Unifying Authentication across CIFS Servers

By Jeremy Allison

email: jeremy@netcom.com

Introduction

- Goal - Single Sign on.
- Kerberos 5 (rfc1510) is the ultimate solution.
- Current CIFS implementations have limited options.
- Samba attempts most of them.

Account Representation Issues

- CIFS clients only use text user name.
- CIFS Servers map this into underlying platform user representation.
- UNIX/Samba uses UNIX 32-bit user ids.
- NT uses Domain prefix followed by 32-bit relative user id (RID).

Account Representation Solutions

- Map client user name to platform id.
  - Samba uses a mapping file to translate 'foreign' user names to UNIX user names.
- Attempt to map last component of NT SID to UNIX user id. Needed to represent 'owner' and ACL's for NT CIFS protocol.
- Remaining issue - keeping id's/names consistent.

Current Authentication Issues

- Native authentication methods differ across CIFS platforms.
  - CIFS has two secure authentication methods defined plus plaintext passwords.
- User representations differ across CIFS platforms.
- No public protocol for account replication.

Authentication issues

- Current CIFS Authentication mechanisms
  - Plaintext passwords - insecure.
  - Challenge/response - two flavors.
    - Lanman hash - legacy. Uses DES and 'magic constant'. Cannot be IETF approved.
    - NT MD4 hash (rfc1186). No salt - vulnerable to dictionary attacks.
- UNIX Authentication mechanism
  - DES crypt with salt. Only 8 characters.
  - No challenge/response - ignores network.

Authentication issues

- Different hash mechanisms means access to plaintext passwords necessary.
- Windows NT logon protocol not specified.
  - Windows NT Domain controller necessary to support Windows NT clients.
- No support for UNIX to UNIX authentication in current CIFS protocols. New dialect required.

Authentication Solutions

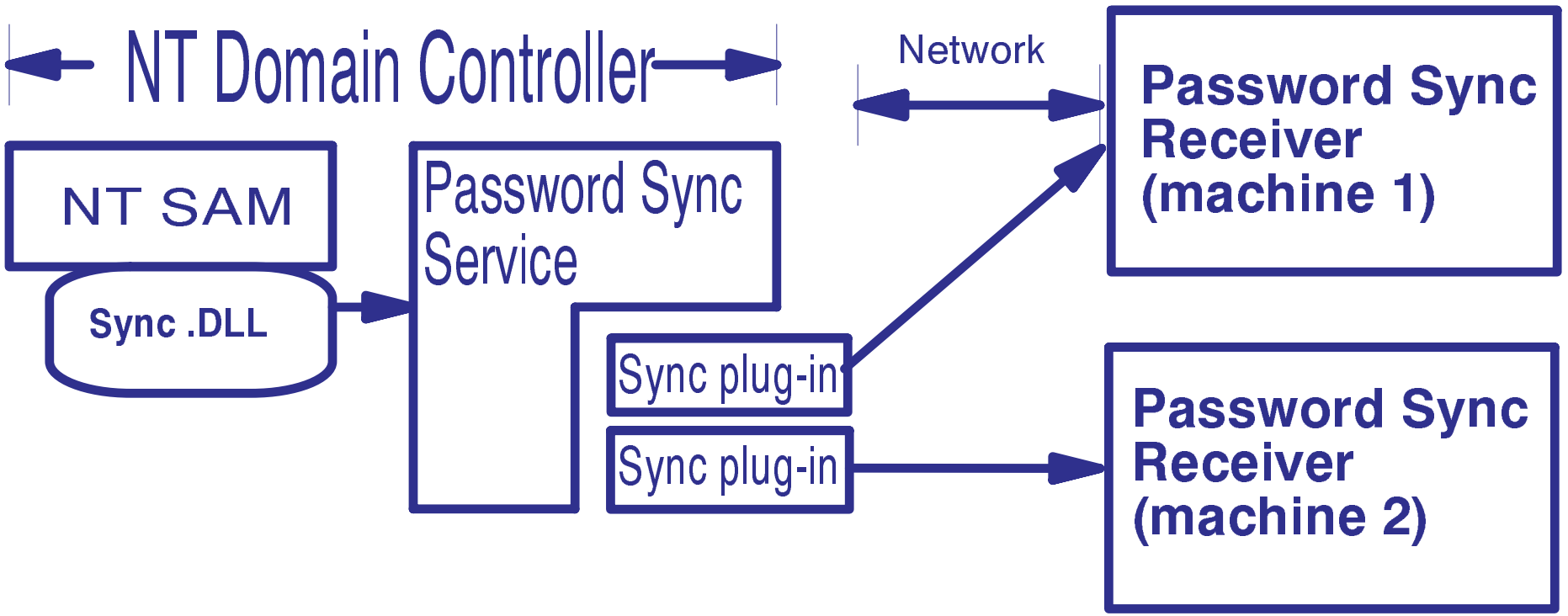
- Pass through authentication.
  - Allows UNIX CIFS server to subordinate authentication to NT.
  - Requires NT Domain controller.
  - Single challenge. 8 byte challenge is returned in negprot call (wrong place).
  - Connection to Domain controller becomes point of failure. If this fails, clients can no longer make new connections.
  - Samba does this very poorly.

Authentication Solutions

- Account replication from NT Domain.
  - No public protocol - Samba Team has invented our own.
  - Depends upon Password Synchronization .DLL and Service running on NT Domain Controller.
  - 'Pluggable' architecture allows NT account replication to different servers.
  - One-way only at present.

Account Replication

- Architecture of PasswordSync code :



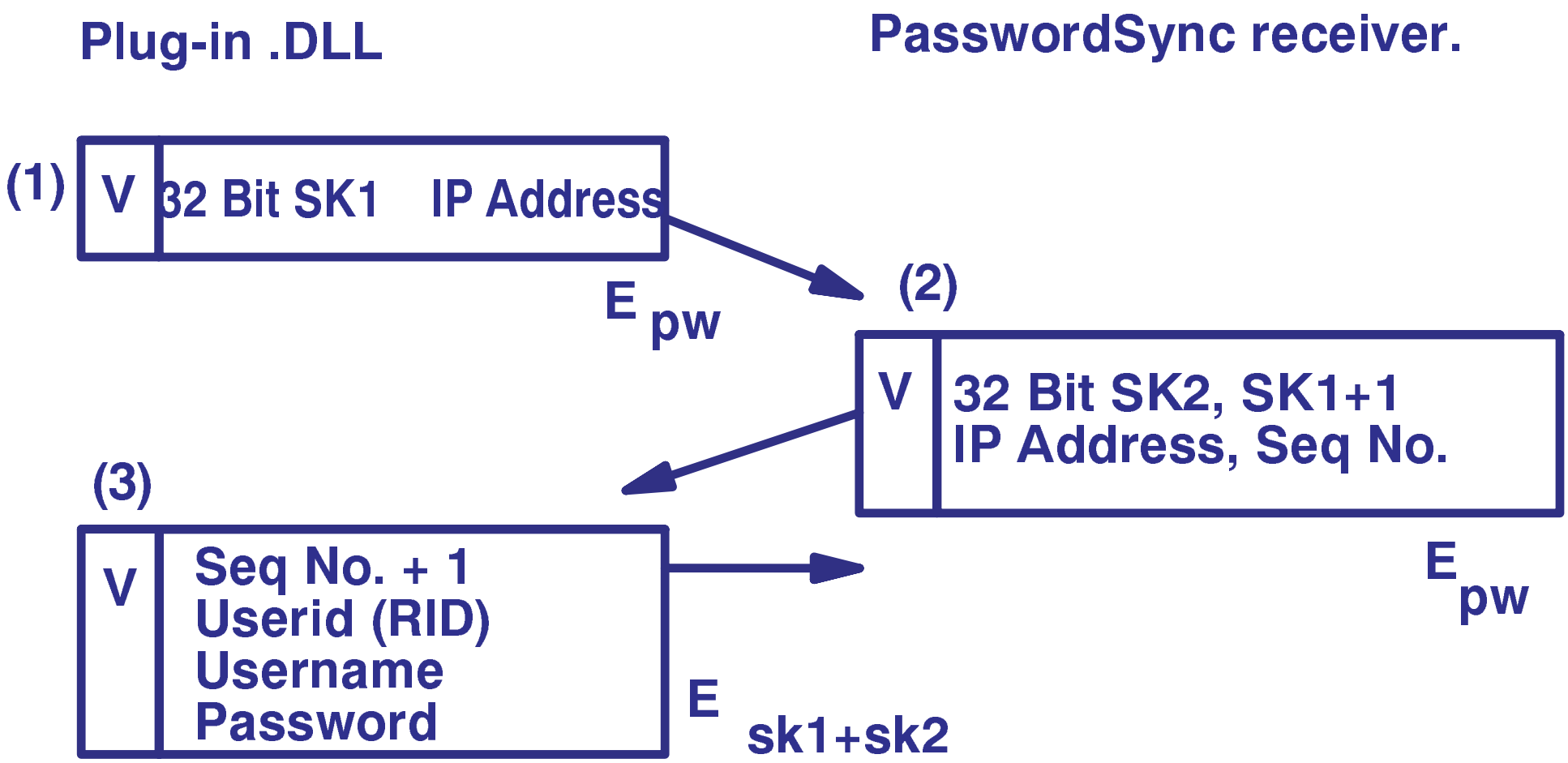
PasswordSync Details

- Service written to allow 'placeholder' for future two-way replication.
- 'Sync.DLL' communicates securely with service via named pipe.
- Sync.DLL gets user name, new plaintext password, NT 'RID'.
- Plug-ins to service allow safer code development.

PasswordSync Network Protocol

- Based on shared secret password. Uses DES encryption.
- Guards against reply and man-in-the-middle attacks.
- Source code will be commercially usable, not under GPL.
- Comments/complaints gratefully received.

PasswordSync Network Protocol



PasswordSync Network Protocol

- V = Version number of protocol.
- SK1 = 32 bit secret key half generated by sending machine.
- SK2 = 32 bit secret key half generated by receiving machine.
- Epw = Encrypted by long term secret key.
- Esk1+sk2 = Encrypted by key generated from concatenation of secret key halves.
- SeqNo = Sequence number for all subsequent messages.

PasswordSync Network Protocol

- Client checks server returns SK1 + 1. Guard against server replay.
- Server generates random SK2, all future client messages will decrypt to garbage if client replay attempted.
- Man-in-the-middle cannot replay messages - incrementing sequence number.
- Man-in-the-middle cannot modify messages - random session key.

PasswordSync Network Protocol

- Future enhancements
  - Better crypto negotiation: choice of ciphers (TripleDes, blowfish etc.).
  - Two-way protocol. Allow UNIX machines to initiate password change onto NT machine.
  - Allow public key crypto once patents expire.
    - Software patents - just say no !

Account Replication : brute force method.

- Dump NT account database to file
  - *As featured in the 'Wall Street Journal'.*
- Securely transfer to UNIX machine. Can be used to 'seed' the accounts on a new machine.
- Use to re-synchronize if incremental methods fail.
- Can be used to force passwords into an NT account database.

Summary

- Account unification possible, but currently clumsy. No solution at present without exposing customers to implementation details.
- If customer satisfaction is really the goal, vendors must cooperate to provide single sign-on authentication solutions without single-source.

Summary

- Kerberos 5 promises to be the universal solution for CIFS single sign-on.
  - Apart from :
    - US Government Encryption law.
    - Vendor specific changes.

References and code availability

- Samba Web site :
  - http://samba.anu.edu.au
- PasswordSync Service and .DLL source code:
  - Available on export controlled Web site as part of Cygnus Solutions Kerbnet product.
- NT Password Dump utility
  - ftp://samba.anu.edu.au/pub/samba/pwdump