security Blob: A1073005A0030A0100
            +GSS-API
                +SPNEGO
                    +negTokenTarg
                        +negResult: Accept Completed (0x0000)
```

Sample "Raw" NTLMSSP Negotiation

```
>SMB (Server Message Block Protocol)
    +Negotiate Protocol Response (0x72)
        Server GUID: B5DCD649F6E9254C8B44A9A1E4C4B25C
        Security Blob: <MISSING>

>SMB (Server Message Block Protocol)
    +Session Setup AndX Request (0x73)
        +Security Blob: 4E544C4D535350000100000978208E0...
            +NTLMSSP
                NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)

>SMB (Server Message Block Protocol)
    +Session Setup AndX Response (0x73)
        +Security Blob: 4E544C4D535350000200000000E000E00...
            +NTLMSSP
                NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)
                +Address List
                    Domain NetBIOS Name: DANCE2K
                    Server NetBIOS Name: DANCE2K
                    Domain DNS Name: dance2k.mcd.maine.rr.com
                    Server DNS Name: dance2k.mcd.maine.rr.com

>SMB (Server Message Block Protocol)
    +Session Setup AndX Request (0x73)
        +Security Blob: 4E544C4D53535000030000001800180...
            +NTLMSSP
                NTLM Message Type: NTLMSSP_AUTH (0x00000003)

>SMB (Server Message Block Protocol)
    +SMB Header
        NT Status: STATUS_SUCCESS (0x00000000)
    +Session Setup AndX Response (0x73)
        Security Blob: <MISSING>
```

Other Services

- LDAP
- HTTP
- Email
- Others?

Sample LDAP SPNEGO

```
›Lightweight Directory Access Protocol
    +Message: Id=2  Search Request
        Base DN: (null)
        Scope: Base (0x00)
        Filter: (objectclass=*)
        Attribute: supportedSASLMechanisms

›Lightweight Directory Access Protocol
    +Message: Id=2  Search Entry
        +Attribute: supportedSASLMechanisms
            Value: GSSAPI
            Value: GSS-SPNEGO

›Lightweight Directory Access Protocol
    +Message: Id=3  Bind Request
        Version: 3
        DN: (null)
        Auth Type: SASL (0x03)
        Mechanism: GSS-SPNEGO

›Lightweight Directory Access Protocol
    +Message: Id=3  Bind Result
        Result Code: SASL bind in progress (0x0e)
        +GSS-API Token
            +GSS-API
                OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                +SPNEGO
                    +negTokenInit
                        +mechType
                            OID: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                            OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                            OID: 1.2.840.113554.1.2.2.3
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        +mechListMIC: psflinux2k$@MCD.MAINE.RR.COM
```

Sample LDAP SPNEGO (continued)

```
›Kerberos (udp 88)
    MSG Type: AS-REQ
›Kerberos (udp 88)
    MSG Type: AS-REP
›Kerberos (udp 88)
    MSG Type: TGS-REQ
›Kerberos (udp 88)
    MSG Type: TGS-REP

›Lightweight Directory Access Protocol
    +Message: Id=5  Bind Request
        Mechanism: GSS-SPNEGO
        +GSS-API Token
            +GSS-API
                OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
                +SPNEGO
                    +negTokenInit
                        +mechType
                            OID: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
                            OID: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Support Provider)
                        +mechToken
                            +krb5_blob: 6082050E06092A864886F71201020201...
                                OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
                                krb5_tok_id: KRB5_AP_REQ (0x0001)
                                +Kerberos

›Lightweight Directory Access Protocol
    +Message: Id=5  Bind Result
        Result Code: Success (0x00)
        +GSS-API Token
            +GSS-API
                +SPNEGO
                    +negTokenTarg
                        negResult: Accept Completed (0x0000)
                        supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
```

For even more detailed information...

- RFCS
  - 2743 (GSSAPI)
  - 1510 (KRB5)
  - 1964 (KRB5 over GSSAPI)
  - 2478 (SPNEGO)
  - 2829 (Authentication Methods for LDAP)
- draft-swift-win2k-krb-user2user-03.txt (expired)
- draft-brezak-spnego-http-04.txt (expired)
- Samba source code!